




# **ML & TF Risk Management Guidelines**

*Version-3*



From: Company Secretariat

**EXTRACT OF THE MINUTES OF 109<sup>TH</sup> MEETING OF THE BOARD OF DIRECTORS OF NRB BANK LIMITED  
HELD ON TUESDAY, 15 DECEMBER 2020**

---

**Agenda no. B-109/20: Memo no. B-914/2020 dated 01.12.2020: Review of the "Money Laundering & Terrorist Financing Risk Management Guidelines".**

Memo no. B-914/2020 dated 01.12.2020 on the captioned subject was placed before the Board. The Board reviewed and after detailed discussion approved "**Money Laundering & Terrorist Financing Risk Management Guidelines**" of NRB Bank Limited as presented in the meeting as detailed in the memo subject to review from time to time as and when required.

**For NRB Bank Limited**  
**Corporate Head Office**  
  
**Company Secretary**

- ☐ AMLD
- ☐ Agent Banking
- ☐ Brand & Communications
- ☐ Chairman's Secretariat
- ☐ Company Secretariat
- ☐ CRMD
- ☐ CAD
- ☐ CBD
- ☐ Cards Division

- ☐ Finance & Accounts
- ☐ Facilities Management
- ☐ FRD
- ☐ HRMD
- ☐ ICCD
- ☐ IT Division
- ☐ MD and CEO's Secretariat
- ☐ Office of the AMD
- ☐ Office of the DMD

- ☐ Operations Division
- ☐ Retail Banking Division
- ☐ RMD
- ☐ SAMD
- ☐ SFU
- ☐ SME Banking Division
- ☐ Security Department
- ☐ Trade Operations
- ☐ Treasury Division



AML & CFT Department

December 01, 2020

Agenda No:

To: The Board of Directors

**Subject: Review of the "Money Laundering & Terrorist Financing Risk Management Guidelines".**

Money laundering and terrorist financing have emerged as potential threats to the global economy. As a nation, we cannot afford to have our country's image tarnished because of money laundering and terrorist financing issues. We have to be vigilant and guard the integrity of our financial system for financial and social stability. Our Honorable Board of Directors approved the previous **"Money Laundering & Terrorist Financing Risk Management Guidelines"** in November, 2017. Since then, the Bangladesh Financial Intelligence Unit (BFIU) has issued a number of circulars and guidelines concerning the prevention of money laundering and terrorist financing. To cope up with the emerging typologies and challenges, we have reviewed the Guideline in line with the Money Laundering Prevention Act, 2012 (Amendment 2015), Anti-Terrorism Act, 2009 (Amendment 2012 and 2013), BFIU Circular – 26 dated June 16, 2020 and the Money Laundering Prevention Rules, 2019.

After being reviewed and approved in the Central Compliance Committee (CCC) meeting held on November 16, 2020, the revised **"Money Laundering & Terrorist Financing Risk Management Guidelines"** was approved in the Senior Management Team (SMT) Meeting held on November 17, 2020, where it was decided that the Guideline will be placed in the subsequent Honorable Board of Directors' Meeting.

Submitted for your kind approval.

Uday Shankar Chaki  
SPO, AML & CFT Department

Sarfuddin Md Redwan Patwary  
SAVP & Deputy CAMLCO

Mamoon Mahmood Shah (CAMLCO)  
Managing Director & CEO (CC)

## **Preface**

Money laundering and financing of terrorism have been topics of great concern to the world leaders, not only as serious and highly sophisticated forms of crime but also as threats to human rights, democracy and the rule of law. It involves hundreds of billions of dollars that are laundered through the international financial institutions. The flow of illicit financing can have devastating effects on the international financial system, which in turn erodes public trust and propagates illegal activities within criminal organizations.

Policy makers are encouraged to implement the requirements stated in the international conventions relating to AML-CFT in their respective countries in fighting against money laundering and terrorist financing. In addition, AML-CFT regimes must find out how much they are compliant with international standards set by the FATF and other international standard setters including regional bodies and relevant groups. In order to measure the degree of compliance, AML-CFT regimes should focus on the AML-CFT framework.

As a nation, we cannot afford to have our country's image tarnished because of money laundering and terrorist financing issues. Since banks are highly vulnerable to being used by money launderers and terrorist financiers to conceal and legitimize the *ill-gotten gains*, we have to be vigilant and guard the integrity of our financial system for financial and social stability. The Bangladesh Financial Intelligence Unit (BFIU) has issued a number of circulars and guidelines concerning the prevention of money laundering and terrorist financing to cope up with the emerging typologies and challenges and we have reviewed the Guideline in line with the Money Laundering Prevention Act, 2012 (Amendment 2015), Anti-Terrorism Act, 2009 (Amendment 2012 and 2013), BFIU Circular – 26 dated June 16, 2020, the Money Laundering Prevention Rules, 2019 and Guidance Notes on Beneficial Owner, Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR), Politically Exposed Persons (PEPs)/Influential Persons (IPs), Prevention of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction and some other circulars issued by the BFIU and Banking Regulation & Policy Department (BRPD), Bangladesh Bank from time to time.

Our Bank will review the “Money Laundering & Terrorist Financing Risk Management Guidelines” in every year and as and when required.



## Table of Contents

Sl. No	Particulars	Page No
	<i>Preface</i>	i
<b>CHAPTER I: AN OVERVIEW OF MONEY LAUNDERING AND TERRORIST FINANCING</b>		
1.1	Policy Statement	1
1.1.1	General Provision	1
1.2	Purpose	1
1.3	Definition of Money Laundering	2
1.3.1	Predicate Offence	2
1.4	Why Money Laundering is done	4
1.5	Why we must combat Money laundering	4
1.6	Process of Money Laundering	5
1.6.1	Placement	5
1.6.2	Layering	6
1.6.3	Integration	6
1.7	How Financial Institution can combat Money Laundering	6
1.8	Penalties under Money Laundering Prevention Act, 2012 (Amendment, 2015)	7
1.9	Definition of Terrorist Financing	8
1.9.1	Penalties for Terrorist Financing	9
<b>CHAPTER II: COMPLIANCE PROGRAM OF NRB BANK</b>		
2.0	Preamble	11
2.1	AML & CFT Compliance Program of NRB Bank	11
2.2	Role of Senior Management	11
2.3	Statement of Commitment of Managing Director & CEO	13
2.4	Central Compliance Committee (CCC)	13
2.4.1	Formation of CCC	13
2.4.2	Responsibilities and Authorities of the CCC	14
2.4.3	Separation of CCC from Internal Control & Compliance Division (ICCD)	16
2.5	Formation of AML & CFT Department	16
2.6	Appointment of CAMLCO	17
2.6.1	Authorities and Responsibilities of CAMLCO	17
2.7	Appointment of DCAMLCO	18
2.8	Branch Anti Money Laundering Compliance Officer (BAMLCO)	19
2.8.1	Responsibilities and Authorities of BAMLCO	19
2.9	Department/Division AML Compliance Officer	22
2.10	Roles & Responsibilities of Account Opening Officer/Operation Manager/ Relationship Manager	23
2.11	Role & Responsibilities of ICCD	23

2.12		Responsibilities of ICCD on Self-Assessment & Independent Testing Procedures	24
2.13		External Auditor	25
<b>CHAPTER III: Essential Elements of ML/TF Risk Management</b>			
3.0		Preamble	26
3.1		Assessment, understanding, management and mitigation of risks	26
	3.1.1	Assessment and Understanding of Risks	26
	3.1.2	Proper governance arrangements	26
	3.1.3	Three Lines of Defense	26
	3.1.4	Adequate transaction monitoring system	27
	3.1.4.1	Analysis of TP exception report	28
	3.1.4.2	Monthly CTR analysis	28
	3.1.4.3	Structuring Report Analysis	28
3.2		Customer Acceptance Policy of NRB Bank	28
	3.2.1	Customer Identification & Verification	29
	3.2.1.1	General Requirements	30
	3.2.1.2	Customer Identification measures	31
	3.2.1.2.1	Individual Account/Joint Account	31
	3.2.1.2.2	Minor Account	33
	3.2.1.2.3	Illiterate Person	34
	3.2.1.2.4	Pardansheen Women	34
	3.2.1.2.5	Blind Man/Woman	35
	3.2.1.2.6	NRB (Non-Resident Bangladeshi) and Foreign National	35
	3.2.1.2.7	Corporate/institutional accounts	36
	3.2.1.2.8	Designated Non-Financial Businesses and Professions (DNFBPs)	39
	3.2.1.2.9	Walk-In-Customers	40
	3.2.1.2.10	Non Face to Face Customers	40
	3.2.1.2.11	Politically Exposed Persons (PEPs)	41
	3.2.2	Customer Unique Identification Code	47
	3.2.3	Exception When Opening a Bank Account	47
	3.2.4	Policy for rejection of customer	48
	3.2.5	Know Your Customer (KYC) and CDD Procedures	48
	3.2.5.1	Standard KYC information & CDD Measures	48
	3.2.5.2	Ongoing CDD measures (Review and update)	49
	3.2.5.3	Risk Grading and Applicable CDD	50
	3.2.5.4	Enhanced CDD measures	51
	3.2.5.5	Simplified CDD measures	51
	3.2.5.6	Timing of CDD	52
	3.2.5.7	In case where conducting the CDD measure is not possible	52
	3.2.5.8	Persons without Standard Identification Documentation	53
	3.2.6	Corresponding Banking	54
	3.2.7	New Technologies	56

	3.2.8	Wire Transfers	56
	3.2.8.1	Cross-border wire transfer	57
	3.2.8.2	Domestic wire transfers	57
	3.2.8.3	Duties of Ordering, Intermediary and Beneficiary Bank in Case of Wire Transfer	58
	3.2.10	Agent Banking	59
	3.2.11	Call Center	60
	3.3	Reporting	61
	3.3.1	Cash Transaction Report (CTR)	61
	3.3.2	Half yearly Self-Assessment Report & Independent Testing Procedures (ITP)	62
	3.3.2.1	Responsibilities of Branch	62
	3.3.2.2	Responsibilities of ICCD	62
	3.3.2.2	Responsibilities of AML & CFT Department/CCC	62
	3.3.3	Quarterly meeting minutes	62
	3.3.4	Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR)	62
	3.3.4.1	Reporting STR/SAR	66
	3.3.5	Whistle Blowing	66
4.0		Record Keeping	67
	4.1	Legal Obligation	67
<b>CHAPTER IV: RECRUITMENT, TRAINING AND AWARENESS</b>			
4.0		Obligations under Circular	68
4.1		Employee Screening	68
4.2		Know Your Employee (KYE)	68
4.3		Training for Employee	69
4.4		Awareness of Senior Management/Board of Directors	70
4.5		Customer Awareness Program	70
4.6		Awareness of Mass People	70
<b>CHAPTER V: TRADE BASED MONEY LAUNDERING</b>			
5.0		Preamble	71
5.1		Basic Trade-Based Money Laundering Techniques	71
	5.1.1	Over- and Under-Invoicing of Goods and Services	72
	5.1.2	Multiple Invoicing of Goods and Services	73
	5.1.3	Over- and Under-Shipments of Goods and Services	73
	5.1.4	Falsely Described Goods and Services	73
5.2		CDD requirements in Trade Finance	74

<b>CHAPTER VI: TERRORIST FINANCING &amp; PROLIFERATION FINANCING</b>			
6.0		Preamble	75
6.1		Legal Obligations	76
6.2		Obligations under Circular	76
6.3		Necessity of Funds by Terrorist	77
6.4		Source of Fund/Raising of Fund	77
6.5		Movement of Terrorist Fund	77
	6.5.1	Formal Financial Sector	77
	6.5.2	Trade Sector	78
	6.5.3	Cash Couriers	78
	6.5.4	Use of Alternative remittance systems (ARS)	78
	6.5.5	Use of Charities and Non Profit Organizations	78
6.6		Targeted Financial Sanctions	79
	6.6.1	TFS related to terrorism and terrorist financing	79
	6.6.2	TFS related to Proliferation	79
6.7		Automated Screening Mechanism of UNSCRs	79
6.8		Requirements of the Reporting Organization	80
6.9		Red Flags pointing to Financing of Terrorism	82
<b>CHAPTER VII: ANTI-BRIBERY AND CORRUPTION (ABC) POLICY</b>			
7.0		Preamble	83
7.1		Bribery	83
7.2		Corruption and Fraud	84
7.3		Initiatives of NRB Bank to protect bribery and corruption	84
	7.3.1	Zero Tolerance to Corruption and Bribery	84
	7.3.2	Governance	84
7.4		ABC compliance Program	85
7.5		Conclusion	86



## **CHAPTER: I**

### **AN OVERVIEW OF MONEY LAUNDERING AND TERRORIST FINANCING**

#### **1.1 Policy Statement**

In recognition of the fact that financial institutions are particularly vulnerable to be used by money launderers, the Board of NRB Bank intends to have an updated policy against which it will assess the adequacy of the internal controls and procedures to counter money laundering. This is the revised policy of the earlier AML policy which was approved by the Board in November 2017. This policy complies with all the requirements of Money Laundering Prevention (MLP) Act 2012 (as amended in 2015) and Anti-Terrorism Act (ATA), 2009 (as amended in 2012 & 2013), guideline & circulars issued by Bangladesh Financial Intelligence Unit (BFIU). This policy will cover the requirements of "Money Laundering & Terrorist Financing Risk Management Guidelines" delivered by BFIU. This policy has been developed prioritizing & taking all the changes in MLP Act 2012 (as amended in 2015) and ATA Act 2009 (as amended in 2012 & 2013), into consideration.

##### **1.1.1 General Provision**

The Policy will become effective upon reviewed by the CCC, SMT and subsequently approved by the Honorable Board of Directors.

All employees of NRB Bank Limited need to comply with the policy and all relevant employees must be thoroughly familiar with and make use of the material contained in this Policy.

This Policy will be kept updated by the Central Compliance Committee (CCC)/AML & CFT Department of the bank. Any change in AML/CFT regulations by the regulator will be notified by the CCC/ AML & CFT Department to the all the employees.

#### **1.2 Purpose**

The purpose of the Guidelines is to outline the legal and regulatory framework for Anti Money Laundering and Combating Financing on Terrorism (AML & CFT) requirements and system across the financial services sector.

- ◆ To identify AML & CFT risk;
- ◆ Assist banks, competent authorities as well as Country in the design and implementation of AML & CFT risk by providing general guidelines and examples of current practice;
- ◆ Support the effective implementation and supervision of national AML & CFT measures, by focusing on risks and on mitigation measures.

### **1.3 Definition of Money Laundering**

Briefly described, "money laundering" is the process by which proceeds from a criminal activity are disguised to conceal their illicit origin.

As per Money Laundering Prevention Act 2012 (amendment 2015), Section 2 (v), Money Laundering is defined as under:

**"Money Laundering" means -**

- i) knowingly move, convert, or transfer proceeds of crime or property involved in an offence for the following purposes:-
  - 1) concealing or disguising the illicit origin/nature, source, location, ownership or control of the proceeds of crime; or
  - 2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
- ii) smuggling money or property earned through legal or illegal means to a foreign country;
- iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or
- iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
- v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
- vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
- vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
- viii) participating in, associating with conspiring, attempting, abetting, instigating or counseling to commit any offence(s) mentioned above;

#### **1.3.1 Predicate Offence**

Predicate Offence means the offences mentioned below, by committing which within or outside the country, the money or property derived from which is laundered or attempt to be laundered, namely:

01.	Corruption and bribery;	15.	Theft or robbery or dacoity or piracy or hijacking of aircraft;
02.	Counterfeiting currency;	16.	Human Trafficking or obtaining money or trying to obtain money or valuable goods giving someone false assurances of employment abroad;
03.	Counterfeiting deeds and documents;	17.	Dowry;
04.	Extortion;	18.	Smuggling and offences related to customs and excise duties;
05.	Fraud;	19.	Tax related offences;
06.	Forgery;	20.	Infringement of intellectual property rights;
07.	Illegal trade of firearms;	21.	Terrorism or financing in terrorist activities;
08.	Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;	22.	Adulteration or the manufacture of goods through infringement of title;
09.	Illegal trade in stolen and other goods;	23.	Offences relating to the environment;
10.	Kidnapping, illegal restrain and hostage taking;	24.	Sexual exploitation;
11.	Murder, grievous physical injury;	25.	Insider trading and market manipulation- Using price sensitive information relating to the capital market in share transactions before it is published for general information to take advantage of the market and attempting to manipulate the market for personal or institutional gain;
12.	Trafficking of women and children;	26.	Organized crime, and participation in organized criminal groups;
13.	Black marketing;	27.	Racketeering; and
14.	Smuggling of domestic and foreign currency;	28.	<i>Any other offence(s) declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official (Bangladesh) Gazette, for the purpose of this Act.</i>

#### **1.4 Why Money Laundering is done**

First, money represents the lifeblood of the organization/person that engages in criminal conduct for financial gain because it covers operating expenses and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.

Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or, alternatively, make them look legitimate.

#### **1.5 Why we must combat Money laundering**

Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a process vital to making crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorism, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences that result. Crime has become increasingly international in scope, and the financial aspects of crime have become more complex due to rapid advances in technology and the globalization of the financial services industry.

Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case if the untaxed proceeds of crime were legitimate. We also pay more taxes for public works expenditures inflated by corruption. And those of us who pay taxes pay more because of those who evade taxes. So we all experience higher costs of living than we would if financial crime including money laundering were prevented.

It is generally recognized that effective efforts to combat money laundering cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies. Accordingly, in order to address the concerns and obligations of these three parties, these Guidance Notes were drawn up.

## **1.6 Process of Money Laundering**

Money laundering is not a single act but a process accomplished in 3 basic stages that may comprise numerous transactions by the launderers. Money laundering process begins after the predicate offences are committed and funds have been generated. The main objective of the money launderer is to transform 'dirty' money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation. Examples of illegal activities that often involve money laundering are: drug trafficking; terrorism; smuggling; fraud; bribery & corruption; robbery & theft; embezzlement; and illegal gambling. There are 3 stages of money laundering-

### **1.6.1 Placement**

The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions. At this stage cash derived from criminal activity is infused into the financial system. The placement makes the funds more liquid since by depositing cash into a bank account can be transfer and manipulated easier. When criminals are in physical possession of cash that can directly link them to predicate criminal conduct, they are at their most vulnerable. Such criminals need to place the cash into the financial system, usually through the use of bank accounts, in order to commence the laundering process.

**Smurfing** – a form of Placement where the launderer makes many small cash deposits instead of a large one to avoid local regulatory reporting requirements applicable to cash transactions. Launderers intend to avoid the threshold of Cash Transaction for elusion the reporting to Regulatory or competent authority. Smurfing is also known as “Structuring”.

### **1.6.2 Layering**

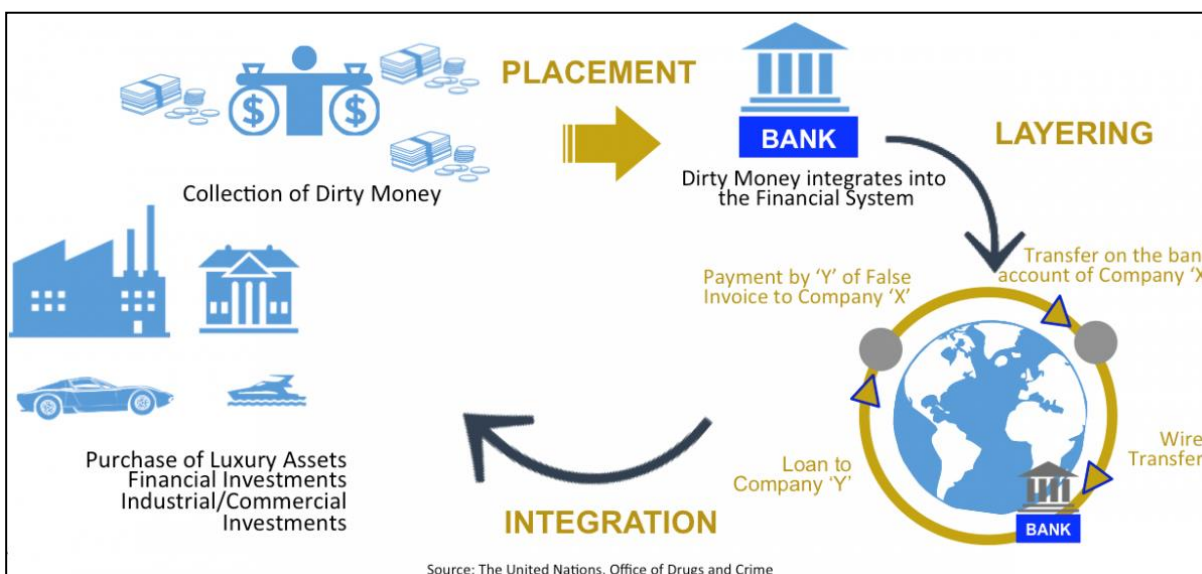
Layering is the process of separating the proceeds of criminal activity from their origin through the use of many different techniques to layer the funds. These include using multiple banks and accounts, having professionals act as intermediaries and transacting through corporations and trusts, layers of complex financial transactions, such as converting cash into traveler's checks, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets, such as art or jewelry. All these transactions are designed to disguise the audit trail and provide anonymity.

Layering usually involves a complex system of transactions designed to hide the source and ownership of the funds. Once cash has been successfully placed into the financial system, launderers can engage in an infinite number of complex transactions and transfers designed to disguise the audit trail and thus the source of the property and

provide anonymity. One of the primary objectives of the layering stage is to confuse any criminal investigation and place as much distance as possible between the source of the ill-gotten gains and their present status and appearance.

### 1.6.3 Integration

It is the stage at which laundered funds are reintroduced into the legitimate economy, appearing to have originated from a legitimate source. Integration is the final stage of the process, whereby criminally derived property that has been placed and layered is returned (integrated) to the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the “cleaned” money into the economy is accomplished by the launderer making it appear to have been legally earned. By this stage, it is exceedingly difficult to distinguish legal and illegal wealth.



*Figure: 3 stages of Money Laundering*

Not all money laundering transactions go through this three-stage process. The three basic stages may occur as separate and distinct phases or may occur simultaneously or, more commonly, they may overlap. Transactions designed to launder funds can for example be effected in one or two stages, depending on the money laundering technique being used. How the basic steps are used depends on the available laundering mechanisms and requirements of the criminal organizations.

## 1.7 How Financial Institution can combat Money Laundering

The prevention of laundering the proceeds of crime has become a major priority for all jurisdictions from which financial activities are carried out. One of the best methods of



preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. The adoption of procedures by which Banks and other Financial Institutions "Know Your Customer" is not only a principle of good business but is also an essential tool to avoid involvement in money laundering. For the purposes of these guidance notes the term Banks and other Financial Institutions refer to businesses carrying on relevant financial business as defined under the legislation.

Thus efforts to combat money laundering largely focus on those points in the process where the launderer's activities are more susceptible to recognition and have therefore to a large extent concentrated on the deposit taking procedures of banks i.e. the placement stage.

Institutions and intermediaries must keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.

## **1.8 Penalties under Money Laundering Prevention Act, 2012 (Amendment, 2015)**

### **i) Offence of Money Laundering and Punishment (Section 4):**

1. According to section 4(1), Money laundering is an offence.
2. According to section 4(2), Any person who commits or abets or conspires to commit the offence of money laundering, shall be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lac, whichever is greater. However, in case of failure of the payment of the fine in due time, the court may issue an order of extra imprisonment considering the amount of the unpaid fine.
3. According to section 4(3), In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved in or related with money laundering or any predicate offence.
4. According to section 4(4), Any entity which commits or abets, assists or conspires to commit the offence of money laundering under this section, subject to the provisions of section 27, measures shall be taken as per sub-section (2) and punished with a fine of not less than twice the value of the property related to the money laundering or taka 20(twenty) lacks, whichever is higher and in addition to this the registration of the said entity shall be liable to be cancelled. However, in case of failure in payment of the fine by the entity in due time, the court may, considering the amount of unpaid fine, issue an order of

imprisonment to the entity's owner, chairman or director or by whatever name he is regarded.

**ii) Punishment for violation of a freezing or attachment order (Section 5):**

Any person who violates a freeze order or order of attachment issued pursuant to this Act shall be punishable with an imprisonment for a maximum period of 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or both.

**iii) Punishment for divulging information (Section 6):**

Whoever contravenes the provisions contained of this act shall be punishable by imprisonment of maximum period of 2 (two) years or a fine, not exceeding Tk. 50 (fifty) thousand or both.

**iv) Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information (Section 7):**

Any person found guilty of an offence under this act shall be punishable by imprisonment of maximum period of 1 (one) year or with a fine not exceeding Tk. 25 (twenty five) thousand or with both.

**v) Punishment for providing false information (Section 8):**

Any person who violates the provisions contained of this act will be punishable by imprisonment of maximum period of 3 (three) years or a fine not exceeding Tk. 50 (fifty) thousand or both.

### **1.9 Definition of Terrorist Financing**

Terrorist financing provides funds for terrorist activities. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Financing of Terrorism is also includes:

- providing or collecting property for carrying out an act of terrorism;
- providing services for terrorism purposes;
- arranging for retention or control of terrorist property; or
- dealing with terrorist property.



The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

- 'If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
  - a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or
  - b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.
- 2) For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b).

According to the article 7 of the Anti-Terrorism Act 2009, (Amendment) 2013 of Bangladesh,

Offence of terrorist financing: Sub-section (1) If any person or entity willfully provides, receives, collects or makes arrangements for money, service or any other property, whether from legitimate or illegitimate source, by any means, directly or indirectly, with the intention that, in full or in part be used-

(a) to carry out terrorist activity;

(b) by terrorist person or entity or in the knowledge that they are to be used by terrorist person or entity;

the said person or entity shall commit the offence of terrorist financing.

Sub-section 2) Conviction for terrorist financing shall not depend on any requirement that the fund, services or any other property mentioned in sub-section (1) were actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act.

### **1.9.1 Penalties for Terrorist Financing**

According to the Section 7 of the Anti-Terrorism Act 2009, (Amendment) 2013 of Bangladesh,

Section 7(3) If any person is found guilty of any of the offences mentioned in sub-sections (1), the person shall be punished with an imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine may be

imposed equal to twice the value of the property involved with the offence or taka 10(ten) lac, whichever is greater.

Section 7(4) If any entity is found guilty of any of the offences mentioned in the sub-sections (1)- (a) steps may be taken in accordance with section 18 and in addition to that a fine may be imposed equal to thrice the value of the property involved with the offence or taka 50 (fifty) lacs, whichever is greater; and

(b) The head of such entity, whether he is designated as Chairman, Managing Director, Chief Executive or any other name, shall be punished with an imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and in addition to that a fine may be imposed equal to twice of the value of the property involved with the offence or taka 20 (twenty) lac, whichever is greater, unless he is able to prove that the said offence was committed without his knowledge or he had tried utmost to prevent the commission of the said offence.

## **CHAPTER: II**

### **COMPLIANCE PROGRAM OF NRB BANK**

#### **2.0 Preamble**

One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. The procedure "Know Your Customer" is not only an essential tool to avoid involvement in money laundering but also a principle of good business. Having a sound knowledge of a Customer's identity, business, Source of income, Pattern of financial transactions, Purpose of transaction is the best method by which we will recognize attempts at money laundering.

#### **2.1 AML & CFT Compliance Program of NRB Bank**

To prevent Money Laundering, Terrorist Financing and Proliferation Financing NRB Bank determined it's compliance program which includes-

1. To prevent ML, TF & PF Senior Management role including their commitment has been declared;
2. Internal policies, procedure and controls- NRB Bank defined AML & CFT policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, self-assessment, independent testing procedure, employee screening, record keeping and reporting to BFIU;
3. Compliance structure includes establishment of Central Compliance Committee (CCC), appointment of Chief Anti Money Laundering Compliance Officer (CAMLCO), Branch Anti Money Laundering Compliance Officer (BAMLCO);
4. Independent audit function- it includes the role and responsibilities of internal audit on AML & CFT compliance and external audit function;
5. Awareness building program includes training, workshop, seminar for bank employees, member of the Board of Directors, owners and above all for the customers on AML & CFT issues.

#### **2.2 Role of Senior Management**

For the purposes of preventing ML, TF & PF, senior management includes members of the board of directors of the bank, or the member of the highest management committee in absence of the board of directors and the Chief Executive Officer (CEO) or the Managing Director (MD) of the bank.

*Obligations under Law (ATA, 2009): The Board of Directors, or in the absence of the Board of Directors, the Chief Executive of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, which are applicable to the reporting agency, have been complied with or not.*

The most important element of a successful AML & CFT program is the commitment of senior management, including the chief executive officer and the board of directors, to the development and enforcement of the AML & CFT objectives which can deter criminals from using their banks for ML, TF & PF, thus ensuring that they comply with their obligations under the laws and regulations.

Board of Directors (BoD) or Highest Management committee (in absence of BoD) shall-

- approve AML & CFT compliance program and ensure its implementation;
- issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- take reasonable measures through analyzing Self-Assessment report and independent testing report summary;
- understand ML & TF risk of the bank, take measures to mitigate those risk;
- CEO or/and MD shall issue statement of commitment to prevent ML, TF & PF in the bank;
- Ensure compliance of AML & CFT program;
- Allocate enough human and other logistics to effective implementation of AML & CFT compliance program;
- Ensure appropriate level of AML & CFT training for employees at all levels throughout the bank;
- Establish proper mechanisms and formulate procedures to effectively implement AML & CFT policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

NRB Bank arranges Board awareness program on AML & CFT issues almost in every year and understand the update position on AML & CFT issues.

Senior Management of the Bank shall advice to “Human Resources Division” for inclusion of AML & CFT compliance in their manual so that it helps to adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the bank. Senior Management shall also instruct the following issues:-

- ❖ Employee Background Screening at the time of recruitment.
- ❖ Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- ❖ Proper weight in the annual performance evaluation of employees for extraordinary preventive action vis a vis for non-compliance;
- ❖ Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;

Senior management shall be responsive of the level of Money Laundering and Terrorist Financing Risk when the bank is exposed to and take a view whether the bank is equipped to mitigate that risk effectively.

### **2.3 Statement of Commitment of Managing Director & CEO**

As per the instruction of Clause-1.2 of BFIU Circular No. 26 dated June 16, 2020, MD & CEO of NRB Bank ensures his commitment on AML & CFT issues mentioning the role and responsibilities of employees of the Bank and advice the direction to implement the commitment in every year. The commitment/message will cover the following issues:-

- ❖ Bank's policy or strategy to prevent ML, TF & PF;
- ❖ Emphasize on effective implementation of bank's AML & CFT compliance program;
- ❖ Clear indication of balance between business and compliance, risk and mitigating measures;
- ❖ Compliance is the responsibility of each employee during their normal course of assignment and ignorance shall not be considered as the excuse for non-compliance;
- ❖ Point of contact for clarification in case of any ambiguity arise;
- ❖ Consequences of non-compliance as per human resources (HR) policy of the bank.

### **2.4 Central Compliance Committee (CCC)**

#### **2.4.1 Formation of CCC**

To keep the banking sector free from the risks related to Money Laundering & Terrorist Financing and for the effective/proper compliance of all existing acts, rules and instructions issued by BFIU time to time, NRB Bank set up a Central Compliance Committee (CCC) that will be directly monitored by the Managing Director and Chief Executive Officer (CEO) of the bank.

CCC includes the following Department/Division Heads of Corporate Head Office:

Sl. No.	List of CCC Members	Position
1.	Chief Anti Money Laundering Compliance Officer (CAMLCO)	Chairman
2.	Head of AML & CFT Dept. & DCAMLCO	Member Secretary
3.	Head of Corporate Banking	Member
4.	Head of FI	Member
5.	Head of CRM	Member
6.	Head of Risk Management Division	Member
7.	Head of FRD & Agent Banking	Member
8.	Head of Cards	Member
9.	Head of Trade Operations	Member
10.	Head of SME	Member
11.	Head of Retail Banking	Member
12.	Head of SAMD	Member
13.	Head of HRD	Member
14.	Head of IT & ADC Ops.	Member
15.	Head of Branches, Corporate Office	Member
16.	Head of Operations Division	Member
17.	Officials of AML & CFT Dept.	Member

## 2.4.2 Responsibilities and Authorities of the CCC

### Responsibilities:

CCC is the prime mover of the Bank for ensuring the compliance of AML & CFT measures. Its main responsibilities are:-

- CCC will conduct meeting on quarterly basis and take decision for the betterment of the Bank on AML & CFT issues. If required, CCC can organize more meeting. This meeting will includes the following matters and its improvement:
  - Know Your Customer (KYC);
  - Transaction Monitoring;
  - STR/SAR identification and reporting;
  - Local Sanction List and UNSCR list;
  - Self-Assessment Procedure;
  - Record Keeping;
  - Training.

AML & CFT Department will implement all the decision taken in the meeting.

- CCC will nominate the BAMLCO for monitoring of Branch compliance on AML & CFT issues.
- CCC will monitor performance of the BAMLCO in the branch level to ensure AML & CFT compliance.
- CCC will develop the bank's policy, procedure and strategies in preventing ML, TF & PF when necessary;
- CCC will ensure maintenance of regular liaison with BFIU, Bangladesh Bank, External Auditors and other Law enforcing agencies through CAMLCO/DCAMLCO.
- CCC will coordinate bank AML & CFT compliance initiatives;
- CCC will ensure training courses, workshops and seminars for the development of compliance knowledge amongst officials as and when required regarding Money Laundering, Terrorist Financing and financing in spreading of trading of mass destructive weapons which will be conducted by AML & CFT Department with help of Training Institute.
- CCC will monitor/evaluate Independent Testing Procedure to be conducted by our Internal Control & Compliance Division and AML & CFT Department.
- CCC will monitor/evaluate effectiveness of Self-Assessment procedure on half yearly basis and ensure it's reporting to BFIU on time.
- CCC will undertake required measures to submit any information, report and/or documents to BFIU, Bangladesh Bank and/or any authority in respect of ML, TF & PF.
- CCC will ensure for reporting of STR/SAR and CTR to BFIU in time and in proper manner through AML & CFT Department.
- CCC will oversee any other issue that may arise from time to time regarding ML, TF & PF.

For shouldering these responsibilities bank authority may consider to give the following authority to CCC-

- appointment of BAMLCO and assign their specific job responsibilities;
- requisition of human resources and logistic supports for CCC and for AML & CFT Department;
- make suggestion or administrative sanction for non-compliance by the employees;
- CCC will directly report to Managing Director & CEO of the Bank.

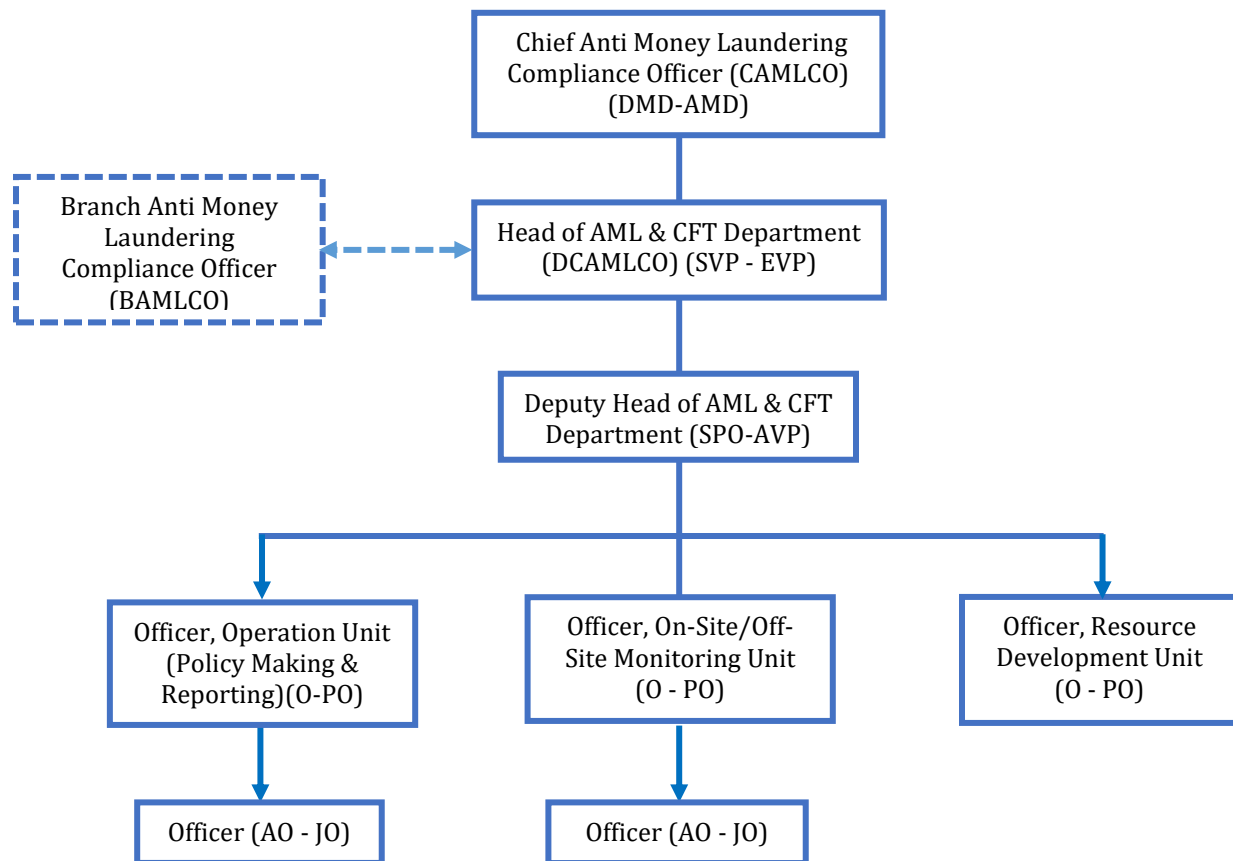


### 2.4.3 Separation of CCC from Internal Control & Compliance Department (ICCD)

As per BFIU Circular No. 26 dated June 16, 2020, CCC shall be an independent and shall be completely separated from Internal Compliance and Control Division (ICCD). There shall not be any member from ICCD to CCC. The ICCD & CCC have to deal with money laundering and terrorist financing assignment assigned to them completely separately.

### 2.5 Formation of AML & CFT Department

As per the BFIU circular No 26 dated June 16, 2020, to carry out the secretarial duties of the Central Compliance Committee (CCC) and to fulfill the obligations to prevent money laundering and terrorist financing, each Bank will formulate the AML & CFT Department. In this connection, NRB Bank has an AML & CFT Department with appropriate number of staff considering the number of branches of the bank, scope of business, number of customers and institutional risk, etc. AML & CFT Department will be headed by Deputy CAMLCO. The organizational structure of AML & CFT Department is given below:





## **2.6 Appointment of CAMLCO**

- ❖ As per BFIU Circular No. 26, CAMLCO will be considered as an official within 2 (two) tier of the Managing Director/Chief Executive Officer of the Bank. Before assigning the CAMLCO to other duties of the Bank, the management has to ensure that the AML & CFT activities of the bank will not be hampered.
- ❖ The position within the organization of the person appointed as CAMLCO will vary according to the size of the bank and the nature of its business, but he or she shall have to be sufficiently senior to command the necessary authority.
- ❖ He/she will have vast knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML, TF & PF. He/she will also have vast knowledge & experience on general banking, investment and foreign exchange business of the bank.
- ❖ If the CAMLCO is changed, it must be informed to BFIU and AACOB without delay by the AML & CFT Department.

### **2.6.1 Authorities and Responsibilities of CAMLCO**

#### **2.6.1.1 Authorities**

CAMLCO must have sufficient authority to implement and enforce AML & CFT policies, procedures and measures. The authorities must include at least the followings:

- CAMLCO shall act on his/her own authority;
- CAMLCO shall exercise the authorities of the CCC as Head of the Committee.
- He/she shall not take mandatorily any permission or consultation from/with the Managing Director & CEO before submission of STR/SAR and any document or information to BFIU;
- He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He/she must have access to any information of the bank;
- He/she shall ensure his/her continuing competence.

#### **2.6.1.2 Responsibilities**

The CAMLCO is responsible for overall oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering, terrorist financing and proliferation financing. Few of the responsibilities are:

- CAMLCO must ensure overall AML & CFT compliance of the bank;
- CAMLCO must take all the responsibilities of CCC as Head of the Committee.
- oversee the submission of STR/SAR or any document or information to BFIU in time;

- maintain the day-to-day operation of the bank's AML & CFT compliance;
- CAMLCO will inform to Managing Director & CEO for proper functioning of CCC;
- CAMLCO shall review and update ML & TF risk assessment & management policy of the bank;
- Confirm the preparation of Half-Yearly Self-Assessment Report and send to BFIU within the time frame.
- corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.
- He/she shall oversee all other issues that may arise from time to time regarding ML, TF & PF.

## **2.7 Appointment of DCAMLCO**

- ❖ As per BFIU Circular No. 26, Bank shall also nominate Deputy of the CAMLCO, who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO). The DCAMLCO will be at least in the rank of 'Senior Vice President' of the bank. DCAMLCO have to have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML & TF.
- ❖ The position within the organization of the person appointed as DCAMLCO will vary according to the size of the bank, the nature of its business and business portfolio, but he or she shall have to be sufficiently senior to command the necessary authority.
- ❖ The Managing Director & CEO shall appoint the DCAMLCO (s) at Corporate Head Office to implement and enforce corporate wide AML & CFT policies, procedures and measures under supervision of CAMLCO;
- ❖ The designated DCAMLCO(s), through the CCC, shall be the central point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML & CFT program after CAMLCO.
- ❖ As the DCAMLCO is responsible for the oversight of all aspects of the bank's AML & CFT activities and is the focal point for all activity within the bank relating to ML & TF after CAMLCO, his/her job description shall have to be clearly set out the extent of the responsibilities given to him/her under supervision of CAMLCO.
- ❖ Before assigning the DCAMLCO(s) to other duties of the bank, the management has to be sure that the AML & CFT activities of the bank will not be hampered; and
- ❖ If the DCAMLCO is changed, it must be informed to BFIU and AACOB without delay.

## **2.8 Branch Anti Money Laundering Compliance Officer (BAMLCO)**

As per BFIU Circular No. 26 dated June 16, 2020, Head of Branch, 2<sup>nd</sup> person of the Branch or GB/Foreign Exchange/Credit related experience senior officials will be nominated as BAMLCO. BAMLCO have to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions (circulars, circular letters, etc.) and Bank's own policies on preventing Money Laundering and Terrorist Financing.

In our Bank, as per decision of the Central Compliance Committee (CCC), the HOB of the Branch will be nominated as "BAMLCO". CSM can be nominated as BAMLCO where CSM is not less than Senior Principal Officer (SPO). AML & CFT Department/CCC will take decision for nomination of the BAMLCO of the branch. Any kind of deviation regarding nomination of BAMLCO, need approval from CAMLCO.

In absence of BAMLCO, Branch management will nominate another officials to ensure his job responsibilities and mitigate the AML & CFT matters and inform AML & CFT Department for the time being. Branch will also inform to AML & CFT Department immediately regarding transfer of BAMLCO.

### **2.8.1 Responsibilities and Authorities of BAMLCO**

#### **2.8.1.1 Responsibilities**

BAMLCO will perform the following responsibilities:

##### **Knowledge on AML & CFT issues**

- Be familiar with laws, circulars, policies, guidelines, national & international initiatives regarding AML & CFT issues.
- BAMLCO must inform/update to all the officials of the branch regarding laws, circulars, Policies, guidelines, national & international initiatives on AML & CFT matters and ensure its meticulous compliance.
- Make sure on boarding customer and transaction have been screening by the system and report to competent authority, if any.

##### **Branch Compliance Program**

- Implement all instructions of AML & CFT Department/CCC regarding AML & CFT issues time to time.

##### **Sanctions Screening**

- Ensure sanction list screening like UN Sanction list, OFAC and EU list and list of organization banned by Bangladesh Government before opening of account and while making any transaction of walk-in customer.
- Reviews suspected matches and reports valid matches to the AML & CFT

Department for onward submission to BFIU.

**Customer Due Diligence**

- Identify and verify the identity of the customer information and documents obtained from the reliable source.
- Ensure the KYC of the new customers and update of KYC of existing customers have done properly.
- Ensure due diligence while establishing relationship with the new customer and also while conducting financial transaction with the existing customer.
- Ensure due diligence when there is a suspicion of money laundering or terrorist financing.
- Ensure due diligence of walk-in customer, online customers and depositor or withdrawer other than account holder.
- Identify the beneficial owner of the account and conduct due diligence of the beneficial owners.
- Keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;

**Enhance Due Diligence (EDD)**

- Confirm approval of CAMLCO/DCAMLCO before opening of PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates.
- Confirm EDD of PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates.
- Comply Enhance Due Diligence (EDD) for the high risk customer and obtain additional information/documents.
- Ensure EDD while establishing and maintaining business relationship and conducting financial transaction with a person or entity of the countries and territories that do not meet international (FATF) standard in combating money laundering.

**Transaction Monitoring**

- Introduce self-auditing, self-assessment and independent testing procedure in the branch and report to Internal Control & Compliance Division and AML & CFT Department in time.
- Ensure regular transaction monitoring to find out any unusual transaction. Records of all transaction monitoring should be kept in the file.
- Review cash transaction to find out any structuring;

- Ensure monitoring of account transaction as per instruction of BFIU as well as AML & CFT Department.
- Detect high risk customer using subjective/objective judgment and ensure proper filing.

**Update Customer Information and TP & KYC**

- Update/Review of Transaction Profile and KYC of the customer as per BFIU circular no. 26 dated June 16, 2020.
- Update customer information with proper justification if any changes required.

**Arrangement of AML & CFT Meeting**

- BAMLCO shall arrange quarterly meeting regarding AML & CFT issues as per instruction of BFIU circular no. 26 dated June 16, 2020 in the branch level and send meeting minutes to AML & CFT Department on time.

**Report Submission to AMLD**

- Review Monthly Cash Transaction Report (CTR), Monthly Identification of STR from CTR analysis, Quarterly Meeting Minutes, Half-yearly Self-Assessment Procedures and send these to AML & CFT Department within the stipulated time period without any fail.
- Review information and documents before submitting those reports to AML & CFT Department for onward submission to BFIU.

**STR/SAR Identification and Reporting**

- Identification of STR/SAR.
- Report STR/SAR by monitoring and analyzing transaction.
- Review the CTR of each month and find out STR/SAR and send it to AML & CFT Department.
- Ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
- Analyze the Cash Transactions immediate below the CTR threshold limit to identify structuring.
- Monitor customer unusual behavior and unusual transaction pattern.
- Considering all the information of the account holder, investigate the purpose of transaction and source of fund with relevant documents, if found any suspicious transactions then report to AML & CFT Department.

**Record Keeping**

- Keep records of customer's identification and transactions at least five years after the termination of relationships with the customers.

- Ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements.
- Ensure confidentiality of the records preserved.
- Ensure AML & CFT related files are available in the branch level and update those files on regular basis.

**Training of employees**

- Provide/arrange training to new employees immediately and refresher training to the employees who obtain training regarding AML & CFT issues two years before.
- Take initiative for training to all officials of the branch.

**Others responsibilities**

- Ensure all the required information and document are submitted properly to AML & CFT Department and any freeze order or stop payment order are implemented properly and without delay;
- Follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
- Create awareness regarding AML & CFT among the customer of the branch.
- Ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.
- Monitor the staff of the branch to check whether any of them are directly or indirectly involved in or is facilitating Money Laundering and Terrorist Financing.

**2.8.1.2 Authorities**

For shouldering these responsibilities, NRB Bank will consider to give the following authority to BAMLCO:

- Generally, BAMLCO will report to Head of Branch/AML & CFT Department regarding all the matters of AML & CFT.
- BAMLCO can independently send STR/SAR to AML & CFT Department, if needed.
- BAMLCO can act independently for ensure compliance regarding AML & CFT issues.

Branch management can appoint BAMLO to help the BAMLCO for smooth operation of the above mentioned responsibilities with the permission of CAMLCO.

**2.9 Department/Division AML Compliance Officer**

To monitor the AML & CFT compliance issues departments/divisions like Trade Operations, CRM, CAD, FI, Agent Banking, FRD, Card Division, and other Corporate Head



Office Department/Division may appoint Department/Division AML Compliance Officer and inform to AML & CFT Department. If any non-compliant issues arise at their end then Department AML Compliance Officer must inform to AML & CFT Department for taking the necessary steps.

## **2.10 Roles & Responsibilities of Account Opening Officer/Operation Manager/Relationship Manager**

- Perform due diligence on prospective clients prior entering into any relationship with Bank;
- Be diligent regarding the identification(s) of account holder and the transactions relating to the account;
- Ensure all required documentation is completed satisfactorily;
- Complete the Transaction Profile (TP) and KYC Profile Form;
- Ongoing monitoring of customer's KYC profile and transaction activity;
- Obtain documentary evidence of large cash deposits;
- Escalate any suspicion to the Supervisor, Head of Branch and/or BAMLCO.

## **2.11 Role & Responsibilities of Internal Control & Compliance Division**

As per BFIU circular no. 26 dated June 16, 2020, "with a goal of establishing an effective AML and CFT regime, it shall have to be ensured that Internal Control & Compliance Division of the bank is equipped with enough manpower who have enough knowledge on the existing acts, rules and regulations, BFIU's instructions on preventing money laundering & terrorist financing and bank's own policies in this matter to review the Self-Assessment Procedure received from the branches and to execute the Independent Testing Procedure appropriately."

Internal Control & Compliance Division of NRB Bank shall have an important role for ensuring proper implementation of bank's AML & CFT Compliance Program. Internal Control & Compliance Division of Bank is equipped with enough manpower and autonomy to look after the prevention of ML & TF. The Internal Control & Compliance Division has to oversee the implementation of the AML & CFT compliance program of the bank and has to review the 'Self-Assessment Procedure' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

Internal auditors should be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable.

The Internal Control & Compliance Division must-

- understand ML & TF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML & CFT Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML & CFT Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU or BB;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
  - employee accountability for ensuring AML & CFT compliance,
  - comprehensiveness of training, in view of specific risks of individual business lines,
  - training of personnel from all applicable areas of the bank,
  - frequency of training,
  - coverage of bank policies, procedures, processes and new rules and regulations,
  - coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
  - penalties for noncompliance and regulatory requirements.

## **2.12 Responsibilities of Internal Control & Compliance Division on Self-Assessment & Independent Testing Procedures**

As per the clause no. 8.2 of BFIU circular no. 26, the Internal Control & Compliance Division shall assess the branch evaluation "Self-Assessment Procedure" received from the branches



and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the AML & CFT Department.

While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the Internal Control & Compliance Division should examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure as per the “Annexure-Gha” of BFIU Circular No. 26. Beside scheduled inspection/audit, Internal Control & Compliance Division will conduct inspection/audit extra minimum 10% branches as per as “Annexure-Gha” of BFIU Circular No. 26 on yearly basis regarding the compliance status on AML & CFT issues and report will be submitted to AML & CFT Department.

Internal Control & Compliance Division should send a copy of the report with the rating of the branches inspected/audited by the Internal Control & Compliance Division to the AML & CFT Department of the bank within the following month of the end of the every Half Year.

In case of Agent Banking, Internal Control & Compliance Division will inspect a minimum 5% Agent Point of the Bank at yearly basis regarding the compliance status AML & CFT issues and report will be submitted to AML & CFT Department.

### **2.13 External Auditor**

- External auditor of NRB Bank will review the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report.
- External auditor shall be risk-focused while developing their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient.

## **CHAPTER: III**

# **ESSENTIAL ELEMENTS OF ML/FT RISK MANAGEMENT**

### **3.0 Preamble**

Bank should be required to have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards in the banking sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities.

### **3.1 Assessment, understanding, management and mitigation of risks**

#### **3.1.1 Assessment and Understanding of Risks**

Risk management requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied. The policies and procedures for CDD, customer acceptance, customer identification and monitoring of the business relationship and operations (product and service offered) will then have to take into account the risk assessment and the bank's resulting risk profile.

NRB Bank has taken appropriate steps to identify and assess their money laundering and terrorist financing risks for customers, countries or geographical areas, products/services and transactions or delivery channels. NRB Bank documents those assessments in order to be able to demonstrate their basis, keep those assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities.

#### **3.1.2 Proper governance arrangements**

Effective ML/TF risk management requires proper governance arrangements. The board of directors or Senior Management should have a clear understanding of ML/TF risks. Information about ML/TF risk assessment should be communicated to the board/senior management in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions.

#### **3.1.3 Three Lines of Defense**

In the context of AML/CFT, the business units (e.g. front office, customer-facing activity) are **the first line of defense** in charge of identifying, assessing and controlling the risks of

their business. As part of the first line of defense, policies and procedures should be clearly specified in writing, and communicated to **all personnel**.

The **second line of defense** includes **the CAMLCO/chief officer** in charge of AML/CFT, the compliance function but also human resources or technology. As part of the second line of defense, the chief officer in charge of AML/CFT should have the responsibility for ongoing monitoring of the fulfilment of all AML/CFT duties. He/she should have a direct reporting line to Managing Director & CEO or the Honorable Board of Directors. The chief AML/CFT officer should also have the responsibility for reporting suspicious transactions.

The **third line of defense** is ensured by the **internal audit** function. Internal audit, the third line of defense, plays an important role in independently evaluating the risk management and controls, and discharges its responsibility to the audit committee of the board of directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with AML/CFT policies and procedures. In addition, **external auditors** also have an important role to play in evaluating banks' internal controls and procedures in the course of their financial audits, and in confirming that they are compliant with AML/CFT regulations and supervisory practice.

### **3.1.4 Adequate transaction monitoring system**

Branch/Agent Banking Division/Concern Division/Department needs to monitor the transactions of customer on a regular basis. The complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized during monitoring. An effective system has to be developed by the banks to review the risk by maintaining a specific time interval; and according to the review, Enhanced Due Diligence (EDD) has to be maintained for accounts that are in high risk category.

Key components of transaction monitoring - An effective monitoring system comprises the following components:

- i. Monitoring performed by the staff who deal directly with customers (e.g. relationship managers) and also by the staff of branch.
- ii. Process the transactions of the customer by the staff of the branch (e.g. counter staff) and
- iii. Regular reviews of past transactions to detect unusual transactions by BAMLCO.

Branch/concern head office division/department should put in place various ways of transaction monitoring mechanism within their branches that includes but not limited to

the followings:

- ❖ Transactions in local currency;
- ❖ Transactions in foreign currency;
- ❖ Transactions above the designated threshold determined by the branch;
- ❖ Cash transactions under CTR threshold to find out structuring;
- ❖ Transactions related with international trade;
- ❖ Transaction screening with local and UN Sanction list.

#### **3.1.4.1 Analysis of TP exception report**

Branch/Agent Banking Division/Concern Division/Department will take a report from the Report Server of TP exception report to analyze the transaction and commensurate with the income/source of fund of the customer. Branch will collect the required documents, if necessary.

#### **3.1.4.2 Monthly CTR analysis**

Branch/Agent Banking Division/Concern Division/Department will generate CTR automatically through our “Report Server” on month basis and analyze those transactions. Branch will also submit a report of “Identification of STR through analyzing CTR” to AML & CFT Department on or before 10<sup>th</sup> day of each month through a prescribed format given by the AML & CFT Department. After analyzing CTR, if branch found any suspicious then branch will raise a STR to AML & CFT Department immediately for onward submission to BFIU.

#### **3.1.4.3 Structuring Report Analysis**

Branch/Agent Banking Division/Concern Division/Department will generate the structuring report periodically from “Report Server” and analyze the transaction. Customers organize transaction in such a way to avoid triggering a reporting of CTR. It is one of most well-known money laundering methods which occurred in the Money Laundering process through Placement. If any suspicious transactions found by the officials then report to AML & CFT Department.

### **3.2 Customer Acceptance Policy of NRB Bank**

NRB Bank develops and implements clear customer acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of ML and TF pursuant to the bank’s risk assessment. When assessing risk, branch should consider the factors relevant to the situation, such as a customer’s background, occupation (including a public or high-profile position), source of income and wealth, country of origin and residence

(when different), products used, nature and purpose of accounts, linked accounts, business activities and other customer-oriented risk indicators in determining what is the level of overall risk and the appropriate measures to be applied to manage those risks.

Such policies and procedures require basic due diligence for all customers and commensurate due diligence as the level of risk associated with the customer varies. Where the risks are higher, banks should take enhanced measures to mitigate and manage those risks.

### **3.2.1 Customer Identification & Verification**

#### **Definition of Customer:**

As per 3.1 of BFIU circular No. 26 dated 16.06.2020, for the purpose of risk management on Money Laundering and Terrorist issues "Customer" is defined as follows:

- Any person or institution maintaining an account of any type with a bank or financial institution or having banking related business;
- the person or institution as true beneficial owner in whose favour the account is operated; the true beneficial owner of the transaction of the accounts operated by the professional intermediaries (such as lawyer/law firm, chartered accountant, etc.) under the existing legal infrastructure;
- high value Occasional Transaction (Wire Transfer, Demand Draft, Pay Order, Telegraphic Transfer) conducted by any person or institution or any person/institution involved in a financial transaction that may pose reputational and other risks to the institution. In this case if a transaction appears abnormal in relation to the usual transaction of the concerned person or institution that transaction will be treated as - "high value".

NRB Bank establishes a systematic procedure for identifying and verifying its customers and, where applicable, any person acting on their behalf and any beneficial owner(s). Generally, Branch should not establish a banking relationship, or carry out any transactions, until the identity of the customer has been satisfactorily established and verified in accordance with FATF Recommendation 10 (Customer Due Diligence).

The identity of customers, beneficial owners, as well as persons acting on their behalf, should be verified by using reliable, independent source documents, data or information. When relying on documents, branch should verify the documents from independent sources. When relying on other sources than documents, the branch must ensure that the methods and sources of information are appropriate, and in accordance with the bank's policies and procedures and risk profile of the customer.

Beneficial Owner refers-

As per 2(4) of Money Laundering Prevention Rules 2019 beneficial owner means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercises ultimate effective control over a legal person or arrangement or holds 20% or more share of a company. Here “ultimately owns or controls” and “ultimate effective controls” refers to situation in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

The definition of beneficial owner means the individual who –

- a) has effective control of a customer; or
- b) owns a prescribed threshold, 20% as per Bangladeshi regulation of the company or legal arrangements.

Identifying the beneficial ownership of a customer one must apply three elements. Any one element or any combination of these three elements satisfies beneficial ownership. These elements are:

- a) who owns 20 or more percent of a company or legal arrangements
- b) who has effective control of the customer;
- c) the person on whose behalf a transaction is conducted

All the concerns of NRB Bank should have to follow the “**Guidelines for Beneficial Owner**” issued by BFIU for details information of Identification of Beneficial Owner which has already been circulated to all the employees vide our instruction circular no. 02/2019 dated March 06, 2019.

### **3.2.1.1 General Requirements**

Branch/Agent Banking Division/Concern Division/Department shall ensure the following aspects while establishing relationship with a customer or providing any banking services or conducting transactions:

- a. Proper Sanction Screening (UNSCRs & Local list) must be done before creating any Customer ID/CIF or opening any account and doing transactions (Remittances, SWIFT & Trade related).
- b. Dedupe should be checked before opening any account. Unique customer identification code for any customer who maintains more than one account or availing more than one facilities shall be used. Such unique identification system

shall facilitate banks to avoid redundancy, and saves time and resources. This mechanism also enables banks to monitor customer transactions effectively.

- c. Proper NID verification through Election Commission Server.
- d. Branch will accept only those customers whose appropriate identity is established by conducting due diligence of the customer.
- e. Documents requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of MLPA-2012(Amendment 2015), ATA-2009 (Amendment 2012 & 2013) & BFIU Directives from time to time.
- f. Accounts for the non-resident Bangladesh citizens are to be opened subject to compliance of Foreign Exchange Regulation Act, 1947, GEFT Vol. 1 and circulars issued by Bangladesh Bank under it.
- g. In case of establishing correspondent banking relationship, the branch/concerned division /department shall follow the guidelines as contained in clause no. 3.13 of BFIU Circular No. 26 dated 16.06.2020 issued by BFIU and amendments issued from time to time meticulously.
- h. In case of establishing any relationship with Politically Exposed Person (PEP)/ Influential Person (IP)/ Chief Executives or Top Level Officials of any International Organization account and their close associates/family members, the branch shall comply the instructions contained in the internal (AML & CFT Department) Instruction Circular No. 02/2019 dated March 06, 2019 mentioning the “Guidance Note of Politically Exposed Persons (PEPs) for all Reporting Organizations” issued by BFIU.

### **3.2.1.2 Customer Identification measures**

#### **3.2.1.2.1 Individual Account/Joint Account**

##### **a. Identify and Verify the Customer**

Branch/Agent Banking Division/Concern Division/Department may open account or establish relationship with any natural person or individual ensuring the followings:

- Collect identification documents as per BRPD circular no. 02 dated February 23, 2020, such as:
  - National ID Card (NID) or
  - Valid Passport/Birth Registration Certificate/Others identity (should be specific),

***“Others identity” can be used for the products under Financial inclusion only which is acceptable by the Banker. No introducer is needed if the NID copy submitted by the customer.***



- Verify the customer NID with Bangladesh Election Commission under “Guidelines on Electronic Know Your Customer (e-KYC)”.
- Collect and verify complete & accurate KYC and other information;
- Risk grading and performing appropriate CDD measures;
- Identification of beneficiary owner(s) and authorized person(s), if any; and
- Name of the customers, beneficiary owner(s) and authorized person(s), if any, are not listed in Targeted Financial Sanctions (TFS) related to TF & PF.
- Required compliances of AML/CFT laws, BFIU circulars & directives.

Any subsequent changes in the customer’s information, required documents should be obtained.

One or more of the following steps is recommended to verify the customer’s identity & addresses. The information obtained should demonstrate that a person of that name exists at the address given and that the applicant is that person.

- i. Check and verify the data of National ID with Election Commission database;
- ii. Recent Utility Bill (not beyond 03 months old);
- iii. Physical verification of Present/Permanent/Official Address by the bank official, if required;
- iv. Third party verification report, if required.

**Operations Division** will send the Welcome Letter to each account holder after immediate following working date of opening the account. Operations Division will collect the Acknowledge receipt/proof of delivery (POD) from the courier service and attached with the Account Opening Form and maintain proper record (physical/electronic) of the same.

#### **b. Verification of Source of Fund/Income Proof**

The following documents should be considered for verification of source of funds/Income proof of the customers:

- Salary Certificate/appointment letter (For salaried person)
- Employee's ID (For ascertaining level of employment)
- Documents in support of beneficial owner's income
- Trade License if the customer declared to be a business person
- E-TIN ( if any)
- Documents of property sale (if any)
- Document of FDR encashment (if any)
- Document of foreign remittance (if any fund comes from outside the country)



- Document of retirement benefit (if any)
- Other Bank statement (if any)

For the income proof document/source of fund of a customer follow the instruction of 65<sup>th</sup> SMT meeting minutes which are given below:

**For Business Person:** Trade License/**E-TIN**/any business document that indicates his/her ownership.

**For Service Holder:** Letter of Introduction/Appointment letter/Pay Slip/Employee ID Card or any other document that proves his/her being in service.

**NRB Account holder or NRB Beneficial Owner:** Letter of Introduction/Pay slip from employer/Work permit/Employee ID card/ Passport with Visa page (for visa category) / Remittance slip / advice or any other document that proves his/her service in abroad.

**For Land Lord:** Rent receipt/Utility Bill/ Rent Agreement/ Any Land related documents i.e. Kajna Receipt, City Jorip, Mutation, Deed, etc.

**For Low Profile Customer (i.e. Farmers, Day labor, self-employed, etc.):** Detail information about source of income of the customer should have to be written in the “Source of Fund” field of UAOF and the reflection of which should be in the Comments/Remarks field of KYC Profile Form by the BAMLCO. If no formal document related to income is available, BM’s positive endorsement will be accepted.

**For House Wife/Spouse:** Any document which indicates the income proves of her/his Spouse/parents or other family members, if required.

**For Student:** Any document which indicates the income proves of his/her parents or other family members, if required.

**For others:** that proves his/her income.

#### **3.2.1.2.2 Minor Account**

Branch/Agent Banking Division/Concern Division/Department may open account or establish relationship with any minor ensuring the followings:

- The account is opened and operated by the natural or legal guardian of the minor on him/her behalf;
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a)** and (b).

- Collect the complete information & the required identification documents of the Beneficial Owner(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a) and (b)**, if any.

#### **3.2.1.2.3 Illiterate Person**

Branch/Agent Banking Division/Concern Division/Department may open account or establish relationship with any illiterate person ensuring the followings:

- The illiterate person is capable of making contract as per contract Act;
- The illiterate person is Bangladeshi national & the account is opened and operated by him/her following standard norms & practices of the Bank;
- Thumb impression & photograph attestation are done as per standard banking practice;
- Physical presence of the illiterate person is required for withdrawal of money;
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a) and (b)**.
- Collect the complete information & the required identification documents of the Beneficial Owner(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a) and (b)**, if any.

#### **3.2.1.2.4 Pardansheen Women**

Branch/Agent Banking Division/Concern Division/Department may open account or establish banking relationship with any Pardansheen Women ensuring the followings:

- Physical presence of the Pardansheen Women is required at the time of opening of account;
- Account is opened or relationship is established by the Pardansheen Women at her freewill and full understanding of the terms and conditions of the bank;
- Her photograph is to be attested by responsible female officer who will confirm her genuineness of photo identification;
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a) and (b)**.
- Collect the complete information & the required identification documents of the Beneficial Owner(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a) and (b)**, if any.

**3.2.1.2.5 Blind Man/Woman**

Branch/Agent Banking Division/Concern Division/Department may open account or establish relationship with any Blind Man/Woman ensuring the followings:

- Physical presence of the Blind Man/Woman is required at the time of opening of account;
- KYC, CDD and other AML & CFT requirements are also applicable to the assistant of the blind man/woman;
- Physical presence of the both blind man/woman and his/her assistant are required at the time of withdrawal of money;
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a)** and (b).
- Collect the complete information & the required identification documents of the Beneficial Owner(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a)** and (b), if any.

**3.2.1.2.6 NRB (Non-Resident Bangladeshi) and Foreign National**

Branch/Agent Banking Division/Concern Division/Department may open account or establish relationship with any Non Residential Bangladeshi or Foreign National ensuring the followings:

- The account is opened & operated in accordance with the sections of Foreign Exchange Regulation Act, 1947, GEFT Vol. 1 and circulars & guidelines issued by Bangladesh Bank under it;
- Required compliances of AML/CFT laws, BFIU circulars & directives, and proper KYC, TP & other documentations, risk grading and performing appropriate CDD measures;
- Identify and verify the customer, authorized customer and beneficial owner (if any).
- Names of the customer, beneficiary owner(s) and authorized person(s), if any, are not listed in Targeted Financial Sanctions (TFS) related to TF & PF.
- Collect identification documents such as:
  - National ID Card, if any;
  - Valid Passport with VISA;
  - Work permit/employer's certificate.
- One or more of the following steps is recommended to verify the customer's identity & addresses. The information obtained should demonstrate that a person of that name exists at the address given and that the applicant is that person.
  - check the national ID with Election Commission database;
  - Enquiring Bangladesh embassy in the country of resident;

- visiting home/office in Bangladesh, if any;
- Sending Welcome Letter to account holder;
- Any other genuine or authenticated sources.

### **3.2.1.2.7 Corporate/Institutional Accounts**

#### **a) Sole Proprietorship Concern**

- Collect documents such as-
  - Updated Trade License issued by City Corporation, Pourasobha, Union Parishad, etc;
  - E-TIN, if any;
  - VAT Registration, if any;
  - Membership certificate of any organization, if any;
- Collect complete information and required documents of each partners as per the clause no. **3.2.1.2.1 (a) and (b)**.
- Collect the complete information & the required identification documents of the Beneficial Owner(s), and verify the same as recommended in the clause no. **3.2.1.2.1 (a) and (b)**, if any.

#### **b) Partnership Concern**

- Collect documents such as:
  - Up-to-date trade license issued by City Corporation, Pourasobha, Union Parishad etc;
  - Partnership deed (Notarized);
  - Registered partnership deed, if registered;
  - Resolution of the Partners, specifying the operational guidelines/instructions of the partnership account;
  - E-TIN Certificate, if any;
  - VAT Registration Certificate, if any;
  - Membership certificate of any organization, if any;
  - Import Registration Certificate (In case of Import Business)
  - Export Registration Certificate (In case of Export Business)
- Collect complete information and required documents of each partners as per the clause no. **3.2.1.2.1 (a) and (b)**.
- Collect complete information and required documents of Power of Attorney Holder, if any /beneficial owner, if any as per the clause no. **3.2.1.2.1 (a) and (b)**.

**c) Private Limited Companies**

- Collect documents such as:
  - Updated trade license issued by City Corporation, Pournasobha, Union Parishad etc;
  - RJSC Certified copy of Memorandum of Association;
  - RJSC Certified copy of Articles of Association;
  - RJSC Certified copy of Certificate of Incorporation;
  - Resolution of the Board of Directors to open an account and clear operating instructions of the account;
  - Schedule X
  - Form XII certified by RJSC;
  - E-TIN Certificate of Institution and Directors;
  - VAT Registration Certificate, if any;
  - Membership certificate of any organization, if any;
  - Import Registration Certificate (In case of Import Business)
  - Export Registration Certificate (In case of Export Business)
- Collect complete information and required documents of at least 5(five) Directors as per the clause no. **3.2.1.2.1 (a)** and **(b)**.
- Collect complete information and required documents of Power of Attorney Holder, if any /beneficial owner, if any as per the clause no. **3.2.1.2.1 (a)** and **(b)**.

**d) Public Limited Companies**

- Collect documents such as:
  - Updated trade license issued by City Corporation, Pournasobha, Union Parishad etc.;
  - RJSC Certified copy of Memorandum of Association;
  - RJSC Certified copy of Articles of Association;
  - RJSC Certified copy of Certificate of Incorporation;
  - RJSC Certificate of Commencement of Business;
  - Resolution of the Board of Directors to open an account and operating instructions of the account;
  - Form XII certified by RJSC;
  - E-TIN Certificate of Institution and Directors;
  - VAT Registration Certificate, if any;
  - Membership certificate of any organization, if any;
  - Import Registration Certificate (In case of Import Business)
  - Export Registration Certificate (In case of Export Business)

- Collect complete information and required documents of at least 5(five) Directors as per the clause no. **3.2.1.2.1 (a)** and (b).
- Collect complete information and required documents of Power of Attorney Holder, if any /beneficial owner, if any as per the clause no. **3.2.1.2.1 (a)** and (b).

**e) Accounts of Samabay Samity/Limited Society/ Clubs/Societies/Charities/ private school/college/Religious Institutions**

- Collect documents such as:
  - **Samabay Samity/Limited Socceity**
    - Copy of constitution / by-laws duly attested by the cooperative members;
    - Information of the office bearers;
    - Resolution for opening account with the bank with mentioning account operating instruction;
    - Certificate of registration;
    - CIF (Customer Identification Form) for the signatories of the Account.
  - **Clubs/Societies/Charities**
    - List of Board of Members/Directors;
    - Copy of constitution / by-laws;
    - Board Resolution opening account with the bank with mentioning account operating instruction;
    - Copy of the Certificate of Registration (if permitted by the Government);
    - CIF of Chairman, Secretary, Accountant and other signatories.
  - **Trust**
    - Certified copy of trust deed;
    - Bio data of members of the Trustee Board;
    - Board Resolution opening account with the bank with mentioning account operating instruction;
    - CIF of all signatories.
  - **Private School/ College/Madrasha/other Religious Institutions**
    - Bio data of the Governing Body or Executive Committee;
    - Board Resolution opening account with the bank with mentioning account operating instruction;
    - CIF of all signatories.
- Collect complete information and verify the same as per the clause no. **3.2.1.2.1 (a)** and (b).

- Collect complete information and required documents of beneficial owner, if any as per the clause no. **3.2.1.2.1** (a) and (b).

**f) Government/Semi Government/Autonomous and Project under their controlled Account**

- Collect documents such as:
  - Permission letter from competent authority for opening and operating of account;
  - CIF of the signatories.

**g) NGO Account**

- Collect documents such as:
  - Original Resolution for opening the Account and Authorization for its operation.
  - Certified true copy of the Constitution /By-laws / Trust Deed / Memorandum & Articles of Association.
  - Certificate of Registration from The Ministry of Social Welfare if it is registered under Voluntary Welfare Agencies Ordinance 1961 / RJSC if it is established under Societies Act 1860.
  - Certificate of Registration from N.G.O Bureau (in case of NGOs funded by overseas donor Agencies).
  - Certificate from Micro Finance Regulatory Authority in applicable cases.
  - List of members of the Governing Body or Executive Committee with their address.
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. **3.2.1.2.1** (a) and (b).
- Collect the complete information & the required identification documents of the Beneficial Owner(s), and verify the same as recommended in the clause no. **3.2.1.2.1** (a) and (b), if any.

**3.2.1.2.8 Designated Non-Financial Businesses and Professions (DNFBPs)**

Branch/Agent Banking Division/Concern Division/Department may open account or establish relationship with Designated Non-financial Businesses and Professions (DNFBPs) such as real estate agents, dealers in precious metals and dealers in precious stones, lawyers, notaries, accountants, Trust and company service providers, etc. who prepare for or carry out transactions for their clients ensuring the followings:



- a. Designated Non-financial Businesses and Professions (DNFBPs) are capable of making contract as per contract Act;
- b. Required compliances of AML/CFT laws, BFIU circulars & directives, and instructions of CCC & this guidelines are done including completion of KYC, TP & other documentations and performing appropriate EDD measures categorizing the account as high risk in addition to applying normal CDD;
- c. AML/CFT measures are also applied to customers of DNFBPs, beneficiary owner(s) and authorized person(s), if any; and
- d. Names of the DNFBPs, their customers, beneficiary owner(s) and authorized person(s), if any, are not listed in Targeted Financial Sanctions (TFS) related to TF & PF.

#### **3.2.1.2.9 Walk-In-Customers**

Branch/Agent Banking Division/Concern Division/Department may provide certain banking services such as issuing DD/PO or serving for TT/MT, cash deposits, cash withdrawal, payment of inward foreign remittances, etc. to a walk-in customer, i.e., a customer without having bank account ensuring the followings:

- Complete and correct information of the Walk-in customer are collected while serving him/her;
- Sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT as ascertained before delivering services;
- Complete and correct information of any person other than customer who deposits or withdraws funds using on-line facilities are duly collected;
- Additionally, in regards to on-line deposit, it is also required to identify the sources of funds as well.

#### **3.2.1.2.10 Non Face to Face Customers**

'Non face to face customer' refers to "the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the bank branch". Branch/ Agent Banking Division/Concern Division/Department may open account or establish relationship with non face to face customers ensuring the followings:

- a) Ensuring that the customer's identity is established by additional ID documents, information provided by the Government Department or agency should be verified.
- b) Certified true copy of Passport/NID must be collected, where there is a non-face to face contract.
- c) Branch/Agent Banking Division/Concern Division/Department is required to physically verify the residential & business addresses of such customers.

### **3.2.1.2.11 Politically Exposed Persons (PEPs)**

PEPs (as well as their family members and persons known to be close associates) are required to be subject to undertake enhanced due diligence by a reporting organization in general. This is because international standards issued by the FATF recognize that PEP may be in a position to abuse their public office, political power for private gains and PEP may use the financial system to launder the illicit gains. As FATF says, these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatizing PEPs as such being involved in criminal activity. The FATF has categorized PEPs into 3 (three) criteria which include:

- a) Foreign PEPs;
- b) Domestic PEPs (known as Influential Persons: IPs in Bangladesh) and
- c) Chief or similar high-ranking positions in an international organization

It is important to note that only foreign PEPs automatically should be treated as high risk and therefore a reporting organization should conduct Enhanced Due Diligence (EDD) in this scenario. However, EDD should be undertaken in case of domestic PEPs (Influential Persons: IPs) and PEPs of the international organization when such customer relationship is identified as higher risk.

A politically exposed person (PEP) is defined by the FATF as an individual who is or has been entrusted with a prominent public functions which include individuals in foreign country and domestic level. So, **PEPs** as per the FATF Standards and **IPs** as per Bangladeshi regulations, are the following individuals but not limited to-

- ◆ Heads of state or government, ministers and deputy or state ministers;
- ◆ Members of parliament or of similar legislative bodies;
- ◆ Members of the governing bodies of political parties (generally only apply to the national governing bodies where a member has significant executive power, eg. over the selection of candidates or distribution of significant party funds);
- ◆ Senior politicians
- ◆ Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
- ◆ Members of courts of auditors or of the boards of central banks;
- ◆ Ambassadors, Charges d'affairs and high-ranking officers in the armed forces;
- ◆ Head or the senior executives or members of the administrative, management or supervisory bodies or State-owned enterprises;
- ◆ Chief, directors, deputy directors and members of the board or equivalent function of an international organizations

Family members of a PEP shall include:

- ◆ spouse, or civil partner
- ◆ children and their spouses or civil partner
- ◆ parents

However, this is not an exhaustive list. Reporting organizations should take a proportionate and risk-based approach to the treatment of family members who do not fall into this definition. A corrupt PEP may use members of his/her wider family to launder the proceeds of corruption on his/her behalf. It may be appropriate to include a wider circle of family members (such as aunts and uncles) in cases where a reporting organization assessed a PEP to pose a higher risk. This would not apply in relation to lower risk PEPs. In low-risk situations, a reporting organization should not apply any EDD measures to someone who is not within the definition above and should apply normal customer due diligence measures. A family member of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

Close associates' of a PEP-

A "known close associate" of a PEP is defined as:

- ◆ an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a PEP
- ◆ an individual who has sole beneficial ownership of a legal entity or a legal arrangement that is known to have been set up for the benefit of a PEP

A 'known close associate' of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

#### **a) Foreign PEPs:**

Branch/Agent Banking Division/Concern Division/Department is required to determine whether the customer is a politically exposed person (PEP). Once PEP is identified, account may be opened or relationship may be established for/with him/her ensuring the followings additional activities:

- The account is opened & operated in accordance with the sections of Foreign Exchange Regulation Act, 1947 and circulars & guidelines issued by Bangladesh Bank under it;
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. 3.2.1.2.1 (a) and (b).
- CAMLCO approval is required to open such account, in absence of CAMLCO, DCAMLCO can approve such account;

- Confirm sanction screening of the customer and beneficial owner (if any) and not listed in Targeted Financial Sanctions (TFS) related to TF & PF.

**b) Influential Persons (IPs)**

Branch/Agent Banking Division/Concern Division/Department is required to determine whether the customer is an IP. Once IP is identified, account may be opened or relationship may be established for/with him/her ensuring the followings additional activities:

- CAMLCO approval is required to open such account, in absence of CAMLCO, DCAMLCO can approve such account;
- Confirm sanction screening of the customer and beneficial owner (if any) and not listed in Targeted Financial Sanctions (TFS) related to TF & PF.
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. 3.2.1.2.1 (a) and (b).

**c) Chief or similar high-ranking positions in an international organization**

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Branch/Agent Banking Division/Concern Division/Department is required to determine whether the customer is a Chief or similar high-ranking positions in an international organization. Once identified, account may be opened or relationship may be established for/with him/her ensuring the followings additional activities:

- The account is opened & operated in accordance with the sections of Foreign Exchange Regulation Act, 1947 and circulars & guidelines issued by Bangladesh Bank under it;
- CAMLCO approval is required to open such account, in absence of CAMLCO, DCAMLCO can approve such account;
- Confirm sanction screening of the customer and beneficial owner (if any) and not listed in Targeted Financial Sanctions (TFS) related to TF & PF.
- Collect the complete information & the required identification documents of the customer(s), and verify the same as recommended in the clause no. 3.2.1.2.1 (a) and (b).

**3.2.1.2.11.1 Close associates, family members of PEPs**

Branch/Agent Banking Division/Concern Division/Department need to identify whether any of their customer is a family member or close associates of PEP. Once identified branch need to follow the instruction of the clause no. 3.2.1.2.10 (a).

**3.2.1.2.11.2 Close associates, family members of IPs**

Branch/Agent Banking Division/Concern Division/Department need to identify whether any of their customer is a family member or close associates of IP. Once identified branch need to follow the instruction of the clause no. 3.2.1.2.10 (b).

**3.2.1.2.11.3 Close associates, family members of Chief or similar high-ranking positions in an international organization**

Branch/Agent Banking Division/Concern Division/Department need to identify whether any of their customer is a family member or close associates of Chief or similar high-ranking positions in an international organization. Once identified branch need to follow the instruction of the clause no. 3.2.1.2.10 (c).

**3.2.1.2.11.4 Various scenario related with PEPs**

A PEP must be treated as a PEP after he or she leaves office for at least 12 months, depending on the risk. This does not apply to family members, who should be treated as ordinary customers, subject to normal customer due diligence obligations from the point that the PEP leaves office. A family member of a former PEP should not be subject to enhanced due diligence measures unless this is justified by the reporting organization's assessment of other risks posed by that customer.

If a person who is a PEP is no longer entrusted with a prominent public function, that person should continue to be subject to risk-based enhanced due diligence for a period of at least 12 months after the date they ceased to be entrusted with that public function. Reporting organizations may apply measures for a longer period to address risks of money laundering or terrorist financing in relation to that person, but the BFIU consider this will only be necessary in the cases of PEPs where a reporting organization has assessed that PEP is posing a higher risk.

**3.2.1.2.11.5 PEPs versus Risk****Do all PEPs pose the same risk?**

No – the risk of corruption will differ between PEPs. Reporting organization has to take appropriate approach that considers the risks an individual PEP poses based on an assessment of:

- ◆ the prominent public functions the PEP holds;

- ◆ the nature of the proposed business relationship;
- ◆ the potential for the product to be misused for the purposes of corruption;
- ◆ any other relevant factors the reporting organization has considered in its risk assessment.

This guidance discusses on how reporting organization may differentiate between PEPs. In this guidance, the terms “lower risk” and “higher risk” are used to recognize that reporting organizations are required to apply Enhanced Due Diligence on a risk-sensitive basis. An overall risk assessment will consider all risk factors that a customer may present and come to a holistic view of what measures should be taken to comply. Not only risk factor means a customer should automatically be treated as posing a higher risk; it is necessary to consider all features of the customer.

#### **3.2.1.2.11.6 Indicators that a PEP might pose a lower risk**

The following indicators suggest a PEP poses a lower risk:

- ◆ If he/she is seeking access to a product the reporting organization has assessed to pose a lower risk.
- ◆ If he/she is from an area where ML/TF risks is lower
- ◆ If he/she does not have executive decision making responsibilities (e.g. an opposition Member of the Parliament)

#### **3.2.1.2.11.7 Indicators that a PEP might pose a higher risk**

The following indicators suggest a PEP poses a higher risk:

##### **a) Higher risk indicator – product**

The reporting organization’s risk assessment finds the product or relationship a PEP is seeking for may be misused to launder the proceeds of large-scale corruption.

##### **b) Higher risk indicators – geographical**

A PEP may pose a greater risk if he/she is entrusted with a prominent public function in a country that is considered as a higher risk for corruption. To draw this conclusion, a reporting organization should have regard to whether, based on information available, the country has the following characteristics:

- ◆ associated with high levels of corruption
- ◆ political instability
- ◆ weak state institutions
- ◆ weak anti-money laundering defense

- ◆ armed conflict
- ◆ non-democratic forms of government
- ◆ widespread organized criminality
- ◆ a political economy dominated by a small number of people/entities with close links to the state
- ◆ lacking a free press and where legal or other measures constrain journalistic investigation
- ◆ a criminal justice system vulnerable to political interference
- ◆ lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector
- ◆ law and culture antagonistic to the interests of whistleblowers
- ◆ weaknesses in the transparency of registries of ownership for companies, land and equities
- ◆ human rights abuses

**c) Higher risk indicators – personal and professional**

The following characteristics might suggest a PEP poses higher risk:

- ◆ personal wealth or lifestyle is inconsistent with known legitimate sources of income or wealth; if a country has laws that do not generally permit the holding of a foreign bank account, a bank should satisfy itself that the customer has authority to do so before opening an account
- ◆ credible allegations of financial misconduct (e.g. facilitated, made, or accepted bribes)
- ◆ responsibility for, or able to influence, large public procurement exercises, particularly where procurement is not subject to competitive tender, or otherwise lacks transparency;
- ◆ responsible for, or able to influence, allocation of scarce government licenses such as mineral extraction concessions or permission for significant construction projects.

**3.2.1.2.11.8 Indicators that a PEP's family or known close associates pose a lower risk**

A family member or close associates of a politically exposed person may pose a lower risk if the PEP himself/herself poses a lower risk.



### **3.2.1.2.11.9 Indicators that a PEP's family or known close associates pose a higher risk**

The following characteristics might suggest a family member or close associates of a politically exposed person poses a higher risk:

- ◆ wealth derived from the granting of government licenses (such as mineral extraction concessions, license to act as a monopoly provider of services, or permission for significant construction projects)
- ◆ wealth derived from preferential access to the privatization of former state assets
- ◆ wealth derived from commerce in industry sectors associated with high-barriers to entry or a lack of competition, particularly where these barriers stem from law, regulation or other government policy
- ◆ wealth or lifestyle inconsistent with known legitimate sources of income or wealth credible allegations of financial misconduct (e.g. facilitated, made, or accepted bribes)
- ◆ appointment to a public office that appears inconsistent with personal merit

For further details follow the “**Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations**” issued by BFIU which has already been circulated to all employees vide our Instruction Circular No. 02/2019 dated March 06, 2019.

### **3.2.2 Customer Unique Identification Code**

Branch/Agent Banking Division/Concern Division/Department should use unique identification code for any customer maintaining more than one account or availing more than one facilities from our bank. Such unique identification system could facilitate banks to avoid redundancy, and saves time and resources. This mechanism also enables banks to monitor customer transactions effectively. Before opening any CIF/Customer Id in CBS/CMS/ABS the maker should perform the following due diligence:

- a) Proper verification/Authentication of Identity Proof (NID/Passport/Birth Registration Certificate);
- b) Sanction Screening
- c) Dedupe Checking

### **3.2.3 Exception When Opening a Bank Account**

Branch/Agent Banking Division/Concern Division/Department may verify the documents of account holder after opening the account, provided that there are adequate safeguards in place to ensure that, before verification has been completed:

- the account is not closed; and
- transaction is not carried out by or on behalf of the account

### 3.2.4 Policy for rejection of customer

According to Clause No. 2 & 3.7 of BFIU Circular 26 dated June 16, 2020,-

- No account shall be opened in anonymous, numbered or fictitious name.
- NRB Bank will not establish any kind of correspondence relationship with shell Bank.
- No account should be opened or operated in the name of any person or entity listed under UNSCRs or their close alliance on suspicion of involvement in terrorist and terrorist financing activities and prescribed or enlisted by Bangladesh Government.
- Not to open or not start the business relationship or not to allow the transaction or close an account where the bank is unable to apply appropriate Customer Due Diligence (CDD) measures i.e. if the bank is unable to verify the identity and/or obtain documents required as per with the risk categorization due to non-cooperation of the customer. Before closing of account, approval has to be taken from Senior Management by the branch and branch will send a prior notice to the customer before closing of account (as per Tail Management Process of NRB Bank). Branch will also send a report to AML & CFT Department regarding opening or closing account of the same customer. If required, AML & CFT Department will convey this information to other branches. Branch may report of this account as STR/SAR if needed.
- No account shall be opened or operated by violation of AML/CFT laws and rules.

### 3.2.5 Know Your Customer (KYC) and CDD Procedures

#### 3.2.5.1 Standard KYC information & CDD Measures

KYC procedures refer to knowing a customer physically and financially. This means to conduct an effective KYC, it is essential to accumulate **complete** and **accurate** information about the prospective customer. **Complete** refers to combination of all information for verifying the identity of the person or entity. For example Name, Profession, Date of Birth, Details Addresses, NID/Passport/Birth Registration Certificate with acceptable photo ID, Phone/Mobile Number, etc. and other necessary information. **Accurate** refers to such complete information that has been verified for accuracy from reliable and independent sources.

Legal Obligations of CDD under MLPA, 2012 (amendment 2015), “The reporting organizations shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to BFIU”.

As per the FATF Recommendation no. 10, financial institutions requires to conduct KYC, Customer Due Diligence (CDD) either simplified or enhanced based on the customer risk profile as well as on-going CDD measures. It also requires that CDD should be undertaken by the financial institutions while establishing business relationship with customer.

The CDD measures to be taken by the Branch/Agent Banking Division/concern division/department as per the FATF standards are as follows:

- a. Identify the customer and verify that customer's identity using reliable, independent source documents, data or information, i.e., complete & accurate information of the customer;
- b. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, as such that the Branches/Agent Banking Division/Concern Divisions/Departments is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include Branches/Agent Banking Division/Concern Divisions/Departments understanding the ownership and control structure of the customer.
- c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

On the basis of risk associated with the customer, Bank have to conduct the following CDD measures -

- Branch/Agent Banking Division/concern division/department is required to collect complete & accurate information of ensuring KYC of the customer before or during establishing business relationship;
- carrying out any occasional transaction through wire transfer;
- In case of occasional transaction of BDT5,00,000.00 and above by the walk-in customer.

### **3.2.5.2 Ongoing CDD measures (Review and update)**

Branch/Agent Banking Division/concern division/department shall take necessary measures to **review** and **update** the KYC of the customer as per clause no. 3.5 (4) of BFIU Circular No. 26 dated June 16, 2020. This procedure shall have to be conducted in every 05 (five) years in case of low risk customers. Furthermore, this procedure shall have to be conducted in every year in case of high risk customers. Moreover, Branch/Agent Banking Division/concern division/department shall update KYC information anytime if there is any particular necessity realized. Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay.

Branch/Agent Banking Division will prepare the Transaction Profile (TP) of customer account considering the risk management regarding AML & CFT issues by own. In this case Branch/Agent Banking Division will monitor previous 6/12 months transaction of the customer and review of the transaction. Any significant changes of transaction compare to prescribed TP, Branch/Agent Banking Division will monitor the transaction. If applicable, Branch/Agent Banking Division will update TP or raise a STR in applicable cases.

### **3.2.5.3 Risk Grading and Applicable CDD**

Branch/Agent Banking Division/concern division/department shall review the KYC & other information they have collected (clause no. 3.2.5.1) for each new customer, assess & evaluate the risk of the customer and categorize them into two groups: High Risk Customers & Low Risk Customers.

The nature and extent of due diligence will depend on the risk perceived by the Branch/Agent Banking Division/Concern Division/Department. However, while preparing customer's risk category Branch/Agent Banking Division/Concern Division/Department should take care to seek only such information from the customer, which is relevant to the risk category.

For the purpose of risk categorization, Branch/Agent Banking Division/Concern Division/Department shall follow the instructions of BFIU Circular No. 26 which is given below:

Customer risk profiles (KYC Profile Form of UAOF) will assist the branch in determining whether the customer or customer category is lower risk or higher risk. As per BFIU Circular No. 26, risk grading of a customer is given below:

<b>Total Risk Score</b>	<b>Risk Rating</b>
<b>&gt;=15</b>	<b>High</b>
<b>&lt;15</b>	<b>Low</b>

For the risk grading of a customer, Branch need to follow the instruction of Annexure Ka (enclosure 2) of BFIU Circular No. 26.

For risk identification, Branch/Agent Banking Division/Concern Division/Department will also follow the instruction in the clause no. 3.2.1.1 (c & d) of ML & TF Risk Assessment Guidelines of NRB Bank.

If the customer or customer category is higher-risk, requires the application of enhanced CDD measures and controls. Branch/Agent Banking Division/Concern Division/

Department shall also apply enhanced due diligence in case of transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes.

Branch/Agent Banking Division/Concern Division/Department shall apply normal due diligence measures in case of individuals or legal entities scored with low risk. In this case, Branch/Agent Banking Division/Concern Division/Department will also follow instruction of the BFIU Circular No. 25 dated January 08, 2020 regarding “**Guidelines of eKYC**”.

Branch/Agent Banking Division/Concern Division/Department shall follow the instruction of clause no. 3.6 of BFIU Circular No. 26.

#### **3.2.5.4 Enhanced CDD measures**

Branch/Agent Banking Division/Concern Division/Department is required to apply enhanced due diligence measures where required in any high risk scenario in addition to performing normal CDD measures as indicated in the clause no. 3.2.5.1 of this guidelines. EDD goes beyond CDD and looks to establish a higher level of identity assurance by obtaining the customer’s identity and address, and evaluating the risk category of the customer. Enhanced due diligence is specifically designed for dealing with high-risk customer.

Enhanced CDD measures includes:

- Obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet, etc.) and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- Making aware the concerned officials about the risk level of the customer.
- May visit to customer’s place and have a visit report.

#### **3.2.5.5 Simplified CDD measures**

Where the risks of money laundering or terrorist financing are lower, the banks are allowed to conduct simplified CDD measures, which should take into account the nature of

the lower risk. The simplified measures should be commensurate with the lower risk factors.

- ❖ In case of transaction less than BDT50,000.00 for walk-in customer, must collect name, address and telephone number of applicant/sender/depositor and recipient/beneficial owner.
- ❖ In case of transaction above BDT50,000.00 but less than BDT5,00,000.00 for walk-in customer, must collect the photo id of the Depositor/Sender/applicant or withdrawal person.
- ❖ Keep simplified CDD for the lower risk customer for opening and operating account under financial inclusion (School student account, farmer account and other No-frill account).

#### **3.2.5.6 Timing of CDD**

Branch/Agent Banking Division/Concern Division/Department must apply CDD measures when it does any of the following:

- a) establishing a business relationship;
- b) carrying out an occasional transaction;
- c) suspecting money laundering or terrorist financing; or
- d) suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification.

#### **3.2.5.7 In case where conducting the CDD measure is not possible**

If conducting the CDD measure becomes impossible because of the non-cooperating behavior of the customer or if the collected information seemed to be unreliable, that is, Branch/Agent Banking Division/Concern Division/Department could not collect satisfactory information on customer identification and could not verify that, Branch/Agent Banking Division/Concern Division/Department should take the following measures:

- must not carry out a transaction with or for the customer through a bank account;
- must not establish a business relationship or carry out an occasional transaction with the customer;
- must terminate any existing business relationship with the customer;
- must consider whether it ought to be making a report to the BFIU through an STR/SAR.



Branch/Agent Banking Division/Concern Division/Department should always consider whether an inability to apply CDD measures is caused by the customer. In this case, the branch or concern Head Office Division should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the branch or concern Head Office Division should consider whether there are any circumstances which give grounds for making a report to CCC/AML & CFT Department for onward submission to BFIU.

If the Branch/Agent Banking Division/Concern Division/Department concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be sent to CCC/AML & CFT Department for onward submission to BFIU. The branch or concern Head Office Division must then retain the funds until consent has been given to return the funds to the source from which they came.

If the Branch/Agent Banking Division/Concern Division/Department concludes that there are no grounds for making a report, it will need to make a decision on the appropriate course of action. This may be retaining the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or returning the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

### **3.2.5.8 Persons without Standard Identification Documentation**

Most of the people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, street children or people, students and minors shall not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approaches and some flexibility considering risk profile of the prospective customers without compromising sufficiently rigorous anti money laundering procedures is recommended. Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances.

Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address. A Head of Branch may authorize the opening of a



business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

For students or other young people, the normal identification procedures set out as above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant's educational institution.

Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

### **3.2.6 Corresponding Banking**

'Cross Border Correspondent banking' shall refer to providing banking services to another bank (respondent) by a bank (correspondent). These kinds of banking services shall refer to credit, deposit, collection, clearing, payment, cash management, international wire transfer, drawing arrangement for demand draft or other similar services. For establishing and maintaining RMAs, the concerned Head Office Division/ Department will follow the approved standard Process Flow as approved by the competent authority.

Before providing correspondent banking service, the concerned Head Office Division/Department must be satisfied with the nature of business of the correspondent or the respondent bank through collection of information as per our questionnaire (which has already been sent to particular divisions/departments) or similar documents with respect to annexure "KHA" as indicated in the BFIU circular no-26 dated June 16, 2020. Divisions/Department shall also collect additional information from open source.

The concerned Head Office Division/Department shall also obtain endorsement from Chief Anti Money Laundering Compliance Officer (CAMLCO) before establishing any correspondent relationship. In absence of CAMLCO, DCAMLCO can provide the endorsement.

The concerned Head Office Division/Department must be sure about the effective supervision of that foreign correspondent or respondent bank by the relevant regulatory authority before establishing and continuing any relationship.

The concerned Head Office Divisions/Departments shall not establish or maintain any correspondent relationship with any shell bank. Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

The concerned Head Office Division/Department shall not establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank.

The concerned Head Office Division/Department shall not establish or maintain any correspondent relationship with any institution which is listed an entity in TFS of UNSCR or OFAC and/or located in a sanctioned country and/or its' owner(s)/director(s), beneficiary owner(s), senior management are not listed in TFS of UNSCR or OFAC.

The concerned Head Office Division/Department shall pay particular attention or conduct Enhanced Due Diligence while establishing or maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standards for the prevention of money laundering and terrorist financing (such as the countries and territories enlisted in High-Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force's Public Statement). Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained.

If any respondent bank allow direct transactions by their customers to transact business on their behalf (i.e. payable through account), the corresponding bank, i.e., the concerned Head Office Division/Department must be sure about the followings:

- 1) The respondent bank has conducted appropriate CDD of the customer; and
- 2) Upon request of the correspondent bank, the respondent bank shall be able to provide all CDD information of the respective customer it has to be ensured that collecting the information on CDD of the respective customer.

Here, 'Payable through accounts' refers to "Corresponding accounts that are used directly by third parties to transact business on their behalf."

The concerned Head Office Division/Department may require to obtain the information regarding the ownership structure, management and sovereign support of the respective correspondent or respondent banks.

Periodic review shall be done by the Financial Institutions Division (FI) of all the correspondent relationship and keeping record of the same as per their approved standard Process Flow.

Concerned Head Office Divisions/Departments must monitor the transactions of such accounts and generate STR report whenever there is any unusual or suspicious transactions.

### **3.2.7 New Technologies**

The KYC procedure should invariably be applied to new technologies including Debit Card/ Credit Card/Internet Banking/ Mobile Banking facility or such other product which may be introduced by the Bank in future that might favor anonymity, and take measures, if needed to prevent their use in money laundering schemes. These measures should be taken before introducing/ launching such newly innovated/modified services.

Branch/Agent Banking Division/Concern Division/Department is required to identify and assess the money laundering or terrorist financing risks that may arise in relation to:

- a) The development of new products and new business practices, including new delivery mechanisms;
- b) The existing products or services and delivery mechanisms;
- c) The use of new or developing technologies for both new and pre-existing products;
- d) Such a risk assessment is to be taken place prior to the launch of the new products, business practices or the use of new or developing technologies; and
- e) It is required to take appropriate measures to manage and mitigate those risks.

### **3.2.8 Wire Transfers**

As per clause no. 9 of BIFU Circular No. 26 dated January 16, 2020, “Wire transfer” refers to such financial transactions that are carried out on behalf of an originator (person or institution) through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution.

Branch/Agent Banking Division/Concern Division/Department may execute any wire transfer ensuring the followings:

- a. Required and accurate originator information, and required beneficiary information, on wire transfers and related messages is maintained , and that the information remains with the wire transfer or related message throughout the payment chain;
- b. Wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information are monitored, and appropriate measures are taken;

- c. When processing wire transfers, it is required to take appropriate action and prohibit conducting transactions with designated persons and entities as per the obligations set out in the relevant United Nations Security Council resolutions & OFAC sanctions, relating to the prevention and suppression of terrorism and terrorist financing.

### **3.2.8.1 Cross-border wire transfer**

As per clause no. 9.1 (1) of BIFU Circular No. 26 dated January 16, 2020, Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

Complete and accurate information of applicant/originator will be collected, preserved and send intermediary/beneficiary bank in case of cross border wire transfer for an amount equivalent to USD 1,000 and above under general/usual remittance or a remittance under special approval. Moreover, in case of transactions below the above mentioned ceiling, applicant's complete and meaningful information has to be preserved.

Beneficiary's complete and meaningful information will be preserved for making payment against remittance through cross-border wire transfers.

Requester's and beneficiaries accurate and complete information will be incorporated in the batch file when single requester sends amount to several beneficiaries through several inter country wire transfers using bundle in a batch file. Moreover, bank will also incorporate the applicant's account number.

#### **Collected & preserved the complete and accurate originator/applicant information such as:**

(i) name; (ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction; (iii) residential or mailing address ; (iv) Passport/NID/Birth Registration Certificate/Any acceptable ID with Photo; (v) Phone/Active Mobile Number.

#### **Collected & preserved the meaningful beneficiary information such as:**

(i) name; (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction; and (iii) Details Address.

### **3.2.8.2 Domestic wire transfers**

As per clause no. 9.1 (2) of BIFU Circular No. 26 dated January 16, 2020, Domestic wire transfers - refers to any wire transfer where the ordering financial institution and

beneficiary financial institution are located in the same country. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country.

In case of domestic wire transfer, a complete and accurate Information will be collected, preserved and sent to intermediary/ beneficiary bank; for an amount less than the above threshold, applicant's complete and accurate information should be preserved. Moreover, beneficiary's complete and meaningful information will be preserved before effecting payments against the domestic Wire transfers.

Banks, providing mobile financial services will use the KYC format provided time to time by Payment System Department. Bangladesh Bank, in addition to the above directives.

Information will be collected as mentioned in clause no. 9.1 (2) of BFIU Circular No. 26, for executing payment instruction (except purchasing goods and services) through wire transfer using debit or credit card.

In case of wire transfer favoring Government/semi-governmental autonomous organizations, compliance of above mentioned instructions is not mandatory. Furthermore, in case of inter-bank transactions (where both the applicant and beneficiary are bank or FI) the Instructions contained under clause no. 9.1 (2) of BFIU Circular No. 26 are not applicable.

Each Beneficiary Bank should have effective risk based policies and procedures for determining reasonable measures to identify wire transfers that lack required applicant information or required beneficiary information such as execution, rejection or suspension of that wire transfer and the appropriate follow-up action.

### **3.2.8.3 Duties of Ordering, Intermediary and Beneficiary Bank in Case of Wire Transfer**

#### **i) Ordering Bank**

The ordering bank should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information. These information has to be preserved minimum for 5 (five) years.

#### **ii) Intermediary Bank**

For cross border and domestic wire transfers, any bank working as an intermediary between ordering bank and beneficiary bank, should ensure that all originator and beneficiary information that accompanies a wire transfer is retained. A record should be kept, for at least five years, by the receiving intermediary financial institution of all/ the

information received from the ordering financial institution (or as necessary another intermediary financial institution).

An intermediary financial institution should have effective risk based policies and procedures for determining reasonable measures to identify wire transfers that lack required originator information or required beneficiary information such as execution, rejection, or suspension of that wire transfer and the appropriate follow-up action. Such measures should be consistent with straight through processing.

### **iii) Beneficiary Bank**

A beneficiary financial institution should initiate risk based procedure to identify wire transfers that lack required originator or required beneficiary information. In case of insufficient originator information concerned parties should collect those information through mutual communication or using any other means. During the payment to receiver/beneficiary, the bank should collect full and accurate information of receiver/beneficiary and should preserve those information for 5 (five) years.

An intermediary financial institution should have effective risk-based policies and procedures for determining reasonable measures to identify wire transfers that lack required originator information or required beneficiary information such as execution, rejection, or suspension of that wire transfer and the appropriate follow-up action. Such measures should be consistent with straight-through processing.

### **3.2.9 Agent Banking**

The Bank shall be equally liable for compliance of all AML & CFT instructions of Agent Banking. Moreover, the following Compliance should be ensure.

- Should introduced Uniform Account Opening Form of BFIU (UAOF) for agent and the customers.
- Awareness to detect & reporting of unusual transactions or activities of agent or customers.
- Agent would be well trained and AML & CFT activities should be included in the Agent Banking Compliance program.

The following steps to be taken to appoint agent and to monitor their activities.

- For selecting an Agent appropriate Screening Mechanism, complete and correct information of agent should be ensure.



- Considering the number, amount & geographical location of the agent Banks needs to categorize them as high, medium and low risk and considering this risk level Banks need to monitor their transactions.
- Ensure on going risk categorization.
- Verification of the AML/CFT compliance status of the agent.
- To verify the AML/CFT compliance status, annual audit shall have to be conducted in case of high risk agent and report should be send to the AML/CFT Department. Furthermore, this procedure shall have to be conducted in a specific interval in case of medium and low risk agent.
- Updated agent list (Jan-June based) should be uploaded in the Bank's website.
- A separate Cancelled/banned Agent list (January-June based) should be uploaded in the Bank's website.

### **3.2.10 Call Center**

Customers can call at the call center with various types of queries related to account, transactions, products & services of NRB bank, documentation procedures, complains, etc. and which are resolved over phone instantly or some of requests/ services are execute through mail or outbound call after proper verification.

Call Center shall identify and verify the customer before delivering any call center related services so that financial information of the customer cannot go to any unauthorized person or third party. Delivery of customers' financial information to unauthorized persons or third parties may be used for money laundering & terrorist financing.

Call Center shall ensure that all types of card and/or card related services are activated by them after collecting & verifying the required documents as per the Bangladesh Bank Guidelines for Foreign Exchange Transactions; circulars issued by Bangladesh Bank, BFIU & NRB bank, Foreign Exchange Regulation Act 1947 & other applicable acts, rules & regulations. Activation of cards without proper identification and verification of customers and/or documents may lead to money laundering and terrorist financing through cards.

Call Center shall ensure that all types of online/internet banking transactions and/or e-commerce transactions are activated by the call center after collecting & verifying the required documents as per the Bangladesh Bank Guidelines for Foreign Exchange Transactions; circulars issued by Bangladesh Bank, BFIU & NRB bank, Foreign Exchange Regulation Act 1947, GEFT vol. 1 & other applicable acts, rules & regulations. Execution of online/internet banking transactions and e-commerce transactions without proper identification & verification of customers and/or documents and/or transactions may facilitate money laundering & terrorist financing.



Call Center or IT Division (ADC Ops) must ensure that the transactions through/of ATMs, all types of cards, POS, SMS banking, mobile app and Internet Banking are monitored on 24 hours 7 days basis for preventing fraudulent transactions, split transactions, unauthorized transactions, cyber-attacks etc. and generate STR whether there is any unusual or suspicious transaction found.

### **3.3 Reporting**

Bank should be obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self-assessment, independent testing procedure etc.) to Bangladesh Financial Intelligence Unit (BFIU) without any delay or in due time. Besides these reporting AML & CFT Department have to produce customer information and documents as per the requirements sought by the different competent authorities like BFIU, Bangladesh Bank, DUDOK, NBR, Tax Office, etc. and maintain confidentiality of those as per instruction of the BFIU Circular letter no. 1/2018 dated April 22, 2018 and BFIU circular no 26 dated June 16, 2020.

#### **3.3.1 Cash Transaction Report (CTR)**

Every branch and Agent Banking Division (if applicable) will generate the monthly Cash Transaction Report (CTR) of Tk. 10 Lac and above for cash transaction per day (Including Online, ATM related any cash Deposit or withdrawal separately) through “Report Server”. Every branch needs to preserve its CTR in their own branch. Every branch will analyze the transaction and follow the below instructions:

- Branches need to identify whether there is any suspicious transaction found by reviewing the Cash Transactions Report. If any suspicious transaction found, branch will raise STR and send it to AML & CFT Department for onward submission to BFIU.
- If no suspicious transaction is identified then branch will send a report as “No suspicious transaction has been found” on or before 10<sup>th</sup> day of the following month to AML & CFT department as per prescribed format.
- AML & CFT Department will also generate automated CTR and check all the CTR related data (Customer information) and submit CTR of all branches through goAML Software.
- AML & CFT Department will also analyze all the transactions related with CTR of all branches, if any suspicious transaction found submit it to BFIU separately and if no suspicious transaction found then inform BFIU through goAML Message Board as “No suspicious transaction has been found” while reporting CTR on or before 21<sup>st</sup> day of the following month.

### **3.3.2 Half yearly Self-Assessment Report & Independent Testing Procedures (ITP)**

To reduce the Money Laundering and Terrorist Financing risk related to the operations in the branch level, BFIU has established Self-Assessment Reporting system (based on January to June and July to December).

#### **3.3.2.1 Responsibilities of Branch**

For preparing the half yearly Self-Assessment report, branch will follow the instruction as per the clause no. 8.1 of BFIU Circular No. 26 dated June 16, 2020 and the report to AML & CFT Department and Internal Control & Compliance Division on or before 15<sup>th</sup> day of the following month of half-yearly.

#### **3.3.2.2 Responsibilities of Internal Control & Compliance Division**

To review the Self-Assessment report and proper judgment of Independent Testing Procedure adequate manpower should be allocated in the Internal Control & Compliance Division with adequate knowledge regarding AML & CFT issues, circulars, laws, rules, etc. For reviewing and conduct audit/inspection to all branches, Internal Control & Compliance Division will follow the instruction as per the clause no. 8.2 of BFIU Circular No. 26 dated June 16, 2020.

#### **3.3.2.2 Responsibilities of AML & CFT Department/CCC**

Based on the received branch self-assessment reports and submitted inspection/audit reports by the Internal Control & Compliance Division, AML & CFT Department will prepare a checklist based evaluation report and take initiatives as per clause no. 8.3 of BFIU Circular No. 26 dated June 16, 2020 and will prepare a report as per the uniform format circulated by the BFIU (Ref: BFIU(Bank Monitoring)/16/2020-2507 dated November 24, 2020) and send to BFIU within 02(two) months of the following half year.

#### **3.3.3 Quarterly meeting minutes**

Branch will conduct meeting separately on quarterly basis as per clause no. 1.3(1)(Sha) of BFIU Circular No. 26 dated June 16, 2020 on AML & CFT issues and send the meeting minutes to AML & CFT Department immediately.

#### **3.3.4 Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR)**

The final output of an Anti Money Laundering (AML) & Combating Financing of Terrorism (CFT) compliance program is reporting of suspicious transaction or reporting of suspicious activity. STR or SAR is an excellent tool for mitigating or minimizing the AML & CFT risk for Bank. Therefore, it is necessary to find out the suspicious transaction and suspicious activity for the safety and soundness of the Bank.

Generally, STR/SAR means a formatted report of suspicious transactions/activities where there is reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seems to be usual manner. Such report is to be submitted by Bank to BFIU.

Suspicious activity can be identified both during the on-boarding or ongoing due diligence of a client as well as during the transaction monitoring process and may be raised by any employee of a reporting organization. Under Section 25(1)(d) of MLPA, 2012, ROs shall have to report any doubtful transaction or attempt of such transaction as defined under Section 2(z) of the same act as suspicious transaction report to the BFIU immediately on its own accord.

As per Section 2(z) of MLPA 2012 Suspicious Transaction means such transactions

- which deviates from usual transactions
- of which there is ground to suspect that
  - The property is the process of an offense
  - It is financing to any terrorist activity, a terrorist group or an individual terrorist
- Which is for the purpose of this Act, any other transaction or attempt of transaction delineated in the instruction issued by BFIU from time to time.

As per Section 2(16) of ATA, 2009, Suspicious Transaction means such transactions

- which deviates from usual transactions
- Which invokes presumption that
  - it is the proceeds of an offence under this Act
  - it relates to financing of terrorist activities or a terrorist person or entity
- For the purpose of this Act, any other transaction or attempt of transaction delineated in the instruction issued by BFIU from time to time.

In case of reporting STR/SAR, Branch/Division/Department should conduct the following 3 stages:

#### **a) Identification of STR/SAR**

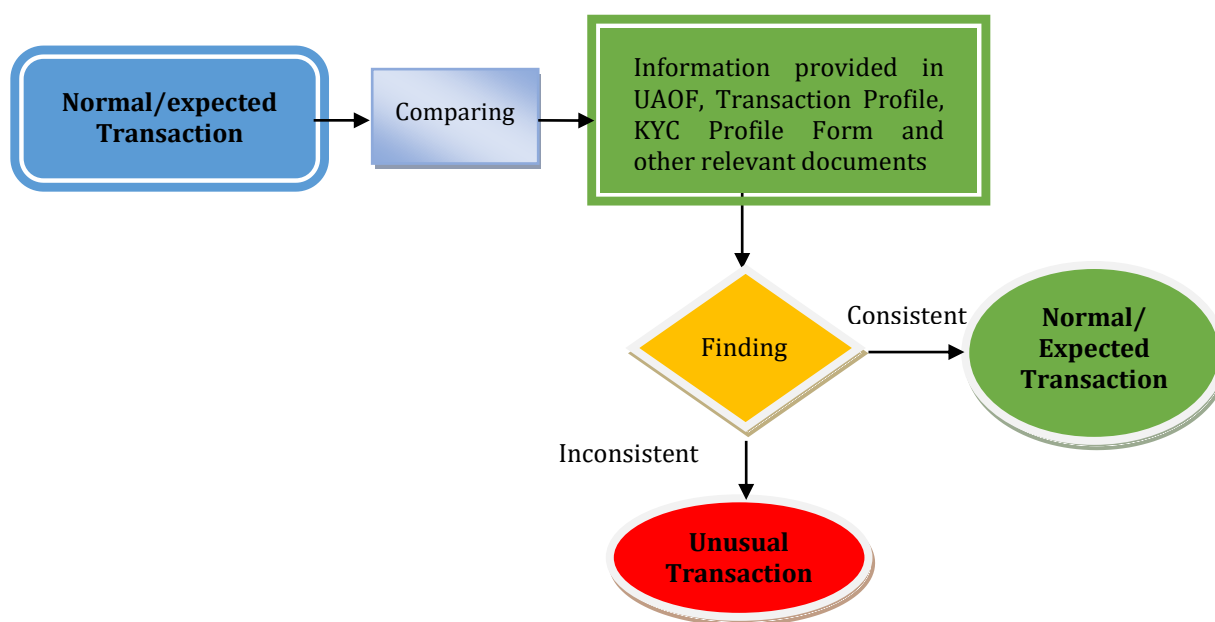
Identification of STR/SAR may be started identifying unusual transaction and activity. Such unusual transaction may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Generally the detection of something unusual may be sourced as follows:

- Comparing the KYC profile, if any inconsistency is found and there is no reasonable explanation;
- By monitoring customer transactions;
- By using red flag indicators.

A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transaction profiles will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises. Section-I provides some red flag indicators for identifying STR/SAR related to ML & TF.

All suspicions reported to the AML & CFT Department should be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the suspicion. All internal enquiries made in relation to the report should also be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

The following chart shows the graphical presentation of identification of STR/SAR-



*Figure: Identification of STR/SAR*

## **b) Evaluation of STR/SAR**

After identification of STR/SAR at branch/Department/division level, BAMLCO shall evaluate the reported transaction or activity in an appropriate manner and shall preserve

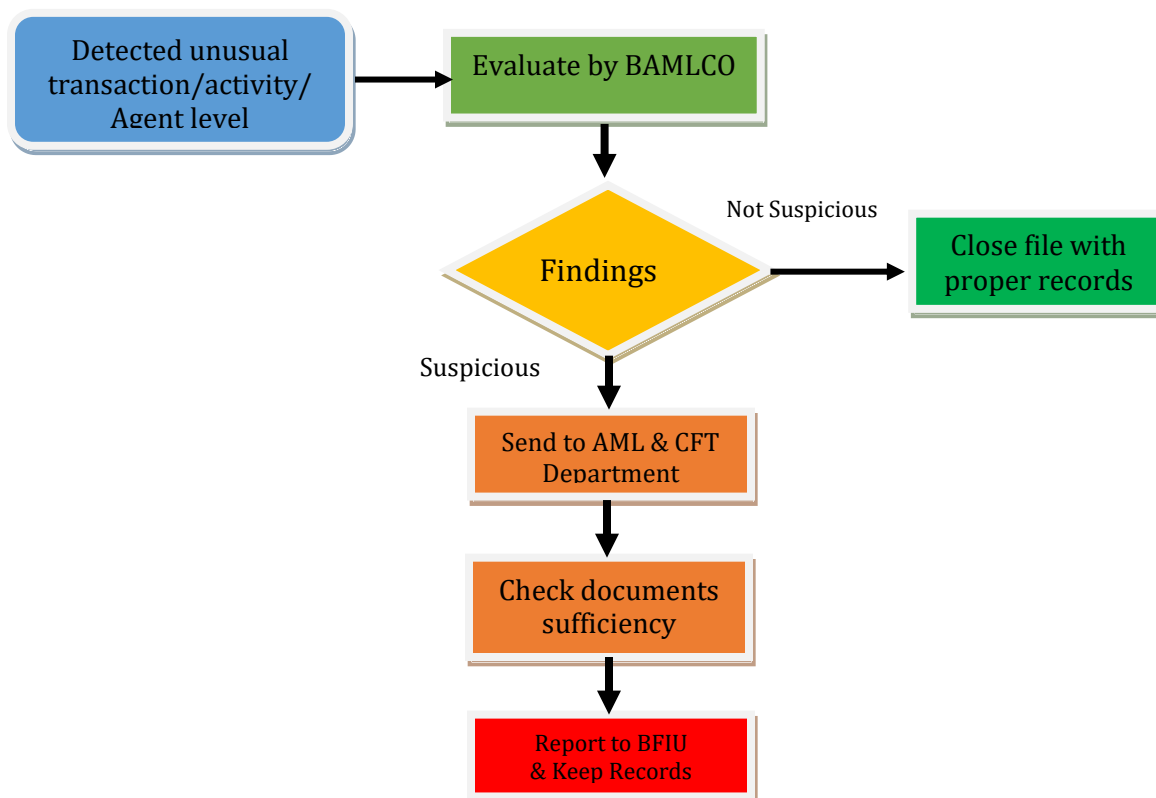
his observations on it in a written format. If the transaction or activity seems to be suspicious, has to be sent to the AML & CFT Department without any delay along with all necessary supportive documents. After receiving report from branch, AML & CFT Department shall review whether the reported suspicious transaction or activity from the branch has been reported in an appropriate manner with all necessary information, data and documents.

### c) Disclosure of STR/SAR

This is the final stage and Bank should submit STR/SAR to BFIU. After checking the sufficiency of the required documents, AML & CFT Department shall submit a suspicious transaction/activity report to BFIU without delay by using goAML web as per instruction mentioned in goAML Manual.

Every stages of evaluation Bank should keep records with proper manner. AML & CFT Department shall submit suspicious transaction/activity report to BFIU if it identifies any transaction or activity as suspicious even though the concerned branch did not identified as suspicious.

For simplification, the flow chart given below shows overall STR/SAR evaluation and reporting procedures:



*Figure: STR/SAR identification and reporting procedures*

#### **3.3.4.1 Reporting STR/SAR**

BFIU implemented a secured online reporting system namely the goAML, which requires the ROs to submit SARs and STRs through this channel. The goAML Web application provides a secure web based interface between the BFIU and its reporting organizations for the electronic upload of reports such as XML files, filling out the online report forms or sending XML files as attachments by secure e-mail, information sharing among stakeholders and other information.

With the help of ICT Department, AML & CFT Department of the Bank shall submit STR/SAR by using goAML web as per instruction mentioned in goAML Manual. (<https://www.bb.org.bd/eservices.php>).

#### **3.3.5 Whistle Blowing**

##### **a) Definition**

Although STR/SAR plays a leading role to prevent Money Laundering, but sometimes for an noticeable reason it may not possible to file STR/SAR in that case bank will establish **“Whistle Blowing Culture”**. **Whistle Blowing** means ‘speaking up’ or raising a concern. It ultimately is the disclosure of information which relates to suspected wrongdoing (generally a breach of a legal, statutory or regulatory requirement or unethical, immoral behaviour) of the law which compromises the Money Laundering and Terrorist Financing.

A Whistle Blower should be mentioned the following things at the time of reporting on suspected issues:

- the names of any individuals involved
- details of the alleged violation/suspected issues
- a summary of the supporting evidence have to be provided

For further details, follow the **“Whistle Blowing Policy and Procedure Manual”** of NRB Bank approved by the Honorable Board of Directors dated January 27, 2019.

##### **b) Confidentiality**

AML & CFT Department has an obligation to handle reports confidentially if the reporter so requests. Reports will be treated in confidential manner. AML & CFT Department will report to competent authority regarding the alleged violation/suspected issues, if required. AML & CFT Department will protect all information received and won't reveal whistle blower existence or identity unless legally required to do so.

### **3.4 Record Keeping**

Record keeping is an essential component of the audit trail that the Laws and Regulations seek to establish in order to assist in any financial investigation and to ensure that criminal funds which are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Banks must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

#### **3.4.1 Legal Obligations**

Obligations under MLPA, 2012, “The reporting organizations shall have to preserve previous records of transactions of any close account for at least 5(five) years from the date of such closure and provide with the information maintained under the clause to BFIU.”

Obligations under MLP Rules, 2019, “The bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners:

- (1) Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;
- (2) The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction;
- (3) The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order.



## **CHAPTER: IV**

### **RECRUITMENT, TRAINING AND AWARENESS**

#### **4.0 Obligations under Circular**

Under obligations of the BFIU Circular No. 26 dated June 16, 2020, “To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, bank should follow proper Screening Mechanism in case of recruitment and ensure proper training for their officials”

#### **4.1 Employee Screening**

Banks are subject to ML & TF risk from its customers as well as from its employee in absence of proper risk mitigating measures. ML & TF risks arise from customers and its mitigating measures have been discussed in several chapters of this guideline. ML & TF risks arose by or through its employees can be minimized if the bank follows fair recruitment procedure. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, Bank should follow the following measures (at least one from below):

- reference check
- background check
- screening through or clearance from Law Enforcement Agency
- personal interviewing
- personal guarantee etc.

Before assigning an employee in a particular job or desk, bank shall examine the consistency and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

#### **4.2 Know Your Employee (KYE)**

Know Your Customer, an essential precaution, must be coupled with Know Your Employees. There are a lot of instances that highlight the involvement of employees in fraudulent transactions and in most cases in association with customers. This therefore brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables. Policies, procedures, job descriptions, internal controls, approval levels, levels of authority, compliance with personnel laws and regulations, code of conduct/ethics, accountability, dual control, and

other deterrents should be firmly in place. And the auditor should be conversant with these and other requirements, and see that they are constantly and uniformly updated. Background screening of prospective and current employees, especially for criminal history, is essential to keep out unwanted employees and identifying those to be removed. It can be an effective risk management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. It can be used effectively, the pre-employment background checks/examines may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. KYE requirements should be included in the banks HR policy.

### **4.3 Training for Employee**

Every employee of the bank shall have at least basic AML & CFT training that should cover all the aspects of AML & CFT measures in Bangladesh. Basic AML & CFT training should be at least day long model having evaluation module of the trainees. Relevant provision of Acts, rules and circulars, guidelines, regulatory requirements, suspicious transaction or activity reporting should be covered in basic AML & CFT training course. To keep the employees updated about AML & CFT measures, bank is required to impart refresher training programs of its employees on a regular basis.

AML & CFT basic training should cover the following-

- an overview of AML & CFT initiatives;
- relevant provisions of MLPA & ATA and the rules there on;
- regulatory requirements as per BFIU circular, circular letters and guidelines;
- STR/SAR reporting procedure;
- ongoing monitoring and sanction screening mechanism;

Besides basic and refresher AML & CFT training, bank shall arrange job specific training or focused training i.e., Trade based money laundering training for the trade professional employees who deal with foreign or domestic trade, UNSCR screening related training for all employees who deal with international transactions, customer relations and account opening; credit fraud and ML related training for all the employees who deal with advance and credit of the bank; customer due diligence and ongoing monitoring of transaction related training for the employees who conduct transaction of customers.

#### **4.4 Awareness of Senior Management/Board of Directors**

Without proper concern and awareness of senior management/Board of Directors of the bank, it is difficult to have effective implementation of AML & CFT measures in the bank. Bank is required to arrange, at least once in a year, an awareness program for all the members of its Board of Directors or members of the highest policy making committee and people engaged with policy making of the bank.

#### **4.5 Customer Awareness Program**

Bank should take proper actions for broadcasting awareness building activities regarding prevention of money laundering and terrorist financing through different mass media under Corporate Social Responsibility (CSR) fund. Branch should arrange awareness build up program for their customer regarding AML & CFT issues.

#### **4.6 Awareness of Mass People**

Prevention of ML & TF largely depends on awareness at all level. Public or mass people awareness on AML & CFT measures provides synergies to bank in implementing the regulatory requirement. For this, BFIU, BB, other regulators as well as the government sometimes arrange public awareness programs on AML & CFT issues. Bank shall participate with public awareness programs on AML & CFT issues which will be arranged by the BFIU, Bangladesh Bank or other regulators. Bank shall also take initiative to arrange public awareness programs like advertisements through billboard, poster, festoon and mass media, distribution of handbills, leaflet and so on.

**CHAPTER: V****TRADE BASED MONEY LAUNDERING****5.0 Preamble**

Banks play an important role in the economy of a country which extend finance to the importer and exporter and undertake on behalf of its customers in various forms which include opening of Letter of Credit, Post import finance in the form of Payment Against Documents (PAD), Loan against Imported Merchandise (LIM), Loan against Trust Receipt (LTR), UPAS (Usance but payment at sight), seller/buyer's credit, issue of shipping guarantee etc. Banks also make fund available for exporter in the form of pre-export financing by opening documentary credit, Pre-shipment Credit(PSC) for RMG sectors, Packing Credit (PC), post-shipment financing by negotiation of export bills, collection of export bills, document against acceptance or document against payment, bill purchasing/discounting against local and foreign export bills, open account transactions and warehouse financing etc. However, problems arise when these funds are abused by some unscrupulous business man or if they adopt unfair means for tax evasion or involve in trade-based money laundering. Their unfair means not only affect the smooth business of the real business community but also act as barrier in the path of sustainable development of a country.

Normally it is assumed that international trade transaction involves only an issuing bank and advising bank on behalf of the importer and exporter. But the fact is not limited to that extent only. There are other parties involved in the trade transactions. They are: negotiating bank, collecting bank, reimbursing bank, remitting bank, confirming bank, transferring bank, intermediary bank, principal, indenter, shipping agents, insurance agents, pre-carriage vessels, vessels, forwarding agents, consignee, notifying parties etc. Thus in addition to core parties issuing bank, advising bank, importer and exporter, multiple financial institutions, multiple agents, multiple documents, rules and regulations and multiple ways to move the goods to and from all these makes the monitoring for money laundering complex.

**5.1 Basic Trade-Based Money Laundering Techniques**

*Trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin.* In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports.

In many cases, this can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers. The basic techniques of trade-based money laundering include:

- over- and under-invoicing of goods and services;
- multiple invoicing of goods and services;
- over- and under-shipments of goods and services; and
- falsely described goods and services.

All of these techniques are not necessarily in use in every country.

### **5.1.1 Over- and Under-Invoicing of Goods and Services**

Money laundering through the over- and under-invoicing of goods and services, which is one of the oldest methods of fraudulently transferring value across borders, remains a common practice today. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

By invoicing the good or service at a price below the “fair market” price, the exporter is able to transfer value to the importer, as the payment for the good or service will be lower than the value that the importer receives when it is sold on the open market.

Alternatively, by invoicing the good or service at a price above the fair market price, the exporter is able to receive value from the importer, as the payment for the good or service is higher than the value that the importer will receive when it is sold on the open market. Several points are worth noting. First, neither of the above transactions would be undertaken unless the exporter and importer had agreed to collude. For example, if Company A were to ship widgets worth \$2 each, but invoice them for \$1 each, it would lose \$1 million a shipment. Such a situation would not make sense unless the exporter and importer were colluding in a fraudulent transaction.

Second, there is no reason that Company A and Company B could not be controlled by the same organisation. In turn, there is nothing that precludes a parent company from setting up a foreign affiliate in a jurisdiction with less rigorous money laundering controls and selling widgets to the affiliate at a “fair market” price. In such a situation, the parent company could send its foreign affiliate a legitimate commercial invoice (e.g. an invoice of \$2 million for 1 million widgets) and the affiliate could then resell (and “re-invoice”) these goods at a significantly higher or lower price to a final purchaser. In this way, the company

could shift the location of its over- or under invoicing to a foreign jurisdiction where such trading discrepancies might have less risk of being detected.

Third, the over and under-invoicing of exports and imports can have significant tax implications. An exporter who over-invoices the value of the goods that he ships may be able to significantly increase the value of the export tax credit (or valued-added tax (VAT) rebate) that he receives. Similarly, an importer who is under-invoiced for the value of the goods that he receives may be able to significantly reduce the value of the import duties (or customs taxes) that he pays. Both of these cases illustrate the link between trade-based money laundering and abuse of the tax system.

### **5.1.2 Multiple Invoicing of Goods and Services**

Another technique used to launder funds involves issuing more than one invoice for the same international trade transaction. By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions.

In addition, even if a case of multiple payments relating to the same shipment of goods or delivery of services is detected, there are a number of legitimate explanations for such situations including the amendment of payment terms, corrections to previous payment instructions or the payment of late fees. Unlike over- and under-invoicing, it should be noted that there is no need for the exporter or importer to misrepresent the price of the good or service on the commercial invoice.

### **5.1.3 Over- and Under-Shipments of Goods and Services**

In addition to manipulating export and import prices, a money launderer can overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with this so-called “phantom shipment” are routinely processed. Banks and other financial institutions may unknowingly be involved in the provision of trade financing for these phantom shipments.

### **5.1.4 Falsely Described Goods and Services**

In addition to manipulating export and import prices, a money launderer can misrepresent the quality or type of a good or service. For example, an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs

documents and what is actually shipped. The use of false descriptions can also be used in the trade in services, such as financial advice, consulting services and market research. In practice, the fair market value of these services can present additional valuation difficulties.

## **5.2 CDD requirements in Trade Finance**

NRB Bank provides export and import business and other trade transaction to their customers. In trade finance different types of customer involve like importers, exporters, foreign/local suppliers, foreign/local buyers, agents of the foreign suppliers, agents of the foreign buyers, agents of foreign principals, beneficiary owners, authorized persons or entities related to an international/local trade transaction.

Branch and Trade Operations and other concern corporate office division must follow the instruction of BFIU Circular No. 24 dated December 10, 2019 regarding “Guidelines for Prevention of Trade Based Money Laundering” issued by BFIU and NRB Bank “Guidelines for Prevention of Trade Based Money Laundering” approved by the honorable of Board of Directors on 25<sup>th</sup> August 2020 for CDD measures of trade customers.



**CHAPTER: VI****TERRORIST FINANCING & PROLIFERATION FINANCING****6.0 Preamble**

Bangladesh has criminalized terrorist financing in line with the International Convention for the Suppression of the Financing of Terrorism (1999). Section 16 of Anti-terrorism Rules, 2013 states the responsibilities of the reporting agencies regarding funds, financial assets or economic resources or related services held in or through them.

A bank that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activity, is committing a criminal offence under the laws of Bangladesh. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism.

Regardless of whether the funds in a transaction are related to terrorists or terrorist activities, business relationships with such individuals or other closely associated persons or entities could, under certain circumstances, expose a bank to significant reputational, operational, and legal risk. This risk is even more serious if the person or entity involved is later shown to have benefited from the lack of effective monitoring or willful blindness of a particular bank and thus was to carry out terrorist acts.

Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, "Terrorist Financing" means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the following offences:

- a) attacks upon a person's life which may cause death;
- b) attacks upon the physical integrity of a person;
- c) kidnapping or hostage taking;
- d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major political and/or economic disruption and major economic loss;

- e) seizure of aircraft, ships or other means of public or goods transport;
- f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of biological and chemical weapons;
- g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;
- h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;
- i) public provocation to commit terrorist offences;
- j) recruitment for terrorism;
- k) training for terrorism.

### **6.1 Legal Obligations**

Under obligations of ATA 2009 (amendment 2012 & 2013), *“Every Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009(amendment 2012 & 2013) and if any suspicious transaction is identified, the agency shall spontaneously report it to BFIU without any delay”.*

*“The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each bank should approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by BFIU under section 15 of ATA, 2009(amendment 2012 & 2013); which are applicable to the bank, have been complied with or not.”*

### **6.2 Obligations under Circular**

Under obligations of BFIU Circular No. 26 dated June 16, 2020, *“Every bank shall establish a procedure by approval of Board of Directors for detection and prevention of financing of terrorism and financing of proliferation of weapons of mass destruction, shall issue instructions about the duties of Bank officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.”*

*“Before any international business transaction, every bank will review the transaction to identify whether the concerned parties of that transactions are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or proscribed by Bangladesh government. Immediately after the identification of any account of any listed individual or entity concerned bank will stop that transaction and inform BFIU the detail information at the following working day.*

### **6.3 Necessity of Funds by Terrorist**

Terrorist/Terrorist organizations need money to operate. Weapons and ammunition are expensive. Major international operations require substantial investments for personnel, training, travel and logistics. Organizations must have substantial fundraising operations, as well as mechanisms for moving funds to the organization and later to terrorist operators.

### **6.4 Source of Fund/Raising of Fund**

In general, terrorist /terrorist organizations may raise funds through: legitimate sources, including through abuse of charitable entities or legitimate businesses and self-financing, criminal activity, state sponsors and activities in failed states and other safe havens.

### **6.5 Movement of Terrorist Fund**

There are three main methods to move money or transfer value. These are:

- ❖ the use of the financial system,
- ❖ the physical movement of money (for example, through the use of cash couriers) and
- ❖ the international trade system.

Often, terrorist organizations will abuse alternative remittance systems (ARS), charities, or other captive entities to disguise their use of these three methods to transfer value. Terrorist organizations use all three methods to maintain ongoing operation of the terrorist organization and undertake specific terrorist activities.

#### **6.5.1 Formal Financial Sector**

Financial institutions and other regulated financial service providers' services and products available through the formal financial sector serve as vehicles for moving funds that support terrorist /terrorist organizations and fund acts of terrorism. The speed and ease with which funds can be moved within the international financial system allow terrorists to move funds efficiently and effectively and often without detection between and within jurisdictions.

Combined with other mechanisms such as offshore corporate entities, formal financial institutions can provide terrorists with the cover they need to conduct transactions and launder proceeds of crime when such activity goes undetected.

### **6.5.2 Trade Sector**

The international trade system is subject to a wide range of risks and vulnerabilities which provide terrorist organizations the opportunity to transfer value and goods through seemingly legitimate trade flows. To exploit the trade system for terrorist financing purposes could assist in the development of measures to identify and combat such activity.

### **6.5.3 Cash Couriers**

The physical movement of cash is one way terrorists can move funds without encountering the AML & CFT safeguards established in financial institutions. It has been suggested that some groups have converted cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside of the financial system. The movement of cash across the borders is prevalent in the cash based economy and where the electronic banking system remains embryonic or is little used by the populace.

Moving money using cash couriers may be expensive relative to wire transfers. As legitimate financial institutions tighten their due diligence practices, it has become an attractive method of transferring funds without leaving an audit trail. When cross border remittance of cash is interdicted, the origin and the end use of cash can be unclear. Cash raised and moved for terrorist purposes can be at very low levels – making detection and interdiction difficult.

### **6.5.4 Use of Alternative remittance systems (ARS)**

Alternative remittance systems (ARS) are used by terrorist organizations for convenience and access. ARS have the additional attraction of weaker and/or less opaque record-keeping and in many locations may be subject to generally less stringent regulatory oversight. Although FATF standards call for significantly strengthened controls over such service providers, the level of anonymity and the rapidity that such systems offer have served to make them a favored mechanism for terrorists.

### **6.5.5 Use of Charities and Non Profit Organizations**

Charities are attractive to terrorist networks as a means to move funds. Many thousands of legitimate charitable organizations exist all over the world that serve the interests of all societies, and often transmit funds to and from highly distressed parts of the globe. Terrorist abuses of the charitable sector have included using legitimate transactions to disguise terrorist cash travelling to the same destination; and broad exploitation of the charitable sector by charities affiliated with terrorist organizations. The sheer volume of funds and other assets held by the charitable sector means that the diversion of even a

very small percentage of these funds to support terrorism constitutes a grave problem.

## **6.6 Targeted Financial Sanctions**

The term Targeted Financial Sanctions (TFS) means both asset freezing and prohibition to prevent funds on other assets from being available, directly or indirectly, for the benefit of designated persons and entities. This TFS is smart solution to combat terrorism, terrorist financing and proliferation financing of weapons of mass destruction (WMD) by state actors or non-state actors from the UN Security Council. In contrast with the economic sanction on a jurisdiction, TFS is imposed on only suspected person or entities while innocent person or entities remain safe.

### **6.6.1 TFS related to terrorism and terrorist financing**

FATF recommendation 6 requires ‘Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of the United Nations Security Council of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolution; or (ii) designated by that country pursuant to resolution 1373(2001)’.

### **6.6.2 TFS related to Proliferation**

FATF recommendation 7 requires ‘Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council of the Charter of the United Nations’.

## **6.7 Automated Screening Mechanism of UNSCRs**

As per advise from Bangladesh Financial Intelligence Unit (BFIU), for effective implementation of TFS relating to TF & PF NRB Bank has already been started automated screening mechanism that prohibit any listed individuals or entities to enter into the banking channel. The bank is operating the system for detecting any listed individuals or entities prior to establish any relationship with them. In particular, bank

need to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individuals or entities could not use the formal financial channel. In a word, bank shall ensure that screening has done before-

- any international relationship or transaction;
- opening any account or establishing relationship domestically

For proper implementation of sanction list screening (OFAC, EU, UN, etc.), all officials of NRB Bank must have enough knowledge about-

- legal obligation and consequences of non-compliance;
- sources of information;
- what to do and how to do with sanction list;
- transactional review;
- how to deal with 'false positives';
- how to deal with actual match;
- how to deal with 'aggrieved person or entity';
- how to exercise 'exemption' requirements;
- listing & de-listing process

## **6.8 Requirements of the Reporting Organization**

As per the "Guidance Notes for Prevention of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction" of BFIU, Bank has to follow the following requirements:

### **A) Sanctions against which Bank should create a compliance program:**

- UNSCRs 1267 and its successor resolutions including UNSCR 2178;
- UNSCRs 1373 and its successors resolutions including UNSCRs 2178
- UNSCRs 1540
- UNSCRs 1718
- UNSCRs 1737 and its successor's resolutions including UNSCRs 2231.

### **B) Requirements for the Sanction regime**

Sanctions regimes narrowly require a specific legal base and/or course of actions for the followings:

- Trade embargos;
- Travel bans;
- Freezing of Assets; and
- Economic sanctions.

Trade embargos and freezing of assets are directly related with the reposting organizations. A reporting organization must ensure that they are not maintaining or continuing business relationship with sanctioned/designated person and not engaged in the trade activities with sanctioned individual, entity or territories. Beneficial ownership issues should be consider very carefully and critically while complying with the sanction regime, as money launderer of sanctioned individual or entities always try to hide them from front person or legal entity.

**C) Following mechanisms should be established by Bank to comply with the Sanction regime:**

- Ensure all relevant sanctions lists (updated) are used electronically to detect the existence of the sanctioned individuals, entities, or territories;
- Ensure that existing arrangements of customer screening are able to detect the relevant lists of named terrorist and sanctioned entities.
- Ensure that existing arrangements of customer screening are able to detect the relevant lists of trade embargos;
- Conduct real-time transaction screening on all cross-border payments, SWIFT and other modes of payments in relation to relevant lists of named terrorist and sanctioned entities, or embargos;
- Freeze the accounts and the relevant transaction in relation to relevant lists of named terrorist and sanctioned entities, or embargos immediately;
- Ensure to detect local sanction lists declared by BFIU;
- Report to the detected incidents to the BFIU without delay;
- Keep records or audit trail for all sorts of monitoring mechanism including the false positives;
- Take necessary training and awareness building arrangements.

**D) As per MLPR Bank should do the followings:**

- Maintain and update the listed individuals and entities in electronic form;
- Regularly run a check at the website of United Nations for updated list;
- Run regular check on the given parameters, including transactional review, to verify;
- In case of a match found the Bank shall immediately stop payment or transaction of funds, financial assets or economic resources;
- Report to the BFIU within the next working day with full particulars.



All the employees of the Bank shall remain vigilant to ensure the bank is not used by terrorist financier and proliferation financier of weapons of mass destruction.

## **6.9 Red Flags pointing to Financing of Terrorism**

### **Behavioral Indicators**

- The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- Use of false corporations, including shell-companies.
- Inclusion of the individual or entity in the United Nations 1267 Sanctions list.
- Media reports that the 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.
- Abuse of non-profit organization.

### **Indicators linked to the financial transactions**

- The use of funds by the non-profit organization 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's normal activity.
- Deposits were structured below the reporting requirements to avoid detection.
- Multiple cash deposits and withdrawals with suspicious references.
- Frequent domestic and international ATM activity.
- No business rationale or economic justification for the transaction.
- Unusual cash activity in foreign bank accounts.
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- Use of multiple, foreign bank accounts.

## **CHAPTER: VII**

# **ANTI-BRIBERY AND CORRUPTION (ABC) POLICY**

### **7.0 Preamble**

ABC (Anti-Bribery/Corruption) is a cause that the entire world is fighting for. All countries, even the developed ones, suffer from the consequences of bribery and corruption to varying degrees. It is well known that bribery and corruption have a link with money-laundering, and they are listed as predicate offenses like some other financial crimes. Clearly, banks have to guard against the risk of being used as conduits for money-laundering and terrorist financing.

NRB Bank committed to maintain a high standard of integrity and to operate fairly, honestly and legally, in order to ensure anti-corruption and bribery issues. NRB Bank is also committed to maintain a high standard of ethical conduct in all business dealings. Bank does not obtain or retain business through any unethical or illegal means, and all contract and transaction related to payments, including those in connection with gifts and other expenditures, are declared with reasonable details. NRB Bank has developed this policy to prohibit inappropriate conduct associated with bribery and corruption.

NRB Bank is committed to a culture of good business ethics and integrity and operates with zero tolerance for any form of corruption or illegal behavior whether direct or indirect.

### **7.1 Bribery**

Generally, Bribery is defined as the offering, giving, receiving, or soliciting of any item of value to influence the actions of an official, or other person, in charge of a public or legal duty.

Bribery is:

- a) giving, offering, promising, directly or indirectly, of a financial or other advantage with the intent to induce another person to improperly perform a function or a activity or to reward a person for improperly performing a function or activity or with the knowledge or belief that the simple act of acceptance of the advantage will constitute the improper performance of a function or activity; or
- b) the requesting, agreeing to receive or accepting of a financial or other advantage where there is an intention that as a consequence a function or activity should be performed improperly; or
- c) the promising, offering or giving of an advantage either directly or indirectly, to a public official as an inducement or reward for the retention of business or an advantage in the conduct of business.

## **7.2 Corruption and Fraud**

Corrupt and Fraudulent activities are not acceptable to or tolerated by NRB Bank. Employees, officers, consultants, contractors, and other third parties are also prohibited from engaging in any form of corrupt or fraudulent activity in their business operations whether related with or not on behalf of NRB Bank.

“Corruption” is defined as the abuse of entrusted power for private gain.

“Fraud” is defined as the intentional, false misrepresentation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury.

### **Action consisting Corruption and Fraud**

The embezzlement, misrepresentation and other financial irregularities usually capture the general acts of fraud and corrupt practices but do not preclude the following:

- any dishonest or fraudulent act
- misrepresentation of bank funds, securities, supplies or other assets
- handling or reporting of money or financial transactions fraudulently or improper way
- willfully conceal the conflicts of interests
- disclosing confidential and proprietary information to outside parties
- manipulation, falsification or alteration of records or documents
- Destruction, removal, or inappropriate use of records, fixtures, and equipment and other physical assets of the Bank.

## **7.3 Initiatives of NRB Bank to protect bribery and corruption**

### **7.3.1 Zero tolerance to bribery and corruption**

NRB Bank Ltd. has zero tolerance towards acts of bribery and corruption and prohibits them in any form, both direct and indirect. NRB Bank will not tolerate its employees or third parties in any kind of relationship with NRB Bank being involved in acts of bribery and corruption.

### **7.3.2 Governance**

The program shall be overseen by Senior Management under the supervision of Managing Director and CEO of the Bank. The overall objective of ABC governance is to establish and

maintain a policy which sets a standard of behaviour that achieves a culture of ethical business practices and compliance with ABC legal and regulatory aspects.

**a) Role and responsibilities**

In order to achieve an effective governance structure, roles and responsibilities should be allocated as follows:

- i) **Senior Management:** Senior Management shall have oversight responsibility to implement the policy and the Bank shall allocate sufficient resources to achieve reasonably effective operations. After proper verification Senior Management including Honorable Board of Directors will approve the policy including modification/changes that may take place.
- ii) **Human Resource Division:** Human Resource Division shall take an action against identified any bribery and corruption activities that may occurred by the employees working in the Bank. Human Resource Division shall circulate to all employees with advice to be vigilant for any bribery and corruption activities by the employees working under Branches/Departments/Divisions/Units/Cells and if any such occurrence is detected, the same shall be reported to Human Resource Division through concerned supervisor and information to be incorporated/uploaded Corporate Memory Management System (CMMS).
- iii) **Internal Control & Compliance Division:** Internal Control & Compliance Division shall special attention to evaluate the activities of Branches/Departments/Divisions/Units/ Cells while conducting their routine audit and report the same accordingly intimation to Human Resource Division and AML & CFT Department.

#### **7.4 ABC compliance Program**

Internal Control and Compliance Division will follow up/monitoring the ABC compliance program to minimize the risk. The following guidance can help the Bank to mitigate bribery and corruption risks:

- Prohibits the promising, offering, giving, solicitation or receiving of anything of value, directly or indirectly through third parties, if improperly intended to influence action or obtain an advantage.
- Prohibits falsifying or concealing any books, records or accounts that relate to the business of the Bank, its customers, suppliers or other business partners
- Defines and identifies the heightened risk of interaction with Public Officials
- Provides employees with the opportunity to report suspected bribery in a confidential manner and protects employees from retaliation for good faith reports
- Notifies employees the consequences of non-compliance

- Obtains strong and visible commitment from Senior Management and the Board of Directors, including a public statement of such commitment by the Bank
- All the employees of the bank follow the instruction of the competent authority like BFIU, Bangladesh Bank, Anti-Corruption Commission, NBR, CIC, Tax Office, Honorable Court, etc.
- Ensure proper verification of the documents of the International trade shall be verified through independent sources
- Ensure before sanctioning any donation, sponsorship, expenses and investment proper verification of the motive, ultimate beneficiary of the same.
- Ensure every dealing of the Banks operations including recruitment, transfer & positing, remuneration, benefit, training shall be done as per the HR Policy of the Bank
- HR policy should be followed before receiving any gift, benefit and hospitality by any employees of the Bank.
- Procurement and selling process shall be done as per the set rules of the Bank and must obtain approval from the proper management of the Bank.
- Ensure training on Anti -Bribery and Corruption

## **7.5 Conclusion**

The Policy, code of conduct shall also reference all employees' personal accountability to protect their Bank, its reputation and themselves from the risks arising from bribery and corruption and set out the consequences for non-compliance. The policy shall apply and easily accessible to all parts of the front, middle and back office. The policy shall apply to, and address, the potential bribery and corruption risks that can arise in different departments like Corporate Affairs, Business Development, Facilities, Human Resources, etc.

-----