



AML & CFT Division  
Corporate Office  
Dhaka

November 8, 2017

Agenda No : 23

To: The Board of Directors

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

In order to comply with the Money Laundering Prevention Act -2012, NRB bank had adopted the "Money Laundering & Terrorist Financing Risk Management Guidelines" in 2013 which was reviewed by our Honorable Board of Directors in November 2015. Subsequently, Bangladesh Financial Intelligence Unit (BFIU) has updated its Circular # 10 by issuing a new Circular # 19, dated September 17, 2017. Accordingly, the management of NRB bank has reviewed and updated the Guidelines in line with the newly issued circular.

Submitted for your kind approval.

Md Towhidu-Zzaman Fuad  
Deputy CAMLCO

Mahbubuzzaman  
CAMLCO

Md. Mehmood Husain  
Managing Director & CEO

## SUMMARY OF REVIEW OF ML&TF RISK MANAGEMENT GUIDELINES

SL No.	Review	Page
01	MD & CEO's Supervision	04
02	Definition of Placement Layer and Integration	07
03	Customer Due Diligence, Enhanced Due Diligence and Simplified Due Diligence	10 – 12
04	KYC Risk Grading	12
05	Online Deposit	12
06	Transaction Monitoring	12
07	Cash Transaction Report[CTR]	12 - 13
08	Half yearly self-assessment report	13
09	KYC/TP	14
10	Organogram of AML Unit	17
11	Client Identification & Verification	22
12	Correspondent Banking	23
13	Politically Exposed Persons [PEPs], Influential Persons [IP] and Head of High Officials of International Organizations	24 - 25
14	Domestic Wire Transfer	27
15	Duties and responsibilities of Ordering, Intermediary and Beneficiary Banks.	28
16	Agent Bank	29
17	Trade Sector	32



From: Company Secretary

Extract of the 57<sup>th</sup> Board Meeting of NRB Bank Limited held on Sunday, 12 November 2017  
at Board Room, Corporate Head Office, Simpletree Anarkali (9<sup>th</sup> Floor), 89 Gulshan Avenue,  
Gulshan-1, Dhaka

Agenda No. B-57/23: Review of "Money Laundering & Terrorist Financing Risk Management Guidelines"

Memo dated 08.11.2017 on the captioned subject was placed before the Board. The Board after detailed discussion approved updated and revised 'Money Laundering & Terrorist Financing Risk Management Guidelines' of NRB Bank Limited as presented in the meeting subject to periodic review as and when deemed necessary and thereafter following resolution was adopted:

"Resolved that updated and revised 'Money Laundering & Terrorist Financing Risk Management Guidelines' of NRB Bank Limited as detailed in the memo be and is hereby approved."

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

**MANAGING CORE RISK IN BANKING**

**Money Laundering & Terrorist Financing Risk  
Management Guidelines**



**Revised on November 2017**

**Central Compliance Committee (CCC)**

**NRB Bank Limited**

## BACKGROUND

### 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. 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), Bangladesh Bank. This policy will cover the requirements of "Money Laundering & Terrorist Financing Risk Management Guidelines" delivered by BFIU, Bangladesh Bank. 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 Board Audit Committee and subsequent approval by the 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.

Sufficient copies of this Policy will be distributed to all Branches of the Bank so that it will be readily available to all relevant employees.

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

#### 1.1.2 PURPOSE

The purpose of this guidance is to outline the legal and regulatory framework for anti-money laundering and combating financing of terrorism (AML/CFT) requirements and systems across the financial services sector. With a view to this, the document interprets the requirements of the relevant laws and regulations, and how they may be implemented in practice. It indicates good industry practices in AML and CFT procedures through a proportionate, risk-based approach; and assists the banks to design and implement the systems and controls necessary to mitigate the risks of the banks being used in connection with money laundering and the financing of terrorism.

#### 1.1.3 SENIOR MANAGEMENT ROLE & COMMITMENT

As part of its anti- money laundering policy NRB Bank will communicate a statement from the Chief Executive Officer that clearly sets forth the policy/guideline against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities on an annual basis. This statement will evidence the strong commitment of the Bank and its senior management to comply with all laws and regulations designed to combat money laundering. *If required, CEO will supervise the overall compliance status of the Bank.* Moreover, for the purposes of preventing ML, TF & PF our Senior Management shall ensure the following:

- 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.

## 1.2 What is Money Laundering

1.2.1 A definition of what constitutes the offence of money laundering under Bangladesh law is set out in Section 2 (Tha) of the Prevention of Money Laundering Act 2012 which is reads as follows: "Money Laundering" means -

(i) knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:- (1) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or Money laundering Prevention Act 4 (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, instigate or counsel to commit any offences mentioned above;

### 1.2.2 Predicate Offense :

"predicate offence" means the offences mentioned below, by committing which within or outside the country, the money or property derived from is laundered or attempt to be laundered, namely:- (1) corruption and bribery; (2) counterfeiting currency; (3) counterfeiting deeds and documents; (4) extortion; (5) fraud; (6) forgery; (7) illegal trade of firearms; Money laundering Prevention Act 6 (8) illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication; (9) illegal trade in stolen and other goods; (10) kidnapping, illegal restrain and hostage taking; (11) murder, grievous physical injury; (12) trafficking of women and children; (13) black marketing; (14) smuggling of domestic and foreign currency; (15) theft or robbery or dacoity or piracy or hijacking of aircraft; (16) human trafficking; (17) dowry; (18) smuggling and offences related to customs and excise duties; (19) tax related offences; (20) infringement of intellectual property rights; (21) terrorism or financing in terrorist activities; (22) adulteration or the manufacture of goods through infringement of title; (23) offences relating to the environment; (24) sexual exploitation; (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; (26) organized crime, and participation in organized criminal groups; (27) racketeering; and (28) any other offence declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official Gazette, for the purpose of this Act.



### 1.3 Why Money Laundering is done?

Criminals engage in money laundering for three main reasons:

- 1.3.1 First, money represents the lifeblood of the organization that engages in criminal conduct for financial gain because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and further the interests of the illegal enterprise, and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.
- 1.3.2 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.
- 1.3.3 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.

### 1.4 Why we must combat Money Laundering

- 1.4.1 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, terrorists, 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.
- 1.4.2 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.
- 1.4.3 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.

### 1.5 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 three recognized forms of the money laundering process. These are:

**1.5.1 Placement-** *is the stage in the crime where money is taken from its source (for example drug sales revenue) and "placed" into a legal activity so that the resultant outflow has the appearance of legally generated proceeds. Placing money into a casino or restaurant business would be good examples of businesses into which "dirty money" could be washed.*

**1.5.2 Layering-** *is the stage that makes tracing of "dirty money" more difficult. By moving money from one location (casino) to another (restaurant) the trail of the money becomes muddled and eventually unfollowable. Separating the proceeds of criminal activity from their source through the use of layers of financial transactions (multiple transfers of funds among financial institutions, early surrender of an annuity without regard to penalties, cash collateralized loans, L/Cs with false invoices/bills of lading, etc.) to disguise the origin of the funds, disrupt any audit trail, and provide anonymity. Launderers want to move funds around, changing both the form of the funds and their location in order to make it harder for law enforcement authorities to identify "dirty" money. At this stage, money launderers use multiple banks and accounts, act as intermediaries and transact through corporations and trusts.*

**1.5.3 Integration-** *is the stage where formerly "dirty money" is now re-integrated into honest business activities, typically through the bank into the bank account of an apparently honest business. Once the funds are layered and distanced from their origins, they are made available to criminals to use and control as apparently legitimate funds which is called 'integration'. The laundered funds are made available for activities such as investment in legitimate or illegitimate businesses, or spent to promote the criminal's lifestyle.*

## **1.6 How Financial Institutions Can Combat Money Laundering**

**1.6.1** 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 their 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.

**1.6.2** 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.

**1.6.3** 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.





## 2. WHAT THE LAW REQUIRES

### 2.1 Requirements under the Money Laundering Prevention Act 2012

The legislation specifically relating to money laundering is contained in the Money Laundering Prevention Act 2012 the provisions of which supersedes whatever may contain in any other Act in force in Bangladesh. So far as financial service providers are concerned, the Act:

- defines the circumstances, which constitute the offence of money laundering and provides penalties for the commission of the offence (See Section 2 Tha of the Act),
- requires banks, financial institutions and other institutions engaged in financial activities to establish the identity of their customers (See Section 19 Ka of the Act),
- requires banks, financial institutions and other institutions engaged in financial activities to retain correct and full information used to identify their customers and transaction records at least for five years after termination of relationships with the customers (See Section 19 Ka of the Act), and
- imposes an obligation on banks, financial institutions and other institutions engaged in financial activities and their employees to make a report to the Bangladesh Bank where:
  - they suspect that a money laundering offence has been or is being committed (See Section 19 Ga of the Act) and;
  - provide customer identification and transaction records to Bangladesh Bank from time to time on demand (See Section 19 Kha of the Act).

### 2.2 The Offence of Money Laundering

The money laundering offences are, in summary:

- 2.2.1 It is an offence for any person to obtain, retain, transfer, remit, conceal or invest moveable or immovable property acquired directly or indirectly through illegal means.. Concealing or disguising the property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights with respect to it.
- 2.2.2 It is an offence for any person to illegally conceal, retain transfer, remit, or invest moveable or immovable property even when it is earned through perfectly legitimate means. It is a defense if the person concerned can prove that the offence was committed without his knowledge or it has occurred despite his best efforts to prevent it.
- 2.2.3 It is also an offence for any individual or entity to provide assistance to a criminal to obtain, retain, transfer, remit, conceal or invest moveable or immovable property if that person knows or suspects that those properties are the proceeds of criminal conduct.

- 2.2.4 It is an offence for banks, financial institutions and other institutions engaged in financial activities not to retain identification and transaction records of their customers.
- 2.2.5 It is an offence for banks, financial institutions and other institutions engaged in financial activities not to report the knowledge or suspicion of money laundering to Bangladesh Bank as soon as it is reasonably practicable after the information came to light.
- 2.2.6 It is also an offence for anyone to prejudice an investigation by informing i.e. tipping off the person who is the subject of a suspicion, or any third party, that a report has been made, or that the authorities are acting, or are proposing to act, in connection with an investigation into money laundering. Preliminary enquiries of a customer to verify identity or to ascertain the source of funds or the precise nature of the transaction being undertaken will not trigger a tipping off offence before a suspicions report has been submitted in respect of that customer unless the enquirer knows that an investigation is underway or that the enquiries are likely to prejudice an investigation. Where it is known or suspected that a suspicions report has already been disclosed to the authorities and it becomes necessary to make further enquiries, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the law enforcement agencies.
- 2.2.7 It is an offence for any person to violate any freezing order issued by the Court on the basis of application made by Bangladesh Bank.
- 2.2.8 It is an offence for any person to express unwillingness, without reasonable grounds to assist any enquiry officer in connection with an investigation into money laundering.

### 2.3 Penalties and punishment for Money Laundering:

Penalties of money laundering and punishment.— (1) For the purposes of this Act, money laundering shall be deemed to be an offence. (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) lacks, whichever is greater. (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) Any entity which commits an offence under this section shall be punished with a fine of not less than twice of the value of the property or taka 20(twenty) lacks, whichever is greater and in addition to this the registration of the said entity shall be liable to be cancelled. (5) It shall not be a prerequisite to charge or punish for money laundering to be convicted or sentenced for any predicate offence. 5. Punishment for violation of an order for freezing or attachment.— Any person who violates a freezing or attachment order issued under this Act shall be punished with imprisonment for a term not exceeding 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or with both. 6. Punishment for divulging information.— (1) No person shall, with an ill motive, divulge any information relating to the investigation or any other related information to any person, organization or news media. Money laundering Prevention Act 8 (2) Any person, institution or agent empowered under this Act shall refrain from using or divulging any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act. (3) Any person who contravenes the provisions of sub-sections (1) and (2) shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or

with both. 7. Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information.- (1) Any person who, under this Act – (a) obstructs or declines to cooperate with any investigation officer for carrying out the investigation; or (b) declines to supply information or submit a report being requested without any reasonable ground; shall be deemed to have committed an offence under this Act. (2) Any person who is convicted under sub-section (1) shall be punished with imprisonment for a term not exceeding 1 (one) year or with a fine not exceeding taka 25 (twenty five) thousand or with both. 8. Punishment for providing false information.- (1) No person shall knowingly provide false information in any manner regarding the source of fund or self-identity or the identity of an account holder or the beneficiary or nominee of an account. (2) Any person who violates the provision of sub-section (1) shall be punished with imprisonment for a term not exceeding 3 (three) years or a fine not exceeding taka 50 (fifty) thousand or with both

## 2.4 How To Prevent Money Laundering:

### 2.4.1 Customer Due Diligence:

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 our 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.

*The CDD obligations compel banks to understand who their customers are to guard against the risk of committing offences under MLPA, 2012 including 'Predicate Offences' and the relevant offences under ATA, 2009.*

*Customer Due diligence (CDD) combines the KYC procedure, Transaction monitoring based on the information and data or documents collected from reliable and independent sources. Each Financial institution is required to perform Customer Due diligence on all prospective clients prior to opening an account. This process is completed by fulfilling the documentation requirements - Account application, KYC, Bank references, Source of fund and Identification. Bank should monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened. Banks therefore need to carry out customer due diligence in the following stages considering the risks of money laundering and terrorist financing.*

- *establishing a business relationship*
- *Carrying out an occasional transaction-Tk. 5,00,000/- & above.*
- *suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification*
- *Branch officials need to consider the confidentiality of the reporting of STR/SAR. They should not make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious.*

*Beneficial owner-The Bank shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from reliable source, such that the bank is satisfied that it knows who the beneficial owner is. Branches should consider following aspects while identifying beneficial ownership included-*

- *Any natural person(Beneficial Owner) operating account on-behalf of customer*



- Any person who has controlling interest or ownership interest on a customer who might be legal entity or legal arrangements.
- Any person or entity who has controlling 20% or above share holding within any or legal entity.
- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercise control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) should consider for other types of legal arrangements.

*Walk-in/One-off customers- Who do not maintain account with the Banks for conducting one-off/Occasional transactions requires to obtain satisfactory evidence of identification.*

#### *2.4.1.1 Simplified Customer Due Diligence (SDD):*

*SDD combines the Name, Address, phone no of Applicant/Sender & Receiver/Beneficiary. SDD should be performed for Occasional Transaction by Walk-in customer (DD, TT, MT, PO, wire Transfer). Walk-in Customer including On-line deposit/withdrawal (Tk. 50,000/- & below).*

*Including the above mentioned information Photo ID of Applicant/Sender & Receiver/Beneficiary should be obtained in-case of withdrawal/deposit of Tk. More than 50,000/- & below Tk. 5,00,000/-.*

*SDD also should be performed for Student/Farmer's account & others No Frill Account –Instruction from Financial Inclusion Department, B Bank.*

#### *2.4.1.2 Others instruction regarding CDD*

- Banks will introduce their own Account opening form by following uniform account opening form of BFIU.
- UCIC
- Bank should collect the announcement of customer about the Transaction Profile of customer account in the specified form.
- TP upgradation-06 Months after account opening
- Risk categorization during Account opening based on the Uniform Account Opening form
- 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. But, banks should update the changes in any information on the KYC as soon as bank gets to be informed. Moreover, bank should 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.
- All provisions of Foreign Exchange Regulations Act, 1947 have to be complied accordingly while opening foreign or Non-resident Bangladeshi Account

#### *2.4.1.3 Enhanced Due Diligence (EDD)*

*Bank should conduct EDD measures, in addition to normal CDD measures under the following circumstances*

- Individual or legal entity scored high risk
- PEPS/IPS/Chief Executives or top level officials of any International organization

- *Transaction identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purpose.*
- *Establishing relation with Persons or entities of countries and territories enlisted as high risk or non-cooperative jurisdiction in the FATF.*

*Where the financial institution is unable to conduct CDD- it should not open the account, commence business relations or perform the transaction or should terminate the business relationship and should consider making a suspicious transaction report in relation to the customer.*

#### 2.4.2 KYC Risk Grading:

KYC procedures refers 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.

NRB Bank shall adopt risk classification of its client on the basis of KYC information in line with the KYC profile form prescribed by the Central Bank. All accounts having a risk rating of 14 and above will be treated as high risk accounts. However, an account can be treated as high risk account on subjective judgment. Prior to opening a high risk account, branch/dept. has to take approval from concerned business (divisional) head concord with CAMLCO or Deputy CAMLCO of the bank. A system based tools should have in place to deter and detect high risk account. Branch will preserve the record of high risk accounts and pay more attention on overall activities of such accounts. **Branch will monitor high risk accounts on regular basis.**

#### 2.4.3 Third Party information/On line deposit:

Before accepting any third party transactions, relevant information must be obtained, kept and preserved by the bank as per regulatory guideline. **Branches collect complete and correct information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit banks should identify sources of funds as well.**

#### 2.4.4 Transaction Monitoring:

Banks 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. There should have adequate systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the relationship. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the Customer. Following reports need to be generated at prescribed frequency to ensure effective monitoring.

- ✓ **Exception Report/ TP Breach Report:** On a regular basis Branch will generate an Exception Report of customers whose accounts transaction volume exceeded the transaction limit (more than 20%) mentioned in transaction profile and review the same. If, after confirming with the client, the transaction trend is to continue the Account Officer is responsible for documenting the reasons why the transaction profile has changed and should amend the KYC profile accordingly.
- ✓ **CTR (Cash Transaction Reporting):** Cash transaction (deposit/withdrawal) for Tk. 10 lac or more in a day falls under CTR threshold. All such transactions are required to submit to Bangladesh Financial Intelligence Unit (BFIU) through GOAML web. Concerned Department of IT will prepare the report as per instruction given in the GOAML manual. If any of Branch do not have such transactions for a specific Month, respective Branch should inform it to the AML/CFT Division & AML/CFT Division has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR. Branches will preserved & review all such transactions to deter & detect

suspicious transaction, if any and report the same immediately to the AML/CFT Division. AML & CFT Division will prepare the report as per instruction provided by the regulator send the same to the BFIU through GOAML web within 72 hours of detection. Every stages of evaluation (whether reported to BFIU or not), banks should keep records with proper manner.

AML/CFT Division has to review all the cash transaction from the branches above the threshold and search for any suspicious transaction. If any suspicious transaction is found, will submit it as 'Suspicious Transaction Report' to the BFIU. Moreover, AML/CFT Division & Branches must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU. In case of cash deposit (regardless of amount) in the Govt. accounts or accounts of the Govt. owned entities, CTR reporting is not required. But in case of cash withdrawal such report is to be submitted.

- ✓ Remittance Transaction Report: A system based tool should be developed by the bank to monitor remittance transactions.

Banks should put in place various ways of transaction monitoring mechanism within their branches that includes but not limited to the followings:

- Manual/Automated monitoring
- 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.
- Monitoring should consider all FX Transaction, BEFTN, RTGS etc.
- To be vigilant to detect Structuring & their reporting
- Should consider various UN resolutions

#### 2.4.5 Half yearly Self-Assessment:

According to the instructions of BFIU, branches of bank need to conduct the Self-Assessment to evaluate them on a half yearly basis. Self-Assessment has to be done through a checklist that is attached with BFIU Master circular.

Before finalizing the evaluation report, there shall have to be a meeting presided over by the branch manager with all concerned officials of the branch. In that meeting, there shall be a discussion on the branch evaluation report; if the identified problems according that report are possible to solve at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations shall have to be jotted down. In the subsequent quarterly meetings on preventing money laundering and terrorist financing, the progress of the related matters should be discussed.

After the end of every half year, the branch evaluation report along with the measures taken by the branch in this regard and adopted recommendations regarding the issue should be submitted to the Internal Audit Department or ICCD of the Head Office and the Central Compliance Unit within the 15th of the next month.





#### 2.4.6 KYC/TP Review:

Branch should take necessary measures to review and update the KYC of the customer to be conducted in every 5(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. But, banks should update the changes in any information on the KYC as soon as bank gets to be informed. Moreover, bank should 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. For newly opened accounts Branch will fixed-up an updated TP after 06(Six) Months of the account opening date by reviewing the transactions and discussion with the said customer. If applicable, Branch should submit the STR.

#### 2.5 Responsibilities of Bangladesh Bank

The Act gives Bangladesh Bank broad responsibility for prevention of money laundering and wide- ranging powers to take adequate measures to prevent money laundering, facilitate its detection, monitor its incidence, enforce rules and to act as the prosecuting agency for breaches of the Act. The responsibilities and powers of Bangladesh Bank are, in summary (See Section 4 and 5 of the Act):

- 2.5.1 To investigate into all money-laundering offences.
- 2.5.2 Supervise and monitor the activities of banks, financial institutions and other institutions engaged in financial activities.
- 2.5.3 Call for reports relating to money laundering from banks, financial institutions and other institutions engaged in financial activities, analyze such reports and take appropriate actions.
- 2.5.4 Provide training to employees of banks, financial institutions and other institutions engaged in financial activities on prevention of money laundering.
- 2.5.5 To authorize any person to enter into any premises for conducting investigations into money laundering offences.
- 2.5.6 Persons authorized by Bangladesh Bank to investigate offences can exercise the same powers as the Officer in Charge of Police Station can exercise under the Code of Criminal Procedure.
- 2.5.7 To do all other acts in attaining the objectives of the Act.
- 2.5.8 The Courts will not accept any offence under the Act for trial unless a complaint is lodged by Bangladesh Bank or any person authorized by Bangladesh Bank in this behalf.





### 3. ANTI- MONEY LAUNDERING POLICY

#### 3.1 Senior Management Obligation

3.1.1 The most important element of a successful anti-money-laundering program is the commitment of senior management, including the chief executive officer and the board of directors, to the development and enforcement of the anti-money-laundering objectives which can determine criminals from using their facilities for money laundering, thus ensuring that they comply with their obligations under the law.

3.1.2 Senior management of NRB Bank Ltd must send the signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of its anti- money laundering policy NRBBL will communicate clearly to all employees on an annual basis a statement from the chief executive officer of NRBBL that clearly sets forth its policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement should evidence the strong commitment of the institution and its senior management to comply with all laws and regulations designed to combat money laundering.

3.1.3 The statement of compliance policy should at a minimum include:

- A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.
- A statement that all activities carried on by the financial institution must comply with applicable governing laws and regulations.
- A statement that complying with rules and regulations is the responsibility of each individual in the financial institution in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations is no excuse for non-compliance.
- The statement should direct staff to a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.
- A statement that employees will be held accountable for carrying out their compliance responsibilities.

#### 3.2. Written Anti-Money Laundering Compliance Policy

3.2.1 At a minimum, the board of directors of NRBBL develop, administer, and maintain an anti-money-laundering compliance policy that ensures and monitors compliance with the Act, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes.

3.2.2 The written anti-money-laundering compliance policy at a minimum should establish clear responsibilities and accountabilities within their organizations to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the law.



#### 4. ORGANIZATIONAL STRUCTURE

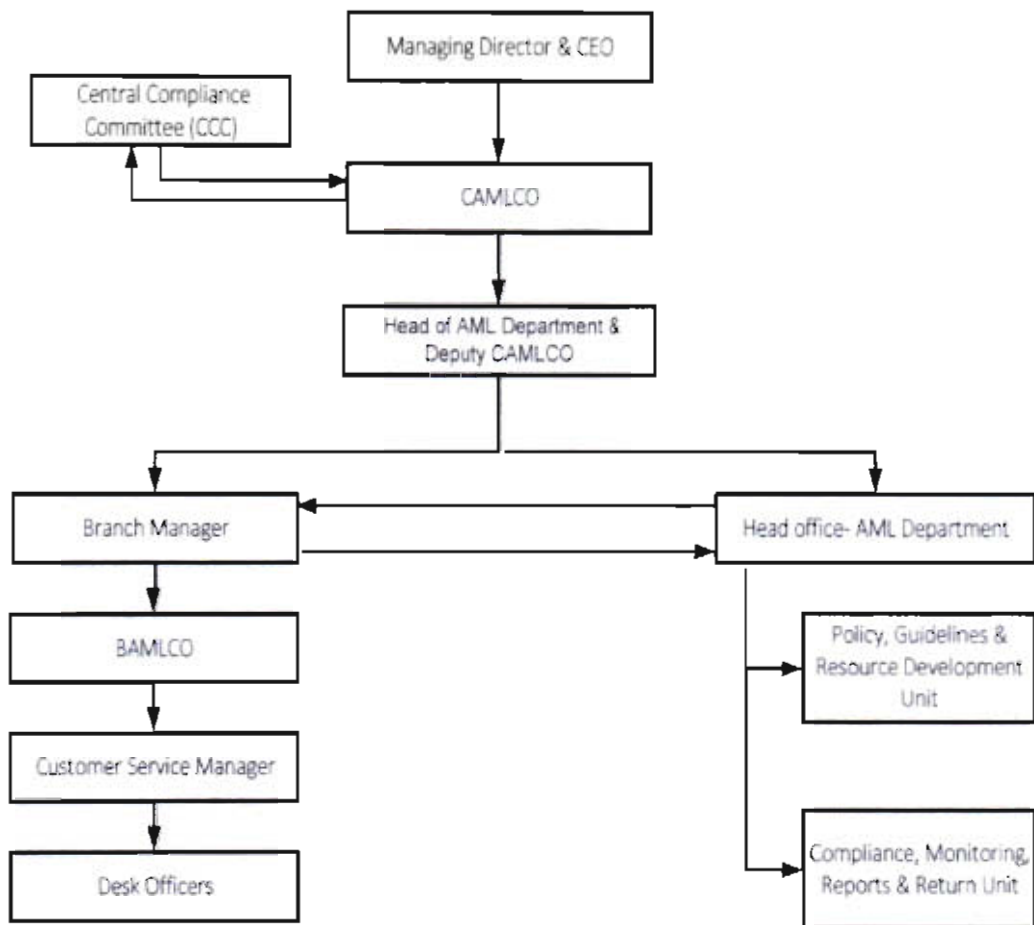
##### 4.1 Organization Structure

4.1.1 Whilst complying with rules and regulations is the responsibility of each individual in NRBBL in the normal course of their assignments, the following individuals and functions will play a vital role in the effectiveness of the Institutions AML program:

- ✓ Account Officer/Relationship Manager
- ✓ Customer Service Officer
- ✓ Operations Staff
- ✓ Branch Anti-Money Laundering Compliance Officer (BAMLCO) Branch Manager (Unit Head)
- ✓ Risk Management /Credit Officer
- ✓ Internal Control Officer
- ✓ Operations & Technology Manager
- ✓ Controller of Branches
- ✓ Deputy Chief Anti Money Laundering Compliance Officer (D-CAMLCO)
- ✓ Chief Anti Money Laundering Compliance Officer (CAMLCO)
- ✓ Chief Executive Officer (CEO)



**ORGANOGRAM OF ANTI MONEY LAUNDERING (AML) UNIT**



4.1.2 The Grid below details the individual responsibilities of the above functions:

Function	Role / Responsibilities
Account Officer/ Relationship Manager/ Staff Responsible for account opening	<ul style="list-style-type: none"> <li>✓ Perform due diligence on prospective clients prior opening an account</li> <li>✓ Be diligent regarding the identification (s) of account holder and the transactions relating to the account</li> <li>✓ Ensure all required documentation is completed satisfactorily</li> <li>✓ Complete the KYC Profile for the new customer</li> <li>✓ Ongoing monitoring of customer's KYC profile and transaction activity</li> <li>✓ Obtain documentary evidence of large cash deposits</li> <li>✓ Escalate any suspicion to the Supervisor, Branch Manager and AMLCO</li> </ul>
Customer Service Officer	<ul style="list-style-type: none"> <li>✓ Support the Account Officer in any of the above roles</li> <li>✓ Perform the Account Officer roles in their absence</li> </ul>
Operations Staff	<ul style="list-style-type: none"> <li>✓ Ensuring that all control points are completed prior to transaction monitoring</li> <li>✓ Ongoing diligence on transaction trends for clients</li> <li>✓ Update customer transaction profiles in the ledger/system</li> </ul>
BAMLCO	<ul style="list-style-type: none"> <li>✓ KYC adherence while customer on-boarding.</li> <li>✓ KYC review.</li> <li>✓ Monitoring Transaction.</li> <li>✓ Identification of suspicious transaction activities and Reporting.</li> <li>✓ Implementation of UNSCR</li> <li>✓ Activities regarding Self-Assessment</li> <li>✓ Suspicious Transaction reporting (STR).</li> <li>✓ Preserving Records.</li> <li>✓ Training of Branch staff.</li> <li>✓ Sending quarterly meeting minutes to CCC.</li> </ul>
Branch Manager (Unit Head)	<ul style="list-style-type: none"> <li>✓ Ensures that the AML program is effective within the branch/unit</li> <li>✓ First point of contact for any AML issues</li> </ul>
Risk Management /Credit Officer/ Internal Control Officer	<ul style="list-style-type: none"> <li>✓ Perform AML Risk Assessment for the Business</li> <li>✓ Perform periodic Quality Assurance on the AML program in the unit</li> <li>✓ Communicate updates in AML laws and internal policies</li> </ul>
Operations & Technology Manager Controller of Branches	<ul style="list-style-type: none"> <li>✓ Ensures that the required reports and systems are in place to maintain an effective AML program</li> <li>✓ Overall responsibility to ensure that the branches have an</li> <li>✓ AML program in place and that it is working effectively</li> </ul>



CAMLCO	<ul style="list-style-type: none"> <li>✓ CAMLCO should be able to act on his own authority;</li> <li>✓ He/she should not take any permission or consultation from/with the MD or CEO before submission of STR/SAR and any document or information to BFIU;</li> <li>✓ He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;</li> <li>✓ He/she must have access to any information of the bank;</li> <li>✓ He/she shall ensure his/her continuing competence.</li> </ul>
Chief Executive Officer (CEO)	Overall responsibility to ensure that the Business has an AML program in place and that it is working effectively & where applicable should observe overall AML/CFT compliance status of the Bank.

## 4.2 Designation of Anti-Money Laundering Compliance Officers (AMLCO)

4.2.1 NRBBL must designate a Chief Anti-Money Laundering Compliance Officer (CAMLCO) at its head office who has sufficient authority to implement and enforce corporate-wide anti-money laundering policies, procedures and measures and who will report directly to the CEO of NRBBL and the board of directors. This provides evidence of senior management's commitment to efforts to combat money laundering and, more importantly, provides added assurance that the officer will have sufficient clout to investigate potentially suspicious activities.

4.2.2 The designated CAMLCO, directly or through the designated department, unit, group, or committee, should be a central point of contact for communicating with the regulatory agencies regarding issues related to the financial institution's anti-money laundering program.

4.2.3 The designated CAMLCO must ensure that at each division, region, branch or unit of the financial unit that deals directly with the public, a senior level officer is appointed as Anti Money Laundering Compliance Officer (AMLCO) to ensure that each division, region, branch or unit is carrying out policies and procedures as required. These officers should report to the CAMLCO regularly on compliance issues and the need for any revisions to policies and procedures. This division, regional, branch or unit level officers may be dedicated solely to the financial institution's anti-money laundering responsibilities or perform the compliance functions in addition to existing duties.

4.2.4 All staff engaged in the NRBBL at all levels must be made aware of the identity of the CAMLCO, his Deputy and the staff's branch/unit level AMLCO, and the procedure to follow when making a suspicious activity report. All relevant staff must be aware of the chain through which suspicious activity reports should be passed to the CAMLCO.

4.2.5 A job description of the Chief Anti-Money Laundering Compliance Officers (CAMLCO) is appended below which may be adapted for creating a suitable job description of the Regional/Branch/ Unit Anti-Money Laundering Compliance Officers (AMLCO):

**POSITION TITLE:** Chief Anti-Money Laundering Compliance Officer(CAMLCO)

**FUNCTION:** The Chief Anti-Money Laundering Compliance Officer (CAMLCO), who will report to the Chief Executive Officer for this responsibility, coordinates and monitors day to day compliance with: applicable money laundering laws, rules and regulations; the Institution's AML Policy (the "Policy"); and the practices, procedures and controls implemented by the Institution.





#### 4.2.1 POSITION RESPONSIBILITIES

- 1) Monitor, review and coordinate application and enforcement of the Bank's/ Institution's compliance policies including Anti-Money Laundering Compliance Policy. This will include: an AML risk assessment; and practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transactions/account activity, and a written AML training plan (refer to Chapter IX);
- 2) To monitor changes of laws/regulations and directives of Bangladesh Bank that may require revisions to the Policy, and making these revisions;
- 3) Respond to compliance questions and concerns of the staff and advice regions/branches/units and assist in providing solutions to potential issues involving compliance and money laundering risk;
- 4) Ensure the Bank's/Institution's AML Policy is complete and up-to-date; maintain ongoing awareness of new and changing business activities and products and identify potential compliance issues that should be considered by the Bank/Institution;
- 5) Actively develop the compliance knowledge of all staff, especially the compliance personnel. Develop and conduct training courses in the Bank/Institution to raise the level of awareness of compliance in the Bank;
- 6) Develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, Regional/ Branch/Unit Heads and Compliance resources to assist in early identification of compliance issues;
- 7) Assist in review of control procedures in the Bank/Institution to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
- 8) To monitor the business' self-Assessment for AML/CFT compliance and any corrective action;
- 9) To manage the Suspicious Activity Reporting Process:
  - Reviewing transactions referred by divisional, regional, branch or unit compliance officers as suspicious;
  - Reviewing the Transaction Monitoring reports (directly or together with account management personnel);
  - Ensuring that internal Suspicious Activity Reports ("internal SARs"):
    - are prepared when appropriate;
    - reflect the uniform standard for "suspicious activity involving possible money laundering" established in the Policy;
    - are accompanied by documentation of the branch's decision to retain or terminate the account as required under the Policy;
    - are advised to other branches of the institution who are known to have a relationship with the customer;
  - are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk.



- Ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the Branch Manager;
- Maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner;
- Manage the process for reporting suspicious activity to Bangladesh Bank authorities after appropriate internal consultation;

#### 4.2.2 Job Characteristics and Requirements

The Chief Anti-Money Laundering Compliance Officer (CAMLCO) should possess:

- ✓ Proven leadership and organizational skills and ability to exert managerial control;
- ✓ Excellent communication skills, with ability to clearly and diplomatically articulate issues, solutions and rationale; an effective trainer to raise the level of awareness of the control and compliance culture;
- ✓ Solid understanding of AML regulatory issues and product knowledge associated with a broad range of relevant financial services, banking activities;
- ✓ High degree of judgment, good problem solving skills and be results oriented to ensure sound implementation of control and compliance processes and procedures;
- ✓ High personal standard of ethics, integrity and commitment to fulfilling the objectives of the position and protecting the interest of the Bank.

The Chief Anti-Money Laundering Compliance Officer (CAMLCO):

- ✓ Must be familiar with the ways in which any of their respective business's products and services may be abused by money launderers;
- ✓ Must be able to assist their respective Institutions develop effective AML policies, including programs to provide AML training to all personnel;
- ✓ Must be able to assist their respective business assess the ways in which products under development may be abused by money launderers in order to establish appropriate AML controls before product is rolled out into the marketplace.
- ✓ Must be capable of assisting their respective business evaluate whether questionable activity is suspicious under the standard set forth in the AML Policy and under any applicable law and regulation;
- ✓ Must attend each year at least one formal AML training program, either internal or external;



## 5.1 RECORD KEEPING

5.1.1 The records prepared and maintained by NRBBL on its customer relationships and transactions should be such that:

- ✓ requirements of legislation and Bangladesh Bank directives are fully met,
- ✓ competent third parties will be able to assess the institution's observance of money laundering policies and procedures,
- ✓ any transactions effected via the institution can be reconstructed,
- ✓ any customer can be properly identified and located,
- ✓ all suspicious reports received internally and those made to Bangladesh Bank can be identified and
- ✓ the institution can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.

5.1.2 Where there has been a report of a suspicious activity or the institution is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client should be retained until confirmation is received that the matter has been concluded.

## 5.2 Identity Verification:

The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may/ may not consider that this is in itself suspicious

### 5.2.1 CLIENT IDENTIFICATION & VERIFICATION

Ascertainment of customer identity:

- When entering into a lasting business relationship,
- When performing a single transaction or deal or conducting financial transaction with the existing customers.
- while remitting money and providing other services at the request of non-account holders; and
- *Before accepting cash or other physical values worth BDT 50,000 or more outside an existing business relationship (Carrying out an occasional transaction-Tk. 50,000/- & above by a walk in customer).*
  - suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification
  - Establishment of purpose of business relationship: When entering into a lasting business relationship, NRB Bank must obtain information on kind and purpose thereof, if this is not clear from the business relationship itself.



- **Identification of Ultimate Beneficial Owner:** Whenever NRB Bank is required to identify a customer, it must establish and verify the identity of the ultimate natural person, - who owns or
  - controls the customer or its assets or
  - on whose behalf the transaction is carried out or the business relationship is established or
  - Who has significant influence over the affairs of the company? or
  - who hold 20% or above share of a company

*Correspondent Banking: Bank should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.*

- *Bank should not establish or continue a correspondent banking relationship with any shell bank. [Here shell bank refers to such banks as are incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with a regulated financial group].*
  - *Correspondent banking relationship shall not be established or continued with those respondent banks that established correspondent banking relationship or maintain account with a shell bank.*
  - *Bank should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries and territories enlisted in Financial Action Task Forces Non-cooperating Countries and Territories list). Enhanced due diligence shall be required in such cases. Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.*
  - *Special attention must be paid to correspondent banking business and adequate security measures must be implemented. Before providing any correspondent banking service bank should collect information that is set out in the Annexure KA of BFIU Master Circular-19, September 17, 2017 & in addition of that required information to be collected from an open source. KYC of all correspondence relationship must be kept by concerned department as per Bangladesh Bank directive.*
- ✓ *While establishing and continuing correspondent banking relationship following drill should be observed so that banking system can not be abused for the purpose of money laundering:*
  - ✓ *Before providing correspondent banking service senior management approval must be obtained on being satisfied about the nature of the business of the respondent bank through collection of information as per format of BFIU, Bangladesh Bank*
  - ✓ *Banks should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.*



- ✓ Banks should not establish or continue a correspondent banking relationship with any shell bank.  
[Here shell bank refers to such banks as are incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with a regulated financial group.]
- ✓ Correspondent banking relationship shall not be established or continued with those respondent banks that established correspondent banking relationship or maintain account with a shell bank.
- ✓ Banks should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries and territories enlisted in Financial Action Task Force's Non cooperating Countries and Territories list). Enhanced due diligence shall be required in such cases. Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.
- ✓ Enhanced Due Diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customers to transact business on their behalf (i.e. payable through account).

The above instructions shall be applicable to the entire existing correspondent banking relationship.

**Politically Exposed Persons (PEPs):** NRB bank recognizes PEPs (Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials) accounts. Prior to entering in such type of relationship, branch has to take approval from concerned business (divisional) head of the bank. PEP accounts will fall under high risk account category by default. Respected Branch Officials Have to adopt an appropriate approach (Information from an open source, various database etc.) to determine whether a customer or the real beneficial-owner of an account is a PEP.

*Banks need to apply enhanced CDD / EDD measures, in addition to normal CDD measures for such High Risk accounts. EDD measures include-*

- *Obtaining additional information regarding identification of customers from independent & reliable sources.*
- *Obtaining additional information on the intended nature of the business relationship and source of funds or source of wealth of the customer.*



- *If required, obtaining approval from CAMLCO to commence or continue the business relationship.*
- *Branch should ensure enhanced & regular monitoring of their Account transactions*

**Influential Persons:** NRB bank recognizes Influential person (Individuals who are or have been entrusted domestically with prominent public functions, for example Head of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials also applicable for family members and close associates) accounts and prior to entering in such type of relationship, branch has to take approval from concerned business (divisional) head of the bank. NRB bank will monitor the transaction on regularly & will apply EDD measures for such accounts.

**Head or High Officials of International Organization:** NRB bank recognizes Head or High officials of international Organization person (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) accounts and prior to entering in such type of relationship, branch has to take approval from concerned business (divisional) head of the bank. NRB bank will monitor the transaction on regularly & will apply EDD measures for such accounts.

**Shell Bank/Forbidden Business:** Payable through accounts and relationships with shell banks are forbidden for NRB Bank and NRB Bank's correspondent banks.

**Sanction Policy:** Bank will follow the sanction policy as and when imposed by Bangladesh Bank, special reference list provided by OFAC, United Nations or other reorganizations acceptable to the NRB Bank. Bank already developed a system based tool "Acuity" to find out the sanction/terrorist organization/individuals names. Before opening an account bank must ensure that list of sanctioned names are being checked through Acuity and genuine match to be refer to CAMLCO for further decision an opening of the account.

### 5.3 Documents Verifying Evidence of Identity and Transaction Records

#### 5.3.1 Records relating to verification of identity will generally comprise:

- a description of the nature of all the evidence received relating to the identity of the verification subject;
- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

#### 5.3.2 Records relating to transactions will generally comprise:

details of personal identity, including the names and addresses, etc. as prescribed by Bangladesh



Bank under AML Circular # 2 and subsequent directives pertaining to: (1) the customer;

- (a) the beneficial owner of the account or product;
- (b) the non-account holder conducting any significant one-off transaction;
- (c) any counter-party;

details of transaction including:

- (a) the nature of such transactions;
- (b) Customer's instruction(s) and authority(ies);
- (c) source(s) and volume of funds;
- (d) destination(s) of funds;
- (e) book entries;
- (f) custody of documentation;
- (g) the date of the transaction;
- (h) the form (e.g. cash, cheque) in which funds are offered and paid out.

5.3.3 These records of identity must be kept for at least five years from the date when the relationship with the customer has ended. This is the date of:

- i. the carrying out of the one-off transaction, or the last in a series of linked one-off transactions;  
or
- ii. the ending of the business relationship; or
- iii. the commencement of proceedings to recover debts payable on insolvency.

#### 5.4 Wire Transfer Transactions

"Wire Transfer" refers those financial transactions in which a bank makes payment at the request of an applicant (individual or entity) using the electronic platform to the beneficiary individual or entity with the help of its other bank or branch.

##### 5.4.1 Other definitions related to wire transfers

- ✓ Cross border wire Transfer refers to as financial transactions in which applicant and beneficiary live in different jurisdictions/countries. Moreover, if at least one transaction of an inter-related payment chain takes place overseas the same will be considered as a cross border wire transfer.
- ✓ Domestic Wire Transfer refers to as financial transactions in which applicant and beneficiary live in a same jurisdiction. In this case, if the process of inter-related payment chain completes in other country/overseas the same should be treated as domestic wire transfer.
- ✓ "Applicant/Originator" is an individual or entity (either customer or non customer) at whose request concerned bank performs wire transfer.
- ✓ "Beneficiary" is an individual/entity (customer or non-customer) in whose favour payment is made.
- ✓ "Complete" will refer as to obtaining/completion of all necessary information to identify the applicant and the beneficiary. For example, Name and address details, Bank Account number



(if any), National Identification Number/Registration Certificate/ Acceptable Photo ID, phone/mobile number etc. of the applicant and beneficiary.

- ✓ By "Accurate", it will mean that the authenticity of information is verified as per clause 5 above.
- ✓ By "Meaningful" it will mean that there are reasons to believe that information under above clause 5 apparently seem appropriate and complete.

#### 5.4.2 Ensuring collection of following information for all types of Wire Transfers:

- ✓ Cross-border Wire Transfer:
  - 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 beneficiary's 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.
- ✓ Domestic Wire Transfer:
  - In case of domestic wire transfer, a complete and accurate information will be collected, preserved and send to intermediary/ beneficiary bank; for an amount less 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 collected as mentioned in section 2(a) above, 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-government/ 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 section 2(a) above 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.*



#### 5.4.3 DUTIES OF ORDERING, INTERMEDIARY AND BENEFICIARY BANK IN CASE OF WIRE TRANSFER

##### *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.*

##### *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.*

##### *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.*

#### 5.5 Investigations

5.5.1 Where an institution has submitted a report of suspicious activity to Bangladesh Bank or where it knows that a client or transaction is under investigation, it should not destroy any relevant records without the agreement of the Bangladesh Bank even though the five-year limit may have been reached.

5.5.2 Financial Institutions should maintain a register or tabular records of all investigations made to it by the Bangladesh Bank and all disclosures to the Bangladesh Bank. The register should be kept separate from other records and contain as a minimum the following details:

- i. the date and nature of the enquiry,
- ii. details of the account(s) involved; and
- iii. be maintained for a period of at least 5 years.





## 5.6 Training Records

So that NRBBL can demonstrate that they have complied with the regulations concerning staff training, they should maintain records which include:

- (i) details of the content of the training program provided
- (ii) the names of staff who have received the training
- (iii) the date on which the training was delivered
- (iv) the results of any testing carried out to measure staff understanding of the money laundering requirements and
- (v) An on-going training plan.

## 6. Agent Banking:

**6.1 Instructions & Compliance:** 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 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 (Janu-June based) should be uploaded in the Bank's web-sight.
  - A separate Cancelled/banned Agent list (January-June based) should be uploaded in the Bank's web-sight

**6.2 New Technology and services:** 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.



## 7. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

### 7.1 Recognition of Suspicious Transactions

As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. It is more than the absence of certainty that someone is innocent. A person would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime. However, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

### 7.2 Reporting of Suspicious Transactions

- 7.2.1 There is a statutory obligation on all staff to report suspicions of money laundering. Section 19 Ga of the Act contains the requirement to report to the Bangladesh Bank. Actual reporting should be made in accordance with an internal reporting procedure to be established by a financial institution for the purposes of facilitating the operation of the reporting obligation.
- 7.2.2 In line with accepted practice, some businesses may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting on to the Anti Money Laundering Compliance Officer or an appointed deputy.
- 7.2.3 NRBBL has a clear obligation to ensure, that each relevant employee knows to which person they should report suspicions, and that there is a clear reporting chain under which those suspicions will be passed without delay to the Chief Anti Money Laundering Compliance Officer.
- 7.2.4 The CAMLCO will be expected to act honestly and reasonably and to make his determinations in good faith. Provided the CAMLCO or an authorized deputy does act in good faith in deciding not to pass on any suspicions report, there will be no liability for non-reporting if the judgment is later found to be wrong.
- 7.2.5 Care should be taken to guard against a report being submitted as a matter of routine to Bangladesh Bank without undertaking reasonable internal enquiries to determine that all available information has been taken into account.



## 8. TRAINING AND AWARENESS

### 8.1 Statutory Requirements

8.1.1 Section 4 (Umah) of the Act requires Bangladesh Bank to provide training to the staff/officers of banks, financial institutions and other institutions engaged in financial activities in order to combat money laundering.

8.1.2 Since financial institutions themselves have responsibilities under the Act in relation to identification, reporting and record retention, it follows that NRBBL must ensure that their staffs are adequately trained to discharge their responsibilities.

8.1.3 It is therefore imperative for NRBBL to take appropriate measures to make employees aware of policies and procedures to prevent money laundering and for identification, record keeping and internal reporting; the legal requirements; and to provide relevant employees with training in the recognition and handling of suspicious transactions.

### 8.2 The Need for Staff Awareness

8.2.1 The effectiveness of the procedures and recommendations contained in this policy must depend on the extent to which staff in institutions appreciates the serious nature of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff of NRBBL must be trained to co-operate fully and to provide a prompt report of any suspicious transactions.

8.2.2 It is, therefore, important that NRBBL will introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.

### 8.3 Education and Training Programs

8.3.1 Timing and content of training packages for various sectors of staff of NRBBL will need to be adapted by individual businesses for their own needs. However it is recommended that the following might be appropriate.

8.3.2 All relevant staff of NRBBL should be educated in the process of the "know your customer" requirements for money laundering prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff of NRBBL should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

8.3.3 Banks shall respond to customers on different matters including KYC and TP attached to the account opening form with proper rationale. Banks shall time to time distribute leaflets among customers to make them aware about money laundering and terrorist financing and also arrange to stick posters in every branch/customer service outlet at a visible place.



#### 8.4 New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting any suspicious transactions to the Anti Money Laundering Compliance Officer (AMLCO) should be provided to all new employees of NRBBL who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

#### 8.5 Customer Service/Relationship Managers/Tellers/Foreign Exchange Dealers

- 8.5.1 Members of staff of NRBBL who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are vital to the organization's strategy in the fight against money laundering. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.
- 8.5.2 It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with non-regular (walk in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

#### 8.6 Processing (Back Office) Staff

Those members of staff of NRBBL who receive completed Account Opening, Payment Order/DD/TT/FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training in the processing and verification procedures. Those members of staff, who are in a position to deal with account opening, or to accept new customers, must receive the training given to cashiers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the organization's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Anti- Money Laundering Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

#### 8.7 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.*

*Besides basic and refreshment 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.*



### 8.8 Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the Act for non-reporting and for assisting money launderers; internal reporting procedures and the requirements for verification of identity and the retention of records.

### 8.9 Anti Money Laundering Compliance Officer

In depth training on all aspects of the Money Laundering Legislation, Bangladesh Bank directives and internal policies will be required for the Anti- Money Laundering Compliance Officer of NRBBL. In addition, the AMLCO will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

### 8.10 Refreshers' Training

In addition to the above relatively standard requirements, training may have to be tailored to the needs of specialized areas of the NRBBL's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Some financial sector businesses may wish to provide such training on an annual basis; others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.

