ANTI MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM POLICY GUIDELINES

National Bank Limited
A Bank for performance with potential

ANTI MONEY LAUNDERING &
COMBATING FINANCING OF TERRORISM
POLICY GUIDELINES
OF
NATIONAL BANK LIMITED

Revised on January 2023

National Bank Limited
A Bank for Performance with Potential

EDITORIAL COMMITTEE

CHAIRMAN	**HOSSAIN AKHTAR CHOWDHURY** Deputy Managing Director & CAMLCO
MEMBER SECRETARY	**TANVIR SUBHAN** Vice President & Deputy CAMLCO
CORE COMMITTEE MEMBER	**KAZI KAMAL UDDIN AHMED** Senior Executive Vice President & Head of Information & Technology Division **SHEIKH AKHTER UDDIN AHMED** Senior Executive Vice President & Head of Human Resources Division
SECOND LAYER COMMITTEE MEMBER	**MD. EHTESHAMUL HAQUE** Senior Assistant Vice President, International Division **SYED RAQUIB ALI** Senior Principal Officer, Information Technology Division **MD. SOHEL RANA** Senior Principal Officer, Human Resources Division **FAISAL AHMED BHUIYAN** Principal Officer, Anti Money Laundering Division **ABU NAYEM SHARIAR** Senior Executive Officer, Anti Money Laundering Division

TABLE OF CONTENTS

Table of Annexure	Page No.

LIST OF ACRONYMS AND ABBREVIATIONS

AD	Authorized Dealer
AML/CFT	Anti-Money Laundering and Combating The Financing of Terrorism
AMLD	Anti Money Laundering Division
AOF	Account Opening Form
APG	Asia Pacific Group on Money Laundering
ATA	Anti Terrorism Act
BAMLCO	Branch Anti Money Laundering Compliance Officer
BB	Bangladesh Bank
BDT	Bangladeshi Taka
BFIU	Bangladesh Financial Intelligence Unit
BoD	Board of Directors
CAMLCO	Chief Anti Money Laundering Compliance Officer
CAP	Customer Acceptance Policy
CBS	Core Banking Solution
CCC	Central Compliance Committee
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFT	Combating The Financing of Terrorism
CIF	Customer Identification File
CPV	Contact Point Verification
CTR	Cash Transaction Report
DCAMLCO	Deputy Chief Anti Money Laundering Compliance Officer
DD	Demand Draft
DNFBP	Designated Non-financial Businesses and Professions
EDD	Enhanced Due Diligence
ERC	Export Registration Certificate
EU	European Union
FATF	Financial Action Task Force
HRD	Human Resources Division
ICCD	Internal Control and Compliance Division
ID	International Division
IP	Influential Person
IRC	Import Registration Certificate
KYC	Know Your Customer
KYE	Know Your Employees
LC	Letter of Credit (Documentary Credits)
MD	Managing Director
ML	Money Laundering
MLPA	Money Laundering Prevention Act
ML/TF	Money Laundering & Terrorist Financing
MVTS	Money Or Value Transfers Service
NBL	National Bank Limited
NCCT	Non-Cooperative Countries and Territories
NFCD	Non Resident Foreign Currency Deposit
NGO	Non Government Organization
NID	National Identity Card
NPO	Non Profit Organization

NRA	National ML & TF Risk Assessment
NRB	Non Resident Bangladeshi
OFAC	Office of Foreign Asset Control
OBU	Off-Shore Banking Unit
PEP	Politically Exposed Person
PF	Proliferation Financing
PO	Pay Order
RBA	Risked Based Approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TBML	Trade Based Money Laundering
TIN	Tax Identification Number
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TP	Transaction Profile
TT	Telegraphic Transfer
UN	United Nations
UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction

Disclaimer

This Guideline is intended to provide general advice to the employees of National Bank Ltd. (NBL). It should never be relied on as a substitute for Money Laundering Prevention Act, 2012 (Amendment, 2015); Anti Terrorism Act, 2009 (Amendment, 2012 and 2013) and BFIU Guidelines.

The term "Guidelines" in this AML/CFT policy guideline indicates "Anti Money Laundering & Combating the Financing of Terrorism Policy Guidelines of National Bank Limited".

The term "Bank" in this policy guideline indicates "National Bank Limited".

The term "Branch" in this policy guidelines includes all branches, Sub-branches, Concerned Head office divisions, cells, departments, Off-Shore Banking Unit (OBU), Subsidiaries (where applicable) of National Bank Limited.

Introduction

Money Laundering and Terrorist Financing has been identified as a major threat to the financial services community. It is important that the management of Banks and other Financial Institutions view Anti Money Laundering and Combating the Financing of Terrorism as part of their risk management strategies and not simply as a stand-alone requirement that is being imposed by the legislation. Money laundering has potentially devastating economic, political, security, and social consequences. The consequences of terrorist activities are also terrific and devastating.

The government of Bangladesh recognized the necessity of enacting legislation in line with international practice and standards. Hence the Money Laundering Prevention Act, 2002 was promulgated by the Government of Bangladesh for the first time which came into force on April 30, 2002. Pursuant to the Money Laundering Prevention Act, 2002, Guidance Notes on Prevention of Money Laundering and instructions issued by Bangladesh Bank and in order to minimize the money laundering risk, National Bank Limited developed its own Anti Money Laundering Policy Guideline in October, 2005 which was approved by the Board of Directors. Subsequently the Money Laundering Prevention Act, 2002 was repealed and the Money Laundering Prevention Ordinance, 2008 was passed with effect from April 15, 2008. The Anti Terrorism Ordinance, 2008 was also passed in 2008 which came into effect from June 11, 2008. The Money Laundering Prevention Act, 2009 and the Anti Terrorism Act, 2009 were promulgated by the Govt. of Bangladesh in line with the above mentioned two Ordinances on February 24, 2009. The Money Laundering Prevention Act, 2009 was repealed and the Money Laundering Prevention Ordinance, 2012 was passed on January 17, 2012. The Anti Terrorism (Amendment) Ordinance, 2012 was also passed on the same day. In line with the above two Ordinances, Money Laundering Prevention Act, 2012 and Anti Terrorism (Amendment) Act, 2012 have been promulgate on February 20, 2012. Later on Anti Terrorism (Amendment) Act, 2013 was circulated on 12.06.2013 and Money Laundering Prevention (Amendment) Act-2015 was circulated on 26.11.2015. Both the Acts have empowered Bangladesh Financial Intelligence Unit (BFIU) to perform the anchor role in combating ML/TF through issuing instructions and directives for reporting agencies and building awareness in the financial sectors. On 16.06.2020, BFIU issued circular-26 for all scheduled banks of Bangladesh where new instructions has been given to prevent money laundering & terrorist financing. With the changes of laws and regulations, the existing Anti Money Laundering and Combating the Financing of Terrorism Policy Guidelines of NBL is required revision. In this regard NBL had revised its Anti Money Laundering and Combating the Financing of Terrorism Policy Guidelines on January 2023.

As a part of revision of Anti Money Laundering and Combating the Financing of Terrorism Policy Guidelines of NBL, the Board of Directors in its 476th Meeting held on 24.01.2023 approved the revised policy guidelines. The revised policy guideline will be named as earlier i.e. “Anti Money Laundering and Combating the Financing of Terrorism Policy Guidelines of National Bank Limited”. It will be applicable to all the Branches, Sub-branches, Head Office as well as Subsidiaries of the Bank. Any new instructions and guidelines of BFIU will be treated as pertinent portion of this policy guideline. It is mentionable that this policy guideline supersedes the Bank’s all previous AML/CFT Policy Guidelines.

CHAPTER 01

AN OVERVIEW ON MONEY LAUNDERING

1.1 What is Money Laundering?

Money Laundering is the practice of disguising illegally obtained funds so that they seem to be legal. It is a crime in many jurisdictions with varying definitions.

- The U.S. Customs Service, an arm of the Department of the Treasury, provides a definition of money laundering as "the process whereby proceeds, reasonably believed to have been derived from criminal activity, are transported, transferred, transformed, converted or intermingled with legitimate funds for the purpose of concealing or disguising the true nature, source, disposition, movement or ownership of those proceeds. The goal of the money laundering process is to make funds derived from, or associated with illicit activity appear legitimate."
- Another definition of Money Laundering under U.S Law is, "… the involvement in any one transaction or series of transactions that assists a criminal in keeping, concealing or disposing of proceeds derived from illegal activities."
- The EU defines it as "the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime."

- As per Sec 2(Fa) of the Money Laundering Prevention Act, 2012 Money Laundering means –
  a. Knowingly transfer, convert, hand over the proceeds of crime derived from an offence for the following purposes:
     i. Concealing or disguising the illicit origin/nature, source, location, ownership or control of the proceeds of crime; or
     ii. Assisting any person for evading the legal consequences of his or her action who is involved in the commission of the predicate offence;
  b. Unlawfully transfer funds or property abroad earned through legal or illegal means;
  c. Knowingly transfer or remit the proceeds of crime into or out of Bangladesh with the intention of hiding or disguising its illegal source;
  d. Conclude or attempt to conclude financial transactions in such a manner as to avoid reporting requirement under this Act;
  e. Convert or transfer or hand over legal or illegal property with the intention to instigate or assist the committing of a predicate offence;
  f. Acquire, possess or use property, knowing that
  g. Such property is the proceeds of a predicate offence; or
  h. Perform such activities so that illegal source of the proceeds of crime may be concealed or disguised; or
  i. Involve or conspire or participate to commit any of the above offences or instigate/encourage/advise anybody to commit any of the above offences.

1.2 Predicate Offences

As per Sec 2(Sha), 'Predicate Offence' means the offences inside or outside the country committing which one can earn or acquire funds or properties and then launders or attempts to launder the same. The predicate offences include –

i. Corruption and bribery;

ii. Counterfeiting currency;
iii. Counterfeiting deeds and documents;
iv. Extortion;
v. Fraud;
vi. Forgery;
vii. Trade of illegal arms;
viii. Illegal dealing in narcotic drugs and substances causing intoxication;
ix. Illegal trade in stolen and other goods;
x. Kidnapping, illegal restrain, hostage-taking;
xi. Murder, grievous bodily injury;
xii. Women and children trafficking;
xiii. Black marketing
xiv. Smuggling of domestic and international currency;
xv. Theft or robbery or piracy or aircraft hijacking;
xvi. Human trafficking/ taking or trying to take any money or valuables from any person by giving false hope of foreign job;
xvii. Dowry;
xviii. Smuggling and offences related to customs and excise duties;
xix. Tax related offences;
xx. Breach of intellectual property rights;
xxi. Financing of terrorism and terrorist activities;
xxii. Production of adulterated commodities or through violation of title;
xxiii. Environmental crime;
xxiv. Sexual exploitation;
xxv. Insider trading & market manipulation- using price sensitive information relating to the capital market in share transactions before it is published before the general public to take advantage of the market and attempting to manipulate the market for personal or institutional gain;
xxvi. Organized crime and joining organized criminal groups;
xxvii. Racketeering; and
xxviii. Any other offences declared as predicate offence by Bangladesh Financial Intelligence Unit (BFIU), with the approval of the government, by notification in the Bangladesh Gazette, for the purpose of this Act.

1.3 Why Money Laundering is done?

Criminals engage in money laundering for three main reasons:

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.

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.

1.4 Why we must combat Money Laundering?

From the viewpoint of banking activities, prevention of Money Laundering has three dimensions:

a. Ethical – taking part in the prevention of crime
b. Professional- ensuring that the Bank is not involved in recycling the proceeds of crime that would call into question its reputation, integrity and if fraud is involved, its solvency
c. Legal – complying with Laws and Regulations that impose a series of specific obligations to financial institutions and their employees.

Money Laundering should also be prevented considering the following aspects:

- Money laundering is a process, vital for 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 to combat the serious consequences that result in. 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 the taxpayers pay more because of the tax evaders. So we all experience higher costs of living than we would if financial crime, including money laundering were prevented.
- Money laundering distorts asset and commodity prices and leads to misallocation of resources. For financial institutions it can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability. The loss of credibility and investor confidence that such crises can bring has the potential of destabilizing financial systems, particularly in smaller economies.
- One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers often use front companies, which co-mingle the proceeds of illicit activity with legitimate fund, to hide the ill-gotten gains. These front companies have access to substantial illicit fund, allowing them to subsidize front company products and services at levels well below market rates. This makes it difficult, if not impossible, for legitimate business to compete against front companies with subsidized funding, a situation that can result in the crowding out of private sector business by criminal organizations.
- Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government, and citizens to criminals. Furthermore, the sheer magnitude of the economic power that accrues to criminals from money laundering has a corrupting effect on all elements of society.
- The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. The bribing of officials and governments undermines the moral fabric in society, and, by weakening collective ethical standards, corrupts our democratic institutions. When money laundering goes unchecked, it encourages the underlying criminal activity from which such money is generated.
- Nations cannot afford to have their reputations and financial institutions tarnished by an association with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions and the underlying criminal activity -- fraud, counterfeiting, narcotics trafficking, and corruption weaken the reputation and standing of any financial institution. Actions by banks to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. A bank tainted by money laundering accusations

from regulators, law enforcement agencies, or the press, runs the risk of prosecution, the loss of good market reputation, and damage to the reputation of the country. It is very difficult and it requires significant resources to rectify a problem that could be prevented with proper anti money laundering controls.

1.5 Stages of Money Laundering

Money laundering is often a diverse and complex process, but it basically involves 3 stages: Placement, Layering and Integration. The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organizations. There are some typical examples.

A. Placement: It is the first stage in separating the illicit fund from their illegal source. Placement is when the cash proceeds from a criminal activity (the dirty money) first enter the financial system. For example, stolen goods are sold for cash, which is then deposited into a bank account. Cash can also be placed into the financial system by:

- Depositing cash into an account or several bank accounts in different locations to avoid detection;
- Buying foreign currency, bank drafts, travelers' cheques or other instruments with the cash;
- Buying stocks and shares;
- Buying business assets and equity investments;
- Commingling criminal cash with legitimate cash in a business account;
- Converting cash from one currency into another currency.

B. Layering: Layering takes the form of a series of transactions designed to distance the money from the initial criminal activity, so that investigators will not be able to follow the trail and identify the perpetrators. Layering often involves the movement of fund from one country to another. Followings are some examples of layering -

- Electronic fund transfer between non-existent / fictitious companies;
- Buying, then selling, an investment product;
- Buying and then surrendering a single premium insurance contract;
- Engaging in international trade transactions;
- Moving fund from one account to another, from one investment to another or even from one country to another.

C. Integration: Integration means that the proceeds of layering are finally moved back into the financial system in such a way that they appear to be normal business funds. This is regarded as the most difficult stage to recognize because the funds appear legitimate. Following are some examples of integration:

- Purchase of property (for personal use or investment);
- Purchase of high value items viz., jewellery, antiques, work of art;
- Purchase of legitimate business.

1.6 Money Laundering Risks

The bank is aware that it is exposed to several risks if an appropriate AML Guideline is not established. Some of them are –

Reputation Risk: This is the risk of loss due to severe impact on the bank's reputation. This may be of particular concern given the nature of the bank's business, which requires maintaining the confidence of depositors, creditors and the general marketplace.

Compliance Risk: It is the risk of loss due to failure of compliance with key regulations governing the bank's operations as per the prescription of the regulator.

Operational Risk: It is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of the banks' programs, ineffective control procedures and failure to practice due diligence.

Legal Risk: This is the risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with law and having a negative legal impact on the bank. The specific types of negative legal impacts can arise by way of fines, confiscation of illegal proceeds, criminal liability etc.

1.7 Penalties for Money Laundering

The penalties for the commissioning of money laundering offences are as follows:

Sec: 4 of MLPA, 2012: Offence of money laundering

- Any person who commits the offence of money laundering, or abets or conspires in the commission of the offence of money laundering, shall be punishable with imprisonment for a minimum period of 4 (four) years and not more than 12(twelve) years and in addition, a fine equivalent to two times of the value of the property involved in the offence or BDT 1,000,000.00 (ten lac), whichever is greater may be imposed.
- Any entity which commits an offense under this section shall be punishable with a fine of not less than two times the value of the property or BDT 2,000,000.00 (twenty lac) whichever is greater and in addition, the registration of the said entity will be liable to be cancelled.

Sec: 5 of MLPA, 2012: Punishment for violation of a freezing or attachment order:

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.

Sec: 6 of MLPA, 2012: Punishment for divulging information:

Imprisonment for not more than 2 (two) years or fine of maximum BDT 50,000.00 (fifty thousand), or both.

Sec: 7 of MLPA, 2012: Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information:

Imprisonment for maximum 1(one) year or a fine of maximum BDT 25,000.00 (twenty five thousand) or both.

Sec: 8 of MLPA, 2012: Punishment for providing false information:

Maximum imprisonment for 3(three) years or a fine of maximum BDT 50,000.00 (fifty thousand) or both.

1.8 Powers of BFIU in Preventing and Restraining the Offence of Money Laundering

As per provision 23 of MLPA, 2012, BFIU is responsible for implementation of MLPA, 2012. In order to carry out the duties and responsibilities, BFIU is empowered to impose penalties upon the reporting organization including bank for non-compliance with their instructions as well the duties and responsibilities as per Sec 25 of MLPA, 2012.

Sec 23(3) of MLPA, 2012

If any reporting organization fails to provide requested information timely pursuant to this section, BFIU may impose fine on such organization BDT 10,000.00 (ten thousand) per day and up to a

maximum of BDT 500,000.00 (five lac). If an organization is fined more than 3 occasions in a financial year, BFIU may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization.

Sec 23(4) of MLPA, 2012

If any reporting organization provides false information or statement requested pursuant to this section, BFIU may impose fine on such organization not less than BDT. 20,000.00 (twenty thousand) but not more than BDT 500,000.00 (five lac). If an organization is fined more than 3 occasions in a financial year, BFIU may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization.

Sec. 23(5) of MLPA, 2012

If any reporting organization fails to comply with any instruction given by BFIU pursuant to this Act, BFIU may fine such organization BDT 10,000.00 (ten thousand) per day and maximum BDT 500,000.00 (five lac) for each such non-compliance. If an organization is fined more than 3 occasions in a financial year, BFIU may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization.

Sec. 23(6) of MLPA, 2012

If any bank fails to comply with the freezing order passed by BFIU pursuant to the power conferred, under Sec. 23(1) (Ga), in that case BFIU can impose minimum fine equivalent to the balance of the related account and maximum two times of the account balance as on the instruction date.

Sec 23(7) of MLPA, 2012

If any person or Reporting Organization fails to pay any fine imposed by BFIU under sections 23 and 25 of this Act, BFIU may recover the amount from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank. In this regard if any amount of the fine remains unrealized, BFIU may submit an application before the court for recovery and the court may pass any order which it deems fit.

Sec 23(8) of MLPA, 2012

If any reporting organization is fined under sub-sections 3, 4, 5 and 6, BFIU may impose a fine on the responsible owner, director, employees and officials or persons employed on a contractual basis of that reporting organization, not less than BDT. 10,000.00 (ten thousand) and a maximum up to BDT 500,000.00 (five lac) and where necessary may direct the relevant organization to take necessary administrative actions.

If any entity violates any provision of the Act, it will be deemed that every owner, partner, director, manager, secretary or any other employee and representative/agent has individually violated such provision under section 27 of the MLP Act, 2012.

1.9 Offences Committed by an Entity

If any offence under MLP Act is committed by an entity, every proprietor, director i.e. any partner or member of the Board of Directors, manager, secretary or any other officer, staff or representative of the said entity who is directly involved in the offence shall be deemed to be guilty of the offence

unless he is able to prove that the said offence has been committed without his knowledge or he took steps to prevent the commission of the said offence.

1.10 Responsibilities of the Reporting Organizations in Preventing Money Laundering

The reporting organizations shall have the following responsibilities in the prevention of money laundering, namely:

a. To preserve complete and correct information with regard to the identity of the customers during the operation of their accounts;
b. If any account of a customer is closed, to preserve previous records of transactions of such account for at least 5(five) years from the date of closure;
c. To provide the information under clause a & b to BFIU from time to time, on its demand;
d. If any doubtful transaction or attempt of such transaction is observed, to report the matter as suspicious transaction report to the BFIU immediately on its own accord.

1.11 What is Terrorism?

Terrorism has been defined in Sec. 6 of the Anti Terrorism Act, 2009 (Amendment, 2012 & 2015) in the following way:

1.11.1 A. If any person or entity for the purpose of endangering the unity, integration, public security or sovereignty of Bangladesh, and with the aim of compelling the government or any entity or any other person to do something or preventing them from doing something by creating panic in the public or a section of the public

i. Kills, seriously injures, kidnaps or obstructs anybody or destroys or attempts to destroy somebody's/entity's/Governments' properties;

ii. Instigate any person to kill, seriously injure, puts in confinement or kidnap or obstruct anybody or instigate any person to damage property belonging to any person or entity or the State or

iii. Using or keeping in one's possession any explosive substance, inflammable substance, arm with the aim of fulfilling the purpose of subsection (i) and (ii);

B. If any person or entity from Bangladesh organizes or takes initiative to commit or instigates or abets someone to commit an offence with a purpose to impede the security of any other state or if any person or entity has any financial involvement to damage any property belonging to any other state or commits or attempts to commit or instigates or abets such offence.

C. If a person or entity possesses or holds or uses any property knowingly that derives from terrorist act or is provided by any terrorist or terrorist groups, the person or the entity will commit the offence of terrorism.

D. If any foreign citizen commits any crime mentioned at 'A', 'B' and 'C' above in Bangladesh, he/she will commit the offence of terrorism.

1.11.1 If any person or entity commits terrorism offence, he/she or the entity whichever the designation may be, will be penalized death sentence or lifetime imprisonment or maximum 20 (twenty) years but not less than 4 (four) years with rigorous imprisonment and in addition imposition of fine for any amount.

1.12 What is financing of terrorism?

As per section 7 of the Anti Terrorism (Amendment, 2012 and 2013) Act, 2009

A. If any person or entity provides or instigates anybody to provide or desires to provide money, services, material support or any other property knowingly to other person or entity with the intention that they would be used or there are reliable grounds to believe that they would be

used or they can be used in full or in part in order to carry out a terrorist act, he/she or the entity will commit the offence of financing terrorism.

B. If any person or entity receives money, services, material support or any other property knowingly with the intention that they would be used or there are reliable grounds to believe that they would be used or they can be used in full or in part in order to carry out a terrorist act, he/she or the entity will commit the offence of financing terrorism.

C. If any person or entity knowingly makes arrangements for collecting money, services, material support or any other property for another person or entity and where there are reliable grounds to believe that the full or the partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization he or she or the entity will commit the offence of financing terrorism.

D. If any person or entity knowingly instigates in such a manner, another person or entity to supply, receive, or arrange money, services, material support or any other property and where there are reliable grounds to believe that the full or the partial amount of the same has been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the entity will commit the offence of financing terrorism.

1.13 Punishment for financing of terrorism

A. As per Sec. 7(6) of the Anti Terrorism (Amendment, 2012 and 2013) Act, 2009, if a person is proved under the sub-section (1) to (4) as mentioned in section 1.10 above that he/she has committed the offence of financing terrorism, he/she will be penalized for imprisonment of maximum 20 (twenty) years but not less than 4 (four) years and in addition to this fine of two times of the value of the property involved with the offence or BDT 1,000,000.00 (ten lac) whichever is greater.

B. (I) As per Sec. 7(6) of Anti Terrorism (Amendment, 2012 and 2013) Act, 2009, if an entity is proved that it has committed the offence of financing terrorism, the entity can be banned by the Government under the power conferred in Sec 18 of the Act and in addition, fine of three times of the amount involved with the offence or BDT 5,000,000.00 (Fifty lac), whichever is greater; and

(II) The head of such entity, Chairman, Managing Director, Chief Executive Officer whatever may be called by shall be punished with an imprisonment of a term up to maximum of 20 years and a minimum of 4 years and in addition to this, fine of two times of the value of the property involved with the offence or BDT 2,000,000 (twenty lac) unless he/she is able to prove that the said offence was committed without his/her knowledge or he/she had tried utmost to prevent the commission of the said offence.

1.14 Powers of BFIU in Combating the Financing of Terrorism

If any reporting organization fails to comply with the directions issued by BFIU under section 15 or knowingly provide any wrong information or false information or statement, the reporting organization shall be liable to pay a fine determined and directed by BFIU, not exceeding BDT 2,500,000.00 (Twenty Five Lac) and Bangladesh bank may suspend the registration or license with a purpose to close the operation of the agency/organization or any branch, service centre, booth or agent of the organization within Bangladesh or where applicable, shall inform the registration/licensing authority about the subject matter to take appropriate action against the organization.

1.15 Why we must combat financing of terrorism?

- Financing terrorism was criminalized under United Nations International Convention for the Suppression of the Financing of Terrorism in 1999. To reinforce the 1999 Convention, United

Nations adopted UNSC Resolutions 1373 and 1390 directing member states to criminalize the Financing of Terrorism and adopt regulatory regimes to detect, deter and freeze terrorists' assets. The resolutions oblige all states to deny financing, support and safe harbor for terrorists.

- Bangladesh has actively involved in multinational and international institutions. Our international relationship and business, banking business in particular are regulated by some domestic and international regulations. So it is mandatory to abide by those regulations. The Financial Action Task Force (FATF), the independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction has revised their previous recommendations and adopted revised 40 recommendations. The revised FATF 40 (forty) Recommendations are recognized as the global anti-money laundering (AML) and combating the financing of terrorism (CFT) standard. Adoption of the revised recommendations demonstrates countries' shared commitment to fight money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction. So we must be involved in international effort to combat the Financing of Terrorism.
- It is increasingly evident that terrorists and their organizations need to raise significant amounts of cash for a wide variety of purposes for recruitment, training, travel and materials as well as often payment for protection of their safe heaven. So to root up terrorism, we must stop the flow of funds that keep them in business.
- The consequences of allowing the financial system to facilitate the movement of terrorist money are so horrendous that every effort must be made to prevent this from happening. So preventing money laundering and combating the financing of terrorism is not only the regulatory requirement but also an act of self interest.

1.16 The Link between Money Laundering and Terrorist Financing

The techniques used to launder money are essentially the same as those used to conceal the sources of and uses for terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected. As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets of organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

1.17 What is Proliferation Financing?

Proliferation is the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services or expertise.

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

1.18 Targeted Financial Sanctions (TFS)

- The term Targeted Financial Sanctions (TFS) means both asset freezing and prohibition to prevent funds on other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. This TFS is a 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.
- 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 under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)'.
- 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 under Chapter VII of the Charter of the United Nations'.

1.19 Prevention of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction

a. Bank shall establish a procedure by the approval of Board of Directors for detection and prevention of financing of terrorism and financing in 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.
b. If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, bank shall send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to BFIU immediately.
c. Bank should preserve in electronic form the updated list of individuals and entities that are involving in the activities of financing of terrorism and financing of proliferation of weapons of mass destruction issued by UNSCR.
d. Bank should review the transaction to identify whether the concerned parties of those 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. Bank should preserve "False Positive" information. 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. (False Positive is a situation whereby a freeze action is taken on the basis of available information and upon further inquiry and receipt of additional clarifying information, such freeze action is determined not to be the correct course of action. An example is a freeze action taken on the basis of mistaken identity)

CHAPTER 02

OBJECTIVE, SCOPE AND EXCEPTION OF POLICY

2.1. Policy Overview

Money Laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities. Terrorist financiers also try to use banking channel to transfer funds concealing their ill motive. Banking System worldwide is susceptible to channeling of funds for such activities.

In conducting business with due skills, care and diligence, the bank should comply with relevant laws, rules, regulations, codes and standards of good practice and anti money laundering & financing of terrorism prevention procedures should be strictly followed. The reason is that the bank employees shall personally be liable if any deviation is found in his/her assigned duties.

National Bank recognizes the fight against money laundering and financing of terrorism as a team effort and has drawn a policy in line with the Money Laundering Prevention Act, 2012 (Amendment, 2015), the Anti Terrorism Act, 2009 (Amendment, 2012 and 2013), Guidance Notes on Prevention of Money Laundering, Money Laundering & Terrorist Financing Risk Management Guidelines and circulars/guidelines issued by BFIU from time to time to combat this threat. So the bank's AML/CFT Policy guidelines will apply to all branches, sub-branches, concerned divisions, subsidiaries (where applicable) and all officers as the official guideline for anti money laundering and combating the financing of terrorism.

2.2. Policy Objective

Broad Objective

To ensure that a system is established within which money laundering and terrorist financing control is managed through stringent and appropriate procedures and the reporting of suspicious transactions and activities, in order to discharge our legal duties.

Specific Objective

Apart from these broad objectives, the specific objectives are:

i. To build up awareness amongst the staff;
ii. To focus on methods of Prevention of Money Laundering and Combating Financing of Terrorism;
iii. To prevent the Bank's products or services from being used as a channel for Money Laundering and Terrorist Financing;
iv. To prevent damage to the Bank's name and reputation by associating with money launderers or terrorists;
v. To ensure that the Bank complies with anti money laundering and preventing terrorist financing legislation/regulations;
vi. To assist regulators/law enforcement agencies in their efforts to investigate and track money launderers & terrorists.

2.3. Policy Scope

This policy addresses the responsibility of management and employees for:

- Implementation of policies, procedures and guidelines;
- Compliance Structure;
- Customer Acceptance Policy (CAP);

- Customer Due Diligence (CDD) & Customer identification and verification process ("Know Your Customer");
- Beneficial Ownership;
- Non face to face customer;
- Correspondent banking;
- IPs, PEPs, DNFBPs;
- Use of Sanction Screening Software;
- Measures to prevent Trade based & Technology based money laundering;
- Monitoring of accounts, activities;
- Preventing, detecting, monitoring and reporting suspected, unusual, confirmed, detected money laundering and terrorist financing issues; (STR/SARs);
- Money laundering and terrorist financing control training & awareness;
- Record keeping.

2.4. Policy Statements

The bank shall not allow its system to be abused by Money Launderers and Terrorists. In order to safeguard against the risk of money laundering and terrorist financing, the following measures are the minimum standards to be observed while conducting banking business:

- To maintain a written AML and CFT policy and related procedures in line with existing local laws & regulations, BFIU's guidelines, international standards and apply it to all business units;
- To build AML/CFT compliance structure as per requirement of competent authorities;
- To provide the CAMLCO and DCAMLCO at Head Office with all reasonable access to information that may be of assistance to him in carrying on his duties;
- To ascertain customer identity before opening an account and/or making an account operational;
- To obtain all account opening documentation requirements as per law;
- To apply appropriate screening process while on boarding the customers;
- To apply Enhanced due diligence for high-risk customers;
- To conduct CDD while serving walk-in customer;
- To maintain correspondent banking relationship with due processes like conducting CDD, EDD & KYC renewal, adverse media screening etc. for maintaining such relationship;
- To report cash transaction to BFIU for the transaction that beyond an upper threshold as fixed by them from time to time;
- To train up the staff on AML & CFT policies and new AML & CFT laws and regulations;
- To retain all the documents related to customers & transactions for a period specified as per local laws in each jurisdiction;
- To maintain a system of internal controls to ensure ongoing AML & CFT compliance by a designated person(s) and take appropriate action, once suspicious transaction/activity is detected, a proper and thorough process for filing STR/SAR is followed as per the requirements of BFIU and applicable laws;
- To comply with the Bank's AML & CFT policies monitored through a combination of internal audit, external audit and regulatory reviews of compliance with relevant anti-money laundering legislation and/or regulations;
- To ensure co-operation and assistance to the relevant law enforcing authorities and the regulator in Bangladesh as per laws;
- To work with industry bodies to promote the highest standards of AML/CFT across the financial service industry.

It is the policy of the Bank to comply with all the provisions of the Money Laundering Prevention Act, 2012 (Amendment, 2015), Anti Terrorism Act, 2009 (Amendment, 2012 and 2013) and other relevant instructions, guidelines and regulations by implementing the same and subsequent procedures.

2.5. Enforcement

As part of risk management, Bank will review the policy from time to time and amend or revise it, if applicable.

Changes to this policy require approval of the Board of Directors. Changes in operating procedures, standards, guidelines and technologies may be authorized by the MD and CAMLCO provided they are consistent with this policy.

The Board of Directors has the authority to approve this policy, and any amendments thereafter. Senior Management is responsible for ensuring the directives implemented and administered in compliance with the approved policy.

Any conflicts in interpretation of this policy should be submitted immediately to the CAMLCO and DCAMLCO for ruling.

2.6. Exceptions to the Policy

Requests for exceptions to this policy must be very specific and may only be granted on specific items, rather than to entire sections. Bank personnel with exceptions are to communicate their requests to the CAMLCO or DCAMLCO.

2.7. Procedures

As financial organizations are committed to prevent money laundering and terrorist financing, the management of National Bank Ltd. (NBL) has taken a strong AML/CFT compliance program. Few activities of the AML/CFT compliance program are:

a) Managing Director shall communicate clearly with all employees on an annual basis by issuing a statement that clearly sets forth its policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities;

b) A Central Compliance Committee (CCC) shall be formed to formulate organizational strategy and program to prevent money laundering, terrorist financing & proliferation financing activities;

c) A High Official with sufficient knowledge and experience shall be nominated as Chief Anti Money Laundering Compliance Officer (CAMLCO) who will be the head of CCC. In this case, 'High official' will be considered as an official whose rank must not be lower than 2 (two) steps of the Managing Director. Another official shall be nominated as deputy of the CAMLCO who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO). The DCAMLCO shall be at least in the rank of 'Senior Vice President' of the bank;

d) Central Compliance Committee (CCC) shall nominate one experienced officer as BAMLCO from each branch. The manager, the second man of the branch shall be nominated as the BAMLCO;

e) BAMLCO shall be the main point of contact and all suspicious activities of the branch are to be reported to him/her directly by the concerned officials of the branch. He/she shall oversee the day-to-day activities at the branch and confirm compliance with BFIU and Head Office instructions;

f) Branch shall form a committee namely Branch Compliance Unit (BCU) headed by BAMLCO consisting with at least four members who will assist BAMLCO to confirm the Compliance in line with AML/CFT activities of the branch;

g) The uniform account opening form including Know Your Customer (KYC) Profile and Transaction Profile (TP) is an integral part of an account relationship. This is mandatory and a vital reference point to all account relationships;

h) Sanction screening software shall be used before opening a new account or giving service to walk-in customer(s) & existing customer(s) to ensure that the identity of the customer(s), beneficial owner(s) and authorized person(s), if any, does not match with terrorists or terrorist organizations as per BFIU sanction list, UN List, OFAC List, Local sanction list etc.

i) Appropriate customer identification, record keeping and reporting are primary points of consideration. In line with MLPA, 2012 (Amendment, 2015) and ATA, 2009 (Amendment, 2012 and 2013), the Bank shall keep all related documents/records for a minimum of 5 (five) years after closure of an account. Relevant records of Walk-in customers should also be preserved for at least five years from the date of such transaction;

j) Anti Money Laundering Division (AMLD) shall regularly collect information/statements from branches as per requirement of competent authorities and issue various circulars to the branches related to AML/CFT;

k) Workshops and Seminars shall regularly be arranged by AMLD and NBTI to keep the workforce up to date with the skills of AML/CFT procedures;

l) Bank shall have the following features in the Core Banking System (CBS):

   i. Customers' information in line with the Uniform A/C Opening form, KYC Profile and Transaction Profile forms provided by BFIU & competent authorities;
   ii. Customers' Risk Assessment on the basis of risk matrix provided by BFIU in the KYC Profile form;
   iii. Introduction of Alert System for the transaction that exceeds the amount declared in transaction profile (TP);
   iv. Auto generation of list/statement of accounts that have been transacted violating the transaction profiles;
   v. Preservation of records of customers for at least 5 (five) years after closing of account;
   vi. Assimilation of information of customers' multiple accounts under a common CIF number;
   vii. Option for searching accounts of customers or any other person as asked by domestic law enforcing agencies, regulatory authorities as well as international organization/agencies such as UN Sanction List, OFAC, EU List etc;
   viii. Option for cross-checking of a new customer's information with the list of persons against whom sanctions have been imposed by domestic and international agencies before inducting him or her as a customer of the bank;
   ix. Option for screening new, existing, potential and Walk-in-Customer with local, UN, OFAC, EU sanction list;
   x. Features mentioned in "Guidelines on Core Banking Solution (CBS) Features and Controls" issued by Bangladesh Bank.

m) Leaflets/handbills shall be printed and distributed among the customers or Banner/Fastoon shall be hung at branch premises to create awareness explaining the laws, regulations and penalties for money laundering and financing of terrorism offences;

n) International Division shall collect AML/CFT Questionnaire from correspondent banks with which bank has a relationship and send it to AMLD for preservation;

o) Branch shall conduct "Self Assessment Report" of its own on a half yearly basis and submit the report to AMLD and Internal Control & Compliance Division (ICCD) in time;

p) During yearly comprehensive audit program, ICCD, Head Office shall examine AML/CFT compliance status of branches and conduct "Independent Testing Procedures" and submit the report to AMLD and respective branches;

q) AMLD shall visit branches to assess the AML/CFT compliance status on a regular basis.

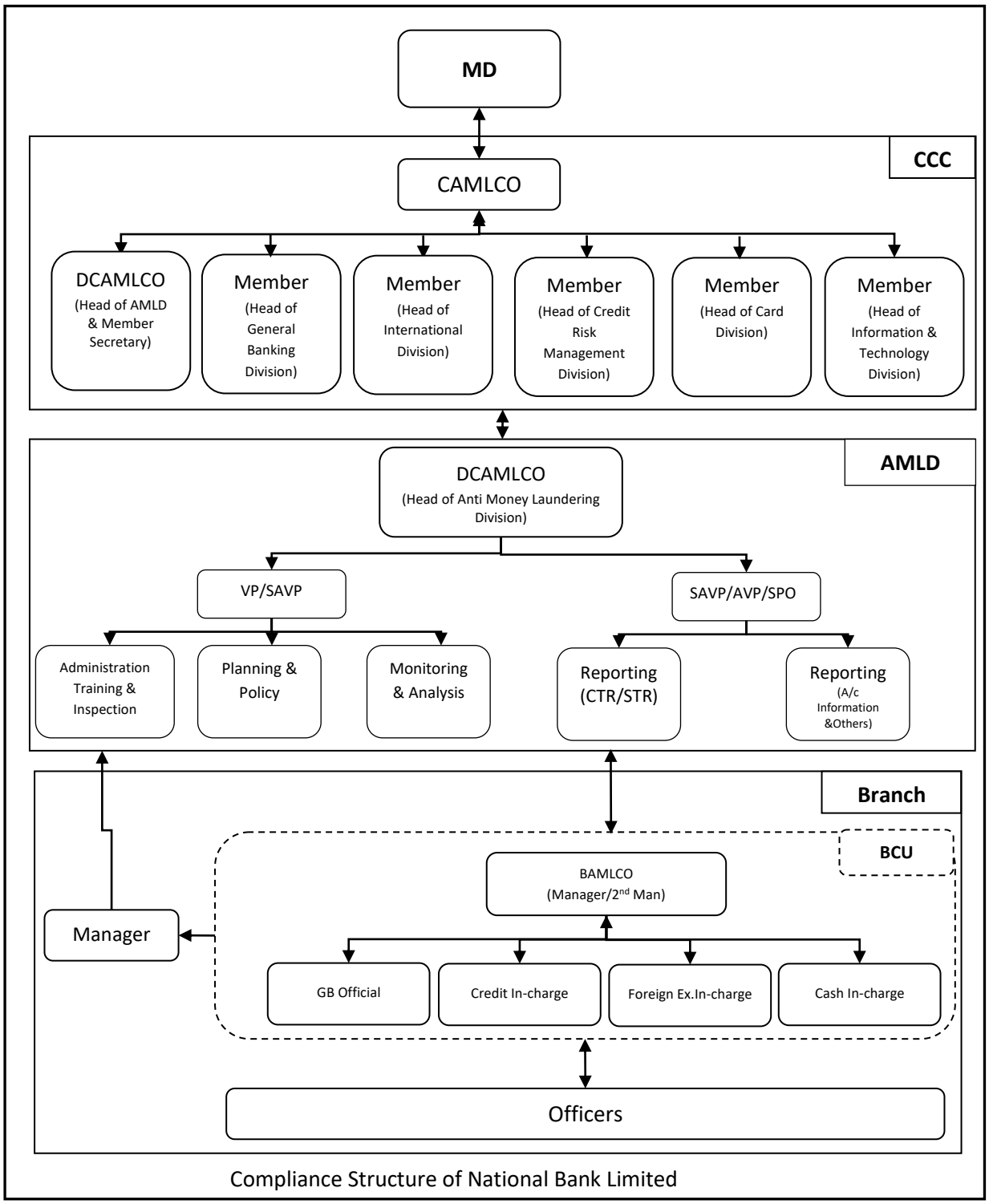
Compliance is the responsibility of each employee. Therefore, all guidelines related to AML/CFT shall be regularly updated and circulated and ensured that all staffs are aware of the local AML/CFT laws, internal guidelines and other policies and procedures. AMLD shall monitor the Bank's AML/CFT policies, domestic laws, international standard, guidelines and instructions of BFIU through a combination of internal audit and CCC.

CHAPTER 03

COMPLIANCE STRUCTURE OF NATIONAL BANK LIMITED

3.1. Compliance Structure

Compliance is a comprehensive program that helps institutions and their employees to conduct operations and activities ethically; with the highest level of integrity, and in compliance with legal and regulatory requirements. In order to ensure compliance, National Bank has developed a Compliance structure to ensure effective implementation of AML/CFT programs.



Compliance Structure of National Bank Limited

Note: Inclusion of any member in CCC can be done by the approval of MD.

3.2. Roles and Responsibilities of Board of Directors

The Board of Directors (Board) has the following roles and responsibilities:

- Understand the AML/CFT measures required by the laws including the MLPA, 2012 & ATA, 2009 and the industry's standards and best practices as well as the importance of implementing AML/CFT measures to prevent the bank from being abused by money launderers and financiers of terrorism;
- Understand their roles and responsibilities in managing ML/TF risks faced by the bank as reporting institution;
- Must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services;
- Maintain accountability and oversight for establishing AML/CFT policies and minimum standards;
- Approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;
- Establish appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the bank's products and services, technology as well as trends in ML/TF;
- Establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the bank;
- Define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;
- Ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;
- Assess the implementation of the approved AML/CFT policies through regular reporting and updates by the Senior Management and Audit Committee; and
- Establish MIS that is reflective of the nature of the bank's operations, size of business, complexity of business operations and structure, risk profiles of products and services of offered and geographical coverage.

3.3. Roles and Responsibilities of Managing Director & Senior Management

The roles & responsibilities of Managing Director & Senior Management are to:

- Understand the AML/CFT measures required by the laws including the Money Laundering Prevention Act, 2012 & Anti Terrorism Act, 2009 along with their amendments, BFIU Circulars & circular letters;
- Be aware of and understand the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;
- Formulate AML/CFT policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the bank and its geographical coverage;
- Establish appropriate 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;

- Undertake review and propose to the Board the necessary enhancements to the AML/CFT policies to reflect changes in the bank's risk profiles, institutional and business structure, delivery channels and geographical coverage;
- Provide timely periodic reporting to the Board on the level of ML/TF risks facing the bank, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which may have an impact on the bank;
- Convey a clear signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service;
- Allocate adequate resources to effectively implement and administer AML/CFT compliance programs that are reflective of the size and complexity of the bank's operations and risk profiles;
- Appoint a chief anti-money laundering compliance officer (CAMLCO) at Head Office;
- Ensure that bank's HR Policy includes at least following issues for proper implementation of AML/CFT measures:
    i. Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML/CFT measures;
    ii. Proper weight shall be given in the annual performance evaluation of employees for extra ordinary preventive action vis-à-vis for non-compliance;
    iii. Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;
    iv. Other measures that shall be taken in case of non-compliance by the bank;
- Ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees;
- Ensure that AML/CFT issues raised are addressed in a timely manner;
- Inform BFIU about the change of CAMLCO without any delay;
- Ensure that the Bank has a comprehensive and effective AML/CFT compliance program and its implementation;
- Managing Director shall announce effective and specific commitment, give the necessary instructions to fulfill the commitments in preventing ML & TF to all the employees of all branches, agent offices, regional offices and the head office and shall ensure the implementation of the commitments. This statement of commitment shall be issued in every year. The followings matters should be included in the Statement of commitment:
    - ✓ 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.

3.4. Formation of Central Compliance Committee (CCC)

Bank shall establish a Central Compliance Committee (CCC) in the Head Office of the bank headed by a high official who will be known as Chief Anti Money Laundering Compliance Officer (CAMLCO) and the Committee shall directly report to the Managing Director.

The bank may also nominate at least one deputy of the CAMLCO, who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO). The DCAMLCO shall be at least in the rank of 'Senior Vice President' of the bank. DCAMLCO shall perform the secretarial duty of the Committee.

CCC shall be formed with at least 7 (Seven) members from the divisional head or senior level officers of different divisions (General Banking Division, International Division, Credit Risk Management Division, Human Resource Division, Card Division, Information & Technology division) along with CAMLCO & DCAMLCO.
Official of ICCD shall not be included in CCC. CCC & I CCD shall perform their own duties related to AML/CFT separately.

3.5. Responsibilities of Central Compliance Committee (CCC)

CCC's main responsibilities are:

- Formulating organizational strategy and program regarding internal control policies and procedures to prevent money laundering, terrorist financing & proliferation financing activities and ensuring the coordination, implementation and review of the same in the Bank;
- Submitting a report on the strategy undertaken for prevention of ML & TF, implementation status of the same to the Managing Director on half yearly basis (January-June, July-December) for onward submission with specific recommendation to the Board of Directors and sending a copy of the report to BFIU;
- Developing circulars regarding transaction monitoring, internal control management, policies and procedures to prevent ML & TF and monitoring the branches to follow the circulars;
- Managing branch's internal compliance and control by appointing BAMLCOs in branches as per section 3.11 of this guidelines and assigning specific written responsibilities to them;
- Arranging meetings for at least four (4) times in a year on quarterly basis to review the overall condition regarding AML/CFT. But CAMLCO can call meeting any time, if necessary;
- Coordinate banks' AML/CFT compliance initiatives;
- Coordinate the ML & TF risk assessment of the bank and review thereon;
- Impart training, workshop, seminar related to AML/CFT for the employee of the bank;
- Taking required measures to submit information, report or documents in time.
- Requisition of human resources and logistic supports for CCC;
- Making suggestion or administrative sanction for non-compliance by the employees;
- Evaluating overall monitoring process and adaptation of changes of rules/regulations and instructions of BFIU and international standards;
- Ensuring the Bank's AML/CFT policies and Risk Assessment & Risk Management Guidelines are complete and up-to-date; maintain ongoing awareness of new and changing business activities & products and identify potential compliance issues that should be considered by the Bank;
- Ensuring the correspondent relationships, trade based transactions, remittance, technology related services and launching new products are maintained as per instructions & guidelines of BFIU;
- Ensuring overseas branches and subsidiaries' activities are in accordance with MLPA, ATA and circulars of BFIU;
- Performing any other responsibilities as instructed by BFIU from time to time.

3.6. Appointment of CAMLCO

The Managing Director shall appoint the CAMLCO at Head Office with sufficient authority to implement and enforce corporate wide AML/CFT policies, procedures and measures and who shall report directly to Managing Director. The CAMLCO shall be an official who is not below than 2 (two) rank from the Managing Director. He/she should 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.

Before assigning any other duties to the CAMLCO of the bank, the management has to be ensured that this will not hamper the AML/CFT activities of the bank. If the CAMLCO is changed, it must be informed to BFIU without delay.

3.7. Authorities & Responsibilities of CAMLCO

Chief Anti Money Laundering Compliance Officer (CAMLCO) must have sufficient authority to implement and enforce corporate wide AML & CTF policies, procedures and measures and who will report to MD & CEO. The CAMLCO is responsible for oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering and terrorist financing.

Authorities of CAMLCO:

- CAMLCO should be able to act on his own authority;
- He/she should not take any permission or consultation from/with the MD before submission of STR/SAR and any document or information to BFIU;
- He/she can access to any information of the bank;
- He/she shall ensure his/her continuing competence.

Few of the responsibilities are to:

- Take all the responsibilities as head of CCC;
- Ensure overall AML/CFT compliance of the bank;
- Oversee the submission of document or information to BFIU in time;
- Maintain the day-to-day operation of the bank's AML/CFT compliance;
- Be liable to MD or BoD for proper functioning of CCC;
- Review and update ML & TF risk assessment & management of the bank;
- Ensure that corrective actions have taken by the bank to address the deficiency identified by the BFIU;
- Act as central point of contact for communicating with the regulatory bodies regarding issues related to the bank's AML/CFT program;
- May choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions.
- 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;
- Monitor changes of laws/regulations and directives of BFIU & other regulators that may require revisions to the Policy, and making these revisions;
- Assist in review of control procedures in the Bank to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
- Oversee all other issues that may arise from time to time regarding ML, TF & PF.

3.8. Appointment of Deputy CAMLCO

Deputy CAMLCO shall not be an official who has lower rank than 'Senior Vice President' of the bank.

He/she should have detail knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML, TF & PF.

As the Deputy CAMLCO 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,

He/she shall also have vast knowledge & experience on general banking, investment/credit and foreign exchange business of the bank.

3.9. Authorities & Responsibilities of Deputy CAMLCO

The authorities & responsibilities of Deputy CAMLCO shall be same as the authorities & responsibilities of CAMLCO but he/she must discharge his/her authorities and responsibilities under command, control & supervision of CAMLCO. Moreover, he/she shall perform routine works in absence of CAMLCO. Few of the responsibilities are to:

- Report directly to the CAMLCO;
- Perform the secretarial duty of CCC and take necessary measures to execute the directives of CCC;
- Perform duty as the in-charge of AMLD;
- Coordinate and monitor day to day compliance with applicable money laundering laws, rules and regulations, this guideline, NBL's practices, procedures and the controls required to be implemented in this regard;
- Respond to compliance questions and concerns of the staff and advise regions/branches and assist in providing solutions to potential issues involving compliance and money laundering risk;
- Arrange training for all staffs, especially for the compliance personnel;
- Participate in the development, testing and training and implementation of new or enhanced system applications for smooth monitoring of transaction;
- Participate in the development, implementation and/ or maintenance of processes and procedures to ensure Anti-Money Laundering compliance with regulatory guidance;
- Provide advice and guidance to Branches and Subsidiaries with regard to AOF, Customer Due Diligence and KYC;
- Maintain and improve the process of identifying and reporting STR/SAR etc;
- Support in review Policies, Process and Guideline in compliance with updated regulations;
- Conduct surprise inspection on Branch;
- Conduct investigation on KYC, ML, and TF issues assigned by Senior Management;
- Prepare report for Senior Management as per Regulatory / internal requirement;
- Respond to queries from BFIU;
- Support in BFIU Audit procedure and compliance thereof.

3.10. Formation & Responsibility of Anti Money Laundering Division (AMLD)

"Anti Money Laundering Division" shall be consisted of sufficient number of employees under supervision of CCC. Deputy CAMLCO shall serve as head of this Division. Employees of AMLD must have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and bank's own policies & guidelines on preventing Money Laundering, Terrorist Financing & Proliferation Financing.

Few of the responsibilities are:

i. Under Supervision of CCC and CAMLCO, AMLD shall ensure the implementation of the yearly programs regarding Prevention of Money Laundering and Combating the Financing of Terrorism;
ii. As per instruction of CCC/CAMLCO, AMLD shall issue circulars in which customer acceptance policy, transaction monitoring system, internal control management and other compliance policy & procedure for preventing ML & TF shall be included;
iii. AMLD shall prepare a checklist based evaluation report of branches based on Self Assessment Report that are received from the branches and based on inspection/audit reports that are received from ICCD, Head Office as per section 11.6.3 of this guidelines;

iv. Based on the Self Assessment report received from the branches, if there is any risky matter observed in any branch, AMLD have to inspect immediately that branch or initiate inspection through ICCD and it should be brought to the notice of CAMLCO/Competent Authority;
v. AMLD shall arrange inspection to the branch that is vulnerable to ML & TF risk & take necessary measures to improve the situation;
vi. AMLD shall report CTR to BFIU on monthly basis;
vii. AMLD shall monitor the CTR to identify suspicious transaction;
viii. AMLD shall submit the STR/SAR to BFIU through goAML;
ix. AMLD shall supervise the branch whether due diligence are being rendered specially in case of accounts of PEPs, IPs and Chief or Higher Management of any International Organization;
x. AMLD shall conduct training courses, workshops and seminars for development of compliance knowledge & awareness among the officials regarding Money Laundering, Terrorist Financing;
xi. AMLD shall arrange AML/CFT related training/workshops for BAMLCO at least every alternative year to inform the updates of AML/CFT issues.
xii. AMLD shall monitor any other issue that may arise from time to time regarding ML, TF & PF;
xiii. AMLD shall perform any other responsibilities as instructed by BFIU and CCC from time to time.

3.11. Appointment of Branch Anti Money Laundering Compliance Officer (BAMLCO)

CCC shall appoint the Branch Anti Money Laundering Compliance Officer (BAMLCO) for each branch; Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her appointment letter.
Branch shall nominate an officer as BAMLCO with filling up a specified format (See Annexure: E) and inform AMLD for initiating the appointing process. Either Manager or Second man of the branch (preferably Manager) shall be nominated as the BAMLCO. If existing BAMLCO changed due to any reason i.e. transfer, retire, resign etc, Branch shall nominate an officer as BAMLCO immediately.
The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and NBL's policy guidelines on preventing Money Laundering, Terrorist Financing & proliferation financing. BAMLCO will be the first point of contact for any AML/CFT issues of the branch.

3.12. Responsibilities of BAMLCO

Few of the responsibilities of BAMLCO are given below:

i. Arrange AML/CFT meeting with all officials of the branch quarterly and shall take effective measures on the following matters after reviewing the compliance according to existing acts, rules and regulations, BFIU's instructions & Head Office instructions on preventing Money Laundering & Terrorist Financing:
   - Know Your Customer (KYC).
   - Transaction Monitoring.
   - Identifying and reporting of Suspicious transaction
   - Local & international sanction list.
   - Self assessment procedures.
   - Record Keeping
   - Training etc.
ii. Inform/update to all the officials of the branch regarding laws, circulars, Policies, guidelines and ensure its meticulous compliance;
iii. Ensure that the KYC of all customers have done properly;

iv. Take necessary measures to review and update the KYC of the customer in every five years in case of low risk customers and in every year in case of high risk customers. Besides, KYC information may be needed to update anytime if there is any particular necessity arise;
v. Verify the logical consistency between the Transaction Profile (TP) and customer's Profession, source of fund & wealth;
vi. Verify the source of fund and profession of the customer has been taken elaborately in every account;
vii. Keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance as per section 5.3(l) of this guidelines; Take initiative to update the accounts immediately which do not have proper KYC, TP, risk grading and required documents;
viii. Ensure that branch officials are conducting CDD while opening of account, conducting transactions, serving walk-in customers and closing a relationship;
ix. Ensure Sanction Screening Software are being used before opening of account and while making transaction;
x. Operate Sanction Screening Software as an authorizer;
xi. Ensure regular monitoring for all transactions including foreign remittance transactions, trade transactions, credit related transactions in order to find out suspicious transactions. This record should be kept properly;
xii. Review CTR to find out STR;
xiii. Review Structuring Report to find out structuring;
xiv. Review TP exception list and take proof/justification for the transactions. If it seems suspicious then report STR;
xv. Monitor High Risk accounts;
xvi. 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;
xvii. Identify Suspicious transaction/activity and report to AMLD;
xviii. Ensure that all the employees of the branch are well aware and capable to identify any suspicious transaction or any attempt of suspicious transaction;
xix. Prepare the Self Assessment Report along with Manager in half yearly basis where true picture has to be reflected and send the report to AMLD & ICCD as per section 11.6.1 of this guidelines. BAMLCO shall discuss about the self assessment report in the quarterly meeting;
xx. Take initiatives to rectify the lapses/irregularities found in the Self Assessment Report;
xxi. Maintain AML/CFT files (See section 13.2 of this guidelines) properly;
xxii. Accumulate the training records of branch officials and take initiatives to train the officers regularly through AMLD;
xxiii. Ensure for keeping records of closed accounts (along with KYC & TP)/vouchers/registers/other documents for minimum for 5 years;
xxiv. Ensure that all the reporting information and document are submitted properly to AMLD and any freeze order or stop payment order are implemented properly & immediately;
xxv. Ensure that corrective actions have taken by the branch to address the deficiency identified by BFIU & ICCD;
xxvi. Ensure that all tasks are done according to this guideline and that shall reflect in Independent Testing Rating (prepared by ICCD);
xxvii. Involve the manager in AML/CFT compliance program if branch manager is not BAMLCO;
xxviii. Perform any other responsibilities as instructed by BFIU and AMLD from time to time.

3.13. Formation & Responsibility of Branch Compliance Unit (BCU)

Every branch shall establish a Branch Compliance Unit (BCU) that shall be formed with at least 4 (four) members including BAMLCO, GB Official, Credit In-charge, Cash In-charge. In case of AD branch, Foreign Exchange In-charge has to be included in the unit along with the other four members. BCU will be headed by BAMLCO. BCU will ensure the overall compliance of AML/CFT issues at the branch level.

BCU's main responsibilities:

i. Support BAMLCO in performing his/her duty & responsibilities;
ii. Ensure implementation of AML/CFT instructions of this Guideline at branch;
iii. Be familiar with laws, regulations, policies, guidelines related to AML/CFT;
iv. Inform all other officers & executives about laws, regulations, policies, guidelines related to AML/CFT;
v. Ensure all account's TP & KYC profile are updated;
vi. Monitor High risk account;
vii. Monitor the foreign remittance transaction;
viii. Review cash transaction to find out structuring;
ix. Ensure regular transaction monitoring to find out suspicious transactions;
x. Ensure improvement of branch rating.
xi. Perform any other responsibilities as instructed by BFIU and AMLD from time to time.

3.14. Roles & Responsibilities of Officials at branch

Officers' role is very important because they directly related with the day to day transactions. The role & responsibilities of the officers are (not limited to):

Officer	Role/Responsibilities
Branch Manager	▪ Understand & Inform all officers & executives regarding AML/CFT laws, circulars and guidelines; ▪ Support BAMLCO & BCU to perform their duties; ▪ Ensure AML/CFT activities of the branch are not hampered before assigning other duties to the BAMLCO; ▪ Take initiative to train all officers & executives through AMLD; ▪ Overall responsibility to ensure that the branch has an AML/CFT compliance program in place and it is working effectively.
Account Opening Officer	▪ Perform Customer due diligence on prospective customers prior opening an account and perform Enhanced due diligence (EDD) for high risk customer; ▪ Collect all documents as per requirement; ▪ Complete the KYC Profile for the new customer and update KYC for existing customers; ▪ Ensure screening for all types of customer; ▪ Escalate any true match hit of sanction screening to BAMLCO; ▪ Be diligent regarding the identification of beneficial owner(s) of an account; ▪ Input accurate & complete information of customer in the system; ▪ Ongoing monitoring of customer transaction activity especially for high risk customers; ▪ Escalate any suspicion to BAMLCO.

Cash Officer	▪ Obtain proof of the source of fund for large transaction which is not matched with customer's profession/business; ▪ Conduct Simplified Customer Due Diligence (SCDD) for occasional transaction below Taka Five lac by walk-in customer; ▪ Conduct Customer Due Diligence (CDD) for occasional transaction of Taka Five lac and above by walk-in customer; ▪ Identify structuring; ▪ Escalate any suspicion transaction/activity to the BAMLCO.
Sub-Branch Incharge	▪ Establish internal monitoring and control system related to AML/CFT under the supervision of Controlling Branch's BAMLCO.
Foreign Exchange Desk Officer	▪ Understand and follow the instruction of BB, BFIU, NBL's Policies, guidelines, circulars & circular letters etc. ▪ Follow the instructions of 'Guidelines for Prevention of TBML of National Bank Limited'.
All Officers	▪ Follow the instruction of BAMLCO; ▪ Get knowledge regarding existing acts, rules and regulations, BFIU's instructions and NBL's AML/CFT policy guidelines; ▪ Be aware of the risk associated with money laundering & terrorist financing; ▪ Conduct CDD where suspicion arise; ▪ Monitor transaction to find out STR; ▪ Escalate any suspicion to the BAMLCO.

3.15. Roles & Responsibilities of Internal Control & Compliance Division (ICCD)

Internal Control and Compliance Division (ICCD) of the bank shall play an important role for ensuring proper implementation of bank's AML/CFT Compliance Program. Bank shall ensure that ICCD is well equipped with enough manpower and autonomy to look after the prevention of ML, TF & PF. The roles & responsibilities are to:

- Oversee the implementation of the AML/CFT compliance program of the bank;
- Execute instant inspection if any risk is found during evaluation of self-assessment report of any branch and report to the AMLD about the inspection;
- Review the 'Self Assessment Report' received from the branches and report to AMLD;
- Execute the 'Independent Testing Procedure' using specified checklist (see Annexure: G) during conducting annual inspection program to different branches;
- Conduct inspection at least 10% of total branches in addition to regular annual inspection for monitoring the money laundering & terrorist financing according to specified checklist (see Annexure: G);
- Sending the copy of each independent test report with rating to AMLD & respective branch;
- Assess the knowledge of the employees about AML/CFT;
- 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;

- Where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;
- 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:
  - The importance of the board and the senior management place on ongoing education, training and compliance;
  - 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.

3.16. Roles & Responsibilities of External Auditor

External auditor may also play an important role in reviewing the adequacy of AML/CFT controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External auditor would be risk-focus while developing their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits in its audit report.

CHAPTER 04

CUSTOMER ACCEPTANCE POLICY

4.1 Customer Acceptance Policy (CAP)

Customers are vitally important for banking business. Increasing competition is forcing banks to pay much more attention to satisfy customers. Our motto is to extend best services to our customers. We are also aware that sometimes customers pose the risk of money laundering and financing terrorism to the financial institutions, particularly to the banks. So the inadequacy or absence of KYC standards can result in serious customer and counterparty risks, especially reputation, operational, legal and concentration risks. The Management of the bank has developed the Customer Acceptance Policy as under:

a. No account in anonymous or fictitious name or account only with numbers shall be opened. Moreover, appropriate due diligence should be taken to block these types of accounts.

b. No account in the name of any person or entity listed under BFIU, UNSCR, OFAC, EU and other local sanction list or their close alliance on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government shall be opened or operated.

c. No banking relationship shall be established with a 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.)

d. Customer should be capable of making contract as per contract Act. In case of minor account, Legal guardian can operate the account of behalf of minor;

e. Branch shall not open an account or establish business relationship, where it is unable to apply appropriate customer due diligence (CDD) measures as per section 5.4 of this guidelines. But branch must be careful to avoid unnecessary harassment of the customer. Branch should follow the instruction as per section 5.7 of this guidelines if conducting the CDD measure is not possible. Where higher risks are identified branch should be required to follow Enhanced Due Diligence (EDD) as per section 5.8 of this guidelines to manage and mitigate the risks.

f. In case of opening a Politically Exposed Person's (PEP) or Influential Person's (IP) account, branch shall comply with the instructions as per section 5.9 of this guidelines. Such type of accounts shall be categorized as high risk and shall require very high level monitoring.

g. In case of establishing correspondent banking relationship, branch shall follow instructions meticulously as per section 5.11 of this guidelines.

h. Accounts for the non-resident Bangladesh citizens are to be opened subject to compliance of Foreign Exchange Regulation Act, 1947 and circulars issued by Bangladesh Bank under it.

i. Circumstances, in which a customer is permitted to act on behalf of another person/entity or when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity, must be in conformity with the established law and practice of banking and appropriate EDD to be applied;

j. It is important to bear in mind that the implementation of this customer acceptance policy must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

k. Branch shall follow AML/CFT laws, BFIU circulars & directives regarding AML/CFT, this guideline, instructions of AMLD & and any other instructions provided by BFIU & competent authority from time to time.

CHAPTER 05

CUSTOMER, KNOW YOUR CUSTOMER, CUSTOMER DUE DILIGENCE & OTHERS

5.1 Definition of Customer

A 'Customer' is defined as:

- A person or entity that maintains an account or has a business relationship with the bank;
- The beneficial owner of an account or business relationship; one on whose behalf the bank account is maintained directly or indirectly. [It has been discussed in detail at Section 5.15 of this guidelines];
- Professional intermediaries (Lawyer, Legal Consultancy Firm, Chartered Accountants etc) appointed to operate an account under the existing legal framework on behalf of the account holder, trust or beneficial owner;
- Any person or entity connected with a high valued occasional transaction or a financial transaction which may pose reputational or other risks to the bank e.g. a wire transfer or issue of a high value demand draft as a single transaction. In this case, "high value" will be considered if any transaction appears unusual in relation to normal transaction of the concerned person/entity's profession/profile;
- Any person or entity defined by BFIU from time to time.

5.2 Risk Based Approach:

- Bank will assess its own ML/TF risk at regular interval based on the instructions given by the BFIU in "ML/TF Risk Assessment Guidelines for Banking Sector''. The nature of the business, customer, product or service, country and geographical location etc. will be taken into consideration in assessing the said risk. This risk assessment report will be used to prevent the risk of ML&TF of the bank;
- According to the risk assessment report, Bank should take Enhanced Due Diligence measure in the cases where money laundering, financing of terrorism/terrorist risk are High;
- According to the risk assessment report, Bank should take Simplified Due Diligence in the cases where money laundering, financing of terrorism/terrorist risk are Low;
- Considering the existing customer's risk, importance and relevance, Bank will take necessary Due Diligence measures. Moreover, Bank will also determine when to conduct or review the due diligence for existing customers considering when due diligence were taken and what type or volume of information was collected previously.

5.3 Know Your Customer (KYC)

To collect & verify customer's identity information in order to manage Money Laundering & Terrorist Financing risk, the following matters should be ensured:

i. For opening customer's account, use the Account Opening Form issued by National Bank Limited. However, as the use of modern technology is more convenient, if applicable, use or take assistance from the modern technologies that are mentioned in the 'Guidelines on e-KYC' issued by BFIU. In case it is not possible to open an account using electronic means, use the hard copy of account opening form.

ii. Collect complete and accurate information for customer identification. To ensure that the banking system does not face the risk of money laundering or terrorist financing, understand the purpose of the customer's account opening and conduct the process of verifying customer identity information/data. Here, "Complete" refers to collection of all information for verifying the identity of the applicant or account holder. For example: name and detail

address of the person, profession, source of funds, Passport/National Identity Card/Birth Registration Certificate with acceptable ID card with photo, phone/ mobile number etc. "Accurate" refers to such complete information whose accuracy has been verified from reliable and independent source;

iii. If any person operate account on behalf of the customer, ensure that the person is properly empowered to operate the account and collect the accurate and complete information of that person;

iv. If an account is operated by trustees/professional intermediaries, collect accurate and complete information of all related persons after reviewing and verifying their legal aspects;

v. Follow the instruction as per section 5.14 of this guidelines for providing services to walk-in customer.

5.4 General Measures of Customer Due Diligence (CDD)

Customer Due Diligence (CDD) includes verifying the identity of the customer (person or entity) on the basis of information, data and documents obtained from reliable and independent sources, verifying the accuracy of the collected information or data and verifying the source of fund and on-going transaction monitoring. Mentionable that KYC is part of CDD. The following measures have to be ensured while conducting CDD:

a. Considering the risks associated with the customer, the CDD has to be performed during:
   i. Establishing business relationships;
   ii. Carrying out occasional transactions for Tk. 5,00,000 or more by Walk-in customer;
   iii. Occasional transactions through wire transfer by customer;
   iv. If there is doubts about the veracity or adequacy of previously obtained customer identification data;
   v. Providing trade finance and trade service facilities;
   vi. Realizing any suspicion of ML/TF, regardless of amount;
   vii. If there is a possibility of tipping-off during dealing with any transaction related to money laundering or terrorist financing, then STR/SAR should be reported without conducting CDD.
b. Collect sufficient information subject to satisfaction for ascertaining the identity of the customer, the underlying purpose of establishing relationship with the bank and the nature of business of the customer. It is to be noted that CDD should be reviewed on-going basis;
c. Conduct On-going CDD to identify inconsistencies of customer's business type, the level & type of risk and the source of fund. Existing data of high risk customers needs to be evaluated, reviewed or updated on a regular basis.
d. The accuracy of the identity information of the customer or the beneficiary owner should be verified at the time of establishing business relationship or after opening of account but before withdrawing money from that account. In case of Occasional customer, such action has to be taken while conducting the transaction. In cases where ML/TF risks are low or identified risk control measures are available or it is not need to be disrupted or closed business relationships, the accuracy of the identity information must be verified as soon as possible after the establishment of the relationship;
e. Identify the beneficial owner (see section 5.15 of this guidelines). Here, take reasonable measures to verify the identity of the beneficial owner based on the information or data obtained from reliable & independent sources;
f. Screen the name & information of customers, walk-in customers (sender/receiver), beneficial owners, owners/directors, authorized persons, related person/entities, countries, ports, point of transshipments, carriers, masters, agents, distributors, Merchants and third parties, if any, in the Sanction screening software before opening a new account or giving service to them to ensure that

the identity does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations as per BFIU sanction list, UN List, OFAC List, Local sanction list etc;

5.5 Simplified Customer Due Diligence (SCDD)

Simplified customer due diligence should be conducted in the following cases:

a. Branch shall collect the name, address and telephone number of the sender/applicant and receiver/beneficiary while making transaction of Walk-in customer amounting bellow taka fifty thousand;
b. Branch shall collect attested copy of photographed ID along with the name, address and telephone number of the sender/applicant/depositor/receiver while making transaction of Walk-in customer amounting taka fifty thousand to five lac;
c. Simplified customer due diligence should be conducted to open or manage low risk accounts i.e. Social Safety Net allowance account, Student account, farmer account and other No-Frill accounts for the purpose of financial inclusion. 'No Frills' account is a basic banking account, such account requires either nil minimum balance or very low minimum balance. Charges applicable to such accounts are low. Services available to such account are limited;
d. Simplified customer due diligence should be conducted to the customer as per instruction mentioned in "Guidelines on e-KYC" of BFIU.

5.6 Other instructions related to CDD:

The below instructions have to be followed during conducting CDD:

a. In case of opening of account, preserve all information & documents by conducting KYC & CDD. In this case, Branch will use Digital KYC form for the accounts which are opened through e-KYC system or Branch will use the KYC form circulated by NBL, Head Office from time to time if Digital KYC form is not possible to use. The KYC form will not be considered as a part of the Account Opening Form or Customer will not fill up the KYC form;
b. If a customer maintains more than one account then a Unique Customer Identification Code (UCIC) may be provided in order to avoid repetition of KYC and to make easier for monitoring transaction. This UCIC will help to track the services availed by customer and to monitor financial transaction of the customer;
c. To manage the ML/TF risk, the branch itself will determine the Transaction Profile (TP) of the customer's account. In this case, branch will determine a specific Transaction Profile based on the customer's past transactions (6/12 months transactions) and will monitor the customer's transaction based on the TP. Branch will investigate if any significant change is observed in customer's transaction compared to TP. Where applicable, Branch will correct the TP or submit STR/SAR for suspicion. In this case, Branch should be careful so that the customer must not be harassed;
d. In KYC procedures, Customer information update is a continuous process. Based on the risk grading of KYC form, Branch shall take necessary measures to review and update the KYC information of the customer in every five years in case of low risk customer and in every year in case of high risk customer. Any changes to the KYC information (e.g. changes in profession/business/ownership/transaction pattern etc) must be updated as soon as it is known. Besides, KYC information can be updated anytime if there is any particular necessity arises. Based on the updated information, it is necessary to reevaluate the risk of the account immediately. Besides, There should be a method to identify the accounts which are shifted from low risk to high risk;
e. Branch shall mark as Dormant to those accounts which were opened before 30 April, 2002 and are yet to update KYC procedures. No withdrawal should be permitted in those accounts;

however, deposit can be permitted. On written request of customer to Manager, these accounts will be fully functional after conducting proper CDD measures. AMLD should preserve data of such accounts at their end.

f. follow the guidelines of CDD as well as EDD measures for the customer in order to provide Privilege banking services to a customer;
g. Conduct EDD while establishing or maintaining a business relationship or conducting transaction with a person/entity (including legal representative, financial institution or any other institution) of the countries and territories 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 Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring mentioned in the Financial Action Task Force's Public Statement).
h. Before establishing a relationship with a foreign bank, Branch should take into consideration about the prevention of Money laundering and terrorist financing measures of the concerned country;
i. In case of opening accounts for foreigners & Non-Residence Bangladeshis (NRB); Foreign Exchange Regulation Act, 1947 and related circulars & guidelines issued by Bangladesh Bank, BFIU & NBL has to be followed along with the instructions of this guidelines;
j. Follow the instruction of "Guidelines for Prevention of Trade Based Money Laundering" in case of account or transaction related to foreign trade.

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, so that bank could not collect satisfactory information on customer identification and could not verify that, branch should take the following measures, if necessary:

a. Branch must not open account, must not start business relationship, or not carry out transaction for such customers or close the existing business relationship;
b. Branch shall preserve & send the information to AMLD regarding non-opening or closing of such accounts. If necessary, AMLD may take necessary action to make these information known to all other branches;
c. Branch may submit STR/SAR against such customer, potential customer, rejected person/entity, if applicable.
d. However, Branch will follow the guidelines of BFIU & NBL, if issued, for opening and managing the accounts of backward or special community.

5.8 Enhanced Due Diligence (EDD) measures

Any additional due diligence measures undertaken over and above the basic due diligence can be termed as Enhanced Due Diligence (EDD). In case of high risk customers, branches need to perform the following tasks in addition to Customer Due Diligence (CDD):

- Obtaining and verifying additional information of the customer from independent and reliable sources (e.g. occupation, volume of assets, information available through public databases, internet, etc.);
- Taking additional measures to ensure the reasons for opening account, the source of funds or source of wealth;
- Conducting on-going Enhanced Monitoring on transactions of the accounts;
- Obtaining approval from CAMLCO, if applicable, to commence or continue the business relationship.

5.9 Accounts of 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 Branch 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:

- Foreign PEPs;
- Influential Persons: IPs (known as Domestic PEPs) and
- 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 Branch should conduct Enhanced Due Diligence (EDD) in this scenario. However, EDD should be undertaken in case of Influential Persons: IPs (domestic PEPs) and PEPs of the international organization when such customer relationship is identified as higher risk.

5.9.1. Foreign PEPs

PEPs refer to "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."

The following individuals of other foreign countries must always be classed as PEPs but not limited to:

i. Heads and deputy heads of state or government;
ii. Ministers, deputy or state ministers and assistant ministers;
iii. Members of parliament and/or national legislatures;
iv. Members of the governing bodies of major political parties;
v. Senior politicians;
vi. Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
vii. Members of court of auditors or the boards of Central banks;
viii. Ambassadors, chargés d'affaires or other senior diplomats;
ix. Heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
x. Head or the senior executives or members of the administrative, management or supervisory bodies of state-owned enterprises
xi. Chief, directors, deputy directors and members of the board or equivalent function of an international organization.

Branch need to perform the following instructions along with CDD measures:

i. Branch shall gather appropriate information through publically open source or different database or other reasonable means to identify whether any of their customer/Beneficial Owner is PEP;
ii. Obtain approval from CAMLCO to commence or continue the business relationship;
iii. Apply EDD measures that are set out in section 5.8 of this guidelines;
iv. The above norms may also be applied to the accounts of the family members & close associates of PEPs. Middle ranking or more junior individual should not be treated as PEP;
v. All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank, BFIU & NBL under this act have to be complied accordingly.

5.9.2. Influential Persons (IPs)/ Domestic PEPs

'Influential persons' refers to, "Individuals who are or have been entrusted domestically with prominent public functions. The following individuals must always be classed as Influential persons but not limited to:

a. Heads and deputy heads of state or government;
b. Senior politicians;
c. Ministers, state ministers and deputy ministers;
d. Members of parliament and/or national legislatures;
e. Members of the governing bodies of major political parties (where a member has significant executive power, e.g. over the selection of candidates or distribution of significant party funds);
f. Members of the governing bodies of local political parties;
g. Secretary, additional secretary, joint secretary in the ministries;
h. Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
i. Governors, deputy governors, executive directors and general managers of central bank;
j. Members of court of auditors or the boards of Central banks;
k. Heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
l. Heads of state-owned enterprises;
m. Ambassadors, chargés d'affaires or other senior diplomats;
n. City mayors or heads of municipalities who exercise genuine political or economic power;
o. Head or the senior executives or members of the administrative, management or supervisory bodies of state-owned enterprises;
p. Board members of state-owned enterprises of national political or economic importance.

Whether an individual is an influential person or not shall depend on the prominence or importance of the function that he/she holds, and the level of corruption in the country, the reputation and personal links of the individual and whether he/she has any links to industries that are prone to corruption. If the individual does not hold sufficient influence to enable them to abuse his/her power for gain, they should not be classified as an influential person.

Branch shall identify whether a customer or a beneficial owner is an IP. They need to perform the following-

- Obtaining and verifying additional information of the customer from independent and reliable sources;
- Obtaining and verifying information on the reasons for opening account, the source of funds or source of wealth of the customer;
- Obtaining approval from CAMLCO, if applicable, to commence or continue the business relationship;
- Conducting regular enhanced monitoring on transactions of the accounts.

5.9.3. Chief/Top Level Officials of International Organizations

'Chief executive of any international organization or any top level official' refers to, "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 boards or equivalent functions." The heads of international organizations and agencies that exercise genuine political or economic influence (e.g. the United Nations, the International Monetary Fund, the World Bank, the World Trade Organization, the International Labor Organization) must always be classed as this category.

Branch may open account or establish relationship with any Chief Executive or top level official of any International Organization (whether as customer or beneficiary owner) ensuring the followings:

i. Obtaining and verifying additional information of the customer from independent and reliable sources;
ii. Obtaining and verifying information on the reasons for opening account, the source of funds or source of wealth of the customer;
iii. Obtaining approval from CAMLCO, if applicable, to commence or continue the business relationship;
iv. Conducting regular enhanced monitoring on transactions of the account;
v. Opening & operating the account in accordance with the sections of Foreign Exchange Regulation Act, 1947 and circulars & guidelines issued by Bangladesh Bank, BFIU & NBL under it, if applicable.

5.9.4. Who should be considered a family member of a PEP?

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. Branches 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 Branch assessed a PEP to pose a higher risk. This would not apply in relation to lower risk PEPs. In low-risk situations, a Branch 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.

5.9.5. 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.

5.9.6. Various scenario related with PEPs/IPs

A PEP/IP must be treated as a PEP/IP 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/IP leaves office. A family member of a former PEP/IP should not be subject to enhanced due diligence measures unless this is justified by the Branch's assessment of other risks posed by that customer.

If a person who is a PEP/IP 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. Branch 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/IPs where a Branch has assessed that PEP/IP is posing a higher risk.

5.9.7. PEPs versus Risk

5.9.7.1. Do all PEPs pose the same risk?

No–the risk of corruption will differ between PEPs. Branch 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 Branch has considered in its risk assessment.

In this guideline, the terms "lower risk" and "higher risk" are used to recognize that Branches 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.

5.9.7.2. What are some 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 Branch has assessed to pose a lower risk.
- If he/she is from a 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)

5.9.7.3. What are indicators that a PEP might pose a higher risk?

The following indicators suggest a PEP poses a higher risk:

5.9.7.3.1. Higher risk indicator – product

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

5.9.7.3.2. 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 Branch 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

5.9.7.3.3. 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.

5.9.7.4. 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.

5.9.7.5. 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

5.9.8. Branches' obligations

a. Branches should have appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is a PEP (or a family member or a known close associate of a PEP) and to manage the risks arising from the Branch's relationship with those customers. This includes where a PEP, family member or close associate is operating via an intermediary or introducer (this may include others in the regulated sector such as banking staff, lawyers, estate agents etc). There are many legitimate reasons for doing so (e.g. a solicitor acting in a property transaction). In these situations, and in line with FATF guidance, Branch should understand as part of their due diligence why a PEP, family member or close associate is using such an arrangement and use that as part of their assessment of risk.

b. Regulations state that in determining whether these systems and procedures are appropriate, a Branch should refer to:
   - Its own risk assessment of the money laundering/terrorist financing risks;
   - An assessment of the extent to which the risk would be increased by a business relationship with a PEP, family member or close associate. BFIU would expect that this is a case-by-case assessment and not an automatic assessment that a relationship creates a high risk of money laundering; and
   - Any information provided by the BFIU. This will include the BFIU"s publication, thematic

reviews, speeches on financial crime issues, BFIU"s annual report.

c. Where a Branch has identified that a customer (or beneficial owner of a customer) does meet the definition of a PEP (or a family member or known close associate of a PEP), the Branch must assess the level of risk associated with that customer and, as a result of that assessment, the extent to which enhanced due diligence measures need to be carried out. The risk factors set out in this guideline will help Branch to consider relevant factors when meeting these obligations. A Branch's assessment and its decision to apply relevant enhanced due diligence measures need to be clearly documented.

d. Branches should make use of information that is reasonably available to them in identifying PEPs, family members or known close associates. This could include the following:
   - Public domain information such as websites of the governments, reliable news sources and work by reputable pressure groups focused on corruption risk. Branches should use a variety of sources where possible.
   - Branch may choose, but is not required, to use commercial databases that contain lists of PEPs, family members and known close associates. A Branch choosing to use such lists would need to understand how such databases are populated and will need to ensure that those flagged by the system fall within the definition of a PEP, family member or close associate.

e. Branch will not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or a family member of a PEP or known close associate of a PEP). A Branch may, after collecting appropriate information and completing its assessment, conclude the risks posed by a customer are higher than they can effectively mitigate; only in such cases it will be appropriate to decline or close that relationship.

f. If, having assessed the risk associated with the customer and decided on an appropriate level of enhanced due diligence measures in line with this guideline, a Branch is unable to apply those measures, a Branch needs to comply with the requirement not to establish, or to terminate, a business relationship.

g. The following measures should be taken where a customer meets the definition of a foreign PEP, IPs/Chief of International Organization posing higher risk or a family member or known close associate of a foreign PEP, IPs/Chief of International Organization posing higher risk:
   - Obtain senior management approval for establishing or continuing business relationships with such persons
   - Take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons
   - Conduct enhanced, ongoing monitoring of those business relationships

   The nature and extent of this due diligence should be appropriate to the risk that the Branch has assessed in relation to the customer. A Branch should apply more extensive measures for relationships assessed as high risk and less extensive measures for lower risk customers.

5.9.9. Measures in lower risk situations

In lower risk situations a Branch may take the following measures:

- Conduct enquiries about a PEP's family or known close associates in a flexible manner except those required to establish whether such a relationship does exist.
- Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP. It is necessary to seek source of wealth information but in all lower risk cases, especially when dealing with products that carry a lower risk of laundering the proceeds of corruption, Branches should minimize the

amount of information they collect and how they verify the information provided (for example, via information sources it has available).

- Oversight and approval of the relationship takes place at a lower level of senior management.
- A business relationship with a PEP or a PEP"s family and close associates is subject to less frequent formal review than it was considered high risk.

5.9.10. Measures in higher risk situations

In higher risk situations a Branch may take the following measures:

- Take more intrusive and exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP
- Oversight and approval of the relationship takes place at a senior level of management
- A business relationship with a PEP (or a PEP"s family and close associates) is subject to more frequent and thorough formal review as to whether the business relationship should be maintained

5.9.11. Beneficial owners of legal entities who are PEPs

Branches should identify when a PEP is a beneficial owner of a customer. It does not require that a legal entity should be treated as a PEP just because a PEP might be a beneficial owner.

Once a Branch is satisfied that a PEP is a beneficial owner then, in line with the risk-based approach, it should assess the risks posed by the involvement of that PEP and, after making this assessment, Branch should apply appropriate measures in accordance with this guideline. These could range from applying customer due diligence measures in cases where the PEP is just a figurehead for an organization (this will vary according to the circumstances of each entity but could be the case even if they sit on the board, including as a non-executive director) through to applying EDD measures, according to the risk assessed in line with this guideline where it is apparent that the PEP has significant control or the ability to use their own funds in relation to the entity.

Where a PEP is a beneficial owner of a corporate customer, then a Branch should not automatically treat other beneficial owners/shareholders of the customer as a PEP or known close associate under the regulations, but may do so having assessed the relationship based on information available to the Branch.

5.10 Designated Non-Financial Businesses and Professions (DNFBPs)

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 customers. Branch must ensure the followings instruction while opening of DNFBPs account:

i. Apply EDD measures that are set out in section 5.8 of this guidelines.
ii. Screening the names of the customer, beneficiary owner(s) and authorized person(s), if any, in the Sanction Screening Software.
iii. AML/CFT laws, BFIU circulars & directives, and instructions of AMLD & this guideline's instruction should be followed for completion of KYC, TP & other documentations, risk grading and performing appropriate CDD measures.

5.11 Correspondent Banking Relationship

'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.

Correspondent Banking relationships create a risk that the customers of other banks may be using the bank to launder funds. It is not necessarily possible to conduct due diligence on the customer base of those banks and as such, these relationships require additional care and attention to guard against becoming unwilling participants in this activity. The following controls need to be implemented for correspondent banking relationships:

i. Bank shall establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank through collection of information as per Annexure: F. Bank shall also obtain approval from its CAMLCO before establishing and continuing any correspondent relationship. Necessary information should be collected from open source in addition of the information of Annexure: G if applicable;
ii. Bank shall establish corresponding banking relationship with foreign bank only if they ensure about the effective supervision on that foreign correspondent/respondent bank by the relevant regulatory authority;
iii. Bank should not establish or maintain any correspondent relationship with any shell bank;
iv. Bank must ensure that respondent banks are not providing any services or maintaining any relationship with shell banks;
v. Bank should conduct EDD 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 Jurisdictions under Increased Monitoring and High-Risk Jurisdictions subject to a Call for Action in the Financial Action Task Force's Public Statement). Where applicable, appropriate and effective measures have to be taken for implementation of counter measures imposed by FATF. 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;
vi. If any respondent bank allow direct transactions by their customers to transact business on their behalf (i.e. payable through account),
    a) The corresponding bank must be sure about the appropriate CDD of the customer has done by the respondent bank.
    b) Moreover, it has to be ensured that collecting the information on CDD of the respective customer is possible by the respondent bank on request of the correspondent bank. Here, 'Payable through accounts' refers to "Corresponding accounts that are used directly by third parties to transact business on their behalf."
vii. Bank must be satisfied with the respondent institution's anti money laundering and financing of terrorism controls;
viii. The relationship and its transactions must be subject to annual reviews. The volume and nature of transactions in correspondent accounts from the institution's high risk jurisdictions, or those with material deficiencies should be monitored against expected levels and destinations, and any material variances should be explored;
ix. Above instructions shall also applicable for existing business relationship with correspondent banks;
x. International Division (ID) shall ensure compliance with the above procedure.

5.12 Accounts of Non Face-to-Face Customers

'Non face to face customer' refers to "the customer who opens and operates his account by using internet or by agent of the bank or by his own professional representative without having physical presence at the bank/ branch". Additional controls are required in respect of non face-to-face customers by applying one or more of the following measures of control:

i. Ensuring that the customer's identity is established by additional ID documents, data or information provided by a government department or agency which may be verified;
ii. At least one additional check should be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID card where there is no face-to-face contact, then a certified true copy should be obtained;
iii. Supplementary measures to verify the documents supplied, or requiring an eligible introducer to certify the customer identification documents must be required; or
iv. Ensuring that the initial deposit in the account is carried out through an account in the customer's name at another scheduled bank;
v. Screening the names of the customer, beneficiary owner(s) and authorized person(s), if any, in the Sanction Screening Software;
vi. AML/CFT laws, BFIU circulars & directives, and instructions of AMLD & this guideline's instruction should be followed for completion of KYC, TP & other documentations, risk grading and performing appropriate CDD measures;
vii. Following the instructions mentioned in "Guidelines on e-KYC" issued by BFIU.

5.13 Automated Screening Mechanism

Bank shall have an automated screening mechanism for combating the terrorist financing & proliferation financing that can prohibit any listed individuals or entities to enter into the banking channel through National Bank. Bank shall introduce a Sanction Screening Software to screen the existing and potential as well as walk-in customer's name against Sanction list of BFIU, UNSCR, OFAC, EU and other local sanction list.

Branch shall operate the Sanction Screening Software to detect the listed individuals or entities prior establishing any relationship. Branch shall screen the customer's name during account opening and any kind of domestic/foreign exchange transaction through the Sanction Screening Software so that any listed individuals or entities could not use the formal financial channel.

Branch shall ensure that screening has done before-

- Any international relationship or transaction;
- Opening any account or establishing relationship domestically.

If any account/transaction is identified which relates to any sectioned person/entity or their associates then branch should freeze the account/transaction and inform BFIU.

5.14 Walk-In/One-off Customers

Walk-in customer means the customer who has no account in the bank but getting some banking facilities. Branch should follow the instructions as under:

- Simplified Customer Due Diligence:
  - Branch shall collect the name, address and telephone number of the sender/applicant and receiver/beneficiary while making transaction bellow taka fifty thousand;
  - Branch shall collect photographed ID card along with the name, address and telephone number of the sender/applicant/depositor/receiver while making transaction of amounting taka fifty thousand to five lac.

- Customer Due Diligence:
  - KYC form (Annexure: D) has to be used for the walk-in customers who make transaction taka five lac & above.
  - Branch shall collect Complete and Accurate information of any person other than customer for using banking facilities. Branch shall collect the complete and accurate sender & receiver or applicant & beneficiary's information such as:
    i. Name;
    ii. Account number (if any);
    iii. Residential or mailing address ;
    iv. Phone/Active Mobile No.;
    v. Photo copy of NID/Passport/Birth Registration with any acceptable ID with Photo.
    vi. Sources of fund and motive of transactions. If applicable, branch may collect documents in this regard.
    vii. Relation between money sender & receiver.
- Branch must screen the name of the sender/applicant or receiver/beneficiary in the Sanction Screening Software.
- All necessary information/documents of walk-in Customer's transaction have to be preserved for at least five years.

5.15 Beneficial Ownership and Control

As per 2(4) of MLPR 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.

5.15.1 Definition:

The definition of beneficial owner means the individual who –

- has effective control of a customer; or
- 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:

- Who owns 20 or more percent of a company or legal arrangements ;
- Who has effective control of the customer;
- The person on whose behalf a transaction is conducted.

Effective control, ownership and persons on whose behalf a transaction is conducted are not mutually exclusive. The beneficial owner must be a natural person and cannot be a company, an organization or a legal arrangement.

5.15.2 Why is it important to identify the beneficial owner?

Corporate entities such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements conduct a wide variety of commercial and entrepreneurial activities. However, despite the essential and legitimate role that corporate entities play in the economy, under certain conditions, they have been misused for illicit purposes, including money laundering (ML), bribery and corruption, insider dealings, tax fraud, terrorist financing (TF), and other unlawful activities. This is because, for criminals trying to circumvent anti-money laundering (AML) and

countering the financing of terrorism (CFT) measures, corporate entities provide an attractive avenue to disguise the ownership and hide the illicit origin.

Various studies conducted by Financial Action Task Force (FATF), World Bank, United Nations Office on Drugs and Crime (UNODC) have explored the misuse of corporate entities for illicit purposes, including for ML/TF. In general, the lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising:

a. The identity of known or suspected criminals,
b. The true purpose of an account or property held by a corporate entities, and/or
c. The source or use of funds or property associated with a corporate entity.

5.15.3 Ways in which beneficial ownership information can be hidden/obscured

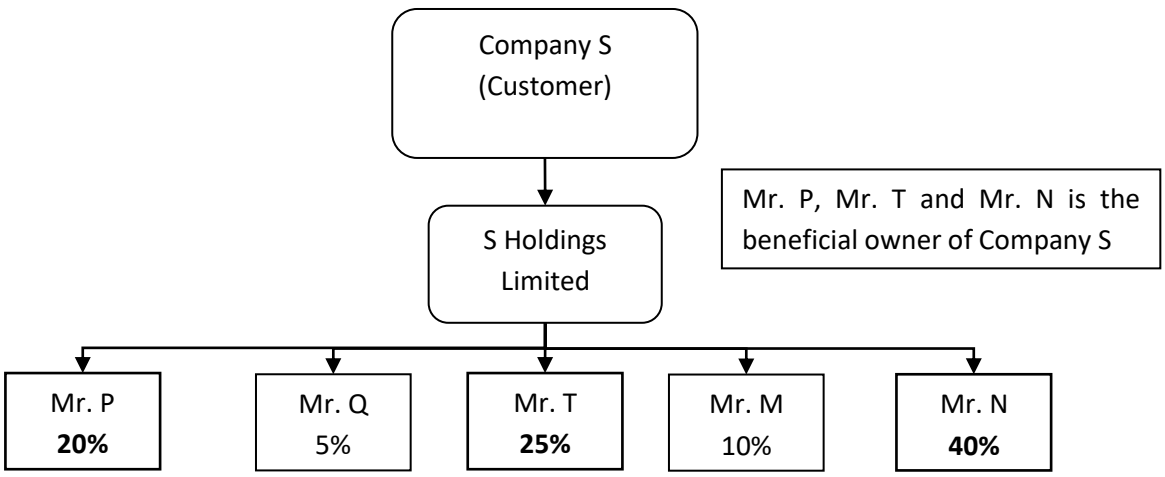
Beneficial ownership information can be obscured through various ways, including but not limited to;

a. Use of shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions,
b. Complex ownership and control structures involving many layers of ownership, sometimes in the name of other legal persons and sometimes using a chain of ownership that is spread across several jurisdictions,
c. Bearer shares and bearer share warrants,
d. Use of legal persons as directors (As per MLPR 2019 Legal person means any entity other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundation, installations, partnerships or associations and other relevantly similar entities),
e. Formal nominee shareholders and directors where the identity of the nominator is undisclosed,
f. Informal nominee shareholders and directors, such as close associates and family,
g. Trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,
h. Use of intermediaries in forming legal persons2, including professional intermediaries such as accountants, lawyers, notaries, trust and company service providers.

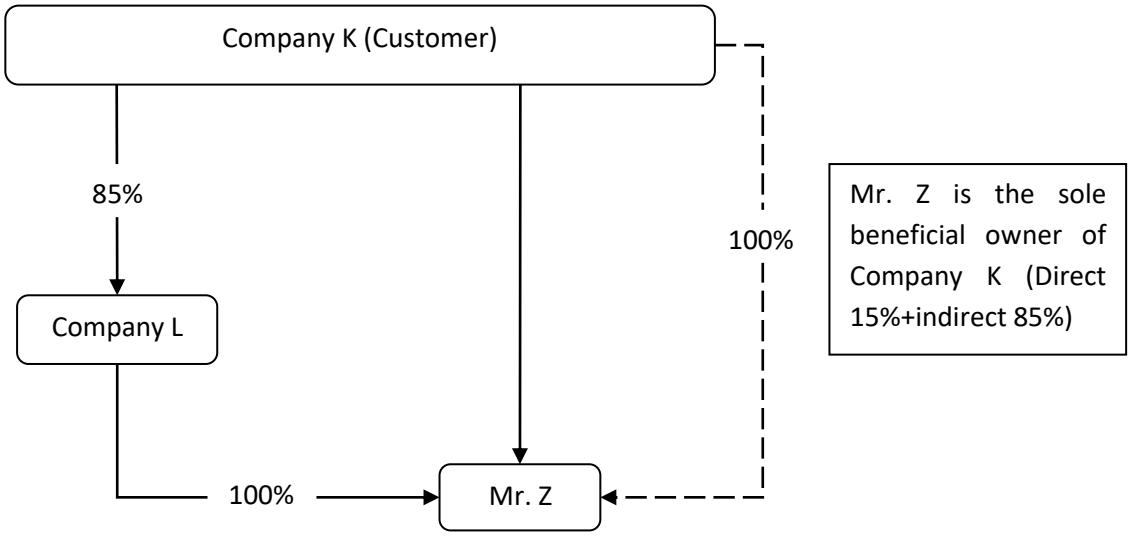
5.15.4 Ownership

The reporting entities should understand the ownership and control structure of the customers. The threshold for controlling interest owns 20% or more of the customer. The ownership can be simple and complex in nature. Few examples are as follows:

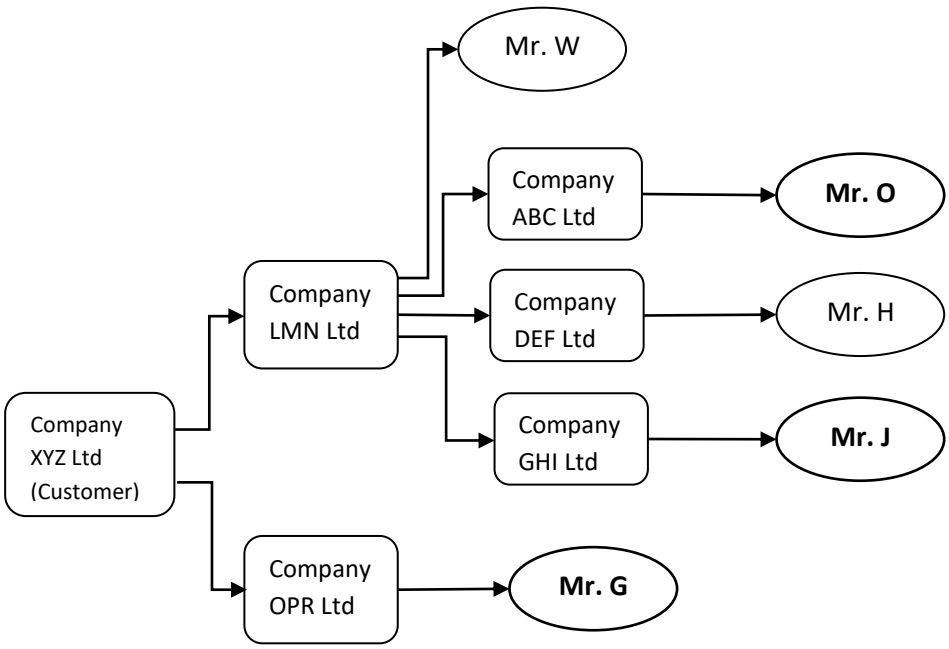
a) Simple ownership



b) Simple (Direct and Indirect) ownership



c) Complex (Multi Level indirect) ownership



Mr. O, Mr. G and Mr. J are beneficial owners of Company XYZ through indirect ownership.

An individual who has a control over a portion of equity directly or via family relationship or via nominee or close associate (whether disclosed or undisclosed) can be considered as a beneficial owner.

Ownership can be spread over a large number of individuals with no individual owning more than 20 percent. For example, a co-operative that has a large number of members is likely to have no individual(s) owning more than 20 percent. In such instance, the effective control element is more likely to determine the beneficial owner(s).

5.15.5 Effective Control

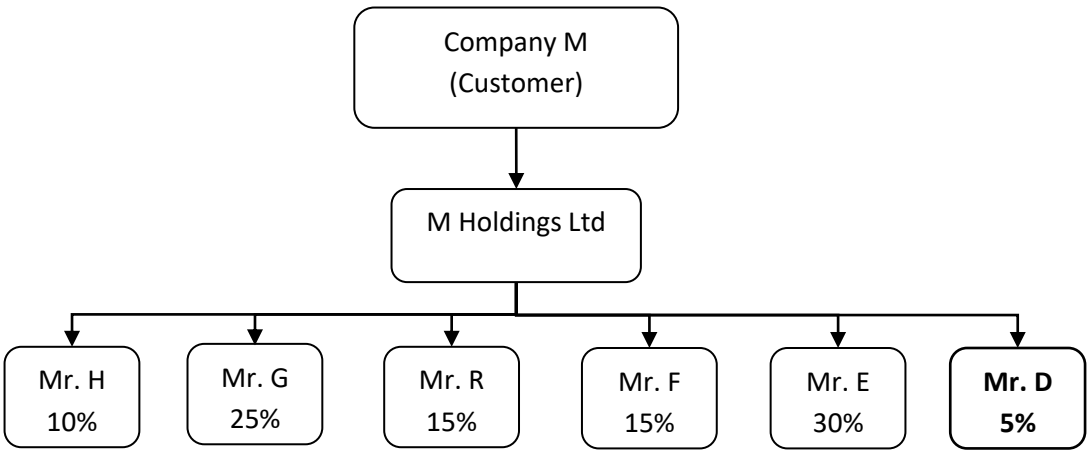
It is essential to understand the customer's governance structure as an aid in identifying those persons that exercise effective control over the customer. In deciding the effective controller(s) in relation to a customer, reporting entities should consider:

a. a person who can hire or terminate a member of senior level management;
b. a person who can appoint or dismiss Directors;
c. Senior managers who have control over daily/regular operations of the person/arrangement (e.g. a CEO, CFO or a Managing Director).

Natural persons may also control the legal person through other means such as:

a. Personal connections to persons in positions such as Executive Directors/ CEOs/ Managing Director or that possess ownership;
b. Significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person;
c. Control without ownership by participating in the financing of the enterprise, or because of close family relationships, historical or contractual associations, or if a company defaults on certain payments;
d. Use, enjoyment or benefiting from the assets owned by the legal person even if control is never exercised.

Effective Control



Mr. D is the managing director of the EFG Bank, which is the main financing source of the company M. In such a situation even if Mr. D holds less than twenty percent (20%) of Company M, he has effective control over the company M through EFG Bank and should be considered as a beneficial owner through effective control.

When a Branch identifies a customer, it should identify the beneficial owner(s) and take all reasonable steps to verify his identity:

a. Where the client is **a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.

b. Where the client is **a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to 20 or more percent of capital or profits of the partnership.

c. Where the client is **an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to 20 or more of the property or capital or profits of the unincorporated association or body of individuals.

d. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

e. Where the client or the owner of the controlling interest is **a company listed on a stock exchange**, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The beneficial owner must also be noted in the case of **non-profit associations**, although earning profit is not the goal of any of them. According to the definition of beneficial owner, the person(s) under whose control the company is opening are indicated in such a case. Usually, they are member of the management board. Exceptions are possible, e.g. if the founders or members of a non-profit association are legal entities, the beneficial owners are defined in the same way as in the case of companies. The same principle applies here, i.e. noting the chairman of the management board is enough is enough if the management board has more than four members. If a person is noted as the beneficial owner due to their position as a member of a managing body, this does not mean that they receive monetary income from the company or that the company operates in their personal interests.

In the event of **a limited partnership fund, civil law partnership, community or other association** of persons that does not have the status of a legal entity, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or via other means and who is the association's:

- founder or person who has handed over property to the asset pool;
- trustee or manager or possessor of the property;
- person ensuring and controlling the preservation of property, where such person has been appointed, or
- the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates

In the case of a **foundation**, the person noted as the beneficial owner is the person who may make payouts from the assets of the foundation, where such person(s) have been specified by name in the articles of association of the foundation. If such persons have not been specified by name in the articles of association, the members of the management board and supervisory board are noted as the beneficial owners.

5.15.6 Person on whose behalf a transaction is conducted

Another part of the definition of beneficial owner is a person on whose behalf a transaction is conducted. This may be the individual who is an underlying client of the customer. This concept is important when considering the relationship between managing intermediaries and their underlying clients. There are various scenarios, many of which are complicated.

An example is, if a Branch knows that someone (person A) is conducting an occasional transaction on behalf of another person (person B), then person A and person B should be identified and verified along with any other beneficial owners.

5.15.7 Beneficial owner of legal arrangements

Legal arrangement includes an express trust, a fiduciary account or a nominee.

All trusts have the common characteristic of causing a separation between legal ownership and beneficial ownership. Legal ownership always rests with the trustee. Beneficial ownership can rest with the author of trust, trustees or beneficiaries, jointly or individually.

Branch should identify and take reasonable measures to verify information about a trust, including, the identities of the author of the trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including those who control through the chain of control or ownership).

Branch are required to obtain trust documents (e.g. deed of trust, instrument of trust, trust declaration, etc.) and the provisions of the trust document must be fully understood within the context of the laws of the governing jurisdiction. The Reporting entities should take reasonable measures to verify trust document through independent means (e.g. Registry of Trust, Notary)

Example: Person 'B' is the author of a trust for the benefit of his child. The trustee seeks to establish a relationship with a financial institution to help manage the assets of the trust. Even though the trustee is the controller of the assets of the trust he may not be the ultimate beneficial owner and the main focus of CDD should include person 'B' as well.

5.15.8 Applying a risk-based approach

A risk-based approach refers how the beneficial ownership of a customer will be verified. Identifying beneficial ownership of a customer is an obligation that must be satisfied, regardless of the level of risk associated with that customer. However, when deciding what reasonable steps should be taken to satisfy that the customer's identity and information is correct, one may vary approach depending on the risk assessment of the customer. The process for assessing customer risk and deciding how to identify and verify beneficial ownership should be set out into the AML/CFT program.

One should apply enhanced customer due diligence and make a suspicious transaction report to the Bangladesh Financial Intelligence Unit (BFIU) where there are reasonable grounds for suspicion of money laundering or terrorist financing.

A risk-based approach allows some flexibility in obligation to use data, documents or information obtained from a reliable and independent source to verify the identity of the beneficial owner(s) of customer. Here is an example of a local business where the customer could be a sole trader or a registered company. The approach should be:

i. Stage one-gather information

   Identify the customer/person seeking to conduct a transaction. Establish the purpose of the relationship. Establish the nature and purpose of their business, and the ownership structure. Ask them for documents and information relating to their expected ongoing/future levels of business. Obtain sufficient information to determine whether they will be subject to enhanced customer due diligence, and then establish their source of funds or wealth/income if enhanced customer due diligence is required. (It is good practice to retain all copies of documents and notes).

ii. Stage two-identify beneficial owners

Identify the beneficial owners (and those with authority to act on behalf of the customer). The appropriate level of customer due diligence (standard, simplified, enhanced) that should apply may become more apparent at the end of stage two – so one may have to return to the customer for further information and documents depending on the level of risk. Take reasonable steps to ensure the information given is correct.

iii. Stage three

Apply a risk based approach to verifying the identity of the beneficial owners.

The risk assessment will set out what to do to verify different types of customers. For example, a well known local family business wants to become customer. Reporting entities must first identify both the customer and the beneficial owner(s) and obtain standard identity documentation such as NID or passports. The risk assessment may lead to treat this customer as lower risk. One may decide that a check in the local business directories, combined with local knowledge, is reasonable steps. If the customer is higher risk, one may apply enhanced customer due diligence, in which case one must obtain information relating to the source of funds or wealth of the customer. Verification of the identity of the beneficial owner(s) is the last step in the process. To verify the beneficial owner(s) appropriate documentations must be obtained so that it is known who the beneficial owner is.

It is appropriate for beneficial ownership identification process to include measures to ensure that make consistent decisions about customers. This process should be in line with risk assessment. If the customer is associated with higher risk factors, internal controls in AML/CFT program should set out when to escalate decisions to a higher level. For example: sign off for new business; ending existing business; or imposing additional controls for risk management.

5.15.9 Customer Due Diligence

The obligation is to determine the individual(s) who are the beneficial owner(s). A beneficial owner is an individual (a natural person). Therefore the beneficial owner can only be an individual, not a company or organization. There may be more than one beneficial owner associated with customers. The task is to identify and verify the identity of all the beneficial owners of the customers.

If the customer is an individual to treat that person as the beneficial owner unless there are reasonable grounds to make the suspect that are acting on behalf of another. If the customer is acting on behalf of another person, anyone will need to establish that person's identity, the beneficial ownership of the customer and any other beneficial owners.

5.15.10 Record keeping

It is a good practice to keep detailed records of all decisions and retain customer due diligence and relevant records in a readily auditable manner. It is important to record the rationale behind any decision is made. Anyone reading the notes years later should be able to understand why such a risk-based decision is taken.

Example 1: Record for ownership and control structure of a legal person

ABC Company Ltd. is a private limited liability company registered under the Companies Act. Mr. A owns 25% of the shares and BC Company Ltd. owns the balance 75% of shares of ABC. Mr. S is Managing Director of ABC Company and; the Board of Directors consists of his wife, Mrs. S, ABC's Chief Financial Officer; and their three children.

In this example, Reporting entities be required to record:

- The ownership of the Company - shared by Mr. A (25% of the shares) and BC Company Ltd.

(75% of the shares);

- The ownership structure of the entity - ABC Company Ltd. is a privately traded.
- The identification of all members the Board of Directors (Mr. S's Family) as they are having effective control;
- Identification of Mr. A as he is having more than 20% of ownership
- Identification of all of the individuals who own or control, directly or indirectly, 20% or more of the shares of BC Company Ltd since it owns 75% of the shares, it also exercises control. However, in a case like this, the Branch must research further to determine whether any individual owns enough shares of BC Company Ltd. that would constitute 20% of ABC Company Ltd., or until the Branch determine that there is no such individual;
- The manner in which the Branch obtained this information; and
- The measures taken to verify accuracy of information.

Example 2: Record for ownership and control structure of partnership

Bengal Developers is a partnership engaged in buying and selling of real estate in Western District owned by two partners (Mr. T and Mr. J). Mr. T and Mr. J have signed a partnership agreement stating that Mr. T will invest Tk. 5,000,000 in the partnership to rent space for the Rainbow Property Developers and other administrative expenses, and Mr. J will be solely responsible for operations of the business. All decisions related to the partnership must be unanimous; in case of a disagreement, either partner can decide to end the partnership. Mr. T & Mr. J will split the profits from the business 50/50. If they decide to end the partnership, Mr. T will get 55% of the proceeds of the sale of the business assets, while Mr. J will get 45%.

In this example the Branch is required to record:

- The ownership structure of the entity, including the details of the partnership between Mr. T & Mr. J;
- Identification of Mr. T and Mr. J as both control the partnership;
- The manner in which, the FI obtained this information; and
- The measures taken to confirm accuracy of information.

Note: The business structure is important in this example as the ownership and control of the partnership is shared between Mr. T & Mr. J. The branch needs to retain a copy of the partnership agreement to meet record keeping requirements as well as confirm the accuracy of the beneficial ownership information obtained. In the absence of such agreement it should be recorded that the partnership exists between Mr. T and Mr. J without having a written agreement.

5.15.11 Who is required to submit data to the Branch in supporting beneficial ownership?

- A private limited company
- General partnership
- Limited partnership
- Commercial association
- Foundation
- Non-profit association
- Economic Interest Grouping

5.15.12 Who are not obliged to submit data of the beneficial owner?

- Apartment association;
- Building association;
- A company listed on the regulated market to which disclosure rules complying with Bangladeshi law or similar international standards are applied, which ensure the sufficient transparency of the data of owners;
- A foundation the goal of whose economic activities is safekeeping or collecting assets

in the interests of the beneficiaries or group of persons specified in the articles of association and that has no other economic activity.

- As gardening associations are ordinary non-profit associations within the legal meaning, then the obligation to submit the data of the beneficial owner applies to them.

5.15.13 Does a branch of a foreign company have to submit the data of the beneficial owner?

The data of the beneficial owner are not submitted in the case of the branch of a foreign company, because the branch is not a legal. A foreign company is responsible for the activities of its branch and enters the data of the beneficial owner in its respective register of beneficial owners.

5.15.14 Who is the beneficial owner in the case of a company whose parent company is a company listed on a regulated market?

Companies listed on the stock exchange do not have to submit the data of beneficial owners, but the subsidiaries belonging to their groups of companies must do it. The same principles that apply to ordinary companies apply here as well: if there are no natural persons among the shareholders of a listed company whose shareholding in the company exceeds 20%, the members of the controlling body of the listed company, i.e. the management board and the supervisory board, are noted as the beneficial owners.

5.15.15 Who is the beneficial owner of a state-owned company or foundation, or a foundation or non-profit association established by a local government (city, town or municipality)?

State-owned companies are ordinary private legal entities. The beneficial owner of a state-owned company is the minister responsible for the area, which represents the state in the company and appoints the members of the supervisory boards of the companies in their area of government, the chairman of the supervisory board/management board of the company and the members of both bodies. For example, the finance minister as the representative of the state, the chairman and members of the supervisory board and the chairman and members of the management board can be considered beneficial owners.

In the case of foundations established by the state where the rights of a founder are exercised by ministries and foundations with state participation, the minister of the respective area, the chairman/members of the supervisory board and the chairman/members of the management board can be considered the beneficial owners. The members of the supervisory board are appointed and the other rights of a founder or shareholder of a foundation of a municipality, town or city, whose sole founder is the municipality, town or city, as well as of a private limited company or public limited company, whose sole shareholder is a municipality, town or city, are exercised by the government of the municipality, town or city, so the mayor of the municipality, town or city or the members of the government of the municipality, town or city can be considered the beneficial owners. The principle applied here is the same: noting the chairman of a body is enough if the body consists of more than four persons. If an association has been established with the state and a local government or several local governments together, none of which have dominant influence over the association, the chairmen or members of the management board or supervisory board of the association are noted as the beneficial owners.

5.15.16 General instruction while identifying beneficial ownership

Branch should consider following aspects while identifying beneficial ownership:

a. If a customer operates a account on behalf of another person, Branch shall collect and preserve complete & accurate information of that person along with the customer;
b. Branch shall collect and preserve complete & accurate information of the person who apparently controls, directly or indirectly, the customer;

c. In case of Company, Branch shall collect and preserve complete & accurate information of the beneficial owner; in that case, the shareholders who have controlling ownership interest in the company shall be treated as beneficial owner. A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 20%);
d. Branch shall collect and preserve complete & accurate information of the CEO if no Natural Person is identified as mentioned in clause b & c.

Note: It is required to conduct CDD of settlor, trustee, protector or any person with similar status or any beneficiary or class of beneficiaries who have hold effective control on trust, in case of identification of beneficial ownership of a legal arrangement.

5.16 Instructions on Agent Banking:

For conducting agent banking activities, bank should follow the following instructions:

(1) The responsibility for complying all instructions related to money laundering and terrorist financing shall be on the agent as well as entirely on the bank/respective branch;
(2) Branch shall be vigilant in identifying and reporting suspicious transactions or activities of agents and customers;
(3) AML/CFT activities should be included in agent banking compliance programs and appropriate training should be given to agents; and
(4) The following steps should be taken for appointing agents and monitoring their activities:
   (a) Ensuring complete and accurate identification of agents by following proper verification or selection process (Screening Mechanism) in selection of agents. In the verification process, the personal details of the agents and information about involvement in criminal activity by the agents will be included;
   (b) Determining the level of risk (high, medium and low) of the agents by considering the volume and number of transactions, physical location, nature of business & ownership and other reasonable factors and monitoring the transactions & activities of the agents by considering the determined level of risk;
   (c) Carrying out risk assessment of the agents on a regular basis;
   (d) Verifying agents' compliance status on AML/CFT;
   (e) Conducting inspection/audit activities for verifying AML/CFT compliance status of the high risk Agents on Annual Basis and sending related reports to AMLD;
   (f) Completion of inspection/audit activities of medium and low risk agents at regular intervals;
   (g) Publishing updated (January-June based) list of agents on Bank's website;
   (h) Publishing of a separate list (January-June basis) of canceled agents based on various complaints/irregularities on Bank's website; and
   (i) In the case of agent banking, the Guidelines on e-KYC issued by BFIU may be followed.

5.17 Risk Categories

While opening of accounts, the concerned officer must assess the risk that the accounts could be used for "money laundering", and must classify the accounts as either High Risk or Low Risk. The risk assessment must be made using the risk parameters as detailed in the KYC Profile form in which following seven risk categories are scored using a scale of 1 to 5:

- Business & Occupation Related Risk
- Product/Service & Channel related Risk
- Geographical Risk
- Relationship Risk
- Transactional Risk
- Transparency Risk

Sl.	Category	Particulars	Risk Score
1.	**Business & Occupation Related Risk**		
1.a.	Business	Jewelry/Gold/ Precious Metal Business, Money Changer/Courier Service/Mobile Banking Agent, Real Estate Developer/Agent, Construction Firm's Contactor/Promoter, Art/Antic dealer, Restaurant/ Bar/ Night Club/ Parlor/ Residential Hotel Business, Export /Import, Export /Import Agent, Manpower Export Business, Business of Weapons, Garments Business/Garments Accessories/ Buying House, Share/Stock Dealer, Broker, Portfolio Manager/Merchant Banker, Software & IT Business, Off shore/ Non Resident Corporation, NGO/NPO, Film production / distribution company, Mobile phone operator / Internet or cable TV operator, Land / House trading broker Firm, Insurance/ Brokerage Agency, Religious Institution/Organization and Educational Institution, Trust, Petrol Pump/ CNG Station Business, Software Business, Ship Braking Business.	5 (High Risk)
		Bank/Leasing/Finance Company, Indenting Business, Outsourcing Business, Law Firm/Engineering Firm/Consultancy Firm, Fuel and Power Generation Company, Print/ Electronic Media, Travel Agent/Truism Company, Merchant with over 10 million taka invested in business, Chain Store/ Shopping Mall, Freight/ Shipping/ Cargo Agent/ CNF Agent, Auto Business (New/Reconditioned Vehicle), Lather & Lather Oriented Product Business, Construction Materials Business.	4 (High Risk)
		Agent Business, Yarn Business / Jhut Business, Transport operator, Manufacturing and Marketing of Pharmaceuticals Business, Cold Storage Business, Advertizing firm, Service Provider, Tobacco and Cigarette Business, Amusement Park/Entertainment Business, Motor Parts Trader/Workshop.	3 (Medium Risk)
		Poultry/ Dairy/ Fishing Firm, Agro Business / Rice Mill Business/ Beverage, Small Business (Investment Less than 50 Lac), Computer/ Mobile Phone Dealer, Manufacturers (Other than arms).	2 (Medium Risk)
1.b.	Occupation	Pilot/Flight Attendant, Trustee.	5 (High Risk)
		Professional (Journalist, Lawyer, Doctor, Engineer, Chartered Accountant, etc.), Director (Private/Public Limited Company), High	4 (High Risk)

		Official of Multinational Company (MNC), Homemaker (Housewife), Information Technology (IT) sector employee, Athlete/ Media Celebrity/ Producer/Director, Freelance Software Developer.	
		Government service, Landlord/Homeowner, Private Service: Managerial.	3 (Medium Risk)
		Teacher (Public/Private/Autonomous Educational Institution), Private Sector Employee, Self-employed Professional, Student, Retiree, Farmer/Fisherman/Laborer.	2 (Medium Risk)
1.c.	Business, Occupation, Person, Entity	Shell Bank/company, Unlicensed bank/NBFI, Unregulated charities, Red light business/ Adult Business, Virtual currencies, Marijuana, Gambling, Person/entity sanctioned by UN/OFAC/OFSI/EU/Bangladesh Government.	Prohibited
2.	**Product/Service Channel related Risk**		
2.a.	Type of Product/ Service	FC Account, RFCD Account	5 (High Risk)
		Current Account	4 (High Risk)
		FDR, SND, Scheme Deposit Account (above Taka 12 lac)	3 (Medium Risk)
		Saving Account, Scheme Deposit Account (below Taka 12 lac)	1 (Low Risk)
2.b.	Type of On-boarding	Internet/Self check-in/Other non Face to Face	5 (High Risk)
		Walk-in customer, Sales Agent	3 (Medium Risk)
		Branch/Relationship Manager	2 (Medium Risk)
3.	**Geographical Risk**		
3.a.	Residential Status	Foreign Citizen	3 (Medium Risk)
		Non-resident Bangladeshi	2 (Medium Risk)
		Resident Bangladeshi	1 (Low Risk)
3.b.	Citizen of sanctioned country or Citizen of High-Risk Jurisdictions or Jurisdictions under Increased Monitoring as per FATF	Yes	5 (High Risk)
		No	1 (Low Risk)
4.	**Relationship Risk**		
4.a.	PEP/IP/ High Official of International Organization	Yes	5 (High Risk)
		No	0 (No Risk)
4.b.	family member /close associates of PEP/IP/High Official of International Organization	Yes	5 (High Risk)
		No	0 (No Risk)

5.	**Transactional Risk**		
5.a.	Customer's Average Yearly Transactions (Individual)	Less than BDT 1 million	1 (Low Risk)
		From BDT 1 million to 5 million	2 (Medium Risk)
		From BDT 5 million to 50 million (5 crores)	3 (Medium Risk)
		More than BDT 50 million (5crores)	5 (High Risk)
5.b.	Customer's Average Yearly Transactions (Entity)	Less than BDT 1 million	0 (No Risk)
		From BDT 1 million to 5 million	1 (Low Risk)
		From BDT 5 million to 50 million (5 crores)	2 (Medium Risk)
		More than BDT 50 million (5 crores)	4 (High Risk)
6.	**Transparency Risk**		
	Customer has Provided credible source of funds	Yes	1 (Low Risk)
		No	5 (High Risk)

If the risk scoring is less than 15, it will indicate low risk and If the risk scoring is 15 and above then it will indicate high risk. A customer can be considered as high risk, even if the rating is less than 15, by taking subjective consideration on beneficial owner & other risks. The risk assessment scores are to be documented in the KYC Profile form.

CHAPTER 06

GENERAL GUIDELINES FOR ACCOUNT OPENING

Generally the customer requires providing their information through the following four basic forms:

A. A/C opening form (individual or corporate)
B. Nominee related information form (in case of individual account)
C. Personal information form
D. Transaction Profile form

Branch shall verify the information provided by the customer using reliable documents to establish his/her satisfaction. When commencing a business relationship, branch should consider recording the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. The customer identification process does not end at the point of application. Branch need to confirm and update information about identity, such as change of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector. It will also depend on the nature of the product or service being offered, and whether personal contact is maintained satisfactorily with the customers. The nature of information/documents required depends on the type of customers (individual/corporate etc).

6.1 Individual Customers

Individual or personal account is one's account at the bank that is used for non-business purposes. Most likely, the service at the bank consists of one of two kinds of accounts or sometimes both: a savings account and a current account. Branch may open account or establish relationship with any natural person or individual ensuring the following:

i. Follow the customer acceptance policy that is set out at section 4.1 of this guidelines;
ii. Follow KYC procedure as per section 5.3 of this guidelines;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. Collect & verify the complete & accurate information & the required identification documents of the beneficiary owner(s), if any.

6.2 Joint Accounts

The Joint Account opened by more than one individual can be operated by single individual or by more than one individual jointly. The documents for joint account are same as documents of individual customer. It is required to obtain clear instruction in writing, signed by all account holders, regarding the operation of the account. The mandate for operating the account can be modified with the consent of all account holders.

Branch may open an account jointly or establish relationship with two or more natural persons or individuals ensuring the following:

i. Follow the customer acceptance policy that is set out at section 4.1 of this guidelines;
ii. Follow KYC procedure as per section 5.3 of this guidelines;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. It is required to obtain clear instruction in writing, signed by all account holders, regarding the operation of the account;
v. Collect & verify the complete & accurate information & the required identification documents of the beneficiary owner(s), if any.

6.3 Corporate or Business Organization

The principal requirements depend on the structure of the corporate or business organizations. Branch shall follow the following instructions:

6.3.1 Sole Proprietorship:

i. Follow the customer acceptance policy that is set out at section 4.1 of this guidelines;
ii. Follow KYC procedure as per section 5.3 of this guidelines;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. Collect & verify the complete & accurate information & the required identification documents of the beneficiary owner(s), if any.

6.3.2 Partnership :

i. Follow the customer acceptance policy that is set out at section 4.1 of this guidelines;
ii. Follow KYC procedure as per section 5.3 of this guidelines;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. Collect & verify the complete & accurate information & the required identification documents of the Authorized person(s)/Power of Attorney Holder(s)/Beneficiary owner(s), if any.

6.3.3 Limited Company:

i. Follow the customer acceptance policy that is set out at section 4.1 of this guidelines;
ii. Follow KYC procedure as per section 5.3 of this guidelines;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. Collect & verify the complete information & the required identification documents of each director, and verify the same;
v. Collect & verify the complete & accurate information & the required identification documents of the Authorized person(s)/Power of Attorney Holder(s)/Beneficiary owner(s), if any.

6.4 Other Corporations (including Association/ Trust/ Club/ Society/ NGO/ Non-trading Concern)

i. Follow the customer acceptance policy that is set out at section 4.1 of this guidelines;
ii. Follow KYC procedure as per section 5.3 of this guidelines;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. Collect & verify the complete & accurate information & the required identification documents of the Authorized person(s)/Power of Attorney Holder(s)/Beneficiary owner(s), if any.

6.5 Powers of Attorney/ Mandates to Operate Accounts

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept.

6.6 Accounts of Minor

Branch may open account or establish relationship with any minor ensuring the following:

i. The Customer acceptance policy that is set out at section 4.1 of this guidelines shall be followed;
ii. KYC procedure as per section 5.3 of this guidelines shall be followed both for Minor & Guardian;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;

iv. Collect & verify the complete & accurate information & the required identification documents of the beneficiary owner(s), if any.

6.7 Illiterate Person

An illiterate person means a person who cannot sign his name. But an illiterate person is competent to contract like any other person. For identification, bankers record his thumb impression and also take a copy of his recent photograph duly attested. Following precautions may be suggested in opening and operation of such accounts:

i. The Customer acceptance policy that is set out at section 4.1 of this guidelines shall be followed;
ii. KYC procedure as per section 5.3 of this guidelines shall be followed;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. Collect & verify the complete & accurate information & the required identification documents of the beneficiary owner(s), if any.

6.8 Non Resident Bangladeshi & Foreign National

Branch may open account or establish relationship with any Non Residential Bangladeshi or Foreign National ensuring the following:

i. The Customer acceptance policy that is set out at section 4.1 of this guidelines shall be followed;
ii. KYC procedure as per section 5.3 of this guidelines shall be followed;
iii. Copy of passport including proof of valid visa, work permit shall be collected;
iv. Collect document for verification of source of funds;
v. Collect & verify the complete & accurate information & the required identification documents of the beneficiary owner(s), if any;
vi. These accounts will be opened & operated in accordance with the sections of Foreign Exchange Regulation Act, 1947 and circulars & guidelines issued by Bangladesh Bank, BFIU & NBL under it.

6.9 Pardanashin ladies

A pardanashin lady is one who remains in complete seclusion and does not transact with people other than members of her family. Though pardanashin lady is legally competent to enter into a contract, she may be able to avoid it on the pretext of undue influence. Therefore, branch should take extra care in this regards. Following precautions may be suggested in opening and operation of such accounts:

i. The Customer acceptance policy that is set out at section 4.1 of this guidelines shall be followed;
ii. KYC procedure as per section 5.3 of this guidelines shall be followed;
iii. Collect & verify documents of identification, Address & Source of fund as per Annexure: A;
iv. Collect & verify the complete & accurate information & the required identification documents of the beneficiary owner(s), if any.

6.10 Provision of Safe Custody, Safety Deposit Boxes and Locker Services

The branches where facilities to hold boxes, parcels and sealed envelopes in safe custody are available, they will follow the Customer acceptance policy & KYC procedures that set out in this guidelines. In addition such facilities shall only be made available to account holders.
The customer identification process does not end at the point of application. Once the account relationship has been established, reasonable steps should be taken by the branch from time to time to ensure that descriptive information is kept updated.

6.11 Persons without Standard Identification Documentation

The socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess standard identification documents.

In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous anti money laundering procedures is recommended. Branch should allow them to open accounts after obtaining a certificate from a responsible person acceptable to the bank including other documents. In such cases, a certifier must be a suitable person, such as a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number. In these cases it may be possible for the bank to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc) who knows the person. 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 manager may authorize the opening of a business relationship if she/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 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.

CHAPTER 07

FOREIGN SUBSIDIARIES, FOREIGN BRANCH & OFF-SHORE BANKING UNIT

7.1 Instructions for Foreign Subsidiaries & Off-Shore Banking Unit

i. All requirements of the MLP Act, 2012; Anti Terrorism Act, 2009, the rules issued under the said acts and guidelines issued by BFIU & NBL from time to time must also be followed by the Foreign Branch/Subsidiaries of NBL;
ii. It should be informed to AMLD if any Foreign Branch/Subsidiary fails to comply the instruction mentioned in the above section 7.1.i. AMLD will take necessary measures to manage the ML/TF risks and inform BFIU regarding the said non-compliance as soon as possible.
iii. All instructions of this policy guidelines shall also be applicable for Off-Shore Banking Unit of NBL;

CHAPTER 08

TRADE BASED MONEY LAUNDERING

8.1 International Trade

Traditional Money Laundering Exchange Vehicles are Cash, Cheque, Traveler's Cheque, Bond, Stock, Gold, Precious Metal, Wire transfer, Insurance policy, Casino chips, Luxury Goods, Antiques, Art etc. but with the change of rapid global financial system Money Laundering & Financing of Terrorism activities evolve and transform quickly which present new threats to our banking system like trade based Money Laundering, Technology based Money Laundering and proliferation financing. So bank officials shall be aware of such techniques of Money Laundering & Financing of Terrorism and keep them updated properly.

The term trade-based Money Laundering and Financing of Terrorism refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origins or finance their activities. In this practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports.

Misuse of International trade system is one of the main methods by the criminals to integrate their proceeds into the formal economy. As evidence emerges that International trade is becoming heaven of dirty money, the basic techniques of trade-based money laundering include:

Typology and indicative description	Information that may be relevant to assessing ML/TF risk
Over Invoicing: By misrepresenting the price of the goods in the invoice and other documentation (stating it at above the true value) the seller/exporter gains excess value as a result of the payment.	• Product taxonomy (i.e. table of product categorization) • Category of goods • Goods description • Unit price of goods • Quantity of goods • Market price of goods
Under invoicing: By misrepresenting the price of the goods in the invoice and other documentation (stating it at below the true value) the buyer/importer gains excess value when the payment is made.	• Product taxonomy • Category of goods • Goods description • Unit price of goods • Quantity of goods • Market price of goods
Multiple invoicing: By issuing more than one invoice for the same goods a seller can justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than one bank to facilitate the payments/transactions.	• Transaction date • Transactional amount • Product description • Invoice number • Presence of account information of other banks on the invoice • Presence of bank chops on invoice
Under shipping: The seller ships less than the invoiced quantity or quality of goods which misrepresenting the true value of goods in the documents. The effect is similar to over invoicing.	• Product category • Product description • Unit price • Units

Typology and indicative description	Information that may be relevant to assessing ML/TF risk
Over shipping: The seller/ exporter ships more than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to under invoicing.	• Product category • Product description • Unit price • Units
Fake Shipping: No goods are shipped and all documentation is completely falsified. Also known as "ghost shipping" or "phantom shipping" or Fictitious Trades.	• Transaction date • Quantity • Unit price of goods • Presence of transport document • Validity of transport document
Structured transaction: Parties may structure a transaction in a way to avoid alerting any suspicion to Banks or to other third parties which become involved. This may simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it.	• Transaction date • Quantity • Unit price of goods • Presence of transport document • Validity of transport document

So branch shall be more careful and pay closer attention to the Trade Financing activities like over/under invoicing, multiple invoicing, over/under shipment, false description of goods/services and inserting complicated/confusing clauses in the Letter of Credit and use of front companies. In this connection all AD Branches and concerned Divisions of HO shall ensure EDD and precautions in this matter-like various sanctions, Red-flags, trade data, Tariff Schedule etc.

8.2 Trade Related CDD Requirements

Branches will consider the following minimum requirements:

- Comply the customer acceptance policy;
- Ensure collection of complete & accurate KYC information of the customers;
- Be careful enough about HS Code, unit price, credit report of supplier, importer's credibility, over / under invoicing, cash incentives, timely collection of Bill of Entry, submission of EXP form etc.
- Collection of required documents & information such as:
    a. Nature of business including major goods, services and jurisdictions the customer deals with;
    b. Usual delivery / transportation mode for goods or services;
    c. Major suppliers and buyers;
    d. Products and services to be utilized from the bank;
    e. The countries with which the importer trades;
    f. Existing/anticipated account activities;
    g. Usual methods and terms of payment and settlement;
    h. Any observations/ratings on the customer by concerned departments;
    i. Any previous suspicious transaction reports filed with BFIU;
    j. Other information from the relevant staff;
    k. Risk Grading Profile for Trade Customers; and
    l. Trade Transaction Profile.
- Verification of the above documents & information through reliable and independent sources;
- Ascertaining and verifying the identity of the beneficial owners of the trade customer;
- Conducting Enhance Due diligence if required;

- Record Keeping;
- Understanding of the business, the principal counterparties, the countries where the counterparties are located and the goods or services that are exchanged, as well as the expected annual transaction volumes and flows to conduct Customer Due Diligence (CDD) for trade customers;
- CDD information should be updated in accordance with this Guideline;
- Maintaining customer-wise trade transaction profile (TTP) including items of Goods, value, volume, production capacity, end-use of goods and principal counterparty names. TTP should be made available to trade processing staff so that they can easily check that a transaction is within the agreed profile of the customer;
- The CDD processes are expected to include ―feed-back loops where a trigger event in a transaction or normal review process leads to new information or questions about a relationship. This updating of the CDD profile ensures that the information in the CDD profile is current. The event reviews may also lead to the status of the relationship with the customer being escalated for decisions related to additional controls being applied or the exit of the customer;
- Branches should follow the process of "customer level risk assessment", use Risk Grading Profile mentioned for every Trade Customers to assess the risk of customer and follow the process of "Transaction Level TBML Risk Assessment & Mitigation through 3 Level review System" to assess & mitigate the transactional risk as mentioned in "Guidelines for Prevention of Trade Based Money Laundering of National Bank Limited".
- Branch are required to screen/check the persons, entities, third parties, goods, country, ports, point of transshipment, carrier, master, agents and/or any other names or entities appearing in LC, sales contract and/or presented document related to trade transactions against the names in the Targeted Financial Sanctions databases of UNSC, OFAC & BFIU. If there is any name match, it is required to take reasonable and appropriate measures to verify and confirm the identity of name(s) match. Once confirmation has been obtained about the true matching, branch must immediately stop the transaction and report it to AMLD so that AMLD can report it to BFIU;
- Branch should aware of the potential red flags related to International Trade as mentioned in "Guidelines for Prevention of Trade Based Money Laundering of National Bank Limited".

CHAPTER 09

TECHNOLOGY BASED MONEY LAUNDERING

Now-a-days Internet Banking, Mobile Banking, SMS Banking, ATM, CDM, POS, Debit/Credit/Pre-paid Card, Virtual Money, Stored value Cards (Gift card, reloadable cards, pay roll cards, etc.) Internet/web based payment system has been identified as the most vulnerable to Money Laundering & Financing of Terrorism vehicle and fraudulent activities. E-commerce/payment has got attractive users for various reasons i.e. convenience, speed, reliability, cost mobility, location, etc. On the other hand, technology has also advanced our ability to monitor and identify suspicious activities. Side by side Money Launderers and criminals are also taking this kind of facilities to legalize their illicit fund. So, "non-face to face customers" should be exercised with EDD with sufficient information and identification. All payment and settlement system (clearing, payment or settlement service or all of them) including cross border transactional activities of our bank shall be governed by the regulations of "Bangladesh Payment and Settlement Systems Regulations 2009" and "BEFTN Operating Rules" in line with AML/CFT procedure, guidelines as prescribed by Bangladesh Bank from time to time.

In case of introduction of technology based new services/system (i.e. internet banking, electronic card, e-KYC, swift transaction platform etc) or development of existing product/services/technology; Bank shall identify ML/TF risk and calculate the degree of risk and take appropriate measures to address the risk related to such product/services/technology. The measures should be taken before introduction of newly invented products/services/technology or the introduction of newly developed products/services/technology.

9.1 Wire Transfer

"Wire transfer" refers to such financial transactions that are carried out on behalf of an originator/applicant (person or institution) through a bank or financial institution by electronic means with a view to making an amount of funds available to a beneficiary person/institution of another bank or financial institution. Here, originator/applicant refers to the person or institution (account holder/non account holder) who request the ordering financial institution to perform the wire transfer. On the other hand, beneficiary refers to the person or institution (account holder/non account holder) who is identified by the originator as the receiver of the requested wire transfer.

9.1.1. Cross-border wire transfers

Cross-border wire transfer means any wire transfer where the originator and the beneficiary bank or financial institution are located in different countries. It may include any chain of wire transfers that has at least one cross-border element. To mitigate the money laundering risk, officers should ensure the following tasks:

i. Under general or special consideration in case of threshold cross-border wire transfers of 1000 (one thousand) or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank. In this information, originator's account number or Unique Transaction Reference Number (incase not having account number) has to be included; so that this transaction can be easily found later. Besides in the beneficiary's information, beneficiary's account number or Unique Transaction Reference Number (incase not having account number) has to be included; so that this transaction can be easily found later.
ii. Furthermore, for cross-border wire transfers, below the threshold (mentioned in above 9.1.1.i) full and meaningful originator/beneficiary information i.e. name, address, account number/ Unique Transaction Reference Number has to be included; so that this transaction can be easily found later.

iii. For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved;
iv. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file has to contain required and accurate originator information, and full beneficiary information. In addition, bank should include the account number or Unique Transaction Reference Number (incase not having account number) of the originator/beneficiary; so that this transaction can be easily found later.

9.1.2. Domestic wire transfers

Domestic wire transfer means any wire transfer where the originator and beneficiary institutions are located in the same country. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to effect the wire transfer may be located in another country. To mitigate the money laundering risk, officers should ensure the following tasks:

i. Branch shall follow the CDD measures as per chapter 5 and instructions of per section 9.1.1 of this guideline to identify and verify the applicant/beneficiary.
ii. In case of wire transfer using credit or debit cards (except purchase of goods and service), Branch shall preserve information as such section 9.1.2(i) in the payment instruction/message;
iii. It is not compulsory to comply above instructions in case of wire transfers in favor of Government/Semi-government/Autonomous organizations. Besides the section 9.1.2(i) also not applicable for interbank transactions.

9.1.3. Other instruction related to wire transfer

i. All parties related to wire transfer must comply the circulars issued by Bangladesh Bank, BFIU & NBL and other applicable acts, rules & regulations;
ii. Branch must follow the instruction of Customer acceptance policy that is set out at section 4.1 of this guidelines and instruction given in section 1.19 of this guidelines.

9.2 Duties of Ordering, Intermediary and Beneficiary Bank in Case of Wire Transfer

9.2.1 Ordering Bank

The ordering bank should ensure that qualifying wire transfers contain complete and accurate originator information, and required meaningful beneficiary information. These information has to be preserved minimum for 5 (five) years and provide these information as desired by the competent authority without delay. Cross border/ domestic wire transfer shall not be executed unless the ordering bank complies the instructions as per section 9.1 of this guidelines.

9.2.2 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. Bank should initiate measures to identify wire transfers that lack required originator or required beneficiary information. 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 develop 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.

9.2.3 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 beneficiary financial institution should develop 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.

9.3 Online Transactions

Investigations of major money laundering and terrorist financing cases as well as fraud cases over the last few years have shown that criminals make extensive use of online transaction system. In most cases, the identity of the depositor or the ultimate beneficiary is not clearly shown in an online transaction instruction. Following the recent focus on terrorist financing, branches are required to include accurate and meaningful originator (name, account number, address and where possible contact phone number) and beneficiary information (account name and/or account number) on all outgoing funds transfers and related messages that are sent, and this information should remain with the transfer or related message throughout the payment chain. Branches should conduct enhanced scrutiny of and monitor for suspicious incoming fund transfers which do not contain meaningful originator information. In case of online transaction, made by a person other than the customer, branches are required to confirm the identity and address of the customer. In such case the branch must collect KYC information as per the format given in Annexure: D.

9.4 Internet Banking

It is recognized that on-line transactions and services are convenient. However, it is not appropriate that bank should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures.

However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied in accordance with this guideline and guidelines of BFIU.

9.5 CDD Requirements for Technology Related Products

- Branch must collect KYC & other information of the customer as per section 5.3 of this guidelines.
- Branch shall conduct CDD measures on customer, authorized person(s) or professional representative, if any, and beneficiary owner(s) as specified in the section 5.4 of this guidelines;
- If the customer is categorized as high risk account, Branch must apply EDD as specified in the section 5.8 of this guidelines.
- Branch shall also conduct CDD measures on agents, distributors, merchants or any other third party(s) related to delivery of technology related customer services, if any, as specified in the section 5.4 of this guidelines;
- Branch shall set limits such as amount limit, maximum number of transactions limit per day, maximum amount limit per transaction, maximum cumulative amount per day, maximum purchase/shopping limit per transaction, maximum cumulative purchase/shopping limit per day, maximum cash withdrawal limit per transaction, maximum cumulative cash withdrawal limit per

day, maximum transaction limit per merchant, geographic limit, etc. considering functionality of product, ML/TF risks, the circulars of the Department of Currency Management & Payment Systems Department of Bangladesh Bank, and Bangladesh Bank other circulars & Guidelines for Foreign Exchange Transactions in addition to their other existing considerations.

- Branch shall take reasonable measures to establish the source of fund of the customer.
- Branch shall take reasonable measures to collect source of fund and complete & accurate information of the third party in case of cash or anonymous repayment by the third party.
- Branch must make a list of high risk accounts and apply applicable ongoing CDD measures.
- Branch must monitor the transactions of accounts which are getting technology based product's facilities in a regular basis and generate STR report whenever there is any unusual or suspicious transaction.
- Branch should ensure that agents, distributors, merchants or any other third party(s) related to technology related services, if any, have their own AML/CFT programs and monitor their CDD compliances.
- Branch should follow the instruction of "Anti Fraud Policy & Procedure" of Western Union (WU) & Money Gram to prevent fraud activities;
- Branch must comply the Guidelines for Foreign Exchange Transactions; circulars issued by Bangladesh Bank, BFIU & NBL, Foreign Exchange Regulation Act 1947 & other applicable acts, rules & regulations.

CHAPTER 10

MONITORING OF TRANSACTION

10.1. Monitoring of Transaction

On-going monitoring is an essential aspect of effective KYC procedures. The Bank can only effectively control and reduce its risk if it has an understanding of normal and reasonable account activity of its customers so that it has a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, it is likely to fail in its duty to report suspicious transactions to the appropriate authorities in cases where it is required to do so.

In order to be vigilant for any significant changes or inconsistencies in the pattern of transactions, monitoring of transactions should be done. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the customer. Possible areas to monitor are: -

a) Transaction type
b) Frequency
c) Unusually large amounts
d) Geographical origin/destination
e) Changes in account signatories

- Branch must supervise customer transactions regularly in manual and / or automated system;
- The transactions which are complex, unusual and apparently have no financial or legitimate purpose should be reviewed with utmost seriousness and initiatives should be taken to identify STR/SAR;
- Branch should identify Structuring and report STR to AMLD for onward submission to BFIU, if applicable, as per instructions given in section 11.2 of this guidelines;
- In transaction monitoring, all foreign currency transactions and technology based transactions should also be included;
- The UN Security Council resolution, Individuals or organizations black listed by the Government of Bangladesh and the jurisdiction that do not meet or have significant deficiencies in complying international standards for the prevention of money laundering and terrorist financing are to be taken into consideration in transaction monitoring;
- Monitoring procedure:
    - Any transaction that does not fit within a customer's TP should be reviewed by the Branch Anti Money Laundering Compliance Officer along with concerned officers, to determine whether the circumstances raise to any suspicion of money laundering.
    - Credit and debit card operations should be monitored closely. Accounts with high credit limits and cash-secured credit cards should be subject to a closer scrutiny.
    - Loans and financial guarantees (such as back-to-back lending and standby letters of credit), especially transactions involving the use of entities established in offshore financial centers, should be closely monitored.
    - An employee should judge a transaction to be suspicious, if in their personal judgment, they know or suspect that the transaction might be connected to any criminal offence or activity as detailed in the predicate offences as per the Money Laundering Prevention Act, 2012 (amendment, 2015) and the Anti Terrorism Act, 2009 (Amendment, 2012 and 2013).

10.2. Monitoring of Structuring

Bank shall take precautionary measures to check "Structuring" (or surfing) at the time of Cash Transaction Reporting. Structuring is a money laundering technique, which involves the splitting up of a large cash deposit into a number of smaller deposit (transaction below the CTR threshold/limit) to evade the suspicious activity requirement of the Bank. Structuring can be done in the following ways:

- Regular deposit of cash into accounts in amounts that fall below the reporting threshold.
- Regular use of cash to purchase "instruments" such as bank cheques and bank drafts, or to load into credit or stored value cards in amounts below the reporting threshold.
- Using multiple branches or agencies, often within a short timeframe, to avoid detection.
- Establishing accounts at multiple banks/branches.
- Using third parties to make deposits into a single account or multiple accounts.

CHAPTER 11

REPORTING

11.1. Cash Transaction Reporting (CTR)

The bellow instructions have to be followed for submitting Cash Transaction Report to BFIU:

i. Bank will submit Cash Transaction Report (CTR) on monthly basis to BFIU through AMLD for deposit & withdrawal of Cash by a single or multiple transactions amounting BDT 10.00 lac & above or its equivalent in foreign currency (Including Online, ATM related any cash Deposit or Withdrawal separately) in customers' accounts in a particular day.
ii. Every month's CTR has to be submitted to BFIU within the 21st day of the following month by using goAML web as per instruction of goAML manual. In the process of monthly CTR, IT Division shall generate the monthly CTR data from CBS. AMLD will collect the CTR data from IT Division for onward submission to BFIU;
iii. If any suspicious transaction is found by reviewing CTR, the branch shall submit it as 'Suspicious Transaction Report' to the AMLD for onward submission to BFIU;
iv. IT Division shall ensure preservation of CTR information at their end for at least five years for downloading branch-wise/consolidated monthly CTR information as and when needed at Head Office or branch level. Branch shall preserve the monthly CTR in a file.
v. Cash deposits in the accounts of government (different ministries, local government and different government divisions), government owned organization, semi government or autonomous institutions are not needed to report in CTR but cash withdrawal from these accounts needed to report in CTR;
vi. Cash deposits in the accounts which are operated for collecting salaries/tuition fees from school, college, universities, educational institutions and for collecting government utility bills (electricity, water, gas etc.) are not needed to report in CTR but cash withdrawal from these accounts needed to report in CTR;
vii. In case of inter-bank and inter-branch cash transactions, it does not need to submit in CTR.

11.2. Suspicious Transactions Reporting (STR) & Suspicious Activity Reporting (SAR)

Suspicious transaction or 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. Under Section 25(1)(d) of MLPA, 2012, Reporting Organizations 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.

11.2.1. Definition of STR/SAR

As per Section 2(z) of Money Laundering Prevention Act, 2012 defines suspicious transaction as follows-

"Suspicious Transaction" means such transaction

i. which deviates from usual transactions;
ii. of which there is ground to suspect that
    (1) the property is the proceeds of an offence,
    (2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;
iii. Any other transaction or attempt of transaction delineated in the instructions issued by BFIU & NBL from time to time.

As per Section 2(16) of Anti-Terrorism Act, 2009 defines suspicious transaction as follows-

"Suspicious transaction" means such transactions –

i. which is different from usual transactions;
ii. which invokes presumption that,

(1) it is the proceeds of an offence under this Act,
(2) it relates to financing of terrorist activities or a terrorist person or entity;

iii. Which is any other transaction or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.

Suspicious Activity (SA) arises from suspicion relating to general behavior of the person in question which creates the knowledge or belief that he or she may be involved in illegal activities out of which proceeds might be generated. Any suspicious attempted transaction also falls in this category.

11.2.2. Reporting Process

The final output of an AML/CFT compliance program is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the AML & CFT risk. Therefore it is necessary to find out the suspicious transaction and suspicious activity for the safety and soundness of the bank.

In order to prepare an effective intelligence report or to have leads for a quality report, a complete STR is an essential requirement, i.e. the information submitted must be sufficient and complete to establish a connection to be made between the person(s) and the suspicious activity/transaction.

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 to the competent authorities i.e. to BFIU. Suspicion basically involves a personal and subjective assessment. The Branches have to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

In case of reporting of STR/SAR, Branches should conduct the following 3 stages:

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:

i. Comparing the KYC profile, if any inconsistency is found and there is no reasonable explanation;
ii. By monitoring customer transactions;
iii. 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. Annexure: I provides some red flag indicators for identifying STR/SAR related to ML & TF.

All suspicions reported to the AMLD should be documented, or recorded properly. The report should include full details of the customer who is the subject of concern and as a full 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.

This stage is very vital for STR/SAR reporting. Monitoring mechanisms should be more rigorous in high-risk areas and supported by adequate information systems to alert management and other appropriate staffs of unusual /suspicious activity. Training of staff in the identification of unusual/suspicious activity should always be an ongoing activity.

Evaluation: This part must be in place at branch level. After identification of STR/SAR at branch 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, it, along with all necessary supportive documents, has to be sent to the AMLD without any delay. Every stages of evaluation, branch should keep records with proper manner. After receiving report from branch, AMLD 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.

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

11.2.3. Documenting Reporting Decisions

In order to control legal risks or for future reference, it is important that adequate records of SARs and STRs are kept. This is usually done by the CAMLCO and would normally include details of:

a) All SARs / STRs made;
b) How the BAMLCO handled matters, including any requests for further information
c) Assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek additional information;
d) The rationale for deciding whether or not to proceed with SAR/STR;
e) Any advice given or action taken about continuing the business relationship and any relevant internal approvals granted in this respect.

These records can be simple or sophisticated, depending on the size of the business and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. The maintenance and retention of such records is important as they justify and defend the actions taken by the BAMLCO and/or other members of staff and should be made available to the Competent Authorities and BFIU upon request.
For practical purposes and ease of reference, a reporting index could be kept and each SAR/STR could be given a unique reference number.

11.2.4. Reporting Guidance

BFIU implemented a secured online reporting system namely the goAML, which requires AMLD to submit SARs and STRs through this channel. The goAML Web application provides a secure web based interface between the BFIU and its Branch 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.

AMLD shall submit STR/SAR by using goAML web as per instruction mentioned in goAML Manual. (https://www.bb.org.bd/eservices.php). AMLD can also submit STR/SAR manually by using the format prescribed by BFIU (https://www.bb.org.bd/bfiu/reporting_forms.php). Bank shall preserve all information on a reported STR until any further instruction by BFIU.

11.2.5. General Instruction for STR/SAR:

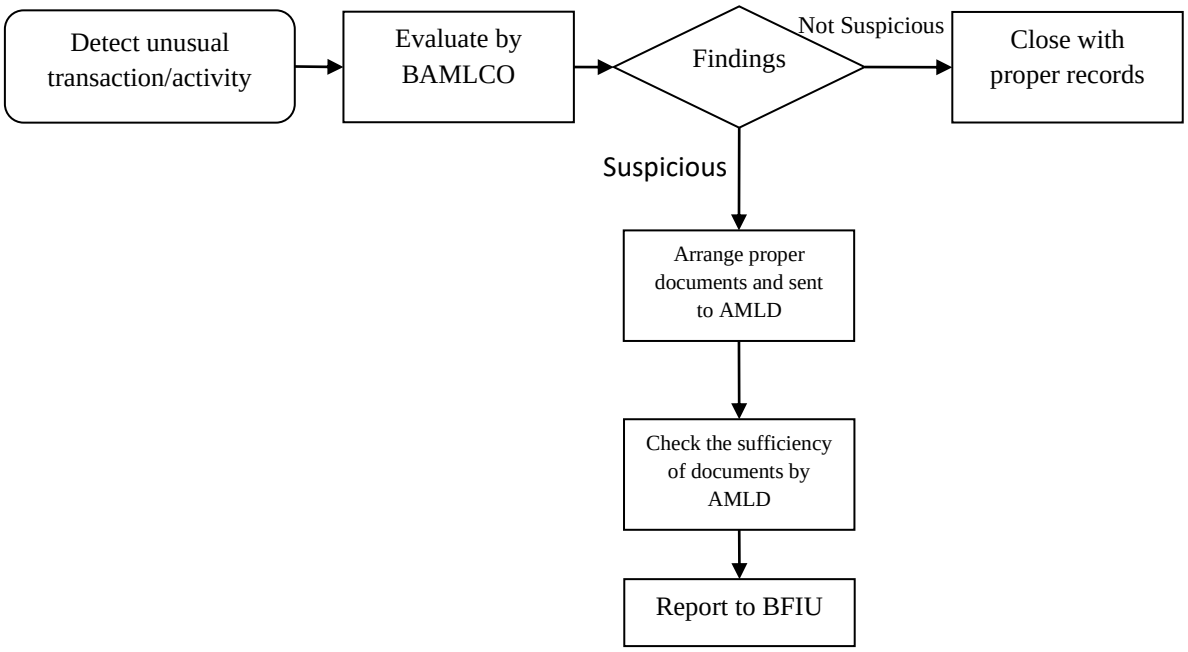
The following instruction shall be followed for submitting STR/SAR to BFIU:

- All officers must be aware & careful for identification of suspicious transaction/activity involved in daily transactions/activities of customers in order to implement the instructions of section 25(1)(gha) of MLPA, 2012 and section 16(1) of ATA, 2009. Some common indicators of suspicious transactions are given in Annexure: I;
- For identifying suspicious transactions, bank officials will consider the definition given in Section 2 (za) of the Prevention of Money Laundering Act, 2012 and Section 2 (16) of the Anti-Terrorism Act, 2009;
- The Branch Money Laundering Prevention Officer should be informed in writing by using Internal Suspicious Transaction Report Form (see Annexure: B) as soon as any suspicious transaction or activity is identified by any officer of the branch. BAMLCO shall analyze the reported transaction or activities immediately and record the observations in detail and preserve it. If the reported transaction/activity is considered as suspicious, BAMLCO shall immediately report it to AMLD as per STR/SAR Form (see Annexure: C) along with the related documents (i.e. Copy of AOF, TP, KYC, Identification documents, Account statement, suspicious transaction's vouchers and other related documents, if any). BAMLCO must preserve the internal suspicious transaction form & STR/SAR form with related documents;
- AMLD shall immediately submit the STR/SAR to BFIU through goAML web as per instruction given in goAML Manual after checking the adequacy of data/information/documents of the suspicious transaction/activity that is reported by the branch and adding relevant information (any any), if applicable;
- AMLD shall submit a transaction/activity as STR/SAR even if it is not identified as suspicious by the branch;
- Branch & AMLD shall keep all the documents of STR/SAR until further notice given by BFIU;
- Bank will follow the "Guidance on Reporting Suspicious Transaction Report for The Reporting Organization" issued by BFIU to identify & report suspicious transaction /activity;
- Suspicious Transactions Reports should not be discussed with anyone other than the BAMLCO and concerned officers of AMLD to avoid the risk of "tipping off".
- Failure to report suspicious and unusual transactions to the AMLD shall be tantamount to gross negligence of duty and disciplinary action;
- Following the submission of a suspicious transaction report, the branch is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal reasons. It must not alert the customer to the fact of the disclosure as to do so will constitute a "tipping-off" offence;

- Particulars of STR forms:

Sl.	Name of Form	From -To	Timing	Format
1	Internal STR/SAR	Officer to BAMLCO	Immediately as and when detect	Annexure: B
2	STR/SAR	BAMLCO to AMLD	Immediately as and when detect	Annexure: C

The following procedures shall be followed to report STR/SAR to BFIU. For simplification, the flow chart given below shows overall STR/SAR evaluation and reporting procedures:



11.2.6. Some Special Scenarios for Reporting

- If a branch fails to perform conducting Customer Due Diligence (CDD) due to the non cooperation of customer and the collected information/data of the customer appears unreliable, branch should submit suspicious transaction/activity report on such customers;
- If branch identifies any account or transaction in the name of listed or proscribed person or entity under any United Nations Security Council Resolution or any person or entity listed or proscribed by Bangladesh Government or any individual or entity directly or indirectly under their control or association, branch must stop transaction of the account and report BFIU with detailed information within the next working day;
- If any news on Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction is published in the media and if any account of any person or entity related to that activity is maintained with the branch, detailed information must be reported to BFIU without any delay.

11.3. Tipping off

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.

A 'tipping off' offence occurs when any person discloses, either to the person who is the subject of a suspicion or any third party, that:

a) Information or documentation on ML/TF has been transmitted to BFIU;
b) A SAR/STR has been submitted internally or to BFIU;
c) Authorities are carrying out an investigation/search into allegations of ML/TF;

Tipping-off may also occur in those cases when an employee approaches the client to collect information about the internal on-going investigation, and through the intense questioning, the client becomes aware of the investigation.

Section 6 of MLPA 2012 and FATF Recommendation 21 prohibits reporting organization, their directors, officers and employees from disclosing the fact that an STR/SAR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the Branch is seeking to perform its CDD obligation in those circumstances. The customer's awareness of a possible STR/SAR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation.

Branch shall 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.

Branch shall report suspicious transaction/activity without performing Customer Due Diligence (CDD) if there is reasonable ground that Tipping Off may take place in the event of performing CDD for any transaction suspected to be related to ML & TF.

11.4. Penalty

As per Section 25 (2) of MLPA, if any reporting organization fails to report STR/SAR, a fine of at least taka 50 (Fifty) Thousand but not exceeding taka 25 (Twenty Five) lacs can be imposed on the reporting organization. In addition to the fine, BFIU may cancel the license or the authorization for carrying out commercial activities of the said organization or any of its branches, service centers, booths or agents, or as the cause may be, shall inform the registration or licensing authority about the fact so as to be relevant authority may take appropriate measures against the organization.

Penalty of Tipping Off

Under section 6 of MLPA, 2012, if any person, institution or agent empowered under this Act divulges 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 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.

11.5. Safe Harbor Provision

In section (28) of MLPA, 2012 provides the safe harbor for persons submitting suspicious reports.

As per Section 28 of MLPA, no suit or prosecution or administrative measures or any other legal proceedings shall lie against any reporting organization or its Board of Directors or any of its officers or staffs for anything which is done in good faith under this Act or Rules made there under for which any person is or likely to be affected.
Disclosure of information in good faith by a Branch or by an employee or director of such a Branch shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

11.6. Self Assessment and Independent Testing Procedures

For prevention of money laundering and combating the financing of terrorism and reviewing the Self Assessment report from Branches and proper judgment of Independent Testing Procedures, adequate manpower should be allocated to ICCD whose have to knowledge regarding AML/CFT related existing Laws, Rules, Instructions of BFIU and instruction of this guideline.

11.6.1. Branch obligations regarding Self Assessment:

a. Each and every branch must assess their performance at half yearly basis as per format given in Annexure: H.

b. Before finalizing the evaluation report, Branch should arrange a meeting presided over by the branch manager with all concerned officials of the branch. In the meeting, Branch will discuss the draft of Branch Evaluation Report and if it is not possible to resolve the identified issues at the branch level, it will refer the matter to the ICCD and AMLD at the Head Office. The progress of the recommendations sent to the head office for resolving the issues will be discussed at the next quarterly meeting.

11.6.2. Obligations of ICCD regarding Self Assessment & Independent Testing Procedure

- ICCD shall assess the branch Self Assessment report 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 AMLD.
- While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the ICCD should examine the AML/CFT activities of the concerned branch using the specified checklists (See Annexure: G) for the Independent Testing Procedure and prepare a report after determining the rating of the branch and send it to the respective branch. Besides, ICCD shall conduct separate inspection on minimum 10% (ten percent) of the total branch in addition of normal course of annual audit based on the checklist of Independent Testing Procedures and prepare a report after determining the rating of the branches.
- The ICCD should send a copy of the report with the rating of the branches inspected/audited by the ICCD to AMLD.

11.6.3. Obligations of AMLD regarding Self Assessment & Independent Testing Procedure

i. Based on Self Assessment reports that received from the branches and inspection/audit reports that submitted by the ICCD, AMLD shall prepare a checklist based evaluation report on the inspected branches in a considered half year time. In that report, beside other topics, the following topics must be included:

   a. Total number of branch and number of self assessment report received from the branches;
   b. The number of branches inspected/audited by ICCD at the time of reporting and the status of the branches (branch wise achieved number);
   c. Same kinds of irregularities that have been seen in maximum number of branches according to the received self assessment report and measures taken by the AMLD to prevent those irregularities;
   d. The general and special irregularities mentioned in the report submitted by the ICCD and the measures taken by the AMLD to prevent those irregularities;
   e. Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as ‘unsatisfactory’ and ‘marginal’ in the received report.

ii. Based on the Self Assessment report received from the branches, if there is any risky matter realized in any branch, AMLD have to inspect instantly that branch or initiate to inspect through ICCD and it should be brought to the notice of the competent authorities.

11.7. Maintain Secrecy

Branch should maintain secrecy strictly about the information of identification or reporting of STR/SAR and shall also ensure proper secrecy of the sensitive information that searched by BFIU and AMLD. In this regard, the instructions given in the circular letter No. 1 issued by BFIU on 22/04/2018 will be followed.

CHAPTER 12

RECRUITMENT, TRAINING AND AWARENESS

12.1. Recruitment

To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, the following instructions should be considered during recruitment of officers:

- Proper Screening Mechanism in case of recruitment. The Human Resources Division (HRD) must ensure that employee screening mechanism is an integral part of the recruitment process; and
- Sufficient number of skilled officers should be posted in AMLD.

ML & TF risks arose by or through its employees can be minimized if fair recruitment procedure is followed. 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, HRD is advised to 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, banks 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.

12.2. 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. KYE requirements should be included in the banks HR policy.

12.3. Training for Employee

Following steps have to be ensured for proper implementation of the AML/CFT program:

i. Providing appropriate AML/CFT training to all employees. Here, appropriate training means the training for officials of different levels & departments on foundation and their activities related AML/CFT and training at regular intervals;
ii. Providing appropriate training and/or taking initiatives to get professional certification by the CAMLCO, DCAMLCO and concerned officers to enhance work efficiency;
iii. Preservation of training related all information & documents.

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, banks

are required to impart refreshment 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;
- Instruction of this guideline, AMLD circular, circular letters and guidelines;
- STR/SAR reporting procedure;
- Ongoing monitoring and sanction screening mechanism.

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.

12.4. AWARENESS

Awareness against money laundering, terrorist financing & financing of proliferation of weapons of mass destruction is the most important activity of the financial institutions. National bank should take different initiatives to build the awareness against Money Laundering & Terrorist financing among the employees, customers and mass people. These awareness building programs also includes the Board of Directors, the policymakers and the Management of the bank.

12.4.1. Awareness of Senior Management

The senior Management of the bank should be aware of the issues related to AML/CFT activities in the country. This is mainly necessary in order to implement the AML/CFT measures in the bank. In this regard, the bank shall arrange, at least once a year, an awareness building program for the members of the Board of Directors of the bank. In absence of the Board of Directors, the members of the highest policy making committee and any other people engaged in making policy for the bank should participate in these awareness building programs.

12.4.2. Awareness of Customer

The customers of the bank are the prime groups that should be made aware of AML/CFT activities taken by the banks. Branch will inform the customer about the reasons for collecting various information and documents from customer during opening of account. Bank shall take initiatives to make aware the customers by hanging banners/festoons at branches showing the impact & consequences of money laundering & terrorist financing over the personal life, society, economy as well as the whole country. Leaflets and handbills shall also be distributed to make aware the customers against money laundering & terrorist financing. In addition, awareness programs & documentaries shall be promoted through various media including mass media to prevent money laundering and terrorist financing.

12.4.3. Awareness of Mass People

There are many negative effects of money laundering and terrorist financing on the society, economy and the country as a whole. The mass people should be made aware of these negative effects. In this connection, the bank should take different steps like circulating/ broadcasting/ telecasting appropriate advertisements and documentaries on radios, televisions and other mass media. In addition, the bank may take different steps like using billboards, posters, festoons, leaflets, handbills and other media to aware the mass people. The bank should also participate in awareness building initiatives arranged by BFIU, Bangladesh Bank, the government and other regulatory bodies.

CHAPTER 13

RECORD KEEPING

13.1. Record Keeping

Branch should preserve the necessary information/documents at least for five years after termination of relationships with the customers:

- All necessary information/documents of customer's domestic and foreign transactions;
- All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer;
- All necessary information/documents of walk-in Customer's transactions.

Branch shall preserve the information/documents related to AML/CFT training, conference, inspection/audit and special audit.

Branch shall present the preserved information/documents as evidence in the judicial process related to criminal activities, if applicable. Branch shall made available the information & documents to the competent authorities upon demand/instruction without delay.

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

- Requirements of legislation and BFIU directives are fully met;
- Competent third parties shall be able to assess the bank's observance of money laundering policies and procedures;
- Any transactions effected via the bank can be reconstructed;
- Any customer can be properly identified and located;
- All suspicious reports received internally and those made to AMLD & BFIU can be identified;
- All cash transactions above Cash Transaction Report (CTR) limit can be identified and retrieved; and
- The bank can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.

Records relating to verification of identity shall generally include:

- 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.

Records relating to transactions shall generally include:

- Details of personal identity, including the names and addresses, etc. as prescribed in this guideline, Uniform Account Opening Form and subsequent directives pertaining to:
    a. The customer;
    b. The beneficial owner of the account or product;
    c. The non-account holder conducting any significant one-off transaction;
    d. The respondent (under correspondent banking relation)
    e. Any counter-party;
- Details of transaction including:
    a. The nature of such transactions;
    b. The volume of transactions and the currency in which it was denominated;
    c. Customer's instruction(s) and authority;
    d. Source(s) of funds;

e. Destination(s) of funds;
f. Book entries;
g. Custody of documentation;
h. The date of the transaction;
i. The form (e.g. Cash, cheque) in which funds are offered and paid out.
j. Cash transaction report (CTR)
k. The parties to the transaction
l. The identity of the person who conducted the transaction on behalf of the customer

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 closing of an account;
ii. The providing of any banking services;
iii. The carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
iv. The ending of the business relationship; or
v. The commencement of proceedings to recover debts payable on insolvency.

Branch should ensure that records pertaining to the identification of the customer, his address (e.g. copies of documents like passports, national ID card, driving licenses, Trade licenses, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended and should be made available to the competent authorities upon request without delay.

13.2. Records to be kept by Branch

With a view to streamlining the AML/CFT activities Branches shall maintain at least following related files in addition to other required files as and when needed for their operational convenience:

i. AML/CFT related Policies & guidelines
ii. AML/CFT related Acts & Rules
iii. AML/CFT related Circulars & circular letters issued by BFIU, AMLD from time to time;
iv. Account Information & Freezing related file as issued by AMLD;
v. MD's yearly message file;
vi. BAMLCO Nomination File;
vii. AML/CFT Training, Workshop/Awareness record file;
viii. Cash Transaction Report file (serially month wise hard copy);
ix. Suspicious Transaction/Activity Report (STR/SAR) file;
x. Quarterly meeting Notice, Agenda and Minutes on AML/CFT issues file;
xi. Self-Assessment report (Half yearly) file;
xii. Internal and External AML/CFT Inspection Report and their Compliances file;
xiii. Independent Testing Procedure (ITP) file;
xiv. Sanction screening file;
xv. False positive file;
xvi. High Risk Account Monitoring (as per KYC) file;
xvii. PEPs & IPs Account Monitoring file;
xviii. Structuring identification file;
xix. Transaction Monitoring file;
xx. Transaction Profile (TP) Exception file;
xxi. Trade Transaction Monitoring file;
xxii. Legacy Account List;
xxiii. Any other files as instructed by AMLD.

13.3. Formats and Retrieval of Records

To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. Branch shall retain all the documents relating to customer identity and transaction at the premises of the branch physically. Simultaneously the branch shall hold the same in electronic form so that they can be reproduced and recollected without undue delay.

However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held in hard copy or electronically must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

13.4. Investigations

When the bank submits a report of suspicious transaction to BFIU or where it is known that a customer or transaction is under investigation, it shall not destroy any records related to the customer or transaction without the approval of BFIU even though the five-year limit may have been reached. To ensure the preservation of such records the bank shall maintain a register or tabular records of all investigations made to it by BFIU or any other authorized agencies and all disclosures to them. The register shall be kept separate from other records and contain as a minimum the following details:

i. The date of submission and reference of the STR/SAR
ii. The date and nature of the enquiry,
iii. The authority who made the enquiry and reference
iv. Details of the account(s) involved; and

Therefore a report of a suspicious transaction or the bank is aware of a continuing investigation into money laundering relating to a customer or a transaction, records relating to the transaction or the customer should be retained until confirmation is received that the matter has been concluded.

13.5. Training Records

The bank shall demonstrate that it has complied with the regulations concerning staff training; it must maintain training records which include:

i. Details of the content of the training programs 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/terrorist financing requirements; and
v. An on-going training plan.

The records of training shall be preserved at Head Office level as well as branch level.

Conclusion

Effective AML/CFT activities have beneficial consequences for financial institutions. Taking effective action against money laundering and terrorist financing makes a positive contribution to the well-being and safety of the institution and its employees and shareholders. The management of NBL is fully aware that this financial system shall not be and cannot be used as a channel for criminal activities. So we should all come forward to combat against this evil force by implementing the instructions of AML/CFT policy guidelines of National Bank Limited.

Annexure

Annexure: A

Indicative documentation required to be submitted by the customer

At the time of opening of account, the following documents needs to be collected from the customer, where applicable. NBL may review & determine the required documents that need to be obtained from customer from time to time based on emerging business needs & guidelines issued by NBL:

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Individuals & Joint Account (including illiterate person, pardanashin ladies, minor & guardian) <u>Key issue:</u> Name Source of Fund Address Telephone	1. Valid Passport 2. National ID card 3. Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) 4. TIN (if any) 5. Valid driving license (if any) 6. Photo of Account Holder(s) 7. Any other documents that satisfy to the bank. **NB:** It is mandatory to provide at least one document mentioned in serial no. 1 to 3. But in case of submitting the birth registration certificate, any other photo ID (issued by a Government department or agency) of the customer has to be supplied with it. If he does not have a photo ID, then a certificate of identity by any **renowned person**** has to be submitted. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number. That certificate must include a photo of the customer which is duly attested by the signing renowned person. **Here **renown person** refers to member of parliament, Mayor, Deputy Mayor and Councilors of the City	• Salary Certificate (for salaried person) • Documents in support of beneficial owner's income (income of house wife, students etc.) • Trade License if the customer declared to be a business person • Employed ID (For ascertaining level of employment). • Self declaration acceptable to the bank. (commensurate with declared occupation) • TIN (if any) • Documents of property sale. (if any) • Other Bank statement (if any) • Document of FDR encashment (if any) • Document of foreign remittance (if any fund comes from outside the country) • Document of retirement benefit/ Bank loan.	• Acknowledgement receipt of thanks letter through postal department. • Third party verification report. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency

	Corporation, Gazetted Officials of 9th grade and above as per National Pay Scale, Teachers of Public University, Chairman and Vice-Chairman of Upazilla Parishad, Chairman of Union Parishad, Mayor and Councilors of Municipality, Professor of Private University, Principal of Private College, Head Master of Private High School, Editor of National Daily Newspaper, Notary Public, Officials of 7th grade and above as per National Pay Scale of Semi Autonomous /Autonomous/ Government Entities and Officials of 9th grade and above as per National Pay Scale of Bangladesh Bank.		

Customer type	**Standard Identification document**	**Document for verification of source of funds**	**Document or strategy for verification of address**
Sole Proprietor ships or Individuals doing business Key issue: • Shop name • Shop Address • Name of proprietor and residence address • Telephone number. • Source of Fund	1. National Id Card of owner 2. Passport of owner 3. Birth Registration Certificate of owner (Printed copy, with seal & signature from the Registrar) 4. Valid driving license of owner (if any) 5. Credit Card of owner (if any) 6. Rent receipt of the shop (if the shop is rental) / Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents). 7. Membership certificate of any association. i.e. Chamber of commerce, market association, trade association i.e.;	• Trade License • TIN • Self declaration acceptable to the bank. (commensurate with nature and volume of business) • Documents of property sale. (if injected any fund by selling personal property) • Other Bank statement (if any) • Document of FDR encashment (if any fund injected by en-cashing personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan (if any) • Personal borrowing (if any)	• Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official. • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government agency.

	Hardware association, cloth Merchant association, hawker's association etc. (if any) 8. Photo of owner(s) 8. Any other documents that satisfy to the bank. **NB:** It is mandatory to provide at least one document mentioned in serial no. 1 to 3. But in case of submitting the birth registration certificate, any other photo ID (issued by a Government department or agency) of the customer has to be supplied with it. If he does not have a photo ID, then a certificate of identity by any **renowned person****		

Customer type	**Standard Identification document**	**Document for verification of source of funds**	**Document or strategy for verification of address**
Partnership firms Key issue: • Legal name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners. • Source of Fund	• Partnership deed/ partnership letter • Registered partnership deed (if registered) • Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. • Passport of partners / National Id Card of partners / Birth Registration Certificate of partners (Printed copy, with seal & signature from the Registrar) • Valid driving license of partners (if any) • Credit Card of partners (if any) • Rent receipt of the shop (if the shop is rental) / Ownership documents of the shop (i.e. purchase	• Trade License • TIN • Documents of property sale. (if injected any fund by selling personal property) • Other Bank statement (if any) • Document of FDR encashment (if any fund injected by en-cashing personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan (if any) Personal borrowing (if any)	• Telephone bill in the name of firm/ partners. • Rent receipt of the shop (if the shop is rental) • Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents). • Acknowledgement receipt of thanks letter through postal department. • Third party verification report. • Physical verification report of bank official Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the

	documents of the shop or inheritance documents) • Membership certificate of any association. i.e. Chamber of commerce, market association, trade association i.e.; Hardware association, cloth Merchant association, hawker's association etc. (if any) • Photo of Partners • Any other documents that satisfy to the bank.		name of the applicant or his/her parent's name. • Address appearing on an official document prepared by a Government Agency

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Accounts of Private Limited Companies <u>Key issue:</u> • Name of the company Address • Principal place of business • Mailing address of the company • Telephone /Fax number	• National Id Card / Passport of all the directors • Certificate of incorporation • Memorandum and Articles of Association • Update list of directors (form XII) • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Photo of account operators • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee, officer or director of the company.	• A copy of last available financial statements duly authenticated by competent authority • Other Bank statement • Trade License • TIN • VAT registration • Bank loan	

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Accounts of Public Limited Companies <u>Key issue:</u> • Name of the company Address • Principal place of business • Mailing address of the company • Telephone /Fax number	• Passport /National ID Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form–XII • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Photo of operators • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee, officer or director of the company.	• A copy of last available financial statements duly certified by a professional accountant • Other Bank statement (If any) • Trade License • TIN • VAT registration • Bank loan • Cash flow statement • Any other genuine source	

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Government-Owned entities	• Permission Letter from Competent Authority to open an account and identification of those who have authority to operate the account. • Passport / National Id Card of the operator (s) • Photo of account operators		
NGO	• Copy of National ID Card / Passport of the operator (s) • Resolution of the board of directors to open an account and identification of those who have authority to operate the account.	• A copy of last available financial statements duly certified by a professional accountant.	

	• Documents of nature of the NGO • Certificate of registration issued by competent authority • Bye-laws (certified) • List of Management • Photo of account operators • Committee/ Directors	• Other Bank statement • TIN • Certificate of Grand/Aid	
Charities or Religious Organizations, <u>Key issue:</u> • Name of the company Address • Principal place of business • Mailing address of the company • Telephone /Fax number • Source of fund	• National Id Card /Passport of the operator (s) • Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the Organizations • Certificate of registration issued by competent authority (if any) • Bye-laws (certified) • List of Management • Photo of account operators • Committee/Directors	• A copy of last available financial statements duly certified by a professional accountant. • Other Bank statement • Certificate of Grant/Aid/donation • Any other legal source	
Clubs or Societies	• Bye-laws • Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the Organizations • Certificate of registration issued by competent authority (if registered) • List of Management • National Id Card / Passport of the operator (s), Chairman, Secretary General, Treasurer etc • Photo of account operators, Chairman, Secretary General, Treasurer etc • Information of Committee Directors	• A copy of last available financial statements duly certified by a professional (if registered). • Other Bank statement • Certificate of Grant/ Aid • Subscription • If unregistered declaration of authorized person/ body.	
Cooperative Societies	• Bye-laws attested by cooperative officer • Details of officers/office bearers • Resolution of the Executive Committee to open an account	• A copy of last available financial statements duly certified by a professional.	

	and identification of those who have authority to operate the account. • Certificate of Registration • National Id Card / Passport of the operator (s), • Photo of account operators	• Other Bank statement Certificate of Grant/ Aid Subscription	
Trusts & foundations. Key issue: • Names of trustees, settlors, beneficiaries and signatories. • Names and addresses of the founder, the managers /directors and beneficiaries • Telephone/ fax numbers.	• Certificate of registration, if registered / • National Id Card/Passport of the trustee (s) • Resolution of the Managing body of the Foundation/Association to open an account and identification of those who have authority to operate the account • The trust Deed for verification with copy certified by the Chairman. (The deed should empower the trustees to open Bank Account) • A list of the names of trustees with their signatures attested by the Chairman. • Bye-laws (certified) • Photo of account operators • Power of Attorney grated to transact business on its behalf	• A copy of last available financial statements duly certified by a professional (if registered) • Other Bank statement • Donation	• Telephone Bill.

Customer type	**Standard Identification document**	**Document for verification of source of funds**	**Document or strategy for verification of address**
Financial Institutions (NBFI)	• Passport / National ID Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form -XII • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf.	• A copy of last available financial statements duly certified by a professional accountant. • Other Bank statement • Trade License • TIN • VAT registration • Cash flow statement	

	• Photo of account operators • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, Holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee, officer or director of the company.		
Embassies	• Valid Passport with VISA of Authorized official. • Clearance from the foreign ministry • Other relevant documents in support of opening account.		
Private School, College & Madrasha	• Passport / National ID Card of the members of Governing Body/ Managing Committee • Resolution of the Governing Body • Photo of account operators		

Annexure: B

Internal Suspicious Transaction/Activity Report Form

Strictly Private & Confidential

To	**Branch Anti Money Laundering Compliance Officer (BAMLCO)**	**Date:**
Form	**Name:** **Designation:**	**Branch/Department:** **Ref. No:**

Details of STR/SAR:

Customer/Entity Name:	Activity/Transaction Date(s):
Account Number(s)(if any):	Related documents of Transaction & Account attached : ☐ YES ☐ NO
Description of activity/transaction(s). *(Nature of transaction, Origin & destination of Transaction etc.)*	
Source of funds and purpose of transaction *(ask customer tactfully, if necessary & avoid tipping off)*	
Reasons why you think the activity/transaction is suspicious (Give as much details as possible) Signature of Bank official	

TO BE COMPLETED BY BAMLCO
ACTION TAKEN TO VALIDATE ☐ Received on _____ ☐ Reviewed account documentation on _____ ☐ Discuss with the manager (if necessary) on _____ ☐ Other _____
AGREED SUSPICIOUS: ☐YES ☐NO
COMMENTS OF BAMLCO: Signature Date. BAMLCO

Annexure: C

SUSPICIOUS TRANSACTION REPORT (STR)

(For Banks and Non Bank Financial Institutions)

A.	Reporting Institution:	
	1. Name of the Bank	National Bank Ltd.
	2. Name of the Branch	
B.	Details of Report:	
	1. Date of sending report	
	2. Is this the addition of an earlier report?	Yes ☐ No ☐
	3. If yes, mention the date of previous report	
C.	Suspect Account Details:	
	1. Account Number	
	2. Name of the Account	
	3. Nature of the Account (Current/savings/loans/others, please specify)	
	4. Nature of Ownership: (Individual/proprietorship/partnership/company/other, pls. specify)	
	5. Date of Opening:	
	6. Address:	
D.	Account holder details:	
	1. Name of the account holder	
	2. Address	
	3. Profession	
	4. Nationality	
	5. Other account(s) number (if any)	
	6. Other business	
	7. Father's Name	
	8. Mother's Name	
	9. Date of birth	
	10. TIN	
	11. NID/Passport/ other doc. no.	
	12. Mobile Number	
E.	Introducer Details:	
	1. Name of introducer	
	2. Account number	
	3. Relation with account holder	
	4. Address	
	5. Date of opening	
	6. Whether introducer is maintaining good relation with bank	

F. Reasons for considering the transaction(s) as unusual/suspicious:

a. ☐ Identity of clients
b. ☐ Activity in account
c. ☐ Background of client
d. ☐ Multiple accounts
e. ☐ Nature of transaction
f. ☐ Value of transaction
g. ☐ Other reason (Pls. Specify)

……

(Mention Summary of suspicion and consequence of events)
[To be filled by the BAMLCO]

G. Suspicious Activity Information:
Summary Characterization of suspicious activity:

a. ☐	Bribery/Gratuity	h. ☐	Counterfeit debit/credit card	o. ☐	Mortgage Loan Fraud
b. ☐	Check Fraud	i. ☐	Counterfeit instrument	p. ☐	Mysterious Disappearance
c. ☐	Check Kitting	j. ☐	Credit card fraud	q. ☐	Misuse of position or self Dealing
d. ☐	Commercial loan fraud	k. ☐	Debit card fraud	r. ☐	Structuring
e. ☐	Computer intrusion	l. ☐	Defalcation /Embezzlement	s. ☐	Terrorist Financing
f. ☐	Consumer loan fraud	m. ☐	False statement	t. ☐	Wire Transfer Fraud
g. ☐	Counterfeit check	n. ☐	Identity Theft	u. ☐	Other …….

H. Transaction Details:

Sl. No.	Date	Amount	Type*

**Cash/Transfer /Clearing /TT/etc.*

Add paper if necessary

I. Counter Part's Details:

Sl. No.	Date	Bank	Branch	Account No.	Amount

J. Has the suspicious transaction/activity had a material impact on or otherwise affected the financial soundness of the bank? Yes ☐ No ☐

K. Has the bank taken any action in this context? If yes, give details.

L. Documents to be enclosed:
1. Account opening form along with submitted documents
2. KYC Profile. Transaction Profile
3. Account statement for last one year
4. Supporting Voucher/correspondence mention in Sl. No. H

Signature:
(BAMLCO)
Name:
Designation:
Phone:
Date:

Annexure: D

KYC for Walk-in/ One -off Customers

As per AML/CFT policy, satisfactory evidence of identification has to be obtained from the applicants who do not maintain accounts with us for conducting one off transactions. You are therefore kindly requested to provide the following details, together with appropriate documentary evidence, before this transaction may proceed.
Thank you for your co-operation.

<table>
<tr><td colspan="2">Name:</td></tr>
<tr><td>Occupation:</td><td>Nationality:</td></tr>
<tr><td>Father/Husband’s name:</td><td>Date of birth:</td></tr>
<tr><td>Mother’s name:</td><td>Phone/Mobile:</td></tr>
<tr><td colspan="2">Ref No. (If Any):</td></tr>
<tr><td colspan="2">Address:</td></tr>
<tr><td colspan="2">Identification Documents: (ID Card number, Passport details etc.):

☐ Photocopy Attached ☐ Photocopy Verified</td></tr>
<tr><td>Value of Transaction:</td><td>Source of Fund:</td></tr>
<tr><td colspan="2">Beneficiary/Remitter Name:
Relation:
Address:
Phone/Mobile:
Account No. (if Any):</td></tr>
<tr><td colspan="2">Purpose of Transaction:</td></tr>
<tr><td>Date:</td><td>Signature of Employee</td></tr>
</table>

Annexure: E

National Bank Limited

_____ Branch

BAMLCO NOMINATION FORM

Date:

1. Name of Officer/Executive: _____.
2. Designation of Officer/ Executive: _____.
3. Date of Joining in NBL: _____ as_____.
4. Date of Joining at the present Branch: _____.
5. Number of training obtained regarding AML & CFT related issues: _____.
6. Last date & place of AML training: _____.
7. Nominated officer/executive has experience in-
   - ☐ Ac opening & KYC maintenance
   - ☐ CTR analyzing
   - ☐ Local Remittance & Foreign Remittance (Inward, Outward)
   - ☐ Batch Operation, RTGS, BEFTN
   - ☐ Over all General Banking
   - ☐ Credit Operation
   - ☐ Foreign Exchange & International Trade
8. The nominated officer has sufficient knowledge on the following:-
   - ☐ Money Laundering Prevention Act-2012 (with Amendment 2015)
   - ☐ Anti Terrorism Act-2009 (with Amendment 2012 & 2013)
   - ☐ AML&CFT Policy Guidelines of NBL
   - ☐ Circulars issued by AMLD, NBL & BFIU
9. Whether the nominated officer/Executive is aware of Sanction Screening Criteria and capable of operating Sanction Screening Software. ☐ YES ☐NO
10. Whether the nominated officer/executive has knowledge regarding computer literature and capable of email communication. ☐ YES ☐NO
11. Reformed BCU Member Information:

Name	Designation	Department/Role
		BAMLCO
		GB Senior Official
		Credit In-charge
		Cash In-Charge
		Foreign Exchange In-charge

12. Mobile Number:_____
13. Functional Designation: ☐ Manager ☐ Second Man

    [As per 3.11 of the AML & CFT Policy Guidelines of NBL either Manager or Second man of the branch (preferably Manager) shall be nominated as the BAMLCO.]

_____ Signature of Proposed BAMLCO (Acknowledged By)

_____ Signature of Branch Manager (Nominated By)

Annexure: F

ANTI-MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM
QUESTIONNAIRE FOR CORRESPONDENT RELATIONSHIP

A. <u>BASIC INFORMATION:</u>

1. Name of Institution: _____
2. Registered Address: _____
3. Website Address: _____
4. Principal Business Activities: _____
5. Regulatory Authority: _____
6. Operational Status:
   • Does your Bank maintain a physical presence in the licensing country? ☐ Yes / ☐ No

B. <u>OWNERSHIP / MANAGEMENT</u>

7. Is your institution listed on any stock exchange? ☐ Yes / ☐ No
   If so, which stock exchange?

   _____
8. If "No" to Q7, please provide a list of the major shareholders holding more than 10% shares in your institution.
   _____
   _____

C. <u>ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CONTROLS</u>

If you answer "no" to any question, additional information can be supplied at the end of the questionnaire.

I. General AML & CFT Policies, Practices and Procedures:

9. Does your institution have in place policies and procedures approved by your institution's board or senior management to prevent Money Laundering and Combat Financing of Terrorism? ☐ Yes / ☐ No
10. Does your institution have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML/CFT framework? ☐ Yes / ☐ No
11. Has your institution developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions? ☐ Yes / ☐ No
12. Does your institution have a policy prohibiting accounts/relationships with shell banks? *(A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)* ☐ Yes / ☐ No
13. Does your institution permit the opening of anonymous or numbered accounts by customers? ☐ Yes / ☐ No
14. Does your institution have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products? ☐ Yes / ☐ No

15. Does your institution have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates? ☐ Yes / ☐ No

16. Does your institution have policies and procedures that require keeping all the records related to customer identification and their transactions? ☐ Yes / ☐ No
If "Yes", for how long? _____

II. Risk Assessment

17. Does your institution have a risk-based assessment of its customer base and their transactions? ☐ Yes / ☐ No

18. Does your institution determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI? ☐ Yes / ☐ No

III. Know Your Customer, Due Diligence and Enhanced Due Diligence

19. Has your institution implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions? ☐ Yes / ☐ No

20. Does your institution have a requirement to collect information regarding its customers' business activities? ☐ Yes / ☐ No

21. Does your institution have a process to review and, where appropriate, update customer information relating to high risk client information? ☐ Yes / ☐ No

22. Does your institution have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information? ☐ Yes / ☐ No

23. Does your institution complete a risk-based assessment to understand the normal and expected transactions of its customers? ☐ Yes / ☐ No

IV. Reportable Transactions for Prevention and Detection of ML/TF

24. Does your institution have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities? ☐ Yes / ☐ No

25. Where cash transaction reporting is mandatory, does your institution have procedures to identify transactions structured to avoid such obligations? ☐ Yes / ☐ No

26. Does your institution screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities or under the UN Security Council Resolution? ☐ Yes / ☐ No

27. Does your institution have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin? ☐ Yes / ☐ No

V. Transaction Monitoring

28. Does your institution have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as traveler's checks, money orders, etc? ☐ Yes / ☐ No

VI. AML Training

29. Does your institution provide AML & CFT training to relevant employees of your organization? ☐ Yes / ☐ No

30. Does your institution communicate new AML related laws or changes to existing AML related policies or practices to relevant employees? ☐ Yes / ☐ No

31. Does your institution provide AML training to relevant third parties if they are employed to carry out some of the functions of your organization? ☐ Yes / ☐ No

Space for additional information:

(Please indicate which question the information is referring to.)

.....

.....

D. <u>GENERAL</u>

29. Does the responses provided in this Declaration applies to the following entities: ☐ Yes / ☐ No

- Head Office and all domestic branches
- Overseas branches (we do not have any Overseas branches)
- Domestic subsidiaries
- Overseas subsidiaries

If the response to any of the above is "No", please provide a list of the branches and / or subsidiaries that are excluded, including the name of the institution, location and contact details.

I, the undersigned, confirm to the best of my knowledge that the information provided in this questionnaire is current, accurate and representative of the anti-money laundering and anti-terrorist financing policies and procedures that are established in my institution.

I also confirm that I am authorized to complete this questionnaire on behalf of my institution.

Signature: _____

Name: _____

Designation: _____

Date: _____

Contact No: _____

Email: _____

Annexure: G

অভ্যন্তরীণ নিরীক্ষা বিভাগ

ন্যাশনাল ব্যাংক লিঃ

প্রধান কার্যালয়

Independent Testing Procedures

[ব্যাংকের অভ্যন্তরীণ নিরীক্ষা বিভাগ মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নলিখিত প্রশ্নমালার যথাযথ উত্তর (ডকুমেন্ট ভিত্তিক) অনুসারে স্কোর প্রদানপূর্বকঃ শাখার মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রমকে মূল্যায়ন করবে। অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক শাখার উপর প্রণীত বার্ষিক নিরীক্ষা প্রতিবেদনে (প্রযোজ্য ক্ষেত্রে পৃথক পরিদর্শন কর্মসূচীর আওতায় শুধুমাত্র Independent Testing Procedures ভিত্তিক প্রতিবেদন প্রণীত হবে) মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ কার্যক্রম মূল্যায়ন সংক্রান্ত আলাদা অধ্যায়ে সমুদয় বিষয়াদি সুপারিশসহ সন্নিবেশ করবে।

(যাচাইয়ের মানদন্ড অনুসারে সম্পূর্ণরূপে পরিপালিত হলে সম্পূর্ণ স্কোর, আংশিক পরিপালনে আংশিক স্কোর এবং উত্তর নেতিবাচক হলে শূন্য স্কোর প্রদান করতে হবে।)

ভিত্তি তারিখঃ

শাখার নাম ঃ

ক্র. নং.	পরিদর্শন ক্ষেত্র	বিষয়		যাচাইয়ের উপায়	মন্তব্য	মোট নম্বর	প্রাপ্ত নম্বর
১	২	৩		৪	৫	৬	
১	**শাখা পরিপালন কর্মকর্তা মূল্যায়ন**	১	ক) শাখায় একজন পরিপালন কর্মকর্তা (BAMLCO) আছেন কি না?	সর্বশেষ অফিস অর্ডার দেখুন এবং অফিস আদেশে BAMLCO এর Job Responsibilities অন্তর্ভুক্ত রয়েছে কিনা যাচাই করুন।		১	
			খ) BAMLCO অভিজ্ঞ ও জ্যেষ্ঠ কি না?	বিএফআইইউ সার্কুলারের নির্দেশনার আলোকে যাচাই করুন।		২	
		২	BAMLCO এর উপর অর্পিত দায়িত্ব যথাযথভাবে পরিপালন করে কিনা?	BAMLCO এর সার্বিক কার্যক্রম পরীক্ষা করুন		৩	
২	**গ্রাহক পরিচিতি (KYC)**	১	ক) হিসাব খোলার ফরম পূরণ করার জন্য প্রয়োজনীয় সকল তথ্য গ্রহণ করা হয়েছে কি না?	শাখায় হিসাব খোলার ক্ষেত্রে প্রয়োজনীয় কার্যক্রম যথাযথভাবে সম্পন্ন করা হয়েছে কি না তা নিশ্চিত হওয়ার জন্য সকল ধরণের হিসাবের কমপক্ষে ৩ টি করে ফরম যাচাই করুন। সংগ্রহীত তথ্য কিভাবে যাচাই করা হয়েছে, তা পরীক্ষা করুন।		২	
		২	ক) গ্রাহকের ব্যক্তি সংক্রান্ত তথ্য যথাযথভাবে যাচাই করা হয়েছে কি না?	কি পদ্ধতিতে যাচাই করা হয়েছে এবং যাচাই এর সপক্ষে সংরক্ষিত দলিলাদি পর্যালোচনা করুন। নমুনা ভিত্তিতে অন্তত ১০টি হিসাবের KYC ফরম ও সংশ্লিষ্ট দলিলাদি যাচাই করুন।		২	
			খ) গ্রাহকের তহবিলের উৎস যাচাই করা হয়েছে কি না?	Risk Based Approach এর ভিত্তিতে অন্তত ১০টি হিসাবের তহবিলের উৎসের সঠিকতা যাচাই করুন।		৪	
			গ) হিসাবের প্রকৃত সুবিধাভোগ (Beneficial Owner) সনাক্ত করা হয় কিনা এবং উহা যাচাই প্রক্রিয়া কি?	বর্ণিত বিএফআইইউ সার্কুলার ও গাইডলাইনস এর ভিত্তিতে ১০টি হিসাবের KYC ফরমের সাথে সংযুক্ত কাগজপত্রাদি/তথ্যাদি যাচাই করে দেখতে হবে।		৪	

		৩	ক) শাখা কর্তৃক গ্রাহক নির্বাচন/হিসাব খোলা/সেবা প্রদানের জন্য ব্যাংকের প্রধান কার্যালয় কর্তৃক প্রণয়নকৃত রিস্ক ম্যানেজমেন্ট গাইডলাইন্সে উল্লিখিত নির্দেশাবলী শাখায় পরিপালন করা হয় কিনা?	রিস্ক রেজিস্টার মোতাবেক শাখা কি ব্যবস্থা নিয়েছে তা পরীক্ষা করুন।		২	
			খ) শাখায় ঝুঁকিভিত্তিক গ্রাহক বিভাজন/শ্রেণীবিন্যাস/ শ্রেণীকরণ করা হয় কি না এবং তা যথাযথ কি না?	অভিন্ন হিসাব খোলার ফরমে প্রদত্ত রিস্ক গ্রেডিং অংশে উল্লেখিত নির্দেশনার সাথে শাখায় ঝুঁকিভিত্তিক গ্রাহক বিভাজন/শ্রেণীবিন্যাস শ্রেণীকরণ পদ্ধতি সংগতিপূর্ণ কি না তা পরীক্ষা করুন।		১	
			গ) উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকি নিরীখে অতিরিক্ত তথ্য ও এতদসংক্রান্ত দলিলাদি সংরক্ষণ ও যাচাই করা হয় কি না (EDD)?	শাখায় সংরক্ষিত উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ালিকাত সংগ্রহপূর্বক সংশ্লিষ্ট হিসাবসমূহ পর্যালোচনাকরত কী ধরণের তথ্য সংগ্রহ করা হয় এবং তা যথেষ্ট কি না পরীক্ষা করুন।		১	
		৪	ক) নির্দিষ্ট সময় পর পর/প্রয়োজন অনুসারে KYC হালনাগাদ করা হয় কি না ?	বিএফআইইউ সার্কুলারের নির্দেশনা মোতাবেক কাগজপত্রাদি/তথ্যাদি যাচাই করুন।		১	
			খ) শাখা কর্তকে ভাসমান/চলন্ত (walk- in / one-off customers) গ্রাহকদের (ডিডি, টিটি, পে অর্ডার, অনলাইন জমা, অনলাইন উত্তোলন ইত্যাদি) ক্ষেত্রে KYC প্রক্রিয়া অনুসরণ করা হয় কি না?	বিএফআইইউ সার্কুলারের নির্দেশনা মোতাবেক কাগজপত্রাদি/তথ্যাদি যাচাই করুন।		২	
		৫	Wire transfer এর ক্ষেত্রে শাখা কর্তক KYC প্রক্রিয়া অনুসরণ করা হয় কি না?	বিএফআইইউ সার্কুলারের নির্দেশনা মোতাবেক পরিপালিত হয়েছে কি না তা সংশ্লিষ্ট কাগজপত্রাদি/তথ্যাদি যাচাই করুন।		১	
		৬	Politically Exposed Persons (PEPs), প্রভাবশালী ব্যক্তি ও আন্তজার্তিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব শাখায় সংরক্ষণ করা হচ্ছে কিনা?	বিএফআইইউ সার্কুলারের নির্দেশনা মোতাবেক নমুনার ভিত্তিতে যাচাই করুন।		৩	
		৭	ক) Credit Card সুবিধা প্রদানে বিএফআইইউ এর নির্দেশনা অনুসরণ করা হয় কি না।	Credit Card ইস্যুর ক্ষেত্রে গ্রাহক পরিচিতি সঠিকভাবে গ্রহণ ও যাচাই করা হয় কি না যাচাই করুন। Credit Card এর ঋণ সীমাগ্রাহকের আয়ের সাথে সংগতিপূর্ণ কিনা যাচাই করুন। শাখা কর্তৃ কেওয়াইসি হালনাগাদ করা হয় কিনা যাচাই করুন।		১	
			খ) Internet banking সুবিধা প্রদানে বিএফআইইউ এর নির্দেশনা অনুসরণ করা হয় কি না।	Internet banking সুবিধা প্রদানে শাখা কর্তৃক সতর্কতামূলক ব্যবস্থা নেয়া হয়েছে তা যাচাই করুন এবং গ্রাহকের ঝুঁকি বিবেচনায় কোন অতিরিক্ত তথ্যাদি নেয়া হয়েছে কি না তা যাচাই করুন।		১	
		৮	Non face to face customer সম্পর্কিত বিএফআইইউ এর নির্দেশনা অনুসরণ করা হয় কি না।	হিসাব খোলার ক্ষেত্রে গ্রাহক পরিচিতি সঠিকভাবে গ্রহণ করা হয় কি না যাচাই করুন এবং গ্রাহকের ঝুঁকি বিবেচনায় কী/কোন ধরণে অতিরিক্ত তথ্যাদি নেয়া হয়েছে তা যাচাই করুন।		১	

৩	**লেনদেন মনিটরিং (Transaction Monitoring)**	১	শাখায় লেনদেন মনিটরিং (Transaction Monitoring) এর কোন কার্যকরী পদ্ধতি চালু আছে কিনা?	মনিটরিং এর পদ্ধতি উল্লেখ করুন (প্রযোজ্য ক্ষেত্রে প্রমাণ সংগ্রহ করুন)। ● ম্যানুয়্যাল পদ্ধতিতে লেনদেন পরীক্ষা করা হলে তা কিভাবে করা হয় তা বিস্তারিত যাচাই করুন। ● অটোমেটেড হলে সিস্টেম জেনারেটেড রিপোর্ট সংগ্রহপূর্বক পর্যালোচনা করুন। ● বিগত সময়ের লেনদেন পরীক্ষণ এর নথি সংগ্রহপূর্বক যাচাই করুন।		৪	
		২	ক) গ্রাহকের পেশা ও আয়ের সাথে সংগতিপূর্ণভাবে লেনদেনের অনুমিত মাত্র (TP) গ্রহণ করা হয় কি না?	প্রযোজ্য ক্ষেত্রে অন্তত ১০টি হিসাবের নমুনা কেস পরীক্ষা করে দেখুন।		২	
			খ) লেনদেনের অনুমিত মাত্রায় (TP) প্রয়োজনীয় সকল তথ্য সন্নিবেশ করা হয়েছে কি না?	সার্কুলারের নির্দেশনা যাচাই করুন।		১	
			গ) অনুমিত মাত্রার সাথে প্রকৃত লেনদেন যাচাই করা হয় কি না?	ন্যূনতম ১০টি হিসাবের মনিটরিং পদ্ধতির নমুনা পরীক্ষা করুন এবং প্রয়োজনে ব্যাংকের অটোমেটেড পদ্ধতি তে উল্লিখিত TP এর সাথে TP ফরমে ঘোষিত অনুমিত মাত্রার মিল আছে কিনা যাচাই করুন।		২	
			ঘ) হিসাব খোলার ৬ মাসের মধ্যে গ্রাহকের লেনদেন পর্যালোচনা পূর্বক TP নির্ধারণ করা হয়েছে কি না?	বিএফআইইউ সার্কুলার মোতাবেক ন্যূনতম ১০টি হিসাবের টিপি যাচাই করুন।		১	
			ঙ) নির্দিষ্ট কোন প্রয়োজন অনুভূত হলে অথব শাখা কর্তৃক নিয়মিত মনিটরিং কার্যক্রমের আওতায় সময়ে সময়ে টিপি হালনাগাদ করা হয়েছে কিনা?	ন্যূনতম ১০টি হিসাবের টিপি যাচাই করুন।		১	
		৩	শাখায় পরিচালিত উচ্চ ঝুঁকিপূর্ণ হিসাবসমূহ তালিকা সংরক্ষণ করা হয় কি না এবং উক্ত হিসাবের লেনদেন মনিটরিং পর্যাপ্ত কি না ?	উচ্চ ঝুঁকি সম্পন্ন হিসাব সমুহের তালিকা সংগ্রহ করুন এবং বিএফআইইউ সার্কুলারের নির্দেশনা মোতাবেক এতদসংক্রান্ত নথি সংগ্রহপূর্বক উক্ত হিসাবসমূহের লেনদেন মনিটরিং পর্যাপ্ত কিনা যাচাই করুন।		৩	
		৪	ক) সন্ত্রাসে অর্থায়ন প্রতিরোধে শাখায় UN Security Council resolution এর আওতায় sanction list ও সন্ত্রাস বিরোধী আইন ২০১৩ এর সংযোজনীতে উল্লেখিত স্থানীয় সন্ত্রাসী তালিকা সংরক্ষণ করা হয় কি না এবং সে মোতাবেক হিসাব খোলা ও লেনদেন কার্যক্রম যাচাই করা হয় কিনা?	● হিসাব খোলা, লেনদেন মনিটরিং এবং অভ্যন্তরীণ ও বৈদেশিক বাণিজ্যের ক্ষেত্রে উভয় তালিকা যাচাই করা হয় কি না। ● এ বিষয়ে শাখা স্বয়ংক্রিয় (Automated) কোন পদ্ধতি অনুসরণ করে কি না যাচাই করুন। অন্তত ১০টি নমুনা কেস পরীক্ষা করে দেখুন।		২	
			খ) False Positive এর তালিকা শাখায় সংরক্ষণ করা হয় কি না?	● UN sanction list ও স্থানীয় সন্ত্রাসী তালিকা যাচাই এ শাখা কর্তৃক কোন False Positive হয়েছে কিনা তা পরীক্ষা করে দেখুন।		১	

		৫১	বৈদেশিক ও অভ্যন্তরীণ বাণিজ্যে ও অর্থায়নের ক্ষেত্রে মানিলন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধে শাখা কর্তৃক কি ব্যবস্থা গ্রহণ করা হয়েছে?**	নমুনাভিত্তিতে ৪/৫ জন গ্রাহকের এলসি ডকুমেন্টসহ সংশ্লিষ্ট গ্রাহকের অন্যান্য সকল হিসাবের নথি সংগ্রহপূর্বক নিম্নের বিষয়াদি যাচাই করুনঃ • Letter of Credit -এ বর্ণিত পণ্যের মূল্য আন্তর্জাতিক মানদন্ডের সাথে যাচাই করা হয়েছে কি না পরীক্ষ করুন। • Supplier/Beneficiary এর Credit report সংগ্রহ করে শাখা কর্তৃক পর্যালোচনা করা হয়েছে কিনা যাচাই করুন। • Beneficiary/Applicant এর country FATF কর্তকে চিহ্নিত Jurisdiction Under increased Monitoring and High risk jurisdictions subject to a call for Action এর অন্তর্ভুক্তহলে EDD করা হয় কি না যাচাই করুন। • Bill of Entry এর original copy সংরক্ষণ করা হয় কিনা যাচাই করুন। • Shipping document Letter of Credit/Proforma invoice এর সাথে সংগতিপূর্ণ কিনা যাচাই করুন।		৫	
		৬	শাখা বৈদেশিক রেমিটেন্সসহ অন্যান্য ইনওয়ার্ড ও আউটওয়ার্ড রেমিটেন্স মনিটরিং করে কি না?	• ইনওয়ার্ড ও আউটওয়ার্ড রেমিটেন্স সংক্রান্ত লেনদেন গ্রাহকের কেওয়াইসি সংক্রান্ত তথ্যাদি নমুনাভিত্তিতে যাচাই করুন।		১	
৪	**নগদ লেনদেন রিপোর্ট (CTR) এবং সন্দেহজনক লেনদেন রিপোর্টিং (STR)**	১	ক) মাসিক ভিত্তিতে এবং নির্ভুলভাবে CTR করা হয় কিনা ?	রেকর্ড/নথি/রেজিষ্টার যাচাই করুন। যেসকল ব্যাংকের প্রধান কার্যালয় কর্তৃক কেন্দ্রীয়ভাবে সিটিআর করা হয় সে ক্ষেত্রে শাখায় মাসিক ভিত্তিতে সিটিআর সংরক্ষণ করা হয় কিনা যাচাই করুন।		৩	
			খ) প্রতি মাসে প্রেরিত সিটিআর এর কপি শাখায় সংরক্ষণ করা হয় কিনা এবং উহা নিয়মিত পর্যালোচনা করা হয় কিনা?	• রিপোর্টিং তালিকা/ফাইল পরীক্ষা করে দেখুন। বিএফআইইউ সার্কুলার মোতাবেক পর্যালোচনা করা হয় কিনা তা এতদসংক্রান্ত নথি যাচাইপূর্বক পরীক্ষা করুন। কেন্দ্রীয়ভাবে সিটিআর করা হলেও শাখা কর্তৃক সিটিআর পর্যালোচনা করা হয় কিনা তাও যাচাই করুন।		৪	
			গ) গ্রাহক কর্তকে রিপোর্টিং সীমার নীচে পুন পুনঃ লেনদেন (Structuring) করার ক্ষেত্রে তা শনাক্ত করার কোন পদ্ধতি শাখায় প্রবর্তিত হয়েছে কি না?	• শাখার ক্যাশ রেজিস্টার পর্যালোচনাপূর্বক সম্ভাব্য হিসাবসমূহ চিহ্নিতকরতঃ তা পর্যালোচনা করুন। এতদ্‌বিষয়ে শাখা কর্তৃক কোন রিপোর্ট জেনারেট করা হয় কিনা যাচাই করুন।		৫	

		২	ক) শাখায় সন্দেহজনক লেনদেন (STR/SAR) চিহ্নিতকরণের কোন পদ্ধতি চালু আছে কি না ?	সন্দেহজনক লেনদেন (STR) এর বিভিন্ন নির্দেশকসমূহের ভিত্তিতে সন্দেহজনক লেনদেন (STR) চিহ্নিতকরণের কোন পদ্ধতি চালু আছে কিনা যাচাই করুন ।		৫	
			খ) সংশ্লিষ্ট সকল কর্মকর্তা STR/SAR সিস্টেম সম্পর্কে অবহিত আছেন কি না ?	শাখার কর্মকর্তাদের সন্দেহজনক লেনদেন চিহ্নিতকরণ ও রিপোর্টকরণ সম্পর্কে পর্যাপ্ত ধারণা আছে কিনা পরীক্ষা করুন।		৩	
৫	**মানিলন্ডারিং প্রতিরোধ বিভাগ/ ডিভিশন বরাবর বিবরণী দাখিল**	১	শাখা কর্তকে প্রয়োজনীয় সংখ্যক বিবরণী মানিলন্ডারিং প্রতিরোধ বিভাগ/ডিভিশন বরাবর দাখিল করা হয় কি না ? শাখা কি যথাসময়ে বিবরণী দাখিল করে ?	• মাসিক ভিত্তিতে সিটিআর (প্রযোজ্যক্ষেত্রে এসটিআর বিবরণী), এবং ষান্মাসিক ভিত্তিতে সেল্ফ অ্যাসেসমেন্ট বিবরণী মানিলন্ডারিং প্রতিরোধ বিভাগ/ডিভিশন বরাবরে প্রেরিত হয় কিনা পরীক্ষা করুন। • বিলম্বে দাখিল অথবা বিবরণী দাখিল করা না হয়ে থাকলে তা অসন্তোষজনক বলে বিবেচিত হবে।		২	
		২	বিবরণীতে প্রদত্ত তথ্য সঠিক ও পূর্ণাঙ্গ কি না ?	এতদ্সংক্রান্ত নথি পরীক্ষা করুন। তথ্যাদি সঠিক ও পরিপূর্ণ না হলে তা অসন্তোষজনক বলে বিবেচিত হবে।		১	
৬	**স্বনির্ধারণী পদ্ধতি**	১	স্বনির্ধারণী পদ্ধতিতে (সেল্ফ অ্যাসেসমেন্ট) শাখার মূল্যায়ন ব্যবস্থা চালু আছে কি না?	বিএফআইইউ সার্কুলারে সাথে সংযুক্ত চেকলিষ্ট ব্যবহারপূর্বক মূল্যায়ন প্রতিবেদন করা হয়েছে কিনা যাচাই করে দেখুন।		১	
		২	আলোচ্য মূল্যায়ন প্রতিবেদন চূড়ান্ত করার পূর্বে শাখা ব্যবস্থাপকের সভাপতিত্বে শাখার সংশ্লিষ্ট কর্মকর্তাদের নিয়ে সভা করা হয়েছে কিনা?	নথি যাচাই করুন।		১	
		৩	ক) মূল্যায়ন প্রতিবেদনে দূর্বলতাসমূহ চিহ্নিত করা হয়েছে কিনা? খ) গৃহীত সিদ্ধান্ত বাস্তবায়নে শাখা কর্তৃক কী পদক্ষেপ গ্রহণ করা হয়েছে এবং পরবর্তী ত্রৈমাসিক সভাগুলোতে পূর্ববর্তী সভার এতদসংশ্লিষ্ট বিষয়ের অগ্রগতি নিয়ে আলোচনা করা হয়েছে কিনা?	নথি যাচাই করুন।		২	
		৪	শাখার নিজস্ব মূল্যায়ন যথাযথ কি না?	নথি যাচাই করুন এবং চেকলিস্টের প্রতিটি পয়েন্ট পর্যালোচনা পূর্বক মূল্যায়ন করুন।		১	
৭	**AML/ CFT বিষয়ে কর্মকর্তাদের জ্ঞান ও সচেতনতা**	১	শাখায় কতজন কর্মকর্তা মানি লন্ডারিং প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন?	এতদবিষয়ে শাখার সংশ্লিষ্ট রেকর্ড দেখুন। এএমএল/সিএফটি বিষয় আন্তর্জাতিক মানদন্ড,জাতীয় নীতিমালা ও আইনকানুন, বিএফআইইউ কর্তৃক জারীকৃত গাইডেন্স নোটস্ ও সার্কুলার ইত্যাদি বিষয়ে অন্তর্ভুক্তিকরণসহ এর ঝুঁকি ব্যবস্থাপনার কলাকৌশল এবং রিপোর্টিং পদ্ধতি সম্পর্কে অন্তত ১(এক) দিন ব্যাপী অনুষ্ঠিত মানি লন্ডারিং বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ বিবেচ্য হবে।		১	

		২	প্রধান নির্বাহী কর্তৃক বাৎসরিক ভিত্তিতে এএমএল/সিএফটি বিষয়ক অঙ্গীকার ঘোষণার কপি সকল কর্মকর্তাকে অবহিতকরণপূর্বক শাখায় সংরক্ষণ করা হয় কিনা এবং এ ব্যাপারে শাখার কর্মকর্তাগণ যথাযথভাবে তা পরিপালন করেছেন কিনা?	নথি পর্যালোচনা করুন।		১	
		৩	শাখার কর্মকর্তাগণ এএমএল/সিএফটি বিষয়ক নীতি, পদ্ধতি ও প্রোগ্রাম এবং জাতীয় নীতিমালাসহ বিএফআইইউ এর গাইডলাইন্স সম্পর্কে অবহিত কি না?	শাখার কর্মকর্তার সাথে সাক্ষাৎকারের ভিত্তিতে মূল্যায়ন করুন।		১	
		৪	প্রশিক্ষণ সংক্রান্ত তথ্য ও দলিলাদি যথাযথভাবে সংরক্ষণ করা হয় কিনা?	নথি পর্যালোচনা করুন।		১	
৮	**রেকর্ড সংরক্ষণ/ সরবরাহ**	১	মানি লন্ডারিং প্রতিরোধ আইন-২০১২ (২০১৫ এর সংশোধনীসহ) এবং ব্যাংকের নিজস্ব নীতিমালা অনুযায়ী গ্রাহকের লেনদেন সম্পর্কিত রেকর্ড যথাযথভাবে সংরক্ষণ করা হয় কিনা ?	মানি লন্ডারিং প্রতিরোধ আইন-২০১২ (২০১৫ এর সংশোধনীসহ) এবং বিএফআইইউ এর সার্কুলার মোতাবেক হিসাবের লেনদেনের তথ্যাদি (যেমন হিসাব খোলার ফরম, লেনদেন বিবরণী, চেক/ভাউচার ইত্যাদি) পরীক্ষা করে দেখুন।		২	
		২	গ্রাহকের KYC সহ CDD প্রক্রিয়া সম্পাদনকালে সংগহীত তথ্য ও দলিলাদি এবং লেনদেন সংক্রান্ত তথ্য ও দলিলাদি বিএফআইইউ এর চাহিদা মোতাবেক যথাসময়ে সরবরাহ করা হয় কি না ?	এতদ্‌সংক্রান্ত নথি পরীক্ষা করুন। যথাসময়ে ও সঠিকভাবে তথ্য সরবরাহ না করলে তা অসন্তোষজনক বিবেচিত হবে।		৩	
৯	**নিরীক্ষা, পরিদর্শন ও অন্যান্য**	১	শাখা ব্যবস্থাপক BAMLCO না হলে শাখা ব্যবস্থাপক AML/CFT প্রোগ্রাম বাস্তবায়নে যথাযথ ভূমিকা পালন করেন কি না?	শাখায় আয়োজিত সভার আলোচ্যসূচী ও শাখা ব্যবস্থাপকের সাথে সাক্ষাৎকারের ভিত্তিতে মূল্যায়ন করুন।		১	
		২	ইতিপূর্বে শাখায় পরিচালিত নিরীক্ষা/পরিদর্শন প্রতিবেদনে উল্লিখিত অনিয়ম/সুপারিশসমূহ যথাযথভাবে পরিপালিত হয়েছে কি না?	সর্বশেষ নিরীক্ষা প্রতিবেদন পরীক্ষা করে দেখুন এবং প্রতিবেদনে বর্ণিত অনিয়মাদি সংশোধনে শাখা কিরূপে ব্যবস্থা গ্রহণ করেছে তা যাচাই করে দেখুন। ✓ ব্যাংকের অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক সর্বশেষ নিরীক্ষা রিপোর্ট পর্যালোচনা করুন এবং পরিপালনের অবস্থা যাচাই করুন। ✓ বাংলাদেশ ব্যাংকের ব্যাংক পরিদর্শন বিভাগ কর্তকে পরিদর্শন কার্যক্রম সম্পন্ন হলে এর রিপোর্টটি (মানিলন্ডারিং অংশটি বিশেষভাবে) পর্যালোচনা করুন এবং পরিপালনের অবস্থা যাচাই করুন। ✓ বাংলাদেশ ব্যাংকের বৈদেশিক মুদ্রা পরিদর্শন বিভাগ কর্তৃক নিরীক্ষা (যদি হয়ে থাকে) এর রিপোর্টটি পর্যালোচনা করুন এবং পরিপালনের অবস্থা যাচাই করুন। ✓ বিএফআইইউ এর নিরীক্ষা (যদি হয়ে থাকে) এর রিপোর্টটি পর্যালোচনা করুন এবং পরিপালনের অবস্থা যাচাই করুন		৪	

		৩	গ্রাহক সচেতনতা বৃদ্ধিকল্পে কি ব্যবস্থা গ্রহণ করা হয়েছে?	গ্রাহক সচেতনতা বৃদ্ধিকল্পে শাখা কী ধরনের কার্যক্রম গ্রহন করেছে তা যাচাই করুন। এ ব্যাপারে গ্রাহকদের লিফলেট বিতরণ এবং শাখার দশ্যেমান স্থানে এ বিষয়ক পোস্টার আছে কিনা যাচাই করুন।		৩	
					সর্বমোটঃ	১০০	

[১] বিশেষ দ্রষ্টব্যঃ অনুচ্ছেদ নং ৩(৫) শুধুমাত্র এডি শাখার জন্য প্রযোজ্য হবে। ননএডি শাখার ক্ষেত্রে ৯৫ নম্বরের মধ্যে প্রাপ্ত নম্বরকে শতকরা রপোন্তর করে সার্বিক রেটিং নির্ণয় করতে হবে।

শাখার মূল্যায়নঃ

ক্রমিক নং	পরিদর্শন ক্ষেত্র	বরাদ্দকৃত মোট নম্বর	প্রাপ্ত নম্বর
১	শাখা পরিপালন কর্মকর্তা মূল্যায়ন	৬	
২	গ্রাহক পরিচিতি (KYC)	২৬	
৩	লেনদেন মনিটরিং	২৩	
৪	সন্দেহজনক লেনদেন এবং নগদ লেনদেন রিপোর্টিং	২০	
৫	মানিলন্ডারিং প্রতিরোধ বিভাগ/ডিভিশন বরাবর বিবরণী দাখিল	৩	
৬	স্বনির্ধারণী পদ্ধতি	৫	
৭	এএমএল/সিএফটি বিষয়ে কর্মকর্তা/ কর্মচারীদের জ্ঞান ও সচেতনতা	৪	
৮	রেকর্ড সংরক্ষণ	৫	
৯	নিরীক্ষা, পরিদর্শন ও অন্যান্য	৮	
	সর্বমোটঃ	১০০	

স্কোর	রেটিং
৯০+-১০০	শক্তিশালী
৭০+-৯০	সন্তোষজনক
৫৫+-৭০	মোটামুটি ভাল
৪০+-৫৫	প্রান্তিক
৪০ ও এর নীচে	অসন্তোষজনক

Annexure :H

ন্যাশনাল ব্যাংক লিঃ

রিপোর্টিং তারিখঃ ...../...../.....

-------- শাখা

শাখা কর্তৃক Self Assessment পদ্ধতির মাধ্যমে নিজস্ব অবস্থান নির্ণয় (জানুয়ারী/জুলাই ২০২... -জুন/ডিসেম্বর ২০২...)

মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন,বিধিমালা,বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নবর্ণিত প্রশ্নমালার বিস্তারিত উত্তর প্রদানের মাধ্যমে Self Assessment পদ্ধতিতে নিজেদের অবস্থান নির্ণয় ঃ

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/ সুপারিশ
১. শাখায় মোট কর্মকর্তার সংখ্যা কত (পদনুযায়ী)? কতজন কর্মকর্তা মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন? (শতকরা হার)	প্রশিক্ষন সংক্রান্ত রেকর্ড যাচাই করতে হবে।		
২. ক) শাখার মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা (BAMLCO) জেষ্ঠ্য ও অভিজ্ঞ কিনা? বিগত দুই বছরে তিনি মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণ পেয়েছেন কিনা? খ) শাখায় মানিলন্ডারিং প্রতিরোধ কার্যক্রম যথানিয়মে পরিপালিত হচ্ছে এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে (BAMLCO) নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় পরীক্ষণ ও পর্যালোচনা করে থাকেন কি না?	BAMLCO কর্তৃক - • KYC কার্যক্রমের যথাযর্থতা পরীক্ষণ করা হয় কিনা? • যথাযথভাবেঃ- লেনদেন পরীক্ষণ এবং সন্দেহজনক লেনদেন রিপোর্ট (ইন্টারনাল রিপোর্টসহ) করা হয় কি না? • যথাযথভাবে রেকর্ড সংরক্ষণ করা হয় কি না? • CTR যাচাই এবং STR শনাক্তকরণে ব্যবস্থা নেয়া হয় কি না? • বৈদেশিক মুদ্রার ইনওয়ার্ড ও আউটওয়ার্ড লেনদেন পরীক্ষণ করা হচ্ছে কিনা?		
৩. BAMLCO সহ শাখার কর্মকর্তাগণ মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?	বিষয়টি যাচাইয়ের পদ্ধতি কী? (বিস্তারিত লিখুন)		
৪. শাখা পর্যায়ে ত্রৈমাসিক ভিত্তিতে মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক সভা অনুষ্ঠিত হয় কি না ?	• সভার আলোচ্যসূচী সকলের অবগতির জন্য বন্টন করা হয় কি না ? • সভায় কী কী গুরুত্বপূর্ণ সিদ্ধান্ত গৃহীত হয়েছে ? • সভায় গৃহীত সিদ্ধান্ত কিভাবে বাস্তবায়িত হয়?		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/ সুপারিশ
৫. সকল প্রকার হিসাব খোলার ও লেনদেন পরিচালনার ক্ষেত্রে মানিলন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং সময়ে সময়ে বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কি না?	• গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? • KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয় কি না? • হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) শনাক্ত করা হয় কি না এবং তা যাচাই এর প্রকিয়া সন্তোষজনক কি না? • উচ্চ ঝুঁকিবিশিষ্ট গ্রাহদের ক্ষেত্রে ঝুঁকির নিরীখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কি না?		
৬. ক) ঝুঁকির ভিত্তিতে শাখা তাদের গ্রাহকদের শ্রেণীবিন্যাস/শ্রেণীকরণ করে কি না? খ) উচ্চ ঝুঁকিসম্পন্ন হিসাবের লেনদেন পরীক্ষণ করা হয় কি না?	• এ পর্যন্ত কতটি উচ্চ ঝুঁকি সম্পন্ন হিসাব শাখায় খোলা হয়েছে? • এ ধরনের হিসাব খোলা ও পরিচালনার ক্ষেত্রে শাখা কী পদক্ষেপ গ্রহণ করেছে? • কী পদ্ধতিতে উচ্চ ঝুঁকিসম্পন্ন হিসাবের লেনদেন পরীক্ষণ করা হয়?		
৭. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব নীতিমালা অনুযায়ী মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কি না?	• এ বিষয়ক নিজস্ব নীতিমালা প্রণয়ন করা হয়েছে কি না? • উক্ত নীতিমালা শাখায় কিভাবে বাস্তবায়িত হচ্ছে?		
৮. শাখা গ্রাহকের KYC Profile এর তথ্য বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা মোতাবেক নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে কি না ?	কী পদ্ধতিতে এরূপ মূল্যায়ন সম্পাদিত হয়ে থাকে?		
৯. শাখা Walk-in-Customer-দের ক্ষেত্রে KYC প্রক্রিয়া অনুসরণ করে কি?	কিভাবে আলোচ্য প্রক্রিয়াটি সম্পন্ন করে থাকে?		
১০. Online ব্যাংকিং এর ক্ষেত্রে হিসাবধারী ব্যতীত অন্য কোন ব্যক্তি অর্থ জমা করলে সেক্ষেত্রে কোন ধরনের KYC প্রক্রিয়া অনুসরণ করা হয় কি?	হয়ে থাকলে কী প্রক্রিয়ায় তা সম্পাদিত হচ্ছে?		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/ সুপারিশ
১১. শাখা কী পদ্ধতিতে গ্রাহকের লেনদেন পরীক্ষণ করে থাকে?	• ব্যাংক শাখা কর্তৃক নির্ধারিত সীমার উপরের লেনদেনের (Threshhold) ভিত্তিতে অথবা অন্য কোন পদ্ধতিতে ; • লেনদেনের অনুমিত মাত্রা (TP) গ্রাহকের পেশা ও আয়ের সাথে সংগতিপূর্ণ কি না তা যাচাই করা হয় কিনা? • ঘোষিত অনুমিত মাত্রার সাথে পরবর্তীতে গ্রাহক কতৃর্ক সম্পাদিত প্রকৃত লেনদেন যাচাই করা হয় কি না? • শাখা কর্তৃক একটি নির্ধারিত Thershhold এর ভিত্তিতে প্রতিদিনের লেনদেন মনিটর করা হয় কিনা? • শাখায় একটি নির্দিষ্ট সময় পর পর নমুনা ভিত্তিতে গ্রাহকের KYC Profile এ প্রদত্ত তথ্যের সাথে লেনদেনের সামঞ্জস্যতা যাচাই করা হয় কিনা?		
১২. সন্ত্রাস বিরধী আইন, ২০০৯ এর অধীন সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধের লক্ষ্যে শাখায় কী ধরনের পদক্ষেপ গ্রহণ করেছে?	• জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশের সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/ সুপারিশ
	লেনদেন কার্যক্রম যাচাই করা হয় কিনা? • শাখায় এ বিষয়ক নিজস্ব কোন পদ্ধতি অনুসরণ করা হয় কিনা? • শাখা কর্তৃক কোন False Positive তালিকা সংরক্ষণ করা হয় কি না? • এরূপ কোন ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা?		
১৩. এ যাবৎ শাখা কর্তৃক কতগুলো সন্দেহজনক লেনদেন (STR) শনাক্ত করা হয়েছে?	• শাখায় সন্দেহজনক লেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? • শাখায় সন্দেহজনক লেনদেন রিপোর্টিং এর জন্য অভ্যন্তরীন রিপোর্টিং ব্যবস্থা চালু রয়েছে কিনা? • শাখা পর্যায়ে নিস্পত্তিকৃত অভ্যন্তরীন রিপোর্ট সংরক্ষণ করা হয় কিনা? • এ যাবৎ কতগুলো STR সনাক্ত করা হয়েছে? কতগুলো AML/CFT Division/Dept. এ রিপোর্ট করা হয়েছে?		
১৪. গ্রাহক কতৃর্ক পুনঃ পুনঃ নগদ লেনদেন রিপোর্টিং (CTR) সীমার নীচে লেনদেন (Structuring) শনাক্ত করার কোন পদ্ধতি শাখা কর্তৃক প্রবর্তিত হয়েছে কিনা?	প্রতিদিনের লেনদেনে Structuring শনাক্ত করার জন্য কোন রিপোর্ট তৈরী করা হচ্ছে কি না বা কোন পদ্ধতি রয়েছে কিনা? (বিস্তারিত লিখুন)		
১৫. শাখা কর্তৃক নিয়মিত ও সঠিকভাবে CTR কেন্দ্রীয় পরিপালন ইউনিটে প্রেরণ করা হচ্ছে কিনা?	• প্রেরিত তথ্যের সঠিকতা কিভাবে যাচাই করা হচ্ছে? • কেন্দ্রীয়ভাবে CTR রিপোর্ট করার ক্ষেত্রে শাখা নিজস্ব CTR রিপোর্ট সংগ্রহপূর্বক পরীক্ষণ কার্যক্রম অব্যাহত রাখে কিনা?		
১৬. মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন, সার্কুলার, প্রশিক্ষণ রেকর্ড, বিবরণী ও অন্যান্য এএমএল/ সিএফটি সংক্রান্ত বিষয়াবলীর আলাদা নথি শাখা কর্তৃক সংরক্ষণ করা হয় কি না? আইন, সার্কুলার ইত্যাদির কপি শাখায় সকল কর্মকর্তা/কর্মচারীদের সরবরাহ করা হয় কি না?	কী কী সংরক্ষণ করা হচ্ছে (বিস্তারিত) লিখুন।		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/ সুপারিশ
১৭. বিএফআইইউ মাস্টার সার্কুলার অনুসারে শাখায় PEPs, প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কি না?	উত্তর হ্যাঁ হলে এই হিসাব খোলা ও পরিচালনার ক্ষেত্রে কী কী ধরণের সতর্কতা অবলম্বন করা হচ্ছে?		
১৮. শাখায় অয়্যার ট্রান্সফার সংক্রান্ত লেনদেনের ক্ষেত্রে বিএফআইইউ এর নির্দেশনা যথাযথভাবে অনুসরণ করা হচ্ছে কি না?			
১৯. প্রধান কার্যালয় ও বাংলাদেশ ব্যাংক, বাংলাদেশ ফাইন্যন্সিয়াল ইন্টেলিজেন্স ইউনিট-এর পরিদর্শন প্রতিবেদনে উল্লেখিত মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ পরিপালন বিষয়ক দুর্বলতা/ অনিয়মসমূহ নিয়মিত করা হয়েছে কি না?	না হয়ে থাকলে প্রতিবন্ধকতাসমূহ কী কী?		
২০. শাখা কর্তৃক বৈদেশিক রেমিটেন্সসহ অন্যান্য ইনওয়ার্ড ও আউটওয়ার্ড বৈদেশিক মুদ্রার লেনদেন পরীক্ষণ করা হয় কি না?	হয়ে থাকলে কিভাবে? ইনওয়ার্ড রেমিট্যান্স সংক্রান্ত লেনদেনে, প্রযোজ্য ক্ষেত্রে, বিএফআইইউ কর্তৃক সময়ে সময়ে সরবরাহকৃত সন্ত্রাসী সংগঠন/ ব্যক্তির তালিকা যাচাই করা হচ্ছে কি না?		
২১. শাখায় বৈদেশিক বাণিজ্য সংশ্লিষ্ট লেনদেন (এলসি, গ্যারান্টি ইত্যাদি) যথযাথভাবে পরীক্ষণ করা হচ্ছে কী না?			
২২. শাখায় ঋণ হিসাব ও এ সংশ্লিষ্ট অন্যান্য লেনদেন যথযাথভাবে পরীক্ষণ করা হচ্ছে কী না?			

শাখা মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তার
নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ
ফোন নং-

শাখা ব্যবস্থাপকের নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ
ফোন নং-

Annexure : I

Common Indicators of Suspicious Transactions

The following are examples of common indicators that may point to a suspicious transaction, whether completed or attempted:

1. General

- Client admits or gives a statement about involvement in criminal activities.
- Client does not want correspondence sent to home address.
- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Client repeatedly uses an address but frequently changes the names involved.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client has only vague knowledge of the amount of a deposit.
- Client presents confusing details about the transaction or knows few details about its purpose.
- Client is secretive and reluctant to meet in person.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Normal attempts to verify the background of a new or prospective client are difficult.
- Client appears to be acting on behalf of a third party, but does not tell you.
- Client insists that a transaction will be done quickly.
- Inconsistencies appear in the client's presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the client.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client uses aliases and a variety of similar but different addresses.
- Client spells his or her name differently from one transaction to another.
- Client provides false information or information that you believe is unreliable.
- Client offers you money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.
- Client is the subject of a money laundering or financing of terrorism investigation.
- The bank is aware from a reliable source (that can include media or other open sources), that a client is suspected of being involved in illegal activity.
- A new or prospective client is known to the bank as having a questionable legal reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

2. Knowledge of Reporting or Record Keeping Requirements

- Client attempts to convince employee not to complete any documentation required for the transaction.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client seems very conversant with money laundering or terrorist activity financing issues.

- Client appears to be structuring amounts to avoid record keeping, client identification or reporting thresholds.
- Client appears to be collaborating with others to avoid record keeping, client identification or reporting thresholds.

3. Identity Documents

- Client provides doubtful or vague information.
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Client refuses to produce personal identification documents.
- Client only submits copies of personal identification documents.
- Client wants to establish identity using something other than his or her personal identification documents.
- Client inordinately delays presenting corporate documents.
- All identification documents presented appear new or have recent issue dates.
- Client presents different identification documents at different times.
- Client alters the transaction after being asked for identity documents.
- Client presents different identification documents each time a transaction is conducted.

4. Cash Transactions

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Client uses notes in denominations that are unusual for the client, when the norm in that business is different.
- Client presents notes that are packed or wrapped in a way that is uncommon for the client.
- Client deposits musty or extremely dirty bills.
- Client makes cash transactions of consistently rounded-off large amounts.
- Client consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Client presents uncounted fund for a transaction. Upon counting, the client reduces the transaction to an amount just below that which could trigger reporting requirements.
- Client conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Client asks the bank to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Large transactions using a variety of denominations.

5. Economic Purpose

- Transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities.
- Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the client.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- No business explanation for size of transactions or cash volumes.

- Transactions of financial connections between businesses that are not usually connected (for example, a food importer dealing with an automobile parts exporter).
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

6. Transactions Involving Accounts

- Opening accounts when the client's address is outside the local service area.
- Opening accounts in other person's names.
- Opening accounts with names very close to other established business entities.
- Attempting to open or operating accounts under a false name.
- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Client frequently uses many deposit locations outside the home branch location.
- Activity far exceeds the activity projected at the time of opening the account.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
- Large transfers from one account to other accounts that appear to be pooling money from different sources.
- Multiple deposits are made to a client's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.
- Frequent deposits in amounts just below BDT 10,00,000.00 which may be considered as structuring/smurfing.
- Regular return of cheques for insufficient funds.

7. Personal Transactions

- Client appears to have accounts with several financial institutions in one geographical area.
- Client has no employment history but makes frequent large transactions or maintains a large account balance.
- The flow of income through the account does not match what was expected based on stated occupation of the account holder or intended use of the account.
- Client makes frequent or large payments through online services.
- Client runs large positive credit card balances.
- Client visits the safety deposit box area immediately before making cash deposits.
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her address.
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Client deposits large endorsed cheques in the name of a third-party.

- Client frequently makes deposits to the account of another individual who is not an employer or family member.
- Client's access to the safety deposit facilities increases substantially or is unusual in light of their past usage.
- Many unrelated individuals make payments to one account without rational explanation.
- Third parties make cash payments or deposit cheques to a client's credit card.
- Client gives power of attorney to a non-relative to conduct large transactions.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Client acquires significant assets and liquidates them quickly with no explanation.
- Client requests movement of funds that are uneconomical.
- High volume of wire transfers are made or received through the account.

8. Corporate and Business Transactions

Some businesses may be susceptible to the mixing of illicit funds with legitimate income. This is a very common method of money laundering. These businesses include those that conduct a significant part of their business in cash. Unusual or unexplained increases in cash deposits made by those entities may be indicative of suspicious activity.

- Accounts are used to receive or disburse large sums but show virtually no normal business-related activities.
- Accounts have a large volume of deposits in drafts and electronic funds transfers, which is inconsistent with the client's business.
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity.
- Business does not want to provide complete information regarding its activities.
- Financial statements of the business differ noticeably from those of similar businesses.
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them.
- Deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations.
- Client maintains a number of trustee or client accounts that are not consistent with that type of business or not in keeping with normal industry practices.
- Client pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments.
- Client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.
- Client makes a large volume of cash deposits from a business that is not normally cash-intensive.
- Client makes large cash withdrawals from a business account not normally associated with cash transactions.
- Client consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad.
- Unexplained transactions are repeated between personal and commercial accounts.
- Activity is inconsistent with stated business.

9. Transactions for Non-Profit Organizations, Non Government Organizations, Charities etc.

- Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organization.
- Sudden increase in the frequency and amounts of financial transactions for the organization, or the inverse, that is, the organization seems to hold funds in its account for a very long period.
- Large and unexplained cash transactions by the organization.
- The organization's directors are outside Bangladesh, particularly if large outgoing transactions are made to the country of origin of the directors and especially if that country is a high-risk jurisdiction.
- Large number of non-profit organizations with unexplained links.
- The non-profit organization appears to have little or no staff, no suitable offices or no telephone number, which is incompatible with their stated purpose and financial flows.
- The non-profit organization has operations in, or transactions to or from, high-risk jurisdictions.

10. Merchant Banking Business

10.1 New business

- A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.
- A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.
- A client with no discernible reason for using the firm's service, e.g. clients whose requirements are not in the normal pattern of the institution's business and could be more easily serviced elsewhere.
- An investor introduced by an overseas bank, affiliate or other investor, when both investor and introducer are based on countries where production of drugs or drug trafficking may be prevalent; and any transaction in which the counterparty to the transaction is unknown.

10.2 Dealing patterns

- A large number of security transactions across a number of jurisdictions.
- Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates.
- Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request.
- Low grade securities purchases and sales, with the proceeds used to purchase high grade securities; and Bearer securities held outside a recognized custodial system.

10.3 Abnormal transactions

- A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.
- Any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading, or early cancellation, especially where cash had been tendered and/or the refund cheque to a third party.
- Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices.
- Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries.

10.4 Settlements payment

- A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction.
- Large transaction settlement by cash.
- Payment by way of third party cheque or money transfer where there is a variation between the account holder, the signatory and the prospective investor, must give rise to additional enquires.

10.5 Delivery

- Settlement to be made by way of bearer securities from outside a recognized clearing system.
- Allotment letters for new issues in the name of persons other than the client.

10.6 Disposition

- Payment to a third party without any apparent connection with the investor.
- Settlement either by registration or delivery of securities to be made to an unverified third party.

11. Credit Card Issuing

In Credit Card business certain product features, functionality, or activity may pose the risk for Money Laundering. The main money laundering risks in Credit Card are associated with Card Issuing and Merchant Acquiring activities. Though the threats and vulnerabilities are changing globally as evolving process, some "Red-Flag" indicators are described below for ready reference and investigating/monitoring unusual/suspicious transaction and risk mitigation thereof at different stages.

11.1 Application, Identification and Underwriting

- Information mismatch from application;
- Application information/address/customer differs from pre-screened applicant;
- Inability to verify card holder identity information;
- Inability to provide government issued identification details;
- Primary/secondary user name appearing on applicable government watch/sanctions lists;
- Change of address to high-fraud area or to problematic jurisdiction, shortly after the card issuance or credit line increase.

11.2 Transaction Monitoring

- Frequent and unusual use of the card for withdrawing cash at ATMs;
- Structuring payments/overpayments: balance on cards may move into regular credit where card holder pay too much or where merchants give credits to an account. Money laundering may be facilitated via refunds of the credit balance;
- Unusual cash advance activity and large payments: the monitoring of incoming cash is critical, as excessive cash payments are often an attribute of money laundering. Credit balance accumulation resulting in refunds (CBRs) should be monitored as they can be used as part of a scheme to launder funds;
- Cross border: cash withdrawal via cards in another jurisdiction permits easy (and potentially high value) cross border movement of funds with a limited audit trial;
- Unusual purchase of goods or services in countries regarded by an institution as posing a heightened risk for Money Laundering.
- Excessive payments on private level credit cards via gift card from the merchant;
- Purchase at merchant on personal cards which are significantly out of pattern with historical spending behavior;
- Merchant credits without offsetting merchant transactions;

11.3 Customer Monitoring

- Excessive customer service calls;
- Abnormal customer contact behavior (e.g. frequent changes of address)

11.4 Card Account Settlement

- Multiple and frequent cash payment or money orders; large, cross-border wire transfer payments;
- Where issuers have access to this information, settlements/from unrelated third parties;
- Where issuers have access to this information, unrelated checking/current account paying multiple credit card accounts;
- Exclusive/ongoing large credit refund.

12. Merchant Acquiring

As with card issuing, the merchant acquiring business presents a unique set of threats that can be associated with either fraud or money laundering. The following lists of "red Flag" represent some of these. It is acknowledged that there may be significant limitations (e.g. data availability), which may impede/hamper/slowdown an Acquiring ability to monitor against all these indicators, but they may be appropriate for consideration when investigating unusual and potentially suspicious transactions.

12.1 Account Set Up

- principal of the merchant appear to be unfamiliar with, or lack a clear understanding of the business;
- Higher risk merchants/product types;
- Lack of reliable third party and/or governmental verification of business;
- The address indicated (or corroborated) is identified as mail drop or other high-risk address, as opposed to a physical street address;
- Proposed transaction volume/refunds/charge-backs inconsistent with one-side visit or merchant/industry peer group;
- The business is relatively new, with little to no operating history that can be evaluated;
- Where appropriate, no government issued identity document, or bureau verification of principals/owners of business;
- Merchant/principals/owners match entries appearing on applicable watch/sanctions lists;

12.2 Transaction and Merchant Monitoring

- Unusual or changing trends in processing volumes (velocity) and value from account opening estimates (e.g. average transaction amount, sales volumes, charge back and refund rates, etc.);
- Out of pattern or excessive cash advance volume or credit refunds;
- Lack of charge activity (i.e. monitoring inactive accounts for possible fraudulent diversions);
- Enhanced monitoring of transaction activity at merchants assessed by an institution as representing a high risk;
- Mismatch of charge-backs with transaction types/volumes;
- Unusual volume, account address changes or other activity immediately following account opening;
- Indications that a Merchant's facility is used by third parties;
- Merchant/Principals/owners potentially appear on government watch/terrorist lists.

Annexure: J

RISK REGISTER

1. ML & TF Risk Register for Customers

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
1.01.	**Retail Banking Customer**				
1.01.1.	A new customer	Likely	Moderate	2 (Medium)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Collect the documents for customer identification, source of fund & address as per types of the account which are indicated in the appendix: A of AML/CFT Policy Guidelines of NBL; 3. Conduct applicable CDD/EDD on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.1-5.8 of AML/CFT Policy Guidelines of NBL; 4. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 5. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
1.01.2.	Walk-in customer (beneficiary is government/ semi government/ autonomous body/ bank & NBFI)	Likely	Major	3 (High)	Follow the instruction for Walk-in Customer mentioned in Section No. 5.14 of Chapter#5 of AML/CFT Policy Guidelines of NBL
1.01.3.	Walk-in customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBFI)	Very likely	Major	4 (Extreme)	Follow the instruction for Walk-in Customer mentioned in Section No. 5.14 of Chapter#5 of AML/CFT Policy Guidelines of NBL
1.01.4.	Non-resident customer (Bangladeshi)	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
1.01.5.	A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.01.6.	A customer making series of transactions to the same individual or entity	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register. 2. Identify & justify the reason(s) of making series of transactions to the same individuals or entity; 3. Collect & preserve complete and accurate information of both the individual/entity for whom series of transactions are made and the transaction maker.
1.01.7.	Customer involved in outsourcing business	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.01.8.	Customer appears to do structuring to avoid reporting threshold	Very Likely	Major	4 (Extreme)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL 2. Identify & justify the reason(s) for such transactions. 3. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
1.01.9.	Customer appears to have accounts with several banks in the same area	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register. 2. Identify & justify the reason(s) for accounts in several banks in the same area.
1.01.10.	Customer who shows curiosity about internal systems, controls and	Very Likely	Major	4 (Extreme)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	policies on internal and regulatory reporting				
1.01.11.	Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Very Likely	Major	4 (Extreme)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.01.12.	Negative news about the customers' activities/ business in media or from other reliable sources	Very Likely	Major	4 (Extreme)	1. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL; 2. Report to BFIU through AMLD as per chapter#11 of AML/CFT Policy Guidelines of NBL; 3. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL;
1.01.13.	Customer is secretive and reluctant to meet in person	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.01.14.	Customer is a mandate who is operating account on behalf of another person/ company.	Likely	Moderate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register. 2. Collect the documents of mandate holder for identification, source of fund & address; 3. Collect a written mandate of authority.
1.01.15.	Large deposits in the account of customer with low income	Very Likely	Major	4 (Extreme)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL 2. Identify & justify the source of fund. 3. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
1.01.16.	Customers about whom BFIU seeks	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Maintain secrecy about BFIU's seeking

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	information (individual)				information to customer & others. 3. Keep all records of transaction of the account.
1.01.17.	A customer whose identification is difficult to check	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction of "In case where conducting of CCD measure is not possible" as per Section No. 5.7 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
1.01.18.	Significant and unexplained geographic distance between the bank and the location of the customer	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify and justify the reason for the ground behind selecting the respective branch. 3. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
1.01.19.	Customer is a foreigner	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction of "Accounts of Non Resident Bangladeshi & Foreign National" in Chapter#4 at Section No. 4.3.9; 3. Comply all provisions of Foreign Exchange Regulation Act, 1947 & issued guidelines, circulars, rules and regulations by Bangladesh Bank under this act.
1.01.20.	Customer is a minor	Likely	Moderate	2 (Medium)	Follow the instruction of "Accounts of Minor" of AML/CFT Policy Guidelines of NBL in Chapter#6 at Section No.6.6;
1.01.21.	Customer is Housewife	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.01.22.	Customers that are politically exposed persons (PEPs) or influential persons (IPs) or chief/senior officials of international organizations and their	Very Likely	Major	4 (Extreme)	Follow the instruction of "Accounts of PEPs" of AML/CFT Policy Guidelines of NBL in Chapter#5 at Section No.5.9.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	family members and close associates				
1.01.23.	Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Give emphasis on beneficial owner. 3. Identify & justify the source of fund.
1.01.24.	Customers doing significant volume of transactions with higher - risk geographic locations.	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason behind the transactions. 3. Report to BFIU through AMLD if it seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
1.01.25.	A customer who brings in large amounts of used notes and/or small denominations	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason behind the transactions. 3. Report to BFIU through AMLD if it seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
1.01.26.	Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.01.27.	Customer is a money changer/ courier service	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	agent / travel agent				
1.01.28.	Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.01.29.	Customer is involved in Manpower Export Business	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Collect the membership certificate of Bangladesh Association of International Recruiting Agencies (BAIRA) of that Agency. 3. Verified the License no. in website of BAIRA.
1.01.30.	Customer has been refused to provide banking facilities by another bank	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify the reason for refusal by other banks; 3. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 4. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
1.01.31.	Accounts opened before 30 April, 2002	Likely	Moderate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction of "Management of Legacy accounts" in Chapter#5 at Section No. 5.17 of AML/CFT Policy Guidelines of NBL.
1.01.32.	Customers with complex accounting and huge transaction	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason(s) of complex accounting and huge transactions; 3. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
1.01.33.	Receipt of donor fund , fund from	Very Likely	Major	4 (Extreme)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	foreign source by micro finance institute (MFI)				
1.01.34.	Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	Very Likely	Major	4 (Extreme)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.02.	**Wholesale Banking Customer**				
1.02.1.	Entity customer having operations in multiple locations				Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.02.2.	Customers about whom BFIU seeks information (large corporate)	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Maintain secrecy about BFIU's seeking information to customer & others. 3. Keep all records of accounts & transaction of the customer.
1.02.3.	Owner of the entity that are Influential Persons (IPs) and their family members and close associates	Very Likely	Major	4 (Extreme)	Follow the instruction of "Accounts of PEPs" of AML/CFT Policy Guidelines of NBL in Chapter#5 at Section No.5.9.
1.02.4.	A new customer who wants to carry out a large transaction. (i.e.transaction amounting 10 million or above)	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason of such transaction. 3. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
1.02.5.	A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason of such transactions. 3. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
1.02.6.	A customer whose identification is difficult to check.	Very Likely	Major	4 (Extreme)	1. Follow the instruction of "In case where conducting of CCD measure is not possible" as per Section No. 5.7 of Chapter#5 of AML/CFT Policy Guidelines of NBL; 2. Follow the instruction of "In case where conducting of CCD measure is not possible" as per Section No. 5.7 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
1.02.7.	Owner of the entity that are Politically Exposed Persons (PEPs) or chief / senior officials of International Organizations and their family members and close associates	Very Likely	Major	4 (Extreme)	Follow the instruction of "Accounts of PEPs" of AML/CFT Policy Guidelines of NBL in Chapter#5 at Section No.5.9.
1.02.8.	Charities or NPOs (especially operating in less privileged areas).	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.03.	**Credit Card Customer**				
1.03.1.	Customer who changes static data frequently	Very Likely	Major	4 (Extreme)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.03.2.	Credit Card customer	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
1.03.3.	Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	Very Likely	Major	4 (Extreme)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.03.4.	Prepaid Card customer	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
1.04.	**International Trade Customer**				
1.04.1.	A new customer (Outward remittance-through SWIFT)	Very Likely	Major		1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in Chapter#8 at Section no. 8.2.
1.04.2.	A new customer (Import/ Export)	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 1. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in Chapter#8 at Section no. 8.2.
1.04.3.	A new customer (Inward remittance-through SWIFT)	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in Chapter#8 at Section no. 8.2.
1.04.4.	A new customer who wants to carry out a large transaction (Import/ Export)	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in Chapter#8 at Section no. 8.2.
1.04.5.	A new customer who wants to carry out a large transaction (Inward/ outward remittance)	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in Chapter#8 at Section no. 8.2.; 3. Identify & verify the reasons of carrying out large transactions; 4. Identify & justify the source of fund.
1.04.6.	A customer wants to conduct business	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
	beyond its line of business (import/ export/ remittance)				Chapter#8 at Section no. 8.2; 3. Identify & justify the source of fund.
1.04.7.	Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in Chapter#8 at Section no. 8.2; 3. Follow the instruction of "Accounts of PEPs" of AML/CFT Policy Guidelines of NBL in Chapter#5 at Section No.5.9.
1.04.8.	A new customer who wants to carry out a large transaction (Import/ Export)	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instructions of AML/CFT Policy Guidelines of NBL mentioned in Chapter#8 at Section no. 8.2; 3. Identify & verify the reasons of carrying out large transactions.
1.04.9.	Correspondent Banks	Very Likely	Major	4 (Extreme)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Conduct applicable CDD on foreign correspondent or respondent bank, owners/directors, beneficiary owner(s), authorized person(s), if any, customers of foreign correspondent or respondent bank, if required, as per Section No. 5.11 of Chapter#5 of AML/CFT Policy Guidelines of NBL; 3. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 4. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 5. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL
1.04.10.	Money services businesses (remittance	Very Likely	Major	4 (Extreme)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL;

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
	houses, exchange houses)				2. Conduct applicable CDD on MVTS providers such as remittance houses, exchange houses, etc. their agents or sub-agents, if any, owners/directors, beneficiary owner(s), authorized person(s), if any, and customers of MVTS providers; 3. Screen names of the MVTS providers such as remittance houses, exchange houses, etc. , their agents or sub-agents, if any, owners/directors, beneficiary owner(s), authorized person(s), if any, customers of MVTS providers, if required, applicant/originator, beneficiary and/or any other names or entities appearing in the process of delivering MVTS 4. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 5. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 6. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL

2. Risk Register for Products & Services (All the products and services of a bank has to be included here)

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
2.1	**Retail Banking Product**				
2.1.1	Accounts for students where large amount of transactions are made (student file)	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the source of fund. 3. Identify & justify the reason(s) of carrying out large transactions to the account. 4. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL.
2.1.2	Gift Cheque	Likely	Moder ate	2 (Medium)	Follow the instruction for Walk-in Customer mentioned in Section No. 5.14 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
2.1.3	Locker Service	Likely	Moder ate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. The facility shall be given only to the account

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
					holders.
2.1.4	Foreign currency endorsement in Passport	Likely	Moderate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction for Walk-in Customer mentioned in Section No. 5.14 of Chapter#5 of AML/CFT Policy Guidelines of NBL; 3. Collect & verify photo copies of passport, Visa & air/railway/bus ticket; 4. Comply FERA 1947 & Bangladesh Bank Guidelines, circulars and instructions issued under FERA 1947; 5. Ensure all other compliances as per instructions & circulars of BB, BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
2.1.5	Large transaction in the account of under privileged people	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the source of fund. 3. Identify & justify the reason(s) of carrying out large transactions to the account.
2.1.6	FDR (less than 2 million)	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.1.7	FDR (2 million and above)	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.1.8	Special scheme deposit accounts opened with big installment and small tenure	Likely	Major	3	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register. 2. Identify & justify the source of fund.
2.1.9	Multiple deposit scheme accounts opened by same customer in a branch	Likely	Moderate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register. 2. Identify & justify the source of fund.
2.1.10	Multiple deposit scheme	Likely	Moderate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason(s) for opening

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	accounts opened by same customer from different location				multiple deposit scheme accounts from different locations
2.1.11	Open DPS in the name of family member Or Installments paid from the account other than the customer's account	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.1.12	Stand alone DPS	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.1.13	Early encashment of FDR, special scheme etc.	Likely	Moderate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.; 2. Identify & justify the reason for early encashment.
2.1.14	Non face to face business relationship /transaction	Very Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction for Non-Face to Face customer mentioned in Section No. 5.12 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
2.1.15	Payment received from unrelated/un-associated third parties	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason for receiving payment from unrelated/un-associated third parties. 3. Indentify the source of fund of the third parties.
2.2 Retail Privilege Facilities					
2.2.1	Pre-Approved Credit Card with BDT 300K limit	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.2.2	Enhanced ATM cash	Likely	Moderate	2 (Medium)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register;

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	withdrawal Limit BDT 100K				2. Identify & justify the reason of such transaction.
2.3 SME Banking Product					
2.3.1	Want to open FDR where source of fund is not clear	Likely	Major	3 (High)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Not open the account. 3. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
2.3.2	Early encashment of FDR	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.3.3	Repayment of loan EMI from source that is not clear	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Monitor the transactions of the all other accounts, if any, of the customer;
2.3.4	Repayment of full loan amount before maturity	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.3.5	Loan amount utilized in sector other than the sector specified during availing the loan	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify the sector where the fund is utilized. 3. Comply with Bangladesh Bank's credits related circulars as well as our banks'. 4. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 5. Monitor the transactions of the all other accounts, if any, of the customer.
2.3.6	In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & verify the source of fund; 3. Comply with Bangladesh Bank's credits related circulars as well as our banks'. 4. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 5. Monitor the transactions of the all other accounts, if any, of the customer.
2.3.7	Source of fund used	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register;

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	as security not clear at the time of availing loan				2. Identify & verify the source of repayment and confirm that source of repayment is consistent with known source of fund.
2.4 Wholesale Banking Product					
2.4.1	Development of new product & service of bank	Likely	Major	3 (High)	1. Bank will consider the ML & TF risk. 2. Bank will ensure that CDD/EDD must be applicable in the product & service;
2.4.2	Payment received from unrelated third parties	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason for receiving payment from unrelated/un-associated third parties. 3. Indentify the source of fund of the third parties.
2.4.3	High Value FDR	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register;
2.4.4	Term loan, SOD(FO), SOD(G-work order), SOD(Garment),SOD(PO), Loan General, Lease finance, Packing Credit, BTB L/C	Likely	Major	3 (High)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Collect the documents for customer identification, source of fund & address; 3. Check customers background, assess borrowers net worth & actual fund requirements and Identify purpose; 4. Ensure that the loan approval & documentations are duly completed; 5. Identify & verify Source of fund used as security/margin, if any; 6. Ensure the utilization of loan in the sector as specified in the Head Office approval; 7. Identify & verify the source of repayment and confirm that source of repayment is consistent with known source of fund; 8. Comply BB credits related circulars as well as our banks' credit policy; 9. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 10. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 11. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
2.4.5	BG(bid bond), BG(PG), BG(APG)	Likely	Moder ate	2 (Medium)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Collect the documents for customer identification, source of fund & address; 3. Check customers background, assess borrowers net worth & actual fund requirements and Identify purpose of loan; 4. Identify & verify the purpose of Bank Guarantee(BG); 5. Collect required documents to identify the underlying transaction of the BG & verify it; 6. Ensure that documentations are duly completed; Identify & verify Source of fund used as security/margin, if any, at the time of availing BG; 7. Ensure the utilization of BG in the sector as specified in the Head Office approval; 8. Identify & verify the reason(s) of claim/encashment guarantee, if any; Comply BB BG and/or Investment/credits related circulars as well as our banks' BG/credit policy, if any; 9. Comply BB credits related circulars as well as our banks' credit policy; 10. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 11. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
2.4.6	L/C subsequent term loan, DP L/C	Likely	Major	3 (High)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Collect the documents for customer identification, source of fund & address; 3. Check customers background, assess borrowers net worth & actual fund requirements and Identify purpose of loan; 4. Ensure that the loan approval & documentations are duly completed; 5. Identify & verify Source of fund used as security/margin, if any, at the time of availing loan; 6. Ensure the utilization of loan in the sector as specified in the Head Office approval; 7. Identify & verify the source of repayment and confirm that source of repayment is consistent

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
					with known source of fund; 8. Comply BB credits related circulars as well as our banks' credit policy; 9. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 10. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 11. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
2.4.7	C.C(H), SOD(G-Business), STL	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 2.4.4 of this Risk Register
2.4.8	OBU	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register 2. Follow the additional CDD as per Section No. 6.3 of AML/CFT Policy Guidelines of NBL if the customer involved with import business; 3. Follow the additional CDD as per Section No. 6.4 of AML/CFT Policy Guidelines of NBL if the customer involved with export business; 4. Check customers background, assess borrowers net worth & actual fund requirements and Identify purpose of loan/investment; 5. Comply BB OBU related circulars as well as our banks' credit policy/circulars; 6. Screen the persons, entities, third parties, goods, country, ports, point of transshipment, carrier, master, agents and/or any other names or entities appearing in sales contract, LC, documents presented and/or SWIFT message related to trade transactions; 7. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 8. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 9. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
2.4.9	Syndication Financing	Likely	Major	3 (High)	Follow the treatment/actions mentioned in 2.4.4 of this Risk Register

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
2.5 Credit Card					
2.5.1	Supplementary Credit Card Issue	Likely	Moderate	2 (Medium)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Identify & verify the relationship of card holder with supplementary card holder, 3. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 4. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 5. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
2.5.2	Frequent use of Card/Cheque	Likely	Moderate	2 (Medium)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.5.3	BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)	Most Likely	Major	4 (Extreme)	Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.5.4	Credit card issuance against ERQ and RFCD accounts	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Comply Bangladesh Bank's guidelines & circulars of issuance of credit card against ERQ and RFCD accounts.
2.6 International Trade					
2.6.1	Line of business mismatch (import/export/remittance)	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason for such transaction.
2.6.2	Under/ Over invoicing (import/ export/	Most Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Ensure that the price of the commodity or service is internationally competitive.

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	remittance)				
2.6.3	Retirement of import bills in cash (import/export/remittance)	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register.
2.6.4	Wire transfer	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction of "wire transfer" at Section No. 8.3 in Chapter#8 of AML/CFT Policy Guidelines of NBL.
2.6.5	Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)	Very Likely	Major	4 (Extreme)	1. Follow the instruction for Walk-in Customer mentioned in Section No. 5.14 of Chapter#5 of AML/CFT Policy Guidelines of NBL. 2. Identify & justify the purpose of transaction.

3. Risk Register for Business practices/delivery methods or channels

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
3.1	**Wire Transfer**				
3.01.1	Online (multiple small transaction through different branch)	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction for Walk-in Customer mentioned in Section No. 5.14 of Chapter#5 of AML/CFT Policy Guidelines of NBL. 3. Identify & justify the reason for such transactions.
3.01.2	BEFTN	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction of "wire transfer" at Section No. 8.3 in Chapter#8 of AML/CFT Policy Guidelines of NBL.
3.01.3	BACH	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction of "wire transfer" at Section No. 8.3 in Chapter#8 of AML/CFT Policy Guidelines of NBL.

3.01.4	IDBP	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Ensure that goods or services are delivered as specified in the sales contract and/or Local LC;
3.01.5	Mobile Banking	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Follow the instruction of "CDD Requirements for Technology Related Products" mentioned in Section no. 9.5 in Chapter#9 of AML/CFT Policy Guidelines of NBL.
3.01.6	Third party agent or broker	Likely	Moderate	3 (High)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL; 3. Identify & justify the source of fund. 4. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 5. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 6. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.

3.2	**Credit Card**				
3.02.1	New Merchant sign up	Likely	Moderate	3 (High)	1. Follow the Customer Acceptance Policy as indicated in Section No. 4.1 Chapter#4 of AML/CFT Policy Guidelines of NBL; 2. Conduct CDD measures for POS (new merchant); 3. Identify & justify the source of fund; 4. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL; 5. Monitor the transactions of the account as per Chapter#9 of AML/CFT Policy Guidelines of NBL; 6. Report to BFIU through AMLD if any activity seems suspicious as per chapter#11 of AML/CFT Policy Guidelines of NBL; 7. Ensure all other compliances as per instructions & circulars of BFIU, AMLD &

					AML/CFT Policy Guidelines of NBL.
3.02.2	High volume transaction through POS	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & verify the reason(s) of high volume transaction through an POS.
3.3	**Alternate Delivery Channel**				
3.03.1	Large amount withdrawn from ATMs	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Monitor the transactions through ATM on 24/7 basis and identify & confirm that the large amount withdrawal from ATM is made by the customer and the transaction is consistent with the approved limit.
3.03.2	Larger amount transaction from different location and different time(mid night) through ATM	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Monitor the transactions through ATM on 24/7 basis and identify & confirm that the large amount withdrawal from ATM is made by the customer and the transaction is consistent with the approved limit; 3. Identify & verify the reason(s) of making large amount transactions from different locations & different time through ATM by the customer.
3.03.3	Large amount of cash deposit in CDM	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the large amount cash deposit through CDM.
3.03.4	Huge fund transfer through internet	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Identify & justify the reason for huge transfer through internet 3. Monitor the transactions through internet on 24/7 basis through call center.
3.03.5	Transaction Profile updated through Internet Banking	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Justify the transaction profile updated through internet with the known source of income; 3. Monitor the transactions through internet on 24/7 basis through call center.
3.03.6	Customer to business transaction-	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Justify the reason for such transaction.

	Online				
3.03.7	Payment Gateway - Internet Banking	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Maintain a register of this type customer 3. Don't allow transaction until risk is reduced.
3.4	**International Trade**				
3.04.1	Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register 2. Follow the instruction of "wire transfer" at Section No. 8.3 in Chapter#8 of AML/CFT Policy Guidelines of NBL.
3.04.2	Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103).	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register 2. Follow the instruction of "wire transfer" at Section No. 8.3 in Chapter#8 of AML/CFT Policy Guidelines of NBL.

4. Risk Register for Country/jurisdiction

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
4.1	Import and export form/to sanction country	Very Likely	Major	4 (Extreme)	1. Reject transaction, if the transaction has not commenced; 2. Stop transaction if the transaction has already commenced; 3. Report the transaction(s) to AMLD for ultimate submission to BFIU without any delay; 4. Ensure all other compliances as per instructions & circulars of Bangladesh Bank, BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
4.2	Transshipments,	Very Likely	Major	4 (Extreme)	1. Reject transaction, if the transaction has not commenced;

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
	container, flag vessel etc. under global sanction				2. Stop transaction if the transaction has already commenced; 3. Report the transaction(s) to AMLD for ultimate submission to BFIU without any delay; 4. Ensure all other compliances as per instructions & circulars of Bangladesh Bank, BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
4.3	Establishing correspondent relationship with sanction bank and/or country	Very Likely	Major	4 (Extreme)	1. Corresponding relationship with sanction bank and/or country are not allowed 2. Stop/Discontinue corresponding relationship with sanction bank or country if the relationship has been already established; 3. Report the name of the sanctioned bank and/or country to AMLD for ultimate submission to BFIU without any delay 4. Ensure all other compliances as per instructions & circulars of BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
4.4	Establishing correspondent relationship with poor AML&CFT practice country	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.5	Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.6	Customer belongs to countries or geographic areas identified by credible sources as	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
	providing funding or support for terrorist activities, or that have designated terrorist organizatio ns operating within their country.				
4.7	Customer belongs to High Risk ranking countries of the Basel AML index.	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.8	Customer belongs to the countries identified by the bank as higher - risk because of its prior experiences or other factors.	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.9	Any country identified by FATF or FSRBs- (FATF style Regional Body) as not having adequate AML&CF T systems	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.10	Any bank	Very	Major	4	1. Not allow any relationship with Shell or any

Sl.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
	that provide service to 'Shell Bank'	Likely		(Extreme)	bank that provide service to shell bank; 2. Stop corresponding relationship or transaction with the shell bank or any bank that provide service to shell bank if the relationship has been established or transaction has been already commenced; 3. Report the transaction(s) to AMLD for ultimate submission to BFIU without any delay; 4. Ensure all other compliances as per instructions & circulars of Bangladesh Bank, BFIU, AMLD & AML/CFT Policy Guidelines of NBL.
4.11	Any bank that allow payable through account	Likely	Moderate	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.12	Any country identified as destination of illicit financial flow	Very Likely	Major	4 (Extreme)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.13	Branches in a Border Area	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.14	Area identified as high risk in the NRA	Likely	Major	3 (High)	1. Follow the treatment/actions mentioned in 1.01.1 of this Risk Register; 2. Conduct Enhanced Due Diligence (EDD) on customer, beneficiary owner(s) and authorized person(s), if any, as per Chapter#5 Section No. 5.8 of AML/CFT Policy Guidelines of NBL.
4.15	Countries subject to UN embargo/sanctions	Very Likely	Major	4 (Extreme)	1. Reject any transaction, if the transaction has not commenced with the countries ; 2. Stop corresponding relationship or if the relationship has been already established or transaction has been started; 3. Report the transaction(s) to AMLD for

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
					ultimate submission to BFIU without any delay; 4. Ensure all other compliances as per instructions & circulars of Bangladesh Bank, BFIU, AMLD & AML/CFT Policy Guidelines of NBL.

5. Register for Regulatory Risk

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
5.1	Not having AML/CFT guideline	Likely	Major	3 (High)	Immediately prepare detailed AML/CFT guideline and have it approved by Board..
5.2	Not forming a Central Compliance Committee (CCC)	Likely	Major	3 (High)	Immediately form a Central Compliance Committee (CCC) as per section no. 3.4 of Chapter#3 of AML/CFT Policy Guidelines of NBL.
5.3	Not having an AML&CFT Compliance Officer	Likely	Major	3 (High)	Immediately appoint a competent AML/CFT compliance officer as per section no. 3.6 of Chapter#3 of AML/CFT Policy Guidelines of NBL.
5.4	Not having Branch Anti Money Laundering Compliance Officer	Likely	Major	3 (High)	Immediately appoint Branch Anti Money Laundering as per section no. 3.11 of Chapter#3 of AML/CFT Policy Guidelines of NBL.
5.5	Not having an AML&CFT program	Likely	Major	3 (High)	Develop proper AML/CFT compliance program as per section no. 2.7 of Chapter#2 of AML/CFT Policy Guidelines of NBL.
5.6	No senior management commitment to comply with MLP and AT Act	Likely	Major	3 (High)	Prepare the senior management commitment to comply with MLP and ATA Act and Share the commitment with Bank officials (at least once in a year)
5.7	Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	Likely	Major	3 (High)	Immediately take action to comply with the AMLD/BFIU circulars, circular letters, instructions etc
5.8	Unique account opening form not followed while opening account	Likely	Major	3 (High)	Meticulously follow the Unique account opening form.
5.9	Non screening of new and existing customers against UNSCR Sanction and OFAC lists	Likely	Major	3 (High)	Screen all new and existing customers against UNSCR and Local Sanction lists through Automated Sanction Screening software.

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
5.10	Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Likely	Major	3 (High)	Follow the Foreign Exchange Regulation Act, 1947 & its assessment while dealing with NRB accounts.
5.11	Complete and accurate information of customer not obtained	Likely	Major	3 (High)	Follow the instructions of KYC, CDD and EDD as per section no. 5.3-5.8 of Chapter #5 of AML/CFT Policy Guidelines of NBL.
5.12	Failure to verify the identity proof document and address of the customer	Likely	Major	3 (High)	Follow the instruction of "In case where conducting of CCD measure is not possible" as per Section No. 5.7 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
5.13	Beneficial owner identification and verification not done properly	Likely	Major	3 (High)	Follow the instruction of "Beneficial Ownership and Control" as per Section No. 5.15 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
5.14	Customer Due Diligence (CDD) not practiced properly	Likely	Major	3 (High)	Follow the instruction of "General Measures of Customer Due Diligence (CDD)" as per Section No. 5.4 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
5.15	Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPS and influential person and senior official of international organization.)	Likely	Major	3 (High)	Follow the instruction of "Enhanced Due Diligence (EDD) measures" and "Accounts of Politically Exposed Persons" as per Section No. 5.6 & 5.7 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
5.16	Failure to complete KYC of customer including walk in customer	Likely	Major	3 (High)	Follow the instruction for Walk-in Customer mentioned in Section No. 5.14 of Chapter#5 of AML/CFT Policy Guidelines of NBL
5.17	Failure to update TP and KYC of customer	Likely	Major	3 (High)	Follow the instruction of KYC, CDD mentioned in Section No. 5.3-5.8 of Chapter#5 of AML/CFT Policy Guidelines of NBL
5.18	Keep the legacy accounts operative without completing KYC	Likely	Major	3 (High)	
5.19	Failure to assess the ML & TF risk of a product or service before launching	Likely	Major	3 (High)	a) Assess the ML & TF risk of a product or service, devise action plan to manage the same before launching the products or service at Head Office level. b) Check whether all the Product Program Guides (PPG) approved by

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
					CCC before launching.
5.20	Failure to complete the KYC of Correspondent Bank	Very Likely	Major	4 (Extreme)	Obtain updated KYC of correspondent bank from time to time mandatorily.
5.21	Senior Management approval not obtained before entering into a Correspondent Banking relationship	Very Likely	Major	4 (Extreme)	Follow the instructions of "Correspondent Banking Relationship" as per Section No. 5.11 of Chapter#5 of AML/CFT Policy Guidelines of NBL.
5.22	Failure to comply with the instruction of BFIU by bank Foreign subsidiary	Very Likely	Major	4 (Extreme)	a) Monitor the AML & CFT activity of foreign subsidiary. b) Obtain confirmation from the subsidiary on compliance.
5.23	Failure to keep record properly	Likely	Major	3 (High)	Keep records as Chapter#3 of AML/CFT Policy Guidelines of NBL.
5.24	Failure to report complete and accurate CTR on time	Very Likely	Major	4 (Extreme)	a) Ensure uniformity of CTR submitted through goAML web. b) Submit complete and accurate CTR on time.
5.25	Failure to review CTR	Likely	Major	3 (High)	Generate CTR from system, Monitor the transactions in CTR by both branch & AMLD on monthly basis and identify suspicious transition, if any.
5.26	Failure to identify and monitor structuring	Likely	Major	3 (High)	Generate structuring from system Identify and monitor structuring on monthly basis. Train officers to detect Structuring.
5.27	Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Likely	Major	3 (High)	Develop system to generate report that facilitate identifying STR, Generate high value transition report, TP exceed report, structuring report from the system to analyze transactions and detect STR.
5.28	Failure to conduct quarterly meeting properly	Likely	Major	3 (High)	Conduct quarterly meeting at branch in line with the agenda and instruction of BFIU Circular No.26. and Send the meeting minutes to AMLD.
5.29	Failure to report suspicious transactions (STR)	Likely	Major	3 (High)	Closely Monitor account transaction and customer activity and report as soon as possible after finding suspicious transactions/ activity.
5.30	Failure to conduct self assessment properly	Likely	Major	3 (High)	Conduct self assessment properly. Portray the actual strength, weakness and position of the branch in self assessment Report.

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
					AMLD shall cross check the self assessment report with independent testing report and inspection report.
5.31	Failure to submit statement/ report to BFIU on time.	Very Likely	Major	4 (Extreme)	Submit statement /report to BFIU timely.
5.32	Submit erroneous statement/ report to BFIU	Very Likely	Major	4 (Extreme)	Check minutely the statements before submitting statement/ report to BFIU. If any error is found, it should be corrected immediately.
5.33	Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Very Likely	Major	4 (Extreme)	Comply with the order for freezing issued by BFIU instantly.
5.34	Not submitting accurate information or statement sought by BFIU or BB.	Very Likely	Major	4 (Extreme)	Check minutely the statements before submitting statement/ report to BFIU. If any error is found, it should be corrected immediately.
5.35	Not submitting required report to senior management regularly	Likely	Major	3 (High)	Submit all the report to senior management timely.
5.36	Failure to rectify the objections raised by BFIU or bank inspection teams on time	Very Likely	Major	4 (Extreme)	Regularize the objections raised by BFIU or BANK inspection teams on time and submit compliance report. AMLD shall follow up to rectify or regularize the irregularities.
5.37	Failure to obtain information during wire transfer	Likely	Major	3 (High)	Information during wire transfer based on the threshold as per Section No. 9.1 of this guidelines to be obtained. Inspection team to check compliance status during audit/ inspection.
5.38	Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely	Major	3 (High)	Responsibilities of ordering, intermediary and beneficiary Bank as per Section No. 9.2 of this guidelines to be complied.
5.39	Failure to scrutinize staff properly	Likely	Major	3 (High)	HR to screen the applicant's details before recruitment & Conduct reference check.
5.40	Failure to circulate BFIU guidelines and circulars to branches	Very Likely	Major	4 (Extreme)	Issue instruction guidelines and circulars timely.
5.41	Inadequate training/ workshop arranged on AML & CFT	Very Likely	Major	4 (Extreme)	a) Arrange workshop on AML & CFT for employees to build up awareness and conduct evaluation test. b) Ensure All the employees of the Bank have received training on AML & CFT. c) MIS on training is to be kept.

Sl.	Risk	Likeli hood	Impact	Risk Score	Treatment/Action
5.42	No independent audit function to test the AML program	Very Likely	Major	4 (Extreme)	ICCD to test the AML program and conduct independent testing procedure.