

December, 2022

ML & TF Risk Assessment & Risk Management Guidelines

Second Edition

AML & CFT Division, Head Office |
COMMUNITY BANK BANGLADESH LIMITED



Preface

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

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

As a nation, we cannot afford to have our country's image tarnished because of money laundering and terrorist financing issues. Since banks are highly vulnerable to being used by money launderers and terrorist financiers to conceal and legitimize the *ill-gotten gains*, we have to be vigilant and guard the integrity of our financial system for financial and social stability. Bangladesh Financial Intelligence Unit (BFIU) has issued a number of circulars and guidelines concerning the prevention of money laundering and terrorist financing to cope up with the emerging typologies and challenges and we have reviewed the previous guideline (which was approved on 5th Meeting of the Honorable Board of Directors held on March 09, 2019) in line with the Money Laundering Prevention Act, 2012 (Amendment 2015), Anti-Terrorism Act, 2009 (Amendment 2012 and 2013), Money Laundering Prevention Rules, 2019, BFIU Circular no- 26 dated June 16, 2020, and Guidance Notes on Beneficial Owner, Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR), Politically Exposed Persons (PEPs)/Influential Persons (IPs), Prevention of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction and some other circulars issued by the BFIU and Banking Regulation & Policy Department (BRPD), Bangladesh Bank from time to time.

Community Bank Bangladesh Limited (CBBL) will review the "Money Laundering and Terrorist Financing Risk Assessment & Risk Management Guidelines" in every alternative year and as and when required.



Table of Contents

Chapter: 1	7
An Overview of Money Laundering	7
1.1 Background:.....	7
1.2 Benefits of the Guideline:.....	7
1.3 Definition of Money Laundering:.....	7
1.4 Predicate Offence:	8
1.5 Property means:	9
1.6 Stages of Money Laundering.....	9
1.6.1 Placement.....	10
1.6.2 Layering	10
1.6.3 Integration.....	10
1.7 Penalties under Money Laundering Prevention Act, 2012 (Amendment, 2015).....	11
1.8 Definition of Terrorist Financing	12
1.9 Penalties for Terrorist Financing:	13
1.10 The Link between Money Laundering and Terrorist Financing	14
1.11 Why We Must Combat ML & TF	14
Chapter: 2	16
International Initiatives on Money Laundering & Terrorist Financing	16
2.1 Introduction.....	16
2.2 The United Nations	16
2.2.1 The Vienna Convention.....	16
2.2.2 The Palermo Convention	16
2.2.3 International Convention for the Suppression of the Financing of Terrorism	17
2.2.4 Security Council Resolution 1267 and Successors	17
2.2.5 Security Council Resolution 1373	17
2.2.6 The Counter-Terrorism Committee	18
2.2.7 Global Program against Money Laundering	18
2.3 The Financial Action Task Force (FATF)	18
2.3.1 FATF 40+9 Recommendations	18
2.3.2 FATF New Standards.....	19
2.3.3 International Cooperation and Review Group (ICRG).....	20
2.4 Asia Pacific Group on Money Laundering (APG)	20
2.5 The Egmont Group of Financial Intelligence Units.....	21
2.6 The Basel Committee on Banking Supervision	21
Chapter: 3	22
National Initiatives on Money Laundering & Terrorist Financing	22
3.1 Introduction.....	22
3.2 Founding Member of APG	22
3.3 Legal Framework.....	22

3.4 Central and Regional Taskforces	22
3.5 Anti-Money Laundering Department.....	23
3.6 Bangladesh Financial Intelligence Unit (BFIU)	23
3.7 National Coordination Committee and Working Committee	23
3.8 National ML & TF Risk Assessment (NRA).....	23
3.9 National Strategy for Preventing ML and TF	24
3.10 Chief Anti-Money Laundering Compliance Officers (CAMLCO) Conference	24
3.11 Egmont Group Memberships	24
3.12 Anti Militants and De-Radicalization Committee	25
3.13 Memorandum of Understanding (MOU) Between ACC and BFIU	25
3.14 Implementation of TFS	25
3.15 Coordinated Effort on the Implementation of the UNSCR.....	25
Chapter: 4.....	26
Legal Requirement & Penalties.....	26
4.1 Requirements under the Money Laundering Prevention Act, 2012 and (Amendment - 2015)	26
4.2. Establishment of Bangladesh Financial Intelligence Unit (BFIU)	26
4.3. Responsibilities of Bangladesh Financial Intelligence Unit.....	27
4.4 Investigation, Prosecution etc.....	27
4.5 Offence Committed by Company:.....	28
4.6 Protection against Proceedings Undertaken in Good Faith	28
4.7 Responsibility of reporting organization in preventing money laundering:	28
4.8 Terrorist financing: Requirements under the MLPA, 2012 (amendment 2015) and ATA (amendment 2012 & 2013).....	29
4.9 The Offence of Terrorist financing.....	30
4.10 Offence of Money Laundering and Punishment:.....	30
Chapter: 5.....	32
AML / CFT Policies and procedures of Community Bank Bangladesh Limited	32
5.1 Institutional Policy.....	32
5.2 Senior Management Commitment.....	33
5.3 Statement of Commitment of Managing Director& CEO.....	33
Chapter: 6.....	35
Compliance Structure of the Bank.....	35
6.1 Central Compliance Committee (CCC).....	35
6.1.1 Formation of CCC.....	35
6.1.2 Responsibilities and Authorities of the CCC	36
6.1.3 Separation of CCC from Internal Control & Compliance Department (ICCD)	37
6.2 Formation of AML & CFT Division	37
6.3 Appointment of CAMLCO.....	38
6.3.1 Authorities and Responsibilities of CAMLCO.....	38
6.4 Appointment of DCAMLCO	39
6.4.1 Authorities & Responsibilities of DCAMLCO.....	39
6.5 Branch Anti Money Laundering Compliance Officer (BAMLCO)	40
6.5.1 Responsibilities and Authorities of BAMLCO.....	40
6.6 Department/Division AML Compliance Officer.....	44



6.7 Roles & Responsibilities of Account Opening Officer/Branch Operation Manager/ Relationship Manager	44
6.8 Role & Responsibilities of Internal Control & Compliance Division	44
6.9 Responsibilities of Internal Control & Compliance Division on Self-Assessment & Independent Testing Procedures	45
6.10 External Auditor	46
Chapter: 7.....	47
Customer Acceptance Policy	47
7.1 Objective and Application of the policy:.....	47
7.2 Definition of customer	48
7.3 Customer Acceptance Criteria	49
7.4 Customer Acceptance Policy	49
Chapter: 8.....	51
AML & CFT Risk Assessment and Risk Management Process of CBBL.....	51
8.1 Risk Based Approach	51
8.2 Risk Management Framework.....	51
8.3 Risk identification.....	51
8.4 Risk assessment	52
8.5 Risk Treatment.....	53
8.6 Risk Monitor and review	53
8.7 Additional tools to help risk assessment.....	54
8.7.1 Applying risk appetite to risk assessment	54
8.7.2 Risk tolerance	55
8.8 Know Your Customer (KYC) Policies	55
8.8.1 Know Your Customer Procedures.....	55
8.8.2 Risk categorization - Based on Activity/KYC Profile.....	56
8.9 Customer Identification	57
8.9.1 Customer Due Diligence	58
8.9.2 What is required for CDD?.....	59
8.9.3 When CDD is required (Timing of CDD)?	59
8.10 Enhanced Customer Due Diligence Measure	60
8.11 Identification of Beneficial Owner	60
8.11.1 Who is Beneficial Owner?.....	60
8.11.2 Why is it important to identify the beneficial owner?	61
8.11.3 Ways in which beneficial ownership information can be hidden/obscured.....	61
8.11.4 Ownership	62
8.12 Politically exposed persons (PEPs)	62
8.12.1 Who are Politically Exposed Persons (PEPs).....	62
8.13 who are influential persons; IPs in Bangladesh.....	63
8.14 Chief or similar high-ranking positions in an international organization.....	63
8.14.1 Various scenario related with PEPs/IPs	63
8.15 Correspondent Banking	65
8.16 Branches and subsidiaries situated/located in foreign jurisdiction.....	66

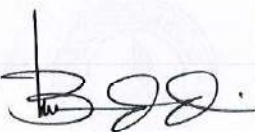


8.17	What Constitutes a Person’s Identity?	67
8.18	Individual Customers	68
8.19	Persons without Standard Identification Documentation	69
8.20	Corporate Bodies and other Entities	70
8.21	Partnerships and Unincorporated Businesses	72
8.22	Powers of Attorney/ Mandates to Operate Accounts	72
8.23	Internet or Online Banking	72
8.24	Walk-in Customers for TT, DD, PO etc.	73
8.25	Provision of Safe Custody and Safety Deposit Boxes	73
8.26	Timing and Duration of Verification	73
Chapter: 9	74
Transaction Monitoring, Reporting and Record Keeping	74
9.1	Record Keeping	74
9.2	Legal Obligations	74
9.3	Transaction Monitoring Process	74
9.4	Cash Transaction Report (CTR)	75
9.5	Half yearly Self-Assessment Report & Independent Testing Procedures (ITP)	76
9.5.1	Responsibilities of Branch	76
9.5.2	Responsibilities of Internal Control & Compliance Division	76
9.5.3	Responsibilities of AML & CFT Division/CCC	76
9.6	Quarterly meeting minutes	76
9.7	Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR)	76
9.7.1	Reporting STR/SAR	79
9.8	Whistle Blowing	80
Chapter: 10	81
Recruitment, Training and Awareness	81
10.1	Employee Screening	81
10.2	Know You Employee (KYE)	81
10.3	Training For Employee	81
10.4	The Need for Staff Awareness	82
10.5	Awareness of Senior Management	83
Chapter: 11	84
Trade based Money Laundering	84
11.1	Recognition of Trade based Money Laundering	84
Chapter: 12	85
Terrorist Financing & Proliferation Financing	85
12.1	Introduction	85
12.2	Obligations under Law and Circular	85
12.3	Obligations under Circular	86
12.4	Necessity of Funds by Terrorist	86
12.5	Sources of Fund/Raising of Fund	86
12.6	Movement of Terrorist Fund	86
12.7	Formal Financial Sector	87
12.8	Trade Sector	87
12.9	Cash Couriers	87

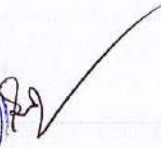


12.10 Use of Alternative Remittance Systems (ARS)	87
12.11 Use of Charities and Non-Profit Organizations	87
12.12 Targeted Financial Sanctions	88
12.13 TFS related to terrorism and terrorist financing-	88
12.14 TFS related to Proliferation-	88
12.15 Automated Sanction Screening Mechanism of UNSCRs	88
▪ Opening any account or establishing relationship domestically:	88
▪ Any international relationship or transaction:	89
➤ For incoming messages:	89
➤ For outgoing messages:	89
Responsibilities of Branch Manager/BAMLCO in areas of Sanction Screening	89
Chapter: 13	90
Anti-Bribery and Corruption (ABC) Policy	90
13.1 Preamble	90
13.2 Bribery	90
13.3 Corruption and Fraud	90
13.4 Initiatives of Community Bank Bangladesh Limited to protect bribery and corruption	91
13.4.1 Zero tolerance to bribery and corruption	91
13.4.2 Governance	91
13.5 ABC compliance Program	92
13.6 Conclusion	93
Annexure-A	94
RISK REGISTER	94
1. ML & TF Risk Register for Customers	94
2. Risk Register for Products & Services (All the products and services of a bank has to be included here)	115
3. Risk Register for Business practices/delivery methods or channels	124
4. Risk Register for Country/jurisdiction	128
5. Register for Regulatory Risk	132
Annexure-B	137
KYC DOCUMENTATION	137
Annexure-C	143
KYC PROFILE FROM FOR WALK-IN CUSTOMER & ONLINE TRANSACTION	143
Annexure-D	144
SUSPICIOUS TRANSACTION REPORT (STR) FORM	144









Chapter: 1

An Overview of Money Laundering

1.1 Background:

This policy sets out:

- a. The obligations of Community Bank Bangladesh Limited (CBBL) with respect to the requirements imposed under the Money Laundering Prevention Act - 2012 (including all amendments-2015), Anti-Terrorism Act - 2009 (including all amendments-2012 & 2013), Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector, Money Laundering Prevention Rules - 2019, Anti -Terrorism Rules, 2013, BFIU Master Circular No. 26 and Guidance notes on Guidelines on Electronic Know Your Customer (e-KYC), Guidelines for Prevention of Trade Based Money Laundering, Guidance Notes for Prevention of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction, Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations, Guidance on Reporting Suspicious Transaction Report for the Reporting Organization, Guidelines for Beneficial Owner dated January 31, 2019 and other instructions & directive of BFIU, Circular issued by Bangladesh Bank & other regulators from time to time.
- b. Requirement imposed on implementation a comprehensive risk-based approach in managing ML/TF risks; and
- c. Role & Responsibility of the Board of Directors, Senior Management, Central Compliance Committee (CCC), CAMLCO, DCAMLCO, BAMLCO, Head Office & Branch Official in putting in place the relevant AML/CFT measure.

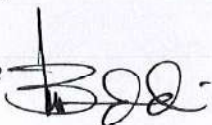
1.2 Benefits of the Guideline:

- a. Enable Community Bank Bangladesh Limited (CBBL) to increase awareness of anti-money laundering & combating the financing of terrorism among all the employees.
- b. Explain our duties and responsibilities under the Money Laundering Prevention act 2012 (amended in 2015) and Anti-Terrorism act 2009 (amended in 2012 & 2013).
- c. Help us to meet the regulatory requirements and international standards.
- d. Understand the consequence of non-compliance
- e. Answer our queries regarding the AML / CFT / KYC / CDD / EDD producer of the Bank.
- f. Introduce us with various AML related monitoring & reporting.

1.3 Definition of Money Laundering:

Money laundering can be defined in a number of ways. But the fundamental concept of Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins. Most countries subscribe to the definition adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property



- or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;
- 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 an offense or offenses or from an act of participation in such an offense or offenses, and;
 - The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

Money Laundering is defined in Section 2 (3) of the Prevention of Money Laundering Act 2009 as follows:

Money Laundering means:

- i) Transfer, conversion, bringing/ remitting funds in and out of Bangladesh the proceeds or properties acquired through commission of a predicate offence [Mentioned in 1.3] for the purpose of concealing or disguising the illicit origin of the property or illegal transfer of properties acquired or earned through legal or illegal means.
- ii) To conduct, or attempt to conduct a financial transaction with an intent to avoid a reporting requirement under this Act (the MLPA, 2009).
- iii) To do or attempt to do such activities so that the illegitimate source of the fund or property can be concealed or disguised or knowingly assist to perform or conspire to perform such activities.

1.4 Predicate Offence:

The offences from which the proceeds derived from committing or attempt to commit the following offences:

01.	Corruption and bribery;	15.	Theft or robbery or dacoity or piracy or hijacking of aircraft;
02.	Counterfeiting currency;	16.	Human Trafficking or obtaining money or trying to obtain money or valuable goods giving someone false assurances of employment abroad;
03.	Counterfeiting deeds and documents;	17.	Dowry;
04.	Extortion;	18.	Smuggling and offences related to customs and excise duties;
05.	Fraud;	19.	Tax related offences;
06.	Forgery;	20.	Infringement of intellectual property rights;

07.	Illegal trade of firearms;	21.	Terrorism or financing in terrorist activities;
08.	Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;	22.	Adulteration or the manufacture of goods through infringement of title;
09.	Illegal trade in stolen and other goods;	23.	Offences relating to the environment;
10.	Kidnapping, illegal restrain and hostage taking;	24.	Sexual exploitation;
11.	Murder, grievous physical injury;	25.	Insider trading and market manipulation- Using price sensitive information relating to the capital market in share transactions before it is published for general information to take advantage of the market and attempting to manipulate the market for personal or institutional gain;
12.	Trafficking of women and children;	26.	Organized crime, and participation in organized criminal groups;
13.	Black marketing;	27.	Racketeering; and
14.	Smuggling of domestic and foreign currency;	28.	Any other offence(s) declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official (Bangladesh) Gazette, for the purpose of this Act.

1.5 Property means:

- Any kind of assets, whether tangible or intangible, movable or immovable, however acquired; or
- Cash, legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.

1.6 Stages of Money Laundering

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

1.6.1 Placement

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

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

1.6.2 Layering

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

Layering usually involves a complex system of transactions designed to hide the source and ownership of the funds. Once cash has been successfully placed into the financial system, launderers can engage in an infinite number of complex transactions and transfers designed to disguise the audit trail and thus the source of the property and provide anonymity. One of the primary objectives of the layering stage is to confuse any criminal investigation and place as much distance as possible between the source of the ill-gotten gains and their present status and appearance.

1.6.3 Integration

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

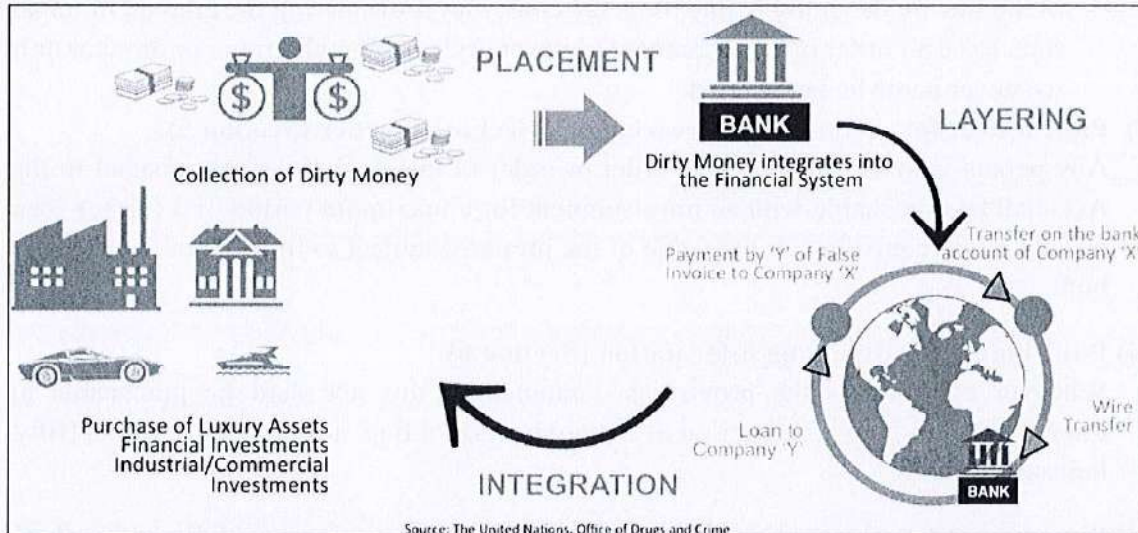


Figure: 3 stages of Money Laundering

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

1.7 Penalties under Money Laundering Prevention Act, 2012 (Amendment, 2015)

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

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

of the fine by the entity in due time, the court may, considering the amount of unpaid fine, issue an order of imprisonment to the entity's owner, chairman or director or by whatever name he is regarded.

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

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

iii) Punishment for divulging information (Section 6):

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

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

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

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

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

1.8 Definition of Terrorist Financing

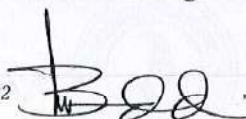
Terrorist financing provides funds for terrorist activities. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud,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

Financing of Terrorism is also includes:

- Providing or collecting property for carrying out an act of terrorism;
- Providing services for terrorism purposes;
- Arranging for retention or control of terrorist property; or
- Dealing with terrorist property.

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

- 1) 'If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
 - a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or





- b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.
- 2) For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b).

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

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

- (a) To carry out terrorist activity;
- (b) By terrorist person or entity or in the knowledge that they are to be used by terrorist person or entity; the said person or entity shall commit the offence of terrorist financing.

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

1.9 Penalties for Terrorist Financing:

According to the Section 7(3) of the Anti-Terrorism Act 2009, (Amendment) 2013, If any person is found guilty of any of the offences mentioned in sub-sections (1), the person shall be punished with an imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine may be imposed equal to twice the value of the property involved with the offence or taka 10(ten) lac, whichever is greater.

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

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

1.10 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.

1.11 Why We Must Combat ML & TF

Money Laundering Has Potentially Devastating Economic, security, and social consequences. Money laundering is a vital process to make crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupted public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences resulted from ML & TF.

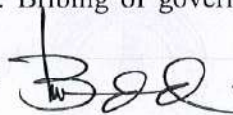
Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection activities more difficult. This loss of revenue generally means higher tax rates than would normally be the case if the untaxed proceeds of crime were legitimate.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

Money laundering distorts assets 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 and even systemic crisis. The loss of credibility and investor's confidence, that such crisis 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 funds, to hide the ill-gotten gains. These front companies have access to substantial illicit funds, 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. Bribing of government officials 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.

A nation cannot afford to have its reputation and financial institutions tarnished by involvement with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions (FIs) and the underlying criminal activities like fraud, counterfeiting, narcotics trafficking, and corruption weaken the reputation and standing of any financial institution. Actions taken by FIs to prevent money laundering are not only a regulatory requirement, but also an act of self-interest.

A financial institution tainted by money laundering accusations from regulators, law enforcement agencies, may lose their good market reputation and damage the reputation of the country. It is very difficult and requires significant resources to rectify a problem that could be prevented with proper program.

Besides its effect on macro level, ML & TF also affects individual financial institution. If a money launderer uses a financial institution for making his/her money legitimate, the business of that financial institution may hamper. If the money launderer withdraws his/her deposited money from an FI before maturity, the FI will face liquidity crisis if the amount is big enough. Moreover, if it is found that an FI was used for ML & TF activities, and it did not take proper action against that ML & TF as per the laws of the country, the FI will have to face legal risk. Finally, the reputation of an FI can also be heavily affected through its involvement with ML & TF activities.

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

Chapter: 2

International Initiatives on Money Laundering & Terrorist Financing

2.1 Introduction

In response to the growing concern about money laundering and terrorist activities, the initiatives taken by international community has acted on many fronts. This part of these Guidelines discusses the various international organizations and their initiatives relating to anti-money laundering (AML) and combating the financing of terrorism (CFT). It further describes the documents and instruments that have been developed for AML & CFT purposes.

2.2 The United Nations

The United Nations (UN) was the first international organization to undertake significant action to fight against money laundering on worldwide basis. The role of the UN is important for several reasons which are following-

First, it is the international organization with the broadest range of membership. The UN, founded in 1945, has 191 members from all across the world.

Second, the UN actively operates a program to fight money laundering; the Global Program against Money Laundering, headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).

Third, and perhaps most important that the UN has the ability to adopt international treaties or conventions that obligate the ratifying countries to reflect those treaties or conventions in their local laws.

In certain cases, the UN Security Council has the authority to bind all member countries through a Security Council Resolution, regardless of other actions on the part of an individual country.

2.2.1 The Vienna Convention

Due to growing concern about the increased international drug trafficking and the tremendous amount of related money entering into financial system, the UN adopted the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) known as Vienna Convention, named after the city in which it was signed. The Vienna Convention deals primarily with provisions to fight the illicit drug trade and related law enforcement issues. At present, nearly 169 countries including Bangladesh are members to the convention. The convention has come into force from November 11, 1990.

2.2.2 The Palermo Convention

In order to fight against internationally organized crimes, the UN adopted the International Convention against Transnational Organized Crime (2000), named after the city in which it was signed as Palermo Convention. The Palermo Convention specifically obligates each ratifying country to:

- Criminalize money laundering and include all serious crimes as predicate offenses of

- money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;
- Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
 - Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyze and disseminate information; and
 - Promote international cooperation.

This convention has come into force from 29th September 2003, having been signed by 147 countries and ratified by 82 countries.

2.2.3 International Convention for the Suppression of the Financing of Terrorism

The financing of terrorism was an international concern prior to the attacks on the United States on 11 September, 2001. In response to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002 with 132 countries signing the convention and 112 countries ratifying it.

The convention requires ratifying states to criminalize terrorism, terrorist organizations and terrorist acts. Under the convention, it is unlawful for any person to provide or collect funds with the (1) intent that the funds be used for, or (2) knowledge that the funds be used to, carry out any of the acts of terrorism defined in the other specified conventions that are annexed to this convention.

2.2.4 Security Council Resolution 1267 and Successors

The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the Sanctions Committee (now called the 1267 Committee). The initial Resolution 1267 of October 15, 1999 dealt with the Taliban and was followed by 1333 of December 19, 2000 on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002), provided some exclusions (1452 of December 20, 2002) and took measures to improve implementation (1455 of January 17, 2003). The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States. The most recent list is available on the website of the 1267 Committee.

2.2.5 Security Council Resolution 1373

Unlike an international convention, which requires signing, ratification, and recognition in local law by the UN member country to have the effect of law within that country, a Security Council Resolution was passed in response to a threat to international peace and security under Chapter VII of the UN Charter, is binding upon all UN member countries. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to:

- deny all forms of support for terrorist groups;
- suppress the provision of safe haven or support for terrorist, including freeing funds or assets of persons, organizations or entities involved in terrorist acts;
- prohibit active or passive assistance to terrorists; and
- cooperate with other countries in criminal investigations and share information about planned terrorist acts.

2.2.6 The Counter-Terrorism Committee

As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism. Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution's measures and report regularly on progress. In this regard, the CTC has asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism in relation to the requirements of Resolution 1373.

2.2.7 Global Program against Money Laundering

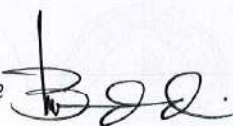
The UN Global Program against Money Laundering (GPML) is within the UN Office of Drugs and Crime (UNODC). The GPML is a research and assistance project with the goal of increasing the effectiveness of international action against money laundering by offering technical expertise, training and advice to member countries upon request.

2.3 The Financial Action Task Force (FATF)

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 34 countries and territories and two regional organizations.

2.3.1 FATF 40+9 Recommendations

FATF adopted a set of 40 recommendations to prevent money laundering. These Forty Recommendations constituted a comprehensive framework for AML and were designed for universal application by countries throughout the world. Although not binding as law upon a country, the Forty Recommendations was widely endorsed by the international community including World Bank and IMF and relevant organizations as the international standard for AML. The Forty Recommendations were initially issued in 1990 and revised in 1996 and 2003 to take account of new developments in money laundering and to reflect developing best practices internationally. To accomplish its expanded mission of combating financing of terrorism FATF adopted nine Special Recommendations in 2001.



2.3.2 FATF New Standards

FATF Plenary has again revised its recommendations in February 2012. The previous 40+9 Recommendations has been accumulated into 40 (forty) recommendations called the FATF Standards. Proliferation financing has been included in the new standards. There is no special recommendation to address the financing of terrorism. All special recommendations have been merged with the 40 recommendations. FATF is now working on the assessment process under the new standards. The following table shows the summary of new standards.

Summary of new FATF 40 standards is shown in the below table:

Group	Topic	Recommendations
1	AML/CFT Policies and Coordination <ul style="list-style-type: none"> • Assessing risks and applying a risk-based approach • National cooperation and coordination 	1-2
2	Money Laundering and Confiscation <ul style="list-style-type: none"> • Money laundering offences • Confiscation and provisional measures 	3-4
3	Terrorist Financing and Financing of Proliferation <ul style="list-style-type: none"> • Terrorist financing offences • Targeted financial sanctions related to terrorism and terrorist financing • Targeted financial sanctions related to proliferation • Non-profit organizations 	5-8
4	Financial and Non-Financial Institution Preventative Measures <ul style="list-style-type: none"> • Financial institution secrecy laws • Customer due diligence and recordkeeping • Additional measures for specific customers and activities • Reliance, controls and financial groups • Reporting of suspicious transactions • Designated non-financial businesses and professions 	9-23
5	Transparency and Beneficial Ownership of Legal Persons and Arrangements <ul style="list-style-type: none"> • Transparency and beneficial ownership of legal persons • Transparency and beneficial ownership of legal arrangements 	24-25
6	Powers and Responsibilities of Competent Authorities and Other Institutional Measures <ul style="list-style-type: none"> • Regulation and supervision • Operational and law enforcement • General requirements • Sanctions 	26-35

7	<p>International Cooperation</p> <ul style="list-style-type: none"> • International instruments • Mutual legal assistance • Mutual legal assistance regarding freezing and confiscation • Extradition • Other forms of international cooperation 	36-40
---	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

2.3.3 International Cooperation and Review Group (ICRG)

The FATF has set up the International Co-operation Review Group (ICRG) as a new process that is designed to notably engage those jurisdictions which are ‘unwilling’ and pose a real risk to the international financial system. The ICRG process is designed to bind members of FATF and FATF Style Regional Body (FSRB) that show effective commitment to the standards against those that evade their international obligations. The time and money that one jurisdiction spend on creating an effective system in that country is wasted if a neighbor remains a safe haven for criminals. The ICRG process is focused on specific threats and specific risk in specific countries. If needed, these jurisdictions may be publicly identified by the FATF Plenary.

The second role of the ICRG is to work with those jurisdictions to convalesce the shortcomings underpinning the judgment of the FATF Plenary. This means there could be a focused follow up process between the ICRG and a specific jurisdiction. If all evaluation reviews and regular follow ups are conducted properly, there should be no duplication or conflict within the FATF family and between the follow up processes.

2.4 Asia Pacific Group on Money Laundering (APG)

The Asia Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 41 members and a number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units. APG is the FATF style regional body (FSRB) for the Asia Pacific region.

APG members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations of the Financial Action Task Force on Money Laundering and Terrorist Financing.

The APG has five key roles:

- To assess compliance by APG members with the global standards through a robust mutual evaluation program;
- To coordinate bi-lateral and donor-agency technical assistance and training in the Asia/Pacific region in order to improve compliance by APG members with the global standards;

- To participate in, and co-operate with, the international anti-money laundering network - primarily with the FATF and with other regional anti-money laundering groups;
- To conduct research and analysis into money laundering and terrorist financing trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities; and
- To contribute to the global policy development of anti-money laundering and counter terrorism financing standards by active Associate Membership status in the FATF.

The APG also assists its members to establish coordinated domestic systems for reporting and investigating suspicious transaction reports and to develop effective capacities to investigate and prosecute money laundering and the financing of terrorism offences.

2.5 The Egmont Group of Financial Intelligence Units

In 1995, a number of governmental units of different countries commonly known as Financial Intelligence Units (FIUs) began working together and formed the Egmont Group of FIUs (Egmont Group), named after the location of its first meeting at the Egmont-Arenberg Palace in Brussels. The purpose of the group is to provide a forum for FIUs to improve support for each of their national AML programs and to coordinate AML initiatives. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs world-wide.

The mission of the Egmont Group has been expanded in 2004 to include specifically financial intelligence on terrorist financing. To be a member of the Egmont Group, a country's FIU must first meet the Egmont FIU definition, which is- 'a central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information:

- concerning suspected proceeds of crime and potential financing of terrorism, or
- Required by national regulation, in order to counter money laundering and terrorist financing.'

2.6 The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of 10 (ten) countries. Each country is represented by their central banks, or by the relevant authorities with formal responsibility for prudential supervision of banking where that authority is not the central bank. The committee has no formal international supervisory authority or force of law. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank/financial institution supervisory issues. These standards and guidelines are adopted with the expectation that the appropriate authorities within each country will take all necessary steps to implement them through detailed measures, statutory, regulatory or otherwise, that best suit that country's national system. Basel Committee has adopted 29 'Core Principles for Effective Banking Supervision' on September, 2012. Three of the Basel Committee's supervisory standards and guidelines related to AML & CFT issues.



Chapter: 3

National Initiatives on Money Laundering & Terrorist Financing

3.1 Introduction

In line with international efforts, Bangladesh has also taken many initiatives to prevent money laundering and combating financing of terrorism and proliferation of weapons of mass destructions considering their severe effects on the country.

3.2 Founding Member of APG

Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40 recommendations. Bangladesh has formally endorsed by the APG Membership out-of-session in September 2014 as the Co-Chair for 2018-2020.

3.3 Legal Framework

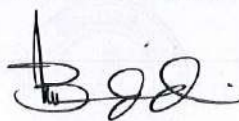
Bangladesh is the first country in the South Asia that has enacted Money Laundering Prevention Act (MLPA) in 2002. To address the shortcomings of the MLPA, 2002 and to meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER), Bangladesh has again enacted Money Laundering Prevention Act in February, 2012 repealing MLPA, 2009. Money Laundering Prevention Rules, 2013 has been framed for effective implementation of the act.

Bangladesh also enacted Anti-Terrorism Ordinance (ATO) in 2008 to combat terrorism and terrorist financing. Subsequently, ATO, 2008 has repealed by Anti-Terrorism Act (ATA), 2009 with the approval of the parliament. To address the gap identified in the Mutual Evaluation Report (MER) of Bangladesh that is adopted in 2009 by APG, some provisions of ATA 2009 have been amended in 2012 and 2013. Anti-Terrorism Rules, 2013 has also been promulgated to make the role and responsibilities of related agencies clear specially to provide specific guidance on the implementation procedure of the provisions of the UNSCRs.

Bangladesh has enacted Mutual Legal Assistance in Criminal Matters Act, 2012 to enhance international cooperation on ML & TF and other related offences. The Government also enacted Mutual Legal Assistance in Criminal Matters Rules, 2013 which mainly emphasize on the process of widest possible range of providing mutual legal assistance in relation to ML & TF and other associated offences.

3.4 Central and Regional Taskforces

The Government of Bangladesh has formed a Central and 7 (Seven) regional taskforces (Chittagong, Rajshahi, Bogra, Sylhet, Rangpur, Khulna and Barisal) on 27 January, 2002 to prevent illegal hundi activities, illicit flow of fund & money laundering in Bangladesh. Head of Bangladesh Financial Intelligence Unit (BFIU) is the convener of that committee. Both the task force's meeting is held bi-monthly. The meeting minutes of the regional task force are discussed in the central task force meeting. Besides high profile cases are discussed in the central task force meeting. The central



task force set out important decisions that are implemented through banks, financial institutions and Government agencies concerned.

3.5 Anti-Money Laundering Department

Anti-Money Laundering Department (AML/D) was established in Bangladesh Bank in June, 2002 which worked as the FIU of Bangladesh. It was the authority for receiving, analyzing and disseminating Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs).

3.6 Bangladesh Financial Intelligence Unit (BFIU)

As per the provision of MLPA, 2012 Bangladesh Financial Intelligence Unit (BFIU) has been established abolishing AML/D as a national central agency to receive, analyze and disseminate STRs/SARs, CTRs and complaints. BFIU has been entrusted with the responsibility of exchanging information related to ML & TF with its foreign counterparts. The main objective of BFIU is to establish an effective system for prevention of money laundering, combating financing of terrorism and proliferation of weapons of mass destruction and it has been bestowed with operational independence. BFIU has also achieved the membership of Egmont Group in July, 2013.

BFIU has continued its effort to develop its IT infrastructure which is necessary for efficient and effective functioning of the unit. In this regard, it has procured goAML software for online reporting and software based analysis of CTRs and STRs. It also has established MIS to preserve and update all the information and to generate necessary reports using the MIS.

3.7 National Coordination Committee and Working Committee

To provide guidance for effective implementation of AML & CFT regime, a National Coordination Committee headed by the Honorable Finance Minister and a Working Committee headed by the Secretary of Bank and Financial Institutions Division of Ministry of Finance were formed consisting representatives from all concerned Ministries, Agencies and regulatory authorities.

3.8 National ML & TF Risk Assessment (NRA)

Bangladesh first conducted National ML & TF Risk Assessment (NRA) in 2011-2012. The methodology used for NRA was developed by Anti-Corruption Commission (ACC), BFIU and Criminal Investigation Department (CID) of Bangladesh Police consulting with Strategic Implementation Plan (SIP) of World Bank. The report was prepared by using the last 10 years statistics from relevant agencies and identified the vulnerabilities of sectors, limitations of legal framework and weaknesses of the institutions on ML & TF.

Second NRA has been conducted by a 'Core Committee' comprises of ACC, BFIU and CID of Bangladesh Police and another 'Working Committee' comprises of 23 members. This report considers the output of institutional, sectoral, geographical risk assessment. It covers all the sectors of the economy, legal and institutional framework. The report identifies some high risk areas for Bangladesh that are corruption, fraud-forgery, drug trafficking, gold smuggling and human trafficking. Banks, non-banks financial institutions, real estate developers and jewelers were identified as most vulnerable sectors for ML & TF. The foreign donation receiving NGO/NPO working in the coastal or border area were identified as vulnerable for TF incidence.

3.9 National Strategy for Preventing ML and TF

National Strategy for Preventing Money Laundering and Combating Financing of Terrorism, 2011-2013 was adopted by the NCC in April 2011. Bangladesh has completed all the action items under the 12(twelve) strategies during that time. A high level committee headed by the Head of BFIU has formulated the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2015-2017 which has been approved by the National Coordination Committee (NCC) on ML/TF. The strategy identifies the particular action plan for all the Ministries, Division and Agency to develop an effective AML/CFT system in Bangladesh. The strategy consists of following 11 (eleven) strategies against 11 (eleven) strategic objectives:

- Updating National ML & TF Risk Assessment Report regularly and introducing Risk Based Approach of monitoring and supervision of all reporting organizations.
- Deterring corruption induced money laundering considering corruption as a high risk.
- Modernization of Border Control Mechanism and depriving perpetrators from use of proceeds of crime to prevent smuggling of gold and drugs, human trafficking, other transnational organized crimes considering the risk thereon.
- Tackling illicit financial flows (IFF) by preventing the creation of proceeds of crime, curbing domestic and cross-border tax evasion and addressing trade based money laundering.
- Discouraging illicit fund transfer by increasing pace of stolen assets recovery initiatives and or recovering the evaded tax.
- Enhancing the capacity of BFIU in identifying and analyzing emerging ML & TF cases including ML&TF risks arising from the use of new technologies.
- Enhancing compliance of all reporting agencies with special focus on new reporting agencies like NGOs/NPOs and DNFbps.
- Expanding investigative capacity and improving the quality of investigation and prosecution of ML & TF cases to deter the criminals.
- Establishing identification and tracking out mechanism of TF & PF and fully implementation of targeted financial sanctions related to TF & PF effectively.
- Boosting national and international coordination both at policy and operational levels.
- Developing a transparent, accountable and inclusive financial system in Bangladesh.

3.10 Chief Anti-Money Laundering Compliance Officers (CAMLCO) Conference

Separate annual conferences for the Chief Anti-Money Laundering Compliance Officers (CAMLCO) of Banks, Financial Institutions, Insurance Companies and Capital Market Intermediaries were arranged by BFIU. It also has arranged a number of training programs, workshops, seminars and road-shows to create awareness among the staff of reporting organizations, regulatory authorities about related issues.

3.11 Egmont Group Memberships

BFIU has achieved the membership of Egmont group in the Egmont plenary on July, 2013 in Sun City, South Africa. Through Egmont membership, BFIU has achieved access to a wider global platform and this will help to establish relationship with other FIUs of different countries to

get benefit by exchanging views, experiences and information via Egmont Secure Web.

3.12 Anti Militants and De-Radicalization Committee

The Government of Bangladesh is very much vigilant against terrorism and violent extremism. An inter-ministerial committee headed by Minister of Home is working actively to prevent and redress of terrorism, to fight against terrorist and the terrorist organizations in a more coordinated way. The committee comprised of high officials from different ministries, law enforcement and intelligence agencies. The committee tried to find out more sensitive and sophisticated ways to create awareness among the general people about the negative impact of terrorism.

3.13 Memorandum of Understanding (MOU) Between ACC and BFIU

Anti-Corruption Commission (ACC) and the Bangladesh Financial Intelligence Unit (BFIU) has signed a Memorandum of Understanding (MoU) on 4 May, 2014 with a view to increasing the scope of cooperation for dealing with money laundering and other financial crimes. The ACC and the BFIU have jointly undertaken various initiatives to fight against money laundering and other financial crimes.

3.14 Implementation of TFS

UN Security Council Resolutions related to TF adopted under Chapter VII of the Charter of UN are mandatory for all jurisdictions including Bangladesh. Bangladesh has issued Statutory Regulatory Order (SRO) No. 398/2012 on 29 November 2012, which was amended and strengthened by SRO No. 188/2013 dated 18 June 2013 under the United Nations (Security Council) Act, 1948. Before the issuance of those SROs, BFIU was used to issue circular letters as a medium of instructions for the reporting organization to implement the requirements of UNSCRs on regular basis.

In addition to the SROs the UNSCRs requirements were also incorporated in the ATA, 2009. Section 20(A) of ATA, 2009 provides that the Government of Bangladesh has power of taking measures for the purposes of implementing United Nations Security Council Resolution No. 1267 and its successor resolutions and United Nations Security Council Resolution No. 1373 and United Nations Security Council resolutions related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing

3.15 Coordinated Effort on the Implementation of the UNSCR

A national committee is coordinating and monitoring the effective implementation of the United Nations Security Council Resolutions (UNSCR) relating to terrorism, terrorist financing and financing of proliferation of weapons of mass destruction. The committee is headed by the Foreign Secretary and comprises of representatives from Ministry of Home Affairs; Bank and Financial Institutions Division, Ministry of Finance; Legislative and Parliamentary Affairs Division, Ministry of Law, Justice and Parliamentary Affairs and Bangladesh Bank.

Chapter: 4

Legal Requirement & Penalties

4.1 Requirements under the Money Laundering Prevention Act, 2012 and (Amendment - 2015)

4.1.1 The legislation specifically relating to money laundering is contained in the Money Laundering Prevention Act, 2012 (Amendment - 2015) the provisions of which supersedes whatever may contain in any other Act in force in Bangladesh. So far as financial service providers are concerned, the Act:

- 4.1.1-a) defines the circumstances, which constitute the offence of money laundering and provides penalties and punishments for the commission of the offence (See Section 4 of the Act),
- 4.1.1-b) requires banks, financial institutions and other institutions engaged in financial activities to establish the identity of their customers (See Section 19 Ka of the Act),
- 4.1.1.-c) requires banks, financial institutions and other institutions engaged in financial activities to retain correct and full information used to identify their customers and transaction records at least for five years after termination of relationships with the customers (See Section 19 Ka of the Act), and
- 4.1.1.-d) imposes an obligation on banks, financial institutions and other institutions engaged in financial activities and their employees to make a report to the Bangladesh Financial Intelligence Unit where:
- 4.1.1.-e) they suspect that a money laundering offence has been or is being committed (See Section 19 Ga of the Act) and;
- 4.1.1.-f) provide customer identification and transaction records to Bangladesh Financial Intelligence Unit from time to time on demand (See Section 19 Kha of the Act).

4.2. Establishment of Bangladesh Financial Intelligence Unit (BFIU)

4.2.1. In order to exercise the power and perform the duties vested in Bangladesh Financial Intelligence Unit under section 24 of this Act, there shall be a separate unit to be called the Bangladesh Financial Intelligence Unit (BFIU).

4.2.2. For the purposes of this Act, the governmental, semi-governmental, autonomous organizations or any other relevant institutions or organizations shall, upon any request or spontaneously, provide the Bangladesh Financial Intelligence Unit with the information preserved or gathered by them. Money laundering Prevention Act the Bangladesh Financial Intelligence Unit may, if necessary, spontaneously provide other law enforcement agencies with the information relating to money laundering and terrorist financing.

4.2.3. The Bangladesh Financial Intelligence Unit shall provide with information relating to money laundering or terrorist financing or any suspicious transactions to the Financial Intelligence Unit of another country on the basis of any contract or agreement entered into with that country under the provisions of this Act and may ask for any such information from any other country.

4.2.4. The Bangladesh Financial Intelligence Unit may also provide with such information to the Financial Intelligence Units of other countries spontaneously where there is no such contract or agreement under sub-section (4).

4.3. Responsibilities of Bangladesh Financial Intelligence Unit

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

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

4.4 Investigation, Prosecution etc.

Under this Act:

- The offences under this act considered as the scheduled offences of Anti-Corruption Commission Act, 2004 (Act V of 2004), will be investigated by Anti-Corruption Commission or by an Officer empowered by Anti-Corruption Commission for this purpose.
- The Offences will be prosecuted by the Special Judge court as appointed under Criminal Law Amendment Act. 1958 (Act XL of 1958).

- If any conflict arises regarding investigation, prosecution and other related provisions, etc. of this Act, the provision of Anti-Corruption Commission Act, 2004 and Criminal Law Amendment Act. 1958 shall prevail.

4.5 Offence Committed by Company:

1. If any offence under this Act committed by a company, every proprietor, director, manager, secretary, or other Officer or representative who is directly involved with the offence shall be deemed to be guilty of such offence: Provided that if any person as aforesaid is not able to prove that such offence has been committed without his knowledge or he has used due diligence to prevent such offence, Explanation: In this section –

- (a) “Company” means any statutory body, partnership concern, association, commercial organization or organization formed with one or more than one person;
- (b) “Director” means any partner or member of the Board of Directors, by whatever name it is called.

2. Registration of any company, if found engaged in money laundering activity either directly or indirectly, shall be liable to be cancelled.

4.6 Protection against Proceedings Undertaken in Good Faith

No suit, prosecution either civil or criminal or other legal proceedings shall lie against government or any government officials or any reporting organizations if any person is affected or likely to be affected due to the proceedings done in good faith under this Act.

4.7 Responsibility of reporting organization in preventing money laundering:

1. For the purpose of preventing and identifying money laundering reporting organizations shall:

- keep, during the operation of accounts, the correct and full information of identification of its clients and
- In case of closed account of any client, keep previous records of transactions of such account for at least five years from the date of closure.
- Provide, from time to time, the records kept under clause (a) and (b) to Bangladesh Bank time to time on demand from Bangladesh Bank.
- Inform proactively and immediately Bangladesh Bank, facts on suspicious/unusual / doubtful or transactions likely to be related to money laundering.

2. If any reporting organizations violate the directions mentioned in sub-section (1) Bangladesh Bank shall take the following actions:

- Bangladesh Bank may impose a fine of not less than Taka ten thousand and such fine may extend to Taka five Lac upon the defaulting reporting organizations.
- Bangladesh Bank may cancel the registration of the company or cancel the license in addition to the fine mentioned in sub-section (a) .The Bangladesh Bank shall inform the permit or license authority of the reporting organizations regarding their failure to keep and furnish information under sub-section (1) so that the concerned authority may, in accordance with the relevant law or rule or regulation framed there under, take necessary action against the concerned reporting organizations for their failure or negligence.

3. Bangladesh Bank will collect the penalty money imposed under subsection (2) in its self-determined manner and shall deposit the collected money into the government treasury.

4.8 Terrorist financing: Requirements under the MLPA, 2012 (amendment 2015) and ATA (amendment 2012 & 2013)

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

Defines the circumstances, which constitute the offence of money laundering and terrorist financing and also provides penalties for commission of such offences;

Requires financial institutions including Banks engaged in financial services to establish the identity of their customers;

Requires financial institutions including Banks to retain correct and full information used to identify their customers and transaction records at least for five years after termination of relationships with the customers; and

Imposes an obligation on financial institutions including Banks and their employees to make a report to the Bangladesh Financial Intelligence Unit (BFIU), where:

They suspect that a money laundering offence or terrorist financing offence has been or is being committed; and

Provide customer identification and transaction records when BFIU asked for from time to time.

4.9 The Offence of Terrorist financing

The terrorist financing offences are, in summary:

- 4.9.1 It is an offence for any person or entity knowingly supply or express intension to supply or knowingly receives or knowingly arrangement for collecting money, service, material support or any other properties or knowingly instigate to supply money, services, material support or other properties, where there is a reasonable grounds to believe that the whole or partial amount have been used or may be used by any means by any terrorist or terrorist groups.
- 4.9.2 It is an offence for any person or entity who claims membership of any proscribes organization or individual under this act.
- 4.9.3 It is also an offence for any individual or entity to provide assistance to a criminal or support the criminal organization or provide shelter to the criminal or aiding or abetting such activities.
- 4.9.4 It is an offence for banks not to retain identification and transaction records of their customers.
- 4.9.5 It is an offence for banks not to report the knowledge or suspicion of terrorist financing to BFIU as soon as it is reasonably practicable after the information came to light.

4.10 Offence of Money Laundering and Punishment:

Punishment against accused Reporting Organization as per provision of MLP Act, 2012

Clause no.	Nature of offense	Punishment
23.3	Failing to submit required information within stipulated time	a) Penalty of Tk. 10,000/= per day up to maximum Tk. 5.00 lac, b) If such penalty is imposed more than 3 times in a financial year, license of the concern Branch/Booth/Agent can cancelled.
23.4	Furnishing false statements	a) Penalty of minimum Tk. 20,000/= and maximum Tk. 5.00 lac, b) If such penalty is imposed more than 3 times in a financial year, license of the concern Branch/Booth/Agent can cancelled.
23.5	Failing to company with any instruction given by BFIU under the act	a) Penalty of minimum Tk. 10,000/= and maximum Tk. 5.00 lac for particular non-compliance issue, b) If such penalty is imposed more than 3 times in a financial year, license of the concern Branch/Booth/Agent can cancelled.
23.6	Failing to company with the instruction of section 23(1) (Ga) regarding Account Freezing or Suspend order by Bangladesh Bank	Minimum Penalty of that Account Balance which will not more than double of balance as per instruction circulation date

23.7	Failing to pay the penalty as per section 23 & 25 of MLPA, 2012	Realize the amount by debiting self-named account of related person/entity/reporting agency with any Bank/Financial Institution/Bangladesh Bank and if any amount remains unpaid, suit will be filed for recovery of the same by the order of Court.
23.8	Penalty have been imposed to owner, Director and employees under payroll or contract service of any reporting agency for noncompliance of AML & CFT instruction	Individual penalty of minimum Tk. 10,000/= and maximum Tk. 5.00 lac along with administrative disciplinary action.
25.2	Any reporting organization failed to discharge their responsibility as per Article 25 (1) of the MPL Act, 2012 like preserving customers proper and full information, record keeping for closed A/C for keeping 5 (five) years, failure of submission return/sending STR to Bangladesh Bank.	a) Penalty of minimum Tk. 50,000/= and maximum Tk. 25.00 lac. b) Additionally, license will be cancelled of that organization or branch, service center, booth of that organization.

Punishment against Accused person or Entity as per provision of MPL Act, 2012

clause no.	Nature of offense	Punishment
4.2	Attempt, assist and make conspiracy for Money Laundering by any person.	Minimum 4 years and maximum 12 years of imprisonment with seizure of double the property acquired through ML or Tk. 10 (ten) lac which one is higher. Additionally, Court can order to forfeit the property acquired through ML or Predicate Offences to the person
4.4	Attempt, assist and make conspiracy by any entity.	Penalty of double the value of property acquired or Tk. 20 (Twenty) lac which one is higher with cancellation of registration /approval.
5	Defying attachment order for moveable properties.	Imprisonment up to 3 years or penalty to the value of attached property/properties or both.
6.3	Disclosure of information	Imprisonment up to 2 years or penalty of maximum Tk. 50,000/= or both.
7.3	Obstructing or non-cooperating in enquiry process.	Imprisonment up to 1 years or penalty of maximum Tk. 25,000/= or both.
8.2	Providing false statements.	Imprisonment up to 3 years or penalty of maximum Tk. 50,000/= or both.

Note: If any Company, Partnership Firm, Society, or Association violates any provisions of the Act, it will be deemed that every owner, partner, directors, employees and officers have individually violated such provisions. (Section 27of the Act.)

Chapter: 5

AML / CFT Policies and procedures of Community Bank Bangladesh Limited

5.1 Institutional Policy

In order to protect Banks reputation and to meet its legal and regulatory obligations, it is essential that Bank should minimize the risk of being used by Money Launderers. With that end in view it will be an obligatory responsibility for all Bank Official, customers and management of the Bank to realize and combat the situation on this critical risk issue:

- Establish clear lines of internal accountability, responsibility and reporting. Primary responsibility for the prevention of money laundering rests with the nature of business which must ensure that appropriate internal controls are in place and operating effectively and that bank Officials are adequately trained. The business is supported in meeting this responsibility by the Legal and Compliance function and by Bank Investigations.
- Given its importance in reputational and regulatory terms, the effectiveness of the money laundering prevention regime across all businesses should form part of the governance oversight responsibilities of all branch managers.
- Document, implement and maintain, procedures and controls which interpret Bank Policy and Bank Standards for each business in the context of applicable laws and regulations and corporate ethical standards. Compliance with such procedures and controls and with Bank Policy and Bank Standards will be effectively monitored.
- Establish an effective “Know Your Customer” Policy for the Bank which will contain a clear statement of management’s overall expectation matching local regulations and establishing specific line of responsibilities.
- Co-operate with any lawful request for information made by government agencies during their investigations into money laundering.
- Support governments, law enforcement agencies and Bangladesh Bank in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal purposes.
- Report money laundering issues to Head Office Management on a regular basis. The Branch Manager responsible to combat Money Laundering shall determine and communicate the content, format and frequency for management reporting.

5.2 Senior Management Commitment

The most important element of a successful anti-money-laundering program is the commitment of senior management, including the Managing Director & Chief Executive Officer and the Board of Directors, to the development and enforcement of the anti-money-laundering objectives which can deter criminals from using their facilities for money laundering, thus ensuring that they comply with their obligations under the law. Senior management must send the signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of its anti-money laundering policy the Community Bank Bangladesh will communicate clearly to all employees on an annual basis a statement from the Chief Executive Officer that clearly sets forth its policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement should evidence the strong commitment of the Community Bank Bangladesh and its Senior Management to comply with all laws and regulations designed to combat money laundering. The statement of compliance policy is:

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

5.3 Statement of Commitment of Managing Director & CEO

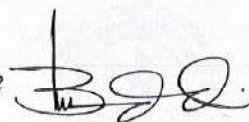
As per the instruction of Clause-1.2 of BFIU Circular No. 26 dated June 16, 2020, MD & CEO of Community Bank Bangladesh Limited (CBBL) ensures his commitment on AML & CFT issues mentioning the role and responsibilities of employees of the Bank and advice the direction to implement the commitment in every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

- Bank's policy or strategy to prevent ML, TF & PF;
- Emphasize on effective implementation of bank's AML & CFT compliance program;
- Clear indication of balance between business and compliance, risk and mitigating measures;
- Compliance is the responsibility of each employee during their normal course of assignment and ignorance shall not be considered as the excuse for non-compliance;

- Point of contact for clarification in case of any ambiguity arise;
- Consequences of non-compliance as per human resources (HR) policy of the bank.

5.4 Disclaimer

This Guideline is intended to provide general advice to the employees of Community Bank Bangladesh. It should never be relied on as a substitute for Money Laundering Prevention (MLP) Act 2012 (as amended in 2015) and Anti-Terrorism Act (ATA), 2009 (as amended in 2012 & 2013), guideline & circulars issued by Bangladesh Financial Intelligence Unit (BFIU).



Chapter: 6

Compliance Structure of the Bank

6.1 Central Compliance Committee (CCC)

6.1.1 Formation of CCC

To keep the banking sector free from the risks related to Money Laundering & Terrorist Financing and for the effective/proper compliance of all existing acts, rules and instructions issued by BFIU time to time, Community Bank Bangladesh Limited (CBBL) set up a Central Compliance Committee (CCC) under the chairmanship of Chief Anti Money Laundering Compliance Officer (CAMLCO) and includes the following Department/Division Heads and other related desk officials of Corporate Head Office:

Sl. No.	List of CCC Members	Position
1.	Chief Anti Money Laundering Compliance Officer (CAMLCO)	Chairman
2.	Head of AML & CFT Division & DCAMLCO	Member Secretary
3.	Deputy Managing Director & CBO	Member
4.	Head of IT Division	Member
5.	Head of Risk Management Division	Member
6.	Head of Operations	Member
7.	Head of CAD	Member
8.	Head of CRM	Member
9.	Chief Marketing Officer	Member
10.	Head of Core Banking System	Member
11.	Head of Cards	Member
12.	Deputy Head of CAD	Member
13.	Manager, Trade Operations	Member
14.	Head of Human Resource Division	Member
15.	Corresponding Banking & Trade Operations	Member
16.	Officials of AML & CFT Dept.	Member

6.1.2 Responsibilities and Authorities of the CCC

Responsibilities:

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

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

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

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

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

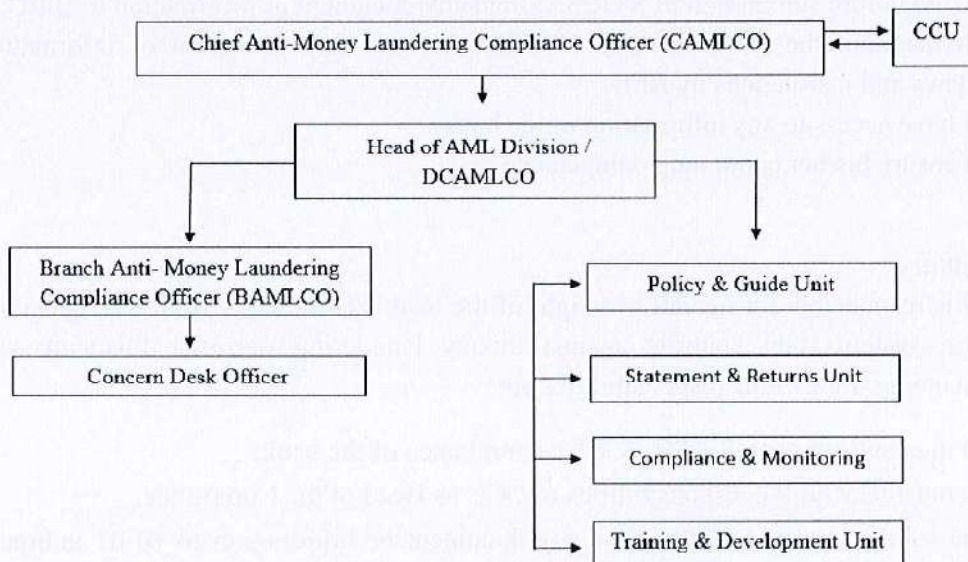
- appointment of BAMLCO and assign their specific job responsibilities;
- requisition of human resources and logistic supports for CCC and for AML & CFT Division;
- make suggestion or administrative sanction for non-compliance by the employees;

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

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

6.2 Formation of AML & CFT Division

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



6.3 Appointment of CAMLCO

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

6.3.1 Authorities and Responsibilities of CAMLCO

6.3.1.1 Authorities

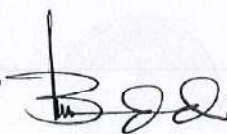
CAMLCO must have sufficient authority to implement and enforce AML & CFT policies, procedures and measures. The authorities must include at least the followings:

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

6.3.1.2 Responsibilities

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

- CAMLCO must ensure overall AML & CFT compliance of the bank;
- CAMLCO must take all the responsibilities of CCC as Head of the Committee.
- oversee the submission of STR/SAR or any document or information to BFIU in time;
- maintain the day-to-day operation of the bank's AML & CFT compliance;
- CAMLCO will inform to Managing Director & CEO for proper functioning of CCC;
- CAMLCO shall review and update ML & TF risk assessment & management policy of the bank;
- Confirm the preparation of Half-Yearly Self-Assessment Report and send to BFIU within the time frame.




- corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.
- He/she shall oversee all other issues that may arise from time to time regarding ML, TF & PF.

6.4 Appointment of DCAMLCO

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

6.4.1 Authorities & Responsibilities of DCAMLCO

- The authorities & responsibilities of CAMLCO shall be same as the authorities & responsibilities of CAMLCO but his/her authorities and responsibilities under command, control & supervision of CAMLCO;
- D-CAMLCO shall exercise the authorities of the CCC as Head of AML & CFT Division;
- D-CAMLCO shall work as a member secretary of Central Compliance Committee (CCC);
- Analyzing and evaluating the self-assessment report and making recommendations;
- Analyzing and evaluating the independent testing procedure and making recommendations;
- Analyzing and evaluating the STRs for sufficiency of data & documents;

- Ensure the CDD & EDD measure for PEPs, IPs, chief executive of international organizations, Non face to face customers and other high risk customers; and monitoring the transactions of such accounts;
- Conducting inspection in the branch and/or subsidiaries, and preparing report there against for transaction of such accounts;
- Designing , imparting & evaluating training, workshops and seminar related to AML 7 CFT for the employee of the bank;
- Ensuring the timely submission of required report to BFIU;
- ensuring the all record keeping requirements in-favor of CCC related to AML/CFT issues;
- Moreover, he/she will be act as current charge in absence of CAMLCO.

6.5 Branch Anti Money Laundering Compliance Officer (BAMLCO)

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

In absence of BAMLCO, Branch management in consultation with AML & CFT Division will nominate another officials to ensure his job responsibilities and mitigate the AML & CFT matters. Branch will also inform to AML & CFT Division immediately regarding transfer of BAMLCO.

6.5.1 Responsibilities and Authorities of BAMLCO

6.5.1.1 Responsibilities

BAMLCO will perform the following responsibilities:

Knowledge on AML & CFT issues

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

Branch Compliance Program

- Implement all instructions of AML & CFT Division/CCC regarding AML & CFT issues time

to time.

Sanctions Screening

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

Customer Due Diligence

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

Enhance Due Diligence (EDD)

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

Transaction Monitoring

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

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

Update Customer Information and TP & KYC

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

Arrangement of AML & CFT Meeting

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

Report Submission to AML & CFT Division

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

STR/SAR Identification and Reporting

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

Record Keeping

- Keep records of customer's identification and transactions at least five years after the termination of relationships with the customers.
- Ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements.
- Ensure confidentiality of the records preserved.
- Ensure AML & CFT related files are available in the branch level and update those files on regular basis.

Training of employees

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

Others responsibilities

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

6.5.1.2 Authorities

For shouldering these responsibilities, Community Bank Bangladesh Limited (CBBL) will consider to give the following authority to BAMLCO:

- Generally, BAMLCO will report to Head of Branch/AML & CFT Division regarding all the matters of AML & CFT.
- BAMLCO can independently send STR/SAR to AML & CFT Division, if needed without consultation to Head of Branch.
- BAMLCO can act independently for ensure compliance regarding AML & CFT issues.

Branch management can appoint BAMLO (if necessary) to help the BAMLCO for smooth operation of the above mentioned responsibilities with the permission of AML & CFT Division.

6.6 Department/Division AML Compliance Officer

To monitor the AML & CFT compliance issues departments/divisions like Trade Operations, CRM, CAD, FI, Agent Banking, FRD, Card Division, and other Corporate Head Office Department/Division may appoint Department/Division AML Compliance Officer and inform to AML & CFT Division. If any non-compliant issues raise at their end then Department AML Compliance Officer must inform to AML & CFT Division for taking the necessary steps.

6.7 Roles & Responsibilities of Account Opening Officer/Branch Operation Manager/ Relationship Manager

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

6.8 Role & Responsibilities of Internal Control & Compliance Division

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

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

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

The Internal Control & Compliance Division must-

- Understand ML & TF risk of the bank and check the adequacy of the mitigating measures;
- Examine the overall integrity and effectiveness of the AML & CFT Compliance Program;
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;

- Determine personnel adherence to the bank’s AML & CFT Compliance Program;
- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- Assess the adequacy of the bank’s processes for identifying and reporting suspicious activity;
- Communicate the findings to the board and/or senior management in a timely manner;
- Recommend corrective action to address the identified deficiencies;
- Track previously identified deficiencies and ensures correction made by the concerned person;
- Examine that corrective actions have taken on deficiency identified by the BFIU or BB;
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- Determine when assessing the training program and materials:
 - Employee accountability for ensuring AML & CFT compliance,
 - Comprehensiveness of training, in view of specific risks of individual business lines,
 - Training of personnel from all applicable areas of the bank,
 - Frequency of training,
 - Coverage of bank policies, procedures, processes and new rules and regulations,
 - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
 - Penalties for noncompliance and regulatory requirements.

6.9 Responsibilities of Internal Control & Compliance Division on Self-Assessment & Independent Testing Procedures

As per the clause no. 8.2 of BFIU circular no. 26, the Internal Control & Compliance Division shall assess the branch evaluation “Self-Assessment Procedure” received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the AML & CFT Division.

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

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

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

6.10 External Auditor

External auditor of Community Bank Bangladesh Limited shall 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 will report incidences of suspected criminal activity uncovered during audits in its audit report.

Chapter: 7

Customer Acceptance Policy

Money Laundering is the generic term use to describe the process by which criminals disguise the original ownership and control of the process by criminal conduct by making such proceeds appear to have derive from a legitimate source. The processes by which criminally derived property may be laundering are extensive. Though criminal money may be successfully laundering without the assistance of the financial sector, the reality is that all over the world hundreds of billions of US dollars of criminal derived money is laundering through banks and financial institutions annually.

Customer are they key to operation of banking business. They are importance parts of survival and success as a whole for the bank. But it is equally important to keep in mind that sometimes criminals enter to banks as customers and pose the risk of money laundering and terrorist financing to the banks.

In our country, commercial banks do not open accounts or deal with customer of unknown identity or have fictitious or imaginary names. Bank will accept only those clients whose identity is established by conducting due diligence appropriate to the risk profile of the client.

As per regulatory requirement every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place to set-up any kind of business relationship with the customer. A concrete Customer Acceptance Policy is very important so that inadequate understanding of a customer's background and propose can be utilized by a bank to a number of risks.

7.1 Objective and Application of the policy:

The primary objective of the policy is to prevent our bank from being used, internationally or unintentionally by illegal or criminal elements for money laundering or terrorist financing activities. Policies are appended as under:

- i) To lay down explicit criteria for acceptance of customer and employee.
- ii) To enable the bank to know/understand the customer and their financial dealings better which would help the bank to manage legal and reputational risk of the bank as well as Money Laundering risk.
- iii) To put in place appreciate controls for detection and reporting of suspicious activities in accordance with applicable laws or laid down procedures.
- iv) To established procedures to verify the bona-fide identification if individual/non individual for opening o accounts.
- v) To ensure that the concerned staffs are adequately trained in KYC, AML & CFT procedures.

- vi) To prevent the Bank from being used, internationally or unintentionally, for ML/TF propose; and
- vii) To identify customers who are likely to pose a higher risk

This policy is applicable to all domestic/foreign Branches /offices/subsidiaries of the Bank and is to be read in conjunction with related operational guidelines issued from time to time by our bank or Bangladesh Bank.

Bank were advised by central of follow detailed and accurate customer identification procedure for opening of accounts and monitoring transaction of a suspicious nature for propose or reporting it to the appropriate authority transaction. This 'know Your Customer' guidelines/'Customer Acceptance policy' has been repeated/revisited in the context of the Recommendations made by the financial Action Task Force (FATF) on Anti-Money Laundering (AML) Standards and on Combating Financing of Terrorism (CFT). Detailed guidelines have been issued based on the Recommendations of the FATF and BFIU indicative suggestions wherever considered necessary. Bank have been advice to ensure that a proper policy framework on 'Know You Customer' and Anti Money Laundering measure with the approval of the Board is formulated and put in place.

7.2 Definition of customer

A 'customer' is defined as:

- A person or entity that maintains as account and/or has a business relationship
- One on whose behalf the account is maintained (i.e. the beneficial owner). Beneficial owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and
- Beneficiaries of transaction conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, etc. as permitted under the law, and
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank say, a wire transfer or issue of a high value demand draft a single transaction.

For the purpose of KYC procedure a 'Customer' is defined in BFIU Circular No. 26 dated 16 June, 2020 as:

- 1) Any person or entity maintaining an account or a business relationship of any type with a bank or financial institution;
- 2) The person or entity as true beneficial owner whose favor directly or indirectly the account is operated;
- 3) Any account holder, the trustee, intermediary or beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc.) under the existing legal infrastructure;

- 4) Any person or institution involved in a high value single transaction conducted in a single occasional Transaction or any person/institution involved in a financial transaction that may pose reputational and other risk to the institution; and
- 5) The person or entity as defined by BUFIU from time to time.

7.3 Customer Acceptance Criteria

Community Bank Bangladesh Limited has been developing clear customer acceptance policy and procedures laying down explicit criteria for acceptance of customer including a description of the types of customer that are like to pose a higher than average risk to a financial institution. In preparing such policies the following important factor are required to be taken into consideration;

- i) Customer's background,
- ii) Country to origin,
- iii) Public or high profile position,
- iv) Linked accounts,
- v) Business activities of customers
- vi) Basic requirement for account opening
- vii) Other risk indicators

It is important that customer acceptance policy is not so restrictive that it result in a denial or access by the general public to financial services, especially for people whom who are financially or socially disadvantages. On the other hand, extending due diligence would be essential for an individual with a high net worth whose source of fund is unclear. Decision to enter into business relationships with higher risk customers, such as public figures or politically exposed person (PEPs) should be taken exclusively at senior management level.

7.4 Customer Acceptance Policy

The following Customer Acceptance Policy indicating the criteria for acceptance of customer shall be followed in the Bank. The branches shall accept customer strictly in accordance with the said policy:

- 1) No account should be opened in anonymous or fictitious name. Branch will collect full & accurate name of clients, prepare proper KYC and preserve documents in conformity with it.
- 2) Permanent of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categories customer into different risk grade. Branch will be accept only those customers whose appreciate identity is established by conducting due diligence to the risk profile of the client;
- 3) Documentation requirement and other information to be collected in respects of different categories of customers depending on perceived risk.
- 4) Not to open an account or close an account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/or obtain

documents required as per risk categories due to non-cooperation of the customer or non-reliability of the data and information furnished to the Bank. Decision to close an account should be taken at a reasonably higher level after giving due notice to the customer explaining the reason for such a decision;

- 5) No account in the name of any person or entity listed United Nations Security Council Resolution (UNSCRs) or their close alliance adopted under chapter VII of the Charter of UN on suspicions of involvement in terrorism or terrorist financing activities and prescribed or enlisted by Bangladesh Government shall be opened or operated;
- 6) No numbered account shall opened;
- 7) No banking relationship shall be established with a shell bank or a shell Company;
- 8) No account shall be opened for person/entities about whom information is available through reliable sources indicating involvement in criminal conduct;
- 9) Circumstance, in which a customer is permitted to act on behalf of another person or entity, should be clearly spelt out in conformity with the established law and practice of financial service as there could be occasions when an account is operated by a mandate holder or where an account it opened by an intermediary in fiduciary capacity;
- 10) Necessary check before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organization etc.;
- 11) The status of customer may change as relation with a customer progresses. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measure to monitor customer's activities throughout the business relation, i.e. review KYC within 1 year for high risk customer and 5 years for low risk customer.

Chapter: 8

AML & CFT Risk Assessment and Risk Management Process of CBBL

8.1 Risk Based Approach

Community Bank Bangladesh Limited has developed Money Laundering and Terrorist Financing Risk Assessment and Risk Management Guidelines 'for identifying, assessing and mitigating ML & TF risks that the bank may encounter in doing its businesses. The guideline outlines the detail process to assess ML & TF risks under business risk considering customers, products, delivery channels and geographical positions. The guideline also include assessment of regulatory risk i.e. risk arises from non-compliance of AML & CFT measures.

This guideline will assist in identifying the bank's AML/CFT risk profile. Understanding the risk profile enables the bank to apply appropriate risk management process to the AML/CFT compliance program to mitigate risk. The risk assessment process enables management to better identify and mitigate gaps in bank's control.

The purpose of this guideline is to:

- provide general information about risks related with the products, services, delivery channels, and geographical locations;
- assist banks to assess their ML & TF risks efficiently;
- enable banks in implementing an AML & CFT program appropriate to their business having regard to the business size, nature and complexity; and
- Provide a broad risk management framework based on high-level principles and procedures that a bank may wish to consider when developing and implementing a risk-based approach to identify, mitigate and manage ML&TF risks.

8.2 Risk Management Framework

The risk management framework consists of:

- Establishing the internal and external context within which the designated service is, or is to be, provided.
- Risk identification;
- Risk assessment or evaluation; and
- Risk treatment (mitigating, managing, control, monitoring and periodic reviews).

8.3 Risk identification

There are two types of risk: business risk and regulatory risk.

Business Risks:

Bank must consider the risk posed by any element or any combination of the elements listed below:

- Customers
- Products and services
- Business practices/delivery methods or channels
- Countries it does business in/with (jurisdictions).

Regulatory risks:

This risk is associated with not meeting the requirements of the Money Laundering Prevention Act - 2012 (including all amendments-2015), Anti-Terrorism Act - 2009 (including all amendments-2012 & 2013), and instructions issued by BFIU. Examples of some of these risks are:

- Customer/beneficial owner identification and verification not done properly
- Failure to keep records properly
- Failure to scrutinize staffs/members properly before appointed
- Failure to train staff adequately
- Not having an AML&CFT program
- Failure to report suspicious transactions or activities
- Non submission of required report to BFIU regularly
- Not having an AML&CFT Compliance Officer
- Failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, IPs)
- Not complying with any order for freezing or suspension of transaction issued by BFIU or BB
- Non submission accurate information or statement requested by BFIU or BB.

8.4 Risk assessment

For assessing risk, we use **Annexure-A**, which is a simple & generic table with Risk Score and Treatment. Each risk element can be rated by:

- The chance of the risk happening—‘**likelihood**’
- The amount of loss or damage if the risk happened —‘**impact**’(consequence)

Risk Score can be found by blending likelihood and impact as follows:

$$\boxed{\text{Likelihood}} \times \boxed{\text{Impact}} = \boxed{\text{Risk Level/Score}}$$

MBL use the risk matrix shown in Table-D (see next page) to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score is to be used to aid decision making and help in deciding what action to take in view of the overall risk. Three levels of risk (likelihood scale), three levels of impact and four levels of risk score are shown in Table B, C and D respectively.

Table B: Likelihood scale

Frequency	Likelihood of an ML & TF risk
Very likely	Almost certain: it will probably occur several times a year
Likely	High probability it will happen once a year
Unlikely	Unlikely, but not impossible

Table C: Impact scale

Frequency	Likelihood of an ML & TF risk
Consequence	Impact – of an ML/TF risk
Major	Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.
Moderate	Moderate level of money laundering or terrorism financing impact. Minor or negligible consequences or effects.

Table D: Risk score table

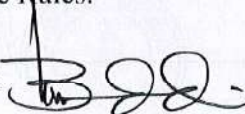
Rating	Impact – of an ML & TF risk
Extreme-4	Risk almost sure to happen and/or to have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level.
High-3	Risk likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.
Medium-2	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.
Low-1	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

8.5 Risk Treatment

Risk treatment is about identifying and testing methods to manage the risks the bank has identified and assessed in the previous process. In doing this, bank needs to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk. Based on the set strategies, policies and procedures and risk type & level & magnitude, risk treatment or action is identified for each risk (**Annex-A**).

8.6 Risk Monitor and review

Keeping records and regular evaluation of the risk plan and AML&CFT program is essential. The risk management plan and AML&CFT program cannot remain static as risks change over time; for example, changes to customer base, products and services, business practices and the law. Once documented, the entity should develop a method to check regularly on whether AML&CFT program is working correctly and well. If not, the entity needs to work out what needs to be improved and put changes in place. This will help keep the program effective and also meet the requirements of the AML&CFT Acts and respective Rules.




8.7 Additional tools to help risk assessment

The following tools or ideas can be useful in helping to manage risk. It can be included in the previous risk assessment process so that the decisions are to be better informed.

8.7.1 Applying risk appetite to risk assessment

Risk appetite is the amount of risk a bank is prepared to accept in pursuit of its business goals. Risk appetite can be an extra guide to the risk management strategy and can also help deal with risks. It is usually expressed as an acceptable/unacceptable level of risk. Some questions to ask are:

- What risks will the bank accept?
- What risks will the bank not accept?
- What risks will the bank treat on a case by case basis?
- What risks will the bank send to a higher level for a decision?

The risk matrix **Table-E** can be used to show the risk appetite of the bank.

In a risk-based approach to AML & CFT the assessment of risk appetite is a judgment that must be made by the bank. It will be based on its business goals and strategies, and an assessment of the ML&TF risks it faces in providing the designated services to its chosen markets.

Table -E: Risk Matrix

LIKELIHOOD (What is the chance it will happen?)	Very Likely	Acceptable Risk Medium 2	Unacceptable Risk High 3	Unacceptable Risk Extreme 3
	Likely	Acceptable Risk Low 1	Acceptable Risk Medium 2	Unacceptable Risk Extreme 3
	Unlikely	Acceptable Risk Low 1	Acceptable Risk Low 1	Acceptable Risk Medium 2
		Minor	Moderate	Major
		IMPACT (How serious is the risk?)		

8.7.2 Risk tolerance

In addition to defining bank's risk appetite, the entity can also define a level of variation to how it manages that risk. This is called risk tolerance, and it provides some flexibility whilst still keeping to the risk framework that has been developed.

8.8 Know Your Customer (KYC) Policies

As per requirement of Money Laundering Prevention (MLP) Act 2012 (as amended in 2015) Community Bank Bangladesh needs to seek satisfactory evidence of the identity of those with whom it deals. Having sufficient information about customer- "Know Your Customer" (KYC)- and making use of that information will underpin all anti-money laundering efforts, and will be the most effective defense against being used to launder the proceeds of crime.

The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. The Bank will seek and retain full information of its customers by using KYC profile form and update it as and when required.

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise.

So, it needs to be sure that the institution is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any bank or investment account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally.

8.8.1 Know Your Customer Procedures

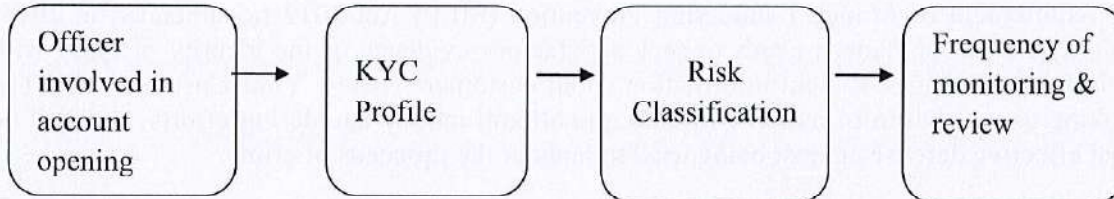
KYC procedure starts from opening account in the name of different clients irrespective of borrowers and depositors. Each officer involved in account opening will be required to perform due diligence on all prospective clients prior to opening an account. This process will be completed by fulfilling the documentation requirements e.g., Account Application, Bank References, Source of funds and Identification for example and also a "Know Your Customer" profile which will be used to record a client's source of wealth, expected transaction activity at its most basic level. KYC profile gives the basic information about the customer like, Name, Address, Tel/Fax Numbers, line of business, Annual sales. (Annexure-B)

Once the identification procedures have been completed and the client relationship is established, the concerned officer will monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened.

The KYC Profile information will also include the observations of the concerned officers when they visit the customer's business place like, the business place is owned or rented, the type of

clients visited, mode of transaction. He/she will record his/her observations and sign the KYC Profile form.

In the case of high net worth Accounts, the information will include net worth of the customer, source of funds etc. The KYC Profile leads to Risk Classification of the Account as High/Low Risk.



8.8.2 Risk categorization - Based on Activity/KYC Profile

When opening accounts, the concerned officer will assess the risk that the accounts could be used for “money laundering”, and will classify the accounts as either High Risk or Low Risk. The risk assessment may be made using the KYC Profile Form in which following seven risk categories are scored using a scale of 1 to 5 where scale 4-5 denotes High Risk, 3- Medium Risk and 1-2 Low Risk:

- Product and Channel Risk
- Type of On-boarding Risk
- Geographic Risk
- Risk classification of country of origin
- Type of Customer and Relationship Risk
- Business and activity Risk
- Transaction Risk
- Transparency Risk

The risk scoring of less than 15 indicates low risk and more than 15 would indicate high risk. The risk assessment scores are to be documented in the KYC Profile Form. However, the concerned officer may override this automatic risk assessment to “Low Risk” if it believes that there are appropriate mitigates to the risk. This override decision must be documented (reasons why) and approved by the BAMLCO.

KYC Profiles and Transaction Profiles must be updated and re-approved at least annually for “High Risk” accounts and in every five years interval for “Low Risk” accounts and as and when falls required. These should, of course, be updated if and when an account is reclassified to “High Risk”, or as needed in the event of investigations of suspicious transactions or other concern.

For Opening of “High Risk” accounts Branch must have to follow the EDD procedure and if the proposed client is a PEP / IP / Chief or High Official of International Organization or family/close associates related to PEP / IP / Chief or High Official of International Organization, as per BFIU Circular branch must have to take approval from CAMLCO Office.

8.9 Customer Identification

It is mandatory to collect and verify the correct and complete identification information of customers to prevent money laundering and terrorist financing and to keep the bank free from risks. KYC (Know Your Customer) procedure shall apply to both individuals and institutions where customer is defined as under:

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

To protect bank from risks of money laundering or/and terrorist financing by customers willful or unwilling activities, the Money Laundering Prevention Guideline clearly states how to conduct Customer Due Diligence at different stages such as:

- while establishing relationship with the customer;
- while conducting financial transaction with the existing customer;
- while remitting money and providing other services at the request of non- account holders; and
- while there is reasonable ground to suspect about the adequacy or veracity of previously obtained customer identification data.

To be sure about the customer’s identity and underlying purpose of establishing relationship with the institution, each institution shall collect adequate information up to its satisfaction.

Explanation: “Satisfaction of the institution” means satisfaction of the appropriate authority that necessary due diligence has been conducted considering the risks of the customers in the light of existing directions. If a person operates an account on behalf of the customer, the concerned bank/financial institution must satisfy itself that the person has due authorization to operate. Correct and complete information of the person, operating the account, are to be collected.

Legal status and accuracy of information of the operators are to be ascertained in case of the accounts operated by trustee and professional intermediaries (such as lawyers/law firm, chartered accountants etc.).

While establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering (such as the countries and territories enlisted in Financial Action Task Force's Non-cooperating Countries and Territories list) enhanced due diligence shall have to be ensured.

The identity of the beneficial owner of the account shall have to be confirmed on the basis of the information obtained from reliable sources up to the satisfaction of the institution:

- Complete and correct information of identity of the persons besides the customer, shall have to be collected and preserved if a customer operate an account on behalf of another person in his/her own name.
- The controller or the owner of the customer shall have to be identified.
- Complete and correct information of identity of the beneficial owners shall have to be collected and preserved. For the purpose of this subsection a person will be treated as a beneficial owner if:
 1. Owns 20% or more of a company or legal arrangements;
 2. Has effective control over the customer; and
 3. The person on whose behalf a transaction is conducted.

8.9.1 Customer Due Diligence

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) Procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources.

Therefore CDD obligations on bank under legislation and are designed to make it more difficult to abuse the banking industry for money laundering or terrorist financing. The CDD obligations compel the banks MLPA, 2012 including 'predicate offences' and the relevant offences under ATA, 2009.

Therefore, banks should be able to demonstrate to their supervisory authority to put in place implement adequate CDD measure considering the risks of money laundering and terrorist financing. Such risk sensitive CDD measure should be based on-

- a) Type of customers;
- b) Business relationship with the customer;
- c) Type of banking products; and
- d) Transaction carried out by the customer.

The adoption of effective KYC standards is an essential part of bank's risk management policies. Banks with inadequate KYC program may be subject to significant risks, especially

legal and reputational risk. Sound KYC policies and producer not only contribute to the bank's overall safety and soundness, they also protect the integrity of the banking system by reducing money laundering, terrorist financing and other unlawful activities.

8.9.2 What is required for CDD?

Branches or authorities subsidiaries or concerned Head Office Divisions are required to:

- a. Identify the customer and verify that customer's identity using reliable, independent source documents, data or information, i.e. **complete & accurate** information of the customer;
- b. Verify that any person purporting to act on behalf of the customer is so authorised, and also verify the identity of that person i.e. complete & accurate information of the authorised person(S);
- c. Identify the beneficial the owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the branch or authorized subsidiary or concerned Head Office Division is satisfied that it knows who the beneficial owner is. It includes collection & preservation of:
 - i) **Complete & accurate** information of the person (s) on whose behalf the customer operates the account;
 - ii) Complete & accurate information of the person (s) on who control(s) the customer; and
 - iii) In case of company, complete & accurate information of the shareholder who controls the company or has 20% or more shares of the company;
- d. Understand and, where relevant, obtain information on the purpose and intended nature of the business relationship.

8.9.3 When CDD is required (Timing of CDD)?

Branches or authorized subsidiaries or concerned Head Office Divisions are required to conduct CDD on the customer and the person conducting the transaction, when:

- a. Established business relationships including opening accounts;
- b. Providing wire transfer (remittance) service [e.g. BEFTN, EFT, RTGS & etc.];
- c. Providing money or value transfer (remittance) service;
- d. Providing trade finance and trade service facilities;
- e. While selling bank's own products, issuing credit cards, payment of dues credit cards and reloading of prepaid/travel cards and any other product;
- f. Carrying out occasional transactions;
- g. It has any suspicious of ML/TF, regardless of amount; or
- h. It has any doubt about the veracity or adequacy of previously obtained information.

8.10 Enhanced Customer Due Diligence Measure

- a. Branch or authorized subsidiaries or concerned Head Office Divisions are to apply enhance due diligence measure where required as identified in the paragraph 3.8 of BFIU Circular 26 dated June 16, 2020, in addition to performing normal CDD measures.
- b. Enhanced CDD measures guidelines:
 - Obtained additional information on the customer (occupation, volume of assets information available through public databases, internet, etc.) and updating more regularly the identification data of customer and beneficial owner.
 - Obtained additional information on the intendant nature of the business relationship.
 - Obtained additional information on the source of funds or source of wealth of the customer.
 - Obtained additional information on the reasons for intendant or performed transactions.
 - Obtaining the approval of CAMLCO Office to establish or continue relationship with PEP / IP / Chief or High Official of International Organization or family/close associates related to PEP / IP / Chief or High Official of International Organization.
 - In case of PEP / IP / Chief or High Official of International Organization or family/close associates related to PEP / IP / Chief or High Official of International Organization data/remarks should input properly in Core Banking Solution and AOF as well.
 - Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
 - Making aware the concerned official about the risk level of the customer.

8.11 Identification of Beneficial Owner

8.11.1 Who is Beneficial Owner?

As per 2(4) of MLPR 2019 beneficial owner means that 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 include those persons who exercise ultimate effective control over legal person or arrangement or holds 20% or more share of a company. Here “ultimately owners 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 and direct control.

1. The definition of beneficial owner means the individual who-
 - a) has effective control of customer; or

- b) Owners a prescribed threshold, 20% as per Bangladeshi regulation of the company or legal arrangements.
2. Identifying the beneficial ownership if a customer one must apply three elements. Any one element or any combination of these three elements satisfies beneficial ownership. These elements are:
 - a. who owns 20 or more percent of a company or legal arrangements
 - b. who has effective control of the customer;
 - c. the person on whose behalf a transaction is conducted
 3. 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.

8.11.2 Why is it important to identify the beneficial owner?

4. Corporate entities such as companies, trusts, foundations, partnerships, and other type of legal person 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 purpose, including money laundering (ML), bribery and corruption, insider dealings, tax fraud, terrorist financing (TF), AND OTHER unlawful activities. This is because, for criminal trying to circumvent anti-money laundering (AML) and countering the financing of terrorist (CFT) measure, corporate entities provide an attractive avenue to disguise the ownership and hide the illicit origin.
5. Various studies conducted by Financial Action Task Force (FATF), World Bank, United Nations Office on Drug and Crime (UNODC) have explored the misuse of corporate entities for illicit purpose, including for ML/TF. In general, the lack of adequate, accurate and timely beneficial ownership information in facilities ML/TF by disguising:
 - a) The identify of known or suspected criminals
 - b) The true purpose of and account or property held by a corporate entities, and/or
 - c) The source or use of funds or property associated with a corporation entity.

8.11.3 Ways in which beneficial ownership information can be hidden/obscured.

- a) Complex ownership and control structures involving many layer of ownership, sometimes in the name of other legal persons and sometime using a chain of ownership that is spread across several jurisdictions,
- b) Bearer shares and Bearer share warrants,
- c) Use of legal persons as director,
- d) Formal nominee shareholders and director where the identity of the nominator is undisclosed,
- e) Informal nominee shareholders and directors, such a close associates and family,

- f) Trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,
- g) Use of intermediaries in forming legal persons including professional intermediaries such as accountants, lawyers, notaries, and trust and company service providers.

8.11.4 Ownership

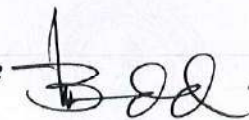
The reporting entities should understand the ownership and control structure of the customers. The shareholder for controlling interest owns 20% or more of the customer. The ownership can be simple and complex in nature.

8.12 Politically exposed persons (PEPs)

Politically Exposed Persons (PEPs) refer to “individuals who are or have with prominent public functions by a foreign country, for example Heads of state or government, senior Politicians, senior government, judicial or military officials, senior executive of state owned corporations, importance political party officials.”

8.12.1 Who are Politically Exposed Persons (PEPs)

- heads of state or government, ministers and deputy or state minister;
- Member of parliament or of similar legislative bodies;
- Member of government bodies of political parties (generally only apply to the national governing bodies where a member has significant executive power, e.g. over the selection of candidates or distribution of significant party funds);
- Senior politician
- Members of supreme courts, of constitutional court or of any judicial body the decisions of which are not subject to further appeal excepts in exceptional circumstance;
- Members of courts of auditors or of the boards of banks;
- Ambassadors, charges d'affairs and high-ranking officers in the armed forces
- Head of the senior executives or members of the administrative, management or supervisory bodies or state-owned enterprises;



- Chief directors, deputy directors and members of the board or equivalent function of an international organizations

8.13 who are influential persons; IPs in Bangladesh

- heads and deputy heads of state or government;
- senior member of ruling party;
- minister, state minister, deputy minister
- member of parliament and/or national legislatures;
- member of governing bodies of major politician parties;
- secretary, additional secretary joint secretary in the ministers;
- judge of supreme courts, constitutional court or other high-level judicial bodies whose decisions are not subject to farther appeal, except in exceptional circumstances;
- governors, deputy governors, executive director and general manager of central bank;
- heads of the arm forces, other high ranking members of the armed forces and heads of the intelligence services;
- have of state-owned enterprises;
- member of the governing or bodies of local political parties;
- Ambassadors, charges d'affairs or other senior diplomats;
- City mayors or heads or municipalities who exercise genuine political or economic power;
- Board member or state-owned enterprises of national political or economic importance.

8.14 Chief or similar high-ranking positions in an international organization.

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

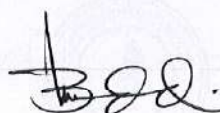
The definition of PEPs & IPs is not intending to cover middle ranking and more junior individuals as mentioned in 1.2, 1.3 and 1.4.

8.14.1 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 leave office. A family member of a former PEP/IP should not be subject to enhanced due diligence measure unless this is justified by the bank assessment of other risks posed 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. Bank may apply measure 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 necessary in the cases of PEPs/IPs where a reporting organization has assessed that PEP/IP is posing a higher risk.

- An assessment of the extent to which the risk would be increase by a business relationship with a PEP, family member of close associate. BFIU would expect that this is a case-by-case assessment and not an automatic assessment that a relationship create a high risk of money laundering ; and
 - Any information provided by the BFIU. This will include the BFIU’s publication, thematic review speeches on financial crime issue, BFIU’s annual report.
- (a) Bank should identified that a customer (or beneficial owner of a customer) does meet the definition of a PEP (or a family member or know close associate of a PEP), Bank must assess the level of risk associated with that customer and, as a result of that assessment, the external to which enhance due diligence measures need to be carried out. The risk factor set in this guidance will help reporting organization to consider relevant factors when meeting these obligations. Bank’s assessment and its decision to apply relevant enhanced due diligence measure need to be documented.
- (b) BFIU expects that Bank have to make use of information that is reasonably available to then in identifying PEPs, family member or known close associates. This could include the following:
- Public domain information such as website of the governments, reliable news sources and work by reputable pressure groups focused on corruption risk. Bank should use a variety of sources where possible.
 - In line with the nature and size of the Bank, It may choose, but is not required, to use commercial database that contain lists of PEPs, family member and close associates. Bank is choosing to use such a lists would need to understand now such database are populated and will need to ensure that those flagged by the system fall within the definition of a PEP, family member and close associate as set out in the regulation and this guidance.
- (c) BFIU expects that Bank will not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or family member of a PEP or known associates of a PEP). Bank may, after collecting appropriate information and completing its assessment, conclude the risks posed by customer are higher than they can effectively mitigate; only in such cases it will be appropriate to decline or close that relationship.
- (d) If, having assessment the risk associated with the customer and decided in an appropriate level of enhanced due diligence measure in line with this guidance, Bank is unable to apply those measures, Bank needs to comply with the requirement not to establish, or to terminate, a business relationship.



(e) The following measure 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 know close associate of a foreign PEP, IPs/Chief of international organization posing higher risk:

- Obtain senior management approval for established or continuing business relationships with such persons
- Weak state institutions
- Weak any-money laundering defense
- Armed conflict
- Non-demarcated forms of governments
- Widespread organized criminality
- A political economic 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 cultural antagonistic to the interested of whistleblowers
- Weakness in the transparency of registers of ownership for companies, land and equities
- Human right abuses

8.15 Correspondent Banking

Instructions for establishing corresponding relationship are as follows:

1. For the purpose of this circular correspondent banking shall mean providing services which are approved by Bangladesh Bank like credit, deposit, collection, clearing, payment or other similar services by one bank (correspondent) to another bank (respondent).
2. While establishing and continuing correspondent banking relationship following drill should be observed so that banking system cannot be abused for the purpose of money laundering :
 - Before providing correspondent banking service senior management approval must be obtained on being satisfied about the nature of the business of the respondent bank through collection of information Banks should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.

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

8.16 Branches and subsidiaries situated/located in foreign jurisdiction

- Reporting organizations (in applicable cases) under Money Laundering Prevention Act, 2009 and Anti-Terrorism Act, 2009 having branches and subsidiaries abroad shall also comply with the provisions of Money Laundering Prevention Act, 2009 and Anti-Terrorism Act, 2009.
- If branch or a subsidiary located abroad, for any reason fails to comply with the instructions of Money Laundering Prevention Act, 2009 and Anti-Terrorism Act, 2009 it shall without any delay report to such cases to Anti Money Laundering Department mentioning the reason of the failure.

8.17 What Constitutes a Person's Identity?

Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, body corporate, partnership etc.). For the purposes of this guidance, the two elements are:

- the physical identity (e.g. name, date of birth, TIN/voter registration/passport/ID number, etc.); and
- the activity undertaken.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non-money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issue should be recorded.

The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the institution's own understanding of the applicant's business.

When commencing a business relationship, it needs to consider recording the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. Documentation about the nature of the applicant's business should also cover the origin of funds to be used during the relationship. For example, funds may be transferred from a bank or the applicant's employer, or be the proceeds of a matured insurance policy, etc.

Once account relationship has been established, reasonable steps should be taken by to ensure that descriptive information is kept up to date as opportunities arise. It is important to emphasize that the customer identification process do not end at the point of application. The need to confirm and update information about identity, such as changes 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.

8.18 Individual Customers

Where verification of identity is required, the following information should be obtained from all individual applicants for opening accounts or other relationships, and should be independently verified by the concerned officer itself:

- True name and/or names used;
- Parent's names;
- Date of birth;
- Current and permanent address;
- Details of occupation/employment and sources of wealth or income

One or more of the following steps is recommended to verify addresses:

- Provision of a recent utility bill, tax assessment or bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- checking the Voter lists;
- checking the telephone directory;
- Record of home/office visit.

The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.

The date of birth is important as an identifier in support of the name, and is helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard. It is also helpful for residence/nationality to be ascertained to assist risk assessment procedures and to ensure that the Bank does not breach UN or other international financial sanctions.

Identification of documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.:-

1. Current valid passport;
2. Valid driving license;
3. Voter ID Card;
4. Armed Forces ID card;
5. A Bangladeshi employer ID card bearing the photograph and signature of the applicant;
or
6. A certificate from any local government organs such as Union Council Chairman, Ward Commissioner, etc. or any respectable person acceptable to the Bank.

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, credit cards, non-

Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which the concerned officer is unfamiliar, either because of origin, format or language, he must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. The concerned officers should also be aware of the authenticity of passports.

Where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. 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.

There is obviously a wide range of documents which might be provided as evidence of identity. It is for each concerned officer to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders, not only the first named, should normally be verified in accordance with the procedures set out above.

Any subsequent change to the customer's name, address, or employment details of which the concerned officer becomes aware should be recorded as part of the "Know Your Customer" process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

Where this is not possible, the relevant details should be recorded on the applicant's file. In case of one-off transactions the details should be recorded in a manner which allows cross reference to transaction records. Such institutions may find it convenient to record identification details on a separate form similar to the example in Annexure C, to be retained with copies of any supporting material obtained.

An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not require or request staff to breach account opening procedures as a favor to an applicant

8.19 Persons without Standard Identification Documentation

Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous anti-money laundering procedures is recommended. The important point is

that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

A certifier must be a suitable person, such as for instance 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 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.

The Branch In-Charge may authorize the opening of a business relationship if he/she 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.

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

8.20 Corporate Bodies and other Entities

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a "brass plate company" where the controlling principals cannot be identified.

Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if the institution becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such

companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such it needs to carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh's.

In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

The following documents should normally be obtained from companies:

- Certified true copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified true copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 20% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.

Where the business relationship is being opened in a different name from that of the applicant, it needs to find out the reason for using the second name makes sense.

The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:



- All of the directors who will be responsible for the operation of the account / transaction.
- All the authorized signatories for the account/transaction.
- All holders of powers of attorney to operate the account/transaction.
- The beneficial owner(s) of the company
- The majority shareholders of a private limited company.

A letter issued by a corporate customer similar to is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the concerned officer already knows their identities and identification records already accord with the requirements of this guideline, there is no need to verify identity again.

When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

8.21 Partnerships and Unincorporated Businesses

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the institution, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable). An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

8.22 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.

8.23 Internet or Online Banking

Banking on the Internet adds a new dimension to banking activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering, and fraud. It is recognized that on-line transactions and services are convenient. However, it will not be appropriate to 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, will not be put into full operation until the relevant account opening provisions have been satisfied in accordance with this Guideline.

8.24 Walk-in Customers for TT, DD, PO etc.

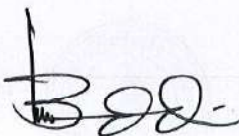
The AML policy requires the bank to obtain satisfactory evidence of identification of applicants for floor services like TT, DD, PO. etc. who do not maintain accounts with the bank for conducting the above-noted services. In case of remitting money through TT, DD, PO. etc. for walk-in customers, he/she will kindly be requested to provide the details, together with appropriate documentary evidence, before the transaction may proceed. The details record will be retained by using a form given in **Annexure C** of this guideline which will allow cross reference to transaction records.

8.25 Provision of Safe Custody and Safety Deposit Boxes

Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it needs to follow the identification procedures set out in this Guideline. In addition such facilities will only be made available to account holders.

8.26 Timing and Duration of Verification

The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed. However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this will be subject to stringent controls which will ensure that any funds received are not passed to third parties. Alternatively, a senior official may be given appropriate authority. This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing. Verification, once begun, will normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, the concerned officer may (or may not) consider that this is in itself suspicious.



Chapter: 9

Transaction Monitoring, Reporting and Record Keeping

9.1 Record Keeping

Record keeping is an essential component of the audit trail that the Laws and Regulations seek to establish in order to assist in any financial investigation and to ensure that criminal funds which are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities. Banks must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

9.2 Legal Obligations

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

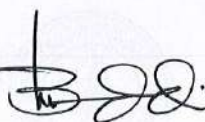
Obligations under MLP Rules, 2019, “The bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners:

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

9.3 Transaction Monitoring Process

The concerned officer is expected to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts i.e. the Transaction Profile (TP) of the Customer as to whether transactions are well covered in terms of all guidelines laid down by BFIU and other laws. Possible areas to monitor could be: -

- A. Transaction type
- B. Frequency
- C. Unusually large amounts
- D. Geographical origin/destination
- E. Changes in account signatories



Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. This will be set in a Transaction Profile (TP) at the time of opening account from the customer. Ideally any deviation from the normally expected TP should be reviewed with human judgment and interaction with customer. Such reviews may result in changing the expected profile or closing the customer account.

It may not be feasible for some specific branches having very large number of customers to track every single account against the TP where a risk based approach will be taken for monitoring transactions based on use of “Customer Categories” and “Transaction Limits” (individual and aggregate) established within the branch. The Customer Category will be assigned at account inception - and may be periodically revised - and will be documented on the Transaction Profile. Transaction Limits will be established by the business subject to agreement by BAMLCO. The Customer Categories and Transaction Limits will be maintained in the manual ledgers or computer systems.

On a monthly basis branch may prepare an exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the “transaction limit” established for that category of customer based on Anti-Money Laundering risk assessment exercise.

The concerned officer will review and sign-off on such exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the “transaction limit” established for that category of customer. The concerned officer will document his/her review by initial on the report, and where necessary will prepare internal Suspicious Activity Reports (SARs) with action plans for approval by the BAMLCO. A copy of the transaction identified will be attached to the SARs.

9.4 Cash Transaction Report (CTR)

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

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

9.5 Half yearly Self-Assessment Report & Independent Testing Procedures (ITP)

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

9.5.1 Responsibilities of Branch

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

9.5.2 Responsibilities of Internal Control & Compliance Division

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

9.5.3 Responsibilities of AML & CFT Division/CCC

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

9.6 Quarterly meeting minutes

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

9.7 Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR)

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

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

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

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

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

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

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

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

a) Identification of STR/SAR

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

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

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



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

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

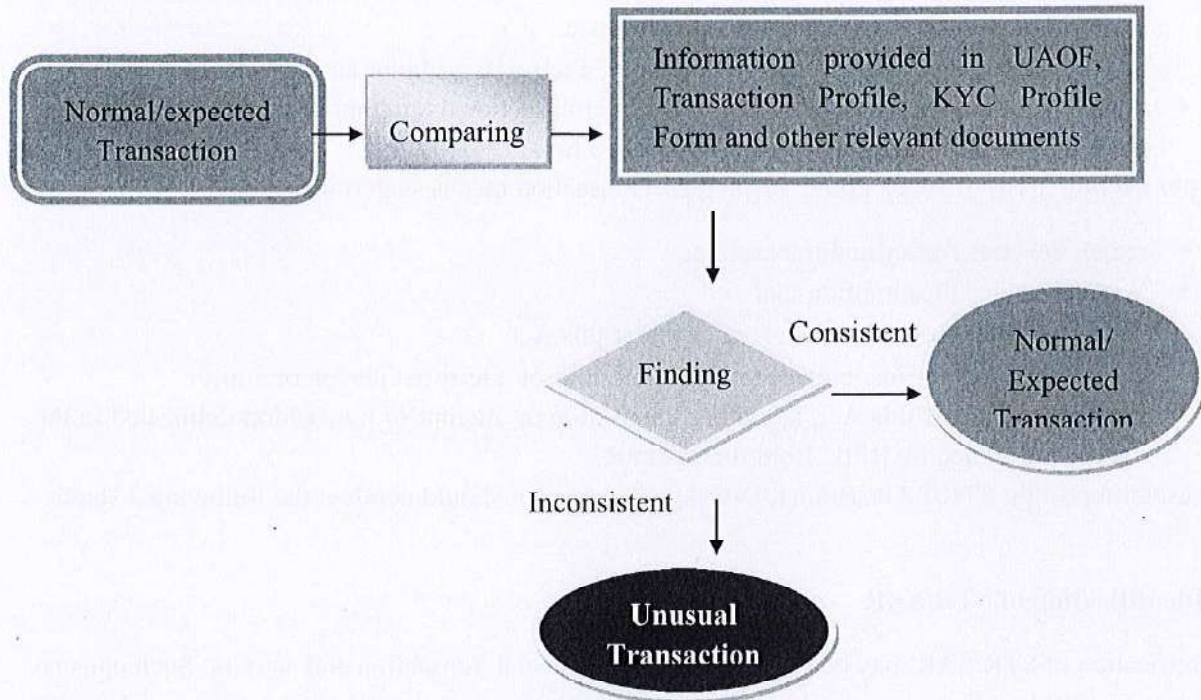


Figure: Identification of STR/SAR

b) Evaluation of STR/SAR

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

c) Disclosure of STR/SAR

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

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

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

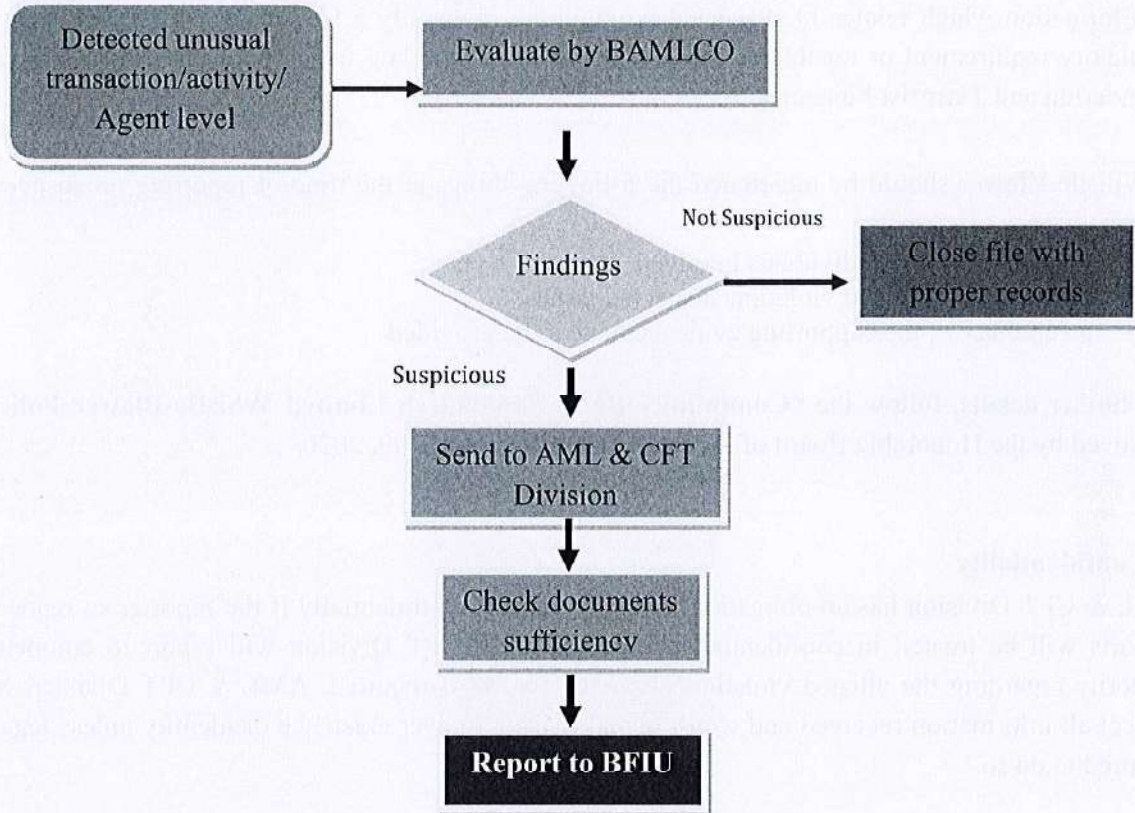


Figure: STR/SAR identification and reporting procedures

9.7.1 Reporting STR/SAR

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

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

9.8 Whistle Blowing

a) Definition

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

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

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

For further details, follow the “**Community Bank Bangladesh Limited Whistle Blower Policy**” approved by the Honorable Board of Directors dated November 09, 2020.

a) Confidentiality

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

Chapter: 10

Recruitment, Training and Awareness

10.1 Employee Screening

Banks are object to ML & TF risk from its customer as well as from its employee in absence of proper risk mitigating measures. ML & TF risk arise from customer and its mitigating measures have been discussed in several chapters of this guideline. ML & TF risks arising by or through its employees can be minimized if the bank follows fair recruitment procedure. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, Banks are advised to follow the following measures (at 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 examine the consistency and capability of the employee and ensure that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

10.2 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 thought checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables. Policies, procedures, job descriptions, internal control, approval levels, level of authority, compliance with personal 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 requirement should be included in the bank HR policy.

10.3 Training For Employee

Every employee of a bank shall have at least basic AML & CFT training that should cover all the aspects of AML & CFT measure in Bangladesh. Basic AML & CFT training should be at least a 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 measure, banks are required to impart refreshment training programs of its employees on a regular basis.

AML & CFT basic training should be following-

- ✓ An overview of AML & CFT initiatives;
- ✓ Relevant provisions of MPLA & ATA and rules there on;
- ✓ Regulatory requirements as per BFIU and the rules there on;
- ✓ STAT/SAR reporting procedure;
- ✓ Ongoing monitoring and sanction screening mechanism;

Beside basic and refreshment AML & CFT training, bank shall arrange job specific training of 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 relation 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 employee who conduct transaction of customers.

10.4 The Need for Staff Awareness

All the staff of Community Bank Bangladesh will be aware of their personal obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff will be trained to co-operate fully and to provide a prompt report of any suspicious transactions, it is, therefore, importance that the bank introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully of their responsibility.

The management of Community Bank Bangladesh will ensure that the staffs are adequately trained in relation to identification, reporting and record retention to ensure that they are adequately trained to discharge their responsibilities. So the Community Bank Bangladesh will take appropriate measure to make employees aware of:

- Policies and procedures to prevent money laundering and for identification, record keeping and internal reporting;
- The legal requirements; and
- To provide relevant employees with training in the recognized and handling of suspicious transactions.

All relevant staff will be educated in the process of the “know your customer” requirement for money laundering prevention purposed. The training in this respect will cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activity at a future date. Relevant staff will be alert to any change in the pattern of customer’s transactions or circumstance that might constitute criminal activity.

Although senior manager may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed in them, their staff and institution itself. Some form of high-level awareness raising training will therefore needed.

10.5 Awareness of Senior Management

Without proper concern and Awareness of senior management of a bank, it is difficult to have effective implementation of AML & CFT measure in the bank. Banks are required to arrange, at least once on a year, an awareness program for all the members of its board of director and or member of the highest policy making committee and people engaged with policy making of the bank.

Chapter: 11

Trade based Money Laundering

11.1 Recognition of Trade based Money Laundering

- a. Trade based Money Laundering (TBML) has been recognized by the financial Action Task force (FATF) in its landmark study published in 2006, as one of the three main methods by which criminal organizations and Terrorist Finance move money for the purpose of disguising its origins and integrating it back into the formal economy. This method of ML is based upon abuse of trade transaction and their financing. The FATF Study 2006 highlighted the increasing attractiveness of TBML as a method for laundering funds, compared with misuse of the financial system (both formal and alternate) and through physical movement of cash (cash smuggling).
- b. APG (2012) study on TBML, done six years after the landmark FATF Study of 2006, has reaffirmed the conclusion of the earlier study that TBML is an important channel for criminal organizations and Terrorist Financing to move money or value to disguise its illicit origin and to integrated it into the formal economy. The rapid growth in the global economy has made international trade and increasingly attractive avenue to move finds through goods and service.
- c. Bangladesh Financial Intelligence Unit (BIFU) in its Money Laundering Terrorist Financing Risk Management Guidelines 2015 mentions that the international trade system is subject it wide range of risks and vulnerabilities which provide terrorist organizations the opportunity to transfer value and goods through seemingly legitimate trade flows. To exploit the trade system for terrorist financing proposed could assist in the development of measure to identify and combat such activity.
- d. Considering the gravity BFIU through Circular No 24 dated December 10, 2019 circulated “Guidelines for Prevention of Trade Based Money Laundering” and instructed all the banks to prepare its own Trade Based Money Laundering policy.
- e. Community Bank Bangladesh Limited as per instruction of BFIU prepared its own Policy on Prevention of Trade Based Money Laundering.

For further details, follow the “**Policy on Prevention of Trade Based Money Laundering**” of Community Bank Bangladesh Limited as approved by the Honorable Board of Directors on their 18th meeting held on November 9, 2020.

Chapter: 12

Terrorist Financing & Proliferation Financing

12.1 Introduction

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

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

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

12.2 Obligations under Law and Circular

Obligations under ATA, 2009

Every Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 and if any suspicious transaction is identified, the agency shall spontaneously report it to Bangladesh Bank without any delay.

The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each bank should approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, 2009; which are applicable to the bank, have been complied with or not.

12.3 Obligations under Circular

<p>Obligation Under BFIU Circular -19; date 17/09/2017</p>	<p>Every Bank shall establish a procedure by approval of Board of Directors for detection and prevention of financing of terrorism and financing of proliferation of weapons of mass destruction, shall issue instructions about the duties of Bank officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.</p> <p>Before any international business transaction, every bank will review the transaction of identify weather the concerned parties of that transaction are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or proscribed by Bangladesh Government. Immediately after the identification of any account of any listed individual or entity concerned bank will stop that transaction and inform BFIU the detail information at the following working day.</p>
------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

12.4 Necessity of Funds by Terrorist

Terrorist organizations need money to operate. Weapons and ammunition are expensive. Major international operations require substantial investments for personnel, training, travel and logistics. Organizations must have substantial fundraising operations, as well as mechanisms for moving funds to the organization and later to terrorist operators. These functions entail considerable risk of detection by authorities, but also pose major challenges to both the terrorists and intelligence agencies.

12.5 Sources of Fund/Raising of Fund

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

12.6 Movement of Terrorist Fund

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

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

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

12.7 Formal Financial Sector

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

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

12.8 Trade Sector

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

12.9 Cash Couriers

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

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

12.10 Use of Alternative Remittance Systems (ARS)

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

12.11 Use of Charities and Non-Profit Organizations

Charities are attractive to terrorist networks as a means to move funds. Many thousands of legitimate charitable organizations exist all over the world that serve the interests of all societies, and often transmit funds to and from highly distressed parts of the globe. Terrorist abuses of the charitable sector have included using legitimate transactions to disguise terrorist cash travelling

to the same destination; and broad exploitation of the charitable sector by charities affiliated with terrorist organizations. The sheer volume of funds and other assets held by the charitable sector means that the diversion of even a very small percentage of these funds to support terrorism constitutes a grave problem.

12.12 Targeted Financial Sanctions

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.

12.13 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)".

12.14 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".

12.15 Automated Sanction Screening Mechanism of UNSCRs

For effective implementation of TFS relating to TF& PF, Community Bank Bangladesh Limited has an automated screening mechanism that can prohibit any listed individuals or entities to enter into the banking channel. Branches need to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individuals or entities could not use the formal financial channel. In a word, branch shall ensure that screening has done before-

- **Opening any account or establishing relationship domestically:**

If any name or entity matches with UNSCR, OFAC and Domestic Sanction list, then account of such person and/or entity will not to be opened and in case

of existing account operation will be stopped and referred this account to the AMLD, Head Office.

▪ **Any international relationship or transaction:**

For screening of cross-border transactions (both incoming and outgoing messages), Community Bank Bangladesh Limited has implemented sanction screening software from SWIFT.

➤ **For incoming messages:**

Incoming MT2 & MT1 type messages (both local and foreign) are filtered against sanction list provided by U.N., U.S.A. and OFAC in Alliance Remote Gateway (ARG). Messages containing any similarities with sanction list are automatically blocked and send to level-2 user for investigation. After screening the message the level-2 user forwards the message to level-1 user with pass or fail recommendation. Level-1 user passes the message or sends back the message to level-2 user for further review.

➤ **For outgoing messages:**

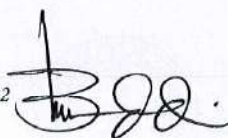
After preparing the MT2 & MT1 type messages (both local and foreign) branch passes the message through SWIFT and sent messages are filtered against sanction list provided by U.N.,

U.S.A. and OFAC in Alliance Remote Gateway (ARG). Messages containing any similarities with sanction list are automatically blocked and send to level-2 user for investigation. After screening the message the level-2 user forwards the message to level-1 user with pass or fail recommendation. If any suspicious transaction found branch is requested to provide additional data and keeps record of those data. Level-1 user passes the message or sends back the message to level-2 user for further review.

Responsibilities of Branch Manager/BAMLCO in areas of Sanction Screening

- ✓ Ensure new customer screening (Individual Name or Entity) before opening an account;
- ✓ Ensure existing customer screening and therefore marking as „False positive/Blacklisted“;
- ✓ If any Individual Name or Entity matches with the UNSCR, OFAC and Domestic Sanction list, instantly inform to Head Office;
- ✓ Ensure maintenance of separate file for “Sanction Screening Records”;
- ✓ Monitor and ensure that sanction screening is done for each case of opening new account and cross-border transaction;

All Branch Managers and BAMLCOs are required to ensure the screening timely and comply with regulating requirement on AML/CFT risk.





Chapter: 13

Anti-Bribery and Corruption (ABC) Policy

13.1 Preamble

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

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

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

13.2 Bribery

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

Bribery is:

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

13.3 Corruption and Fraud

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

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

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

Action consisting Corruption and Fraud

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

- Any dishonest or fraudulent act
- Misrepresentation of bank funds, securities, supplies or other assets
- Handling or reporting of money or financial transactions fraudulently or improper way
- Willfully conceal the conflicts of interests
- Disclosing confidential and proprietary information to outside parties
- Manipulation, falsification or alteration of records or documents
- Destruction, removal, or inappropriate use of records, fixtures, and equipment and other physical assets of the bank.

13.4 Initiatives of Community Bank Bangladesh Limited to protect bribery and corruption

13.4.1 Zero tolerance to bribery and corruption

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

13.4.2 Governance

The program shall be overseen by Senior Management under the supervision of Managing Director and CEO of the Bank. The overall objective of ABC governance is to establish and maintain a policy which sets a standard of behavior that achieves a culture of ethical business practices and compliance with ABC legal and regulatory aspects.

a) Role and responsibilities

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

- i) **Senior Management:** Senior Management shall have oversight responsibility to implement the policy and the Bank shall allocate sufficient resources to achieve reasonably effective operations. After proper verification Senior Management including Honorable Board of Directors will approve the policy including modification/changes that may take place.
- ii) **Human Resource Division:** Human Resource Division shall take an action against identified any bribery and corruption activities that may occurred by the employees working in the

Bank. Human Resource Division shall circulate to all employees with advice to be vigilant for any bribery and corruption activities by the employees working under Branches/Departments/Divisions/Units/Cells and if any such occurrence is detected, the same shall be reported to Human Resource Division through concerned supervisor.

iii) **Internal Control & Compliance Division:** Internal Control & Compliance Division shall special attention to evaluate the activities of Branches/Departments/ Divisions/Units/ Cells while conducting their routine audit and report the same accordingly intimation to Human Resource Division and AML & CFT Division.

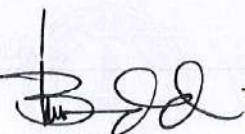
13.5 ABC compliance Program

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

- Prohibits the promising, offering, giving, solicitation or receiving of anything of value, directly or indirectly through third parties, if improperly intended to influence action or obtain an advantage.
- Prohibits falsifying or concealing any books, records or accounts that relate to the business of the Bank, its customers, suppliers or other business partners
- Defines and identifies the heightened risk of interaction with Public Officials
- Provides employees with the opportunity to report suspected bribery in a confidential manner and protects employees from retaliation for good faith reports
- Notifies employees the consequences of non-compliance
- Obtains strong and visible commitment from Senior Management and the Board of Directors, including a public statement of such commitment by the Bank
- All the employees of the bank follow the instruction of the competent authority like BFIU, Bangladesh Bank, Anti-Corruption Commission, NBR, CIC, Tax Office, Honorable Court, etc.
- Ensure proper verification of the documents of the International trade shall be verified through independent sources
- Ensure before sanctioning any donation, sponsorship, expenses and investment proper verification of the motive, ultimate beneficiary of the same.
- Ensure every dealing of the Banks operations including recruitment, transfer & positing, remuneration, benefit, training shall be done as per the HR Policy of the Bank
- HR policy should be followed before receiving any gift, benefit and hospitality by any employees of the Bank.
- Procurement and selling process shall be done as per the set rules of the Bank and must obtain approval from the proper management of the Bank.
- Ensure training on Anti -Bribery and Corruption

13.6 Conclusion

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



Annexure-A

RISK REGISTER

1. ML & TF Risk Register for Customers

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport (if any) acceptable document to the Bank. Monitoring the transaction. Response: Acceptable Risk
Walk-in customer (beneficiary is government/semi government/ autonomous body/ bank & NBF1)	Likely	Minor	=1(Low)	CDD should be ensured. Short KYC should be obtained. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport (if any) acceptable document to the Bank. Response: Acceptable Risk
Walk-in customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBF1)	Likely	Moderate	=2(Medium)	CDD should be ensured. Short KYC should be obtained. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport (if any) acceptable document to the Bank. Response: Acceptable Risk
Non-resident customer (Bangladeshi)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport (if any) acceptable document to the Bank. Monitoring the transaction. Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	Likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD must be applied. Monitor the transaction. Marked as STR Response: Acceptable Risk
A customer making series of transactions to the same individual or entity	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Monitor the transaction. Marked as STR Response: Acceptable Risk
A customer or a group of customer making lots of transactions to the same individual or group	likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport (if any) acceptable document to the Bank. CDD should be ensured & EDD must be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR Response: Acceptable Risk.

[Handwritten signature]



Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer involved in outsourcing business	likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport (if any) acceptable document to the Bank. CDD should be ensured & EDD must be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Response: Acceptable Risk.
Customer appears to do structuring to avoid reporting threshold	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.
Customer appears to have accounts with several banks in the same area	likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction. Marked as STR Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employce, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employce, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR.

[Handwritten signature]



[Handwritten signature]

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Negative news about the customers' activities/ business in media or from other reliable sources	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk..
Customer is secretive and reluctant to meet in person	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitor the transaction. Verify physically. Response: Unacceptable Risk.
Customer is a mandate who is operating account on behalf of another person/ company.	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.

[Handwritten signature]



Risk	Likelihood	Impact	Risk Score	Treatment/Action
Transactions by beneficiaries using Student account & Farmers account	Likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Obtain/check documents of beneficial owner. Monitor the transaction. Report as STR Response: Acceptable Risk
Joint account opened with minor/ women & transactions to the account	Likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR
Large deposits in the account of customer with low income	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.

[Handwritten signature]



Risk	Likelihood	Impact	Risk Score	Treatment/Action
Transaction does not match with business profile	Likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR Response: Acceptable Risk
Customers about whom BFIU seeks information (individual)	Likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR Response: Acceptable Risk
A customer whose identification is difficult to check	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Significant and unexplained geographic distance between the bank and the location of the customer	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Account Opening branch is far from residential address of account holder	Likely	Moderate	=2(Medium)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction. Verify physically. Encourage to opening the account to the nearest branch. Response: Acceptable Risk
Customer is a foreigner	Likely	Major	=3(High)	Obtain approval from Head Office. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.
Non Resident Customer	Likely	Major	=3(High)	Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction.
Customer is a minor	Likely	Major	=3(High)	Beneficiary Owner information must be obtained. Verify the source of income. CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitor the transaction Response: Unacceptable Risk.

[Handwritten signature]



Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer is Housewife	Likely	Major	=3(High)	Beneficiary Owner information must be obtained. Verify the source of income. CDD should be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Monitor the transaction Report as STR Response: Unacceptable Risk.
Customers that are politically exposed persons(PEPs) or influential persons (IPs) or chief/senior officials of international organizations and their family members and close associates	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.
Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Very likely	Moderate	=3(high)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customers doing significant volume of transactions with higher-risk geographic locations.	Very likely	Moderate	=3(high)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.
A customer who brings in large amounts of used notes and/or small denominations	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Response: Acceptable Risk
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)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank. Report as STR. CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank. Transaction is not allowed until risk is reduced. Monitoring the Transaction regularly. Response: Unacceptable Risk.



Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer is a money changer/ courier service agent / travel agent	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any)/ acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Transaction Monitoring regularly. Response: Unacceptable Risk.
Customer is involved in Manpower Export Business	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring Transaction. Report as STR. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer has been refused to provide banking facilities by another bank	Likely	Major	=3(High)	Identify the reason behind non acceptance by other Banks. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Accounts opened before 30 April, 2002	Likely	Moderate	=2(Medium)	Update KYC profile Marked as dormant if KYC is not updated. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Monitor the transaction. Response: Acceptable Risk
Customers with complex accounting and huge transaction	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Receipt of donor fund , fund from foreign source by micro finance institute (MFI)	Likely	Major	=3(High)	CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Verify source of fund. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Genuineness of submitted documents is difficult to ensure	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction Verify physically. Response: Acceptable Risk
Counterfeiting of security documents	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.

[Handwritten Signature]



[Handwritten Signature]

Risk	Likelihood	Impact	Risk Score	Treatment/Action
High net worth with no clear identifiable sources of income	Likely	Major	=3(High)	<p>Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>CDD must be ensured & EDD should be applied</p> <p>Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank.</p> <p>Transaction is not allowed until risk is reduced</p> <p>Monitor the transaction regularly</p> <p>Response: Unacceptable Risk.</p>
Customer has been refused to provide banking facilities by another Bank	Likely	Moderate	=2(Medium)	<p>Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>CDD must be ensured & EDD should be applied</p> <p>Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank.</p> <p>Monitor the transaction regularly</p> <p>Response: Acceptable Risk</p>
Accounts of SME, NGOs, Trusts, Charity, Co-operative Societies, MLM Co etc.	Likely	Major	=3(High)	<p>Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>CDD must be ensured & EDD must be applied</p> <p>Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank.</p> <p>Transaction is not allowed until risk is reduced</p> <p>Monitor the transaction regularly</p> <p>Response: Unacceptable Risk.</p>

Risk	Likelihood	Impact	Risk Score	Treatment/Action
A corporate customer whose ownership structure is unusual and excessively complex	Very likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Anonymous account transactions	Very likely	Major	=4(Extreme)	Do not accept as customer
Wholesale Banking Customer				
Entity customer having operations in multiple locations	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction. Verify physically. Encourage to opening the account to the nearest branch. Response: Acceptable Risk
Customers about whom BFIU seeks information (large corporate)	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Report as STR CDD must be ensured & EDD must be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Owner of the entity that are Influential Persons (IPs) and their family members and close associates	Likely	Major	=3(High)	Obtain senior management approval before establishing such business relationship. Transaction is not allowed until risk is reduced Verify source of fund. Report as STR CDD must be ensured & EDD must be applied. Monitor the Transaction. Response: Unacceptable Risk.



Risk	Likelihood	Impact	Risk Score	Treatment/Action
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly.. Response: Unacceptable Risk.
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Report as STR Response: Unacceptable Risk.
A customer whose identification is difficult to Check.	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Owner of the entity that are Politically Exposed Persons (PEPs) or Influential Persons (IPs)/ chief / senior officials of International Organizations and their family members and close associates	Likely	Major	=3(High)	Obtain senior management approval before establishing such business relationship. Verify source of fund. Report as STR CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Monitor the Transaction. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Charities or NPOs (especially operating in less privileged areas).	Likely	Major	=3(High)	<p>Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD must be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.</p>
Credit Card Customer				
Customer who changes static data frequently	Likely	Major	=3(High)	<p>Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Response: Unacceptable Risk.</p>

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Credit Card customer	Likely	Major	=3(High)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Response: Acceptable Risk
Prepaid Card customer	Likely	Minor	=1(Low)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied. Monitor transaction. Response: Acceptable Risk

[Handwritten Signature]



International Trade Customer				
A new customer (Outward remittance-through SWIFT)	Likely	Moderate	=2(Medium)	<p>CDD must be ensured & EDD should be applied.</p> <p>Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>Monitor the transaction.</p> <p>To check the name of the beneficiary in the sanctioned list</p> <p>Marked as STR if the customer not provide the required documents</p> <p>Obtain the information regarding purpose of remittance.</p> <p>Response: Acceptable Risk</p>
A new customer (Import/Export)	Likely	Moderate	=2(Medium)	<p>CDD must be ensured & EDD should be applied.</p> <p>Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>To check the name of the beneficiary / applicant in the sanctioned list</p> <p>Monitor the transaction.</p> <p>Valid IRC & ERC should be obtained.</p> <p>Response: Acceptable Risk</p>
A new customer (Inward remittance-through SWIFT)	Likely	Moderate	=2(Medium)	<p>CDD must be ensured & EDD should be applied.</p> <p>Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>To check the name of the remitter in the sanctioned list</p> <p>Monitor the transaction.</p> <p>Marked as STR if the customer not provide the required documents</p> <p>Response: Acceptable Risk</p>
A new customer who wants to carry out a large transaction (Import/ Export)	Likely	Moderate	=2(Medium)	<p>CDD must be ensured & EDD should be applied.</p> <p>Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>To check the name of the beneficiary / applicant in the sanctioned list</p> <p>Monitor the transaction.</p> <p>Valid IRC & ERC should be obtained.</p> <p>Response: Acceptable Risk</p>

A new customer who wants to carry out a large transaction (Inward/ outward remittance)	Likely	Major	=3(High)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank To check the name of the beneficiary / remitter in the sanctioned list Monitor the transaction. Report as STR if the customer not provide the required documents Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
A customer wants to conduct business beyond its line of business (import/ export/ remittance)	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. IRC & ERC should be obtained. Report as STR if the customer not provide the required documents Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	Likely	Major	=3(High)	Obtain senior management approval before establishing such business relationship. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify source of fund. Monitor the transaction. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.

[Handwritten signature]



Correspondent Banks	Likely	Moderate	=2(Medium)	<p>To be satisfied about the nature of the business of the correspondent through collection of information.</p> <p>Obtain senior management approval before establishing correspondent relationship.</p> <p>No relation with Shell Bank.</p> <p>CDD must be ensured & EDD must be applied before establishing correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standard for the prevention of Money Laundering & Terrorist Financing.</p> <p>Obtain the extensive information about their policies & procedures on prevention of Money Laundering & Terrorist Financing.</p> <p>Response: Acceptable Risk</p>
Money services businesses (remittance houses, exchange houses)	Likely	Moderate	=2(Medium)	<p>To be satisfied about the nature of the business of the correspondent through collection of information.</p> <p>Obtain senior management as well as Bangladesh Bank approval before establishing Agency arrangement</p> <p>No relation with Shell Bank.</p> <p>CDD must be ensured & EDD must be applied before establishing Agency arrangement with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standard for the prevention of Money Laundering & Terrorist Financing.</p> <p>Obtain the extensive information about their policies & procedures on prevention of Money Laundering & Terrorist Financing.</p> <p>Response: Acceptable Risk</p>

[Handwritten signature]



[Handwritten signature]

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

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)	Likely	Major	=3(High)	Obtain information of Beneficiary Owner. Verify source of income. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Gift Cheque	Likely	Minor	=1(Low)	Check Standard ID(NID/passport/, Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied. Obtain information of Beneficiary before payment Response: Acceptable Risk
Locker Service	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk
Foreign currency endorsement in Passport	Likely	Minor	=1(Low)	The customer should be account holder or relative of account holder. Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied. Response: Acceptable Risk

Large transaction in the account of under privileged people	Likely	Major	=3(High)	Verify source of income. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Marked as STR Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
FDR (less than 2 million)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Response: Acceptable Risk
FDR (2 million and above)	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Special scheme deposit accounts opened with big installment and small tenure	Likely	Moderate	=2(Medium)	Verify the source of fund. CDD should be ensured Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Report as STR Response: Acceptable Risk
Multiple deposit scheme accounts opened by same customer in a branch	Likely	Moderate	=2(Medium)	Verify the source of fund. CDD should be ensured Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Report as STR Response: Acceptable Risk

[Handwritten Signature]



Multiple deposit scheme accounts opened by same customer from different location	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced. Marked as STR Response: Unacceptable Risk.
Open DPS in the name of family member Or Installments paid from the account other than the customer's account	Likely	Major	=3(High)	Obtain the information of Beneficiary Owner. Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Stand-alone DPS	Likely	Moderate	=2(Medium)	CDD should be ensured Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk
Early encashment of FDR, special scheme etc.	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk
Non face to face business relationship/transaction	Very Likely	Major	=4(Extreme)	Do not accept business relationship. Response: Unacceptable Risk
Payment received from unrelated/un-associated third parties	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.

[Handwritten Signature]



Retail Privilege Facilities				
Pre- Approved Credit Card with BDT 300K limit	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Enhanced ATM cash withdrawal Limit BDT 100K	Likely	Moderate	=2(Medium)	CDD should be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
SME Banking Product				
Want to open FDR where source of fund is not clear	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Early encashment of FDR	Likely	Minor	=1(Low)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured Response: Acceptable Risk
Repayment of loan EMI from source that is not clear	Likely	Major	=3(High)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.

Repayment of full loan amount before maturity	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Transaction is not allowed until risk is reduced Response: Unacceptable Risk
Loan amount utilized in sector other than the sector specified during availing the loan	Likely	Major	=3(High)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport (if any) acceptable document to the Bank. Report as STR Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	Likely	Major	=3(High)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Unacceptable Risk.
Source of fund used as security not clear at the time of availing loan	Likely	Major	=3(High)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Wholesale Banking Product				
Development of new product & service of bank	Likely	Moderate	=2(Medium)	CDD should be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk

Payment received from unrelated third parties	Likely	Major	=3(High)	Transaction is not allowed until risk is reduced CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Report as STR Response: Unacceptable Risk.
High Value FDR	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Term loan, SOD(FO), SOD(G-work order), SOD(Garment),SOD(PO), Loan General, Lease finance, Packing Credit, BTB L/C	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
BG(bid bond), BG(PG), BG(APG)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
L/C subsequent term loan, DP L/C	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Verify the documents Response: Acceptable Risk

C.C(H), SOD(G-Business), STL	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Verify the value of mortgage property. Response: Acceptable Risk
OBU	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Syndication Financing	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the documents Monitor the transaction. Response: Acceptable Risk
Credit Card				
Supplementary Credit Card Issue	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Frequent use of Card Cheque	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk

[Handwritten Signature]



BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Credit card issuance against ERQ and RFCD accounts	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
International Trade				
Line of business mismatch (import/export/remittance)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Under/ Over invoicing (import/export/remittance)	Likely	Major	=3(High)	Verify the price of goods/services quoted in the invoice. Monitor the transaction. CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Unacceptable Risk.
Retirement of import bills in cash (import/export/remittance)	Likely	Moderate	=2(Medium)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk

Wire transfer	Likely	Moderate	=2(Medium)	<p>CDD must be ensured & EDD should be applied.</p> <p>In case of threshold cross-border wire transfer of 1000 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.</p> <p>In case of threshold domestic wire transfer of at least 25,000 BDT, full and accurate information of the originator has to be collected & preserved and has to be sent to intermediary/beneficiary bank.</p> <p>For the domestic wire transfers below the threshold full and meaningful originator information has to be preserved.</p> <p>Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>Monitor the transaction.</p> <p>Response: Acceptable Risk</p>
Remittance (Western Union & Others)	Likely	Moderate	=2(Medium)	<p>Check Standard ID (NID /, Birth Registration Certificate along with recent photo ID/ Valid passport (if any) acceptable document to the Bank</p> <p>CDD must be ensured & EDD must be applied.</p> <p>Monitor the transaction.</p> <p>Response: Acceptable Risk</p>
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)	Likely	Major	=3(High)	<p>Check Standard ID (NID /, Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>Monitor the transaction.</p> <p>CDD must be ensured & EDD must be applied.</p> <p>Transaction is not allowed until risk is reduced</p> <p>Response: Unacceptable Risk.</p>

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

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Online (multiple small transaction through different branch)	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
BEFTN	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD should be ensured & EDD should be applied. Response: Acceptable Risk
BACH	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Check TP Response: Acceptable Risk
IDBP	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD should be ensured & EDD should be applied. Comply with circulars issued by Head Office from time to time Response: Acceptable Risk

Mobile Banking	Likely	Moderate	=2(Medium)	<p>Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>Screening Mechanism should be followed to appoint agent or cash point</p> <p>CDD must be ensured & EDD must be applied</p> <p>Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank</p> <p>Response: Acceptable Risk</p>
Third party agent or broker	Likely	Moderate	=2(Medium)	<p>Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>Screening Mechanism should be followed to appoint agent.</p> <p>CDD must be ensured & EDD must be applied</p> <p>Response: Acceptable Risk</p>
Direct contact with the customer	Likely	Minor	=1(low)	<p>Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>CDD should be ensured & EDD should be applied</p> <p>Response: Acceptable Risk</p>
Credit Card				
New Merchant sign up	Likely	Moderate	=2(Medium)	<p>Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>Monitor the transaction.</p> <p>CDD must be ensured & EDD should be applied.</p> <p>Response: Acceptable Risk</p>

[Handwritten signature]



High volume transaction through POS	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk
Alternate Delivery Channel				
Large amount withdrawn from ATMs	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk
Larger amount transaction from different location and different time(mid night) through ATM	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Report as STR Response: Acceptable Risk
Large amount of cash deposit in CDM	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD should be ensured & EDD should be applied. Response: Acceptable Risk
Huge fund transfer through internet	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.

Online/Internet	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD must be applied. Response: Acceptable Risk
Transaction Profile updated through Internet Banking	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Verify customer's email ID. Response: Acceptable Risk
Customer to business transaction-Online Payment Gateway -Internet Banking	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103).	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk

[Handwritten Signature]



4. Risk Register for Country/jurisdiction

Risk	Likelihood	Impact	Risk score	Treatment/Action
Import and export from/to sanction country	Very Likely	Major	=4(Extreme)	Do not accept the business relationship. Response: Unacceptable Risk
Transshipments, container, flag vessel etc. under global sanction	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD must be applied. Response: Unacceptable Risk.
Establishing correspondent relationship with sanction bank and/or country	Very Likely	Major	=4(Extreme)	Do not accept the business relationship. Response: Unacceptable Risk
Establishing correspondent relationship with poor AML&CFT practice country	Likely	Major	=3(High)	Particular attention should be paid & EDD must be applied while establishing a correspondent banking relationship. Detailed information on the beneficial ownership of such banks shall have to be obtained. Extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained. . Approval from senior management should be obtained Transaction is not allowed until risk is reduced Response: Unacceptable Risk.

<p>Customer belongs to higher risk geographic locations such as High Intensity Financial Crime Areas</p>	<p>Likely</p>	<p>Major</p>	<p>=3(High)</p>	<p>CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Monitor the transaction Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.</p>
<p>Customer belongs to countries or geographic areas identified by credible sources a providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.</p>	<p>Likely</p>	<p>Major</p>	<p>=3(High)</p>	<p>CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Transaction is not allowed until risk is reduced Monitor the transaction Report as STR Response: Unacceptable Risk.</p>

[Handwritten signature]



Customer belongs to High Risk ranking countries of the Basel AML index.	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Transaction is not allowed until risk is reduced Monitor the transaction Report as STR Response: Unacceptable Risk
Customer belongs to the countries identified by the bank as higher-risk because of its prior experiences or other factors.	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Monitor the transaction Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Any country identified by FATF or FSRBs- (FATF style Regional Body) as not having adequate AML&CFT systems	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Any bank that provide service to 'Shell Bank'	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk

Any bank that allow payable through account	Likely	Major	=3(High)	Particular attention should be paid & EDD must be applied while establishing a correspondent banking relationship Detailed information on the beneficial ownership of such banks shall have to be obtained. . Extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained. . Approval from senior management should be obtained CDD must be ensured Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Any country identified as destination of illicit financial flow	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Branches in a Border Area	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Physical verification. Response: Acceptable Risk
Area identified as high risk in the NRA	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Countries subject to UN embargo/sanctions	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk

[Handwritten Signature]



[Handwritten Signature]

Publicly known vulnerable areas	Likely	Major	=3(High)	<p>Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank</p> <p>CDD must be ensured & EDD must be applied</p> <p>Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank</p> <p>Physical verification. Transaction is not allowed until risk is reduced Response: Unacceptable Risk.</p>
Drug (Source, Destination & Trafficking Countries)	Very Likely	Major	=4(Extreme)	<p>Do not accept as customer</p> <p>Response: Unacceptable Risk</p>

5. Register for Regulatory Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML/CFT guideline	Unlikely	Major	=2(Medium)	There must have AML/CFT Guidelines in the Bank.
Not forming a Central Compliance Unit (CCU)	Unlikely	Major	=2(Medium)	CCU must be formed in the Bank.
Not having an AML&CFT Compliance Officer	Unlikely	Major	=2(Medium)	There must have a BAMLCO of all the Branches of the Bank.
Not having Branch Anti Money Laundering Compliance Officer	Unlikely	Major	=2(Medium)	There must have a BAMLCO of all the Branches of the Bank.
Not having an AML&CFT program	Unlikely	Major	=2(Medium)	The concerned Department will ensure AML/CFT compliance program
No senior management commitment to comply with MLP and AT Act	Unlikely	Major	=2(Medium)	There must have senior management commitment to comply with MLP and AT Act
Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	Unlikely	Major	=2(Medium)	All AML/BFIU circular must be followed.

Not complying Freezing order issued by BFIU	Unlikely	Major	=2(Medium)	All Branches/ Divisions at Head Office must comply Freezing order issued by BFIU
Unique account opening form not followed while opening account	Unlikely	Major	=2(Medium)	All branches must follow unique account opening form while opening the account.
Non screening of new and existing customers against UNSCR Sanction and OFAC lists	Unlikely	Major	=2(Medium)	All branches must screen new and existing customers against UNSCR Sanction and OFAC lists
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Unlikely	Major	=2(Medium)	All branches must follow Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.
Complete and accurate information of customer not obtained	Unlikely	Major	=2(Medium)	All branches must obtain complete and accurate information of customer.
Failure to verify the identity proof document and address of the customer	Very likely	Major	=4(Extreme)	Close the account. Response: Unacceptable Risk
Beneficial owner identification and verification not done properly	Likely	Major	=3(High)	Check Standard ID (NID/passport/, Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Identification & verification to be done through thanks letter or physical verification (if necessary) Monitor the transaction. CDD must be ensured & EDD must be applied. Report STR. Response: Unacceptable Risk.
Customer/ Beneficial owner identification & verification not done properly	Unlikely	Major	=2(Medium)	Maintain KYC properly. Identification & verification to be done through thanks letter or physical verification (if necessary) Response: Acceptable Risk
Customer Due Diligence (CDD) not practiced properly	Unlikely	Major	=2(Medium)	CDD must be ensured & EDD must be applied properly. Response: Acceptable Risk
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.)	Unlikely	Major	=2(Medium)	EDD must be applied in case of all High Risk customers. Response: Acceptable Risk

Bod



Failure to complete KYC of customer including walk in customer	Likely	Moderate	=2(Medium)	Monitor the transaction. CDD should be ensured & EDD must be applied. Report as STR. Response: Acceptable Risk
Failure to update TP and KYC of customer	Likely	Moderate	=2(Medium)	Monitor the transaction. CDD must be ensured & EDD should be applied. Marked as stop payment Report STR. Response: Acceptable Risk
Keep the legacy accounts operative without completing KYC	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Mark the account as dormant. Response: Acceptable Risk
Failure to assess the ML & TF risk of a product or service before launching	Unlikely	Moderate	=1(Low)	AML/CFT guidelines must be followed while launching product or service. Response: Acceptable Risk
Failure to complete the KYC of Correspondent Bank	Very likely	Major	=4(Extreme)	Do not establish business relationship. Response: Unacceptable Risk
Senior Management approval not obtained before entering into a Correspondent Banking relationship	Very likely	Major	=4(Extreme)	Do not establish business relationship. Response: Unacceptable Risk
Failure to comply with the instruction of BFIU by bank Foreign subsidiary	likely	Major	=3(High)	Foreign subsidiary must be complied with the instruction of BFIU. Response: Unacceptable Risk.
Failure to keep record properly	Unlikely	Major	=2(Medium)	Preserve all records relevant with the account for 5 years after closer the account. Response: Acceptable Risk
Failure to report complete and accurate CTR on time	Unlikely	Major	=2(Medium)	The Bank shall be more careful to report complete accurate CTR on time. Response: Acceptable Risk
Failure to review CTR	Unlikely	Major	=2(Medium)	The Bank shall be more careful to review CTR . Response: Acceptable Risk
Failure to identify and monitor structuring	Unlikely	Major	=2(Medium)	The Bank shall be more careful to identify and monitor structuring Monitor the transaction. Response: Acceptable Risk

Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Unlikely	Major	=2(Medium)	The Bank shall be more careful for the timely detection and reporting of suspicious activity Monitor the transaction. Response: Acceptable Risk
Failure to conduct quarterly meeting properly	Unlikely	Major	=2(Medium)	Conduct quarterly meeting properly. Response: Acceptable Risk
Failure to report suspicious transactions	Unlikely	Major	=2(Medium)	The Bank shall be more careful to report STR duly.
Failure to conduct self-assessment properly	Unlikely	Major	=2(Medium)	Conduct self-assessment properly. Response: Acceptable Risk
Failure to submit statement/report to BFIU on time	Unlikely	Major	=2(Medium)	Accountability of the concerned department should be introduced to ensure submission of all required reports to BFIU in time. Response: Acceptable Risk
Submit erroneous statement/report to BFIU	Unlikely	Major	=2(Medium)	All Branches/Divisions at Head Office must submit accurate information requested by BFIU Response: Acceptable Risk
Not complying with any order for freezing or suspension of transaction issued by BFIU or	Unlikely	Major	=2(Medium)	All branches must complied BFIU or BB instructions. Response: Acceptable Risk
Not submitting accurate information or statement sought by BFIU or BB.	Unlikely	Major	=2(Medium)	Accurate information or statement must be submitted to BFIU or BB as per requirement. Response: Acceptable Risk
Not submitting required report to senior management regularly.	Likely	Moderate	=2(Medium)	Required reports must be submitted to senior management regularly. Response: Acceptable Risk
Failure to rectify the objections raised by BFIU or bank inspection teams on time	Likely	Major	=3(High)	All objections raised by BFIU or bank inspection teams must be rectified on time Response: Acceptable Risk
Failure to obtain information during wire transfer	Likely	Major	=3(High)	Obtain information of applicant & Beneficiary. Stop the Transaction. Transaction is not allowed until risk is reduced Response: Unacceptable Risk
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely	Major	=3(High)	Obtain information of applicant & Beneficiary. Preserve the information for minimum 5 years. Response: Unacceptable Risk.

Failure to scrutinize staff properly	Unlikely	Major	=2(Medium)	Concerned division will scrutinize staff properly before appointment. Response: Acceptable Risk
Failure to circulate BFIU guidelines and circulars to branches	Unlikely	Major	=2(Medium)	Concerned division must circulate BFIU guidelines and circulars to branches. Response: Acceptable Risk
Inadequate training/workshop arranged on AML & CFT	Unlikely	Major	=2(Medium)	Bank shall take adequate measure to provide proper training to Staff members. Response: Acceptable Risk
No independent audit function to test the AML program	Unlikely	Major	=2(Medium)	Bank must be introduced to independent audit function to test the AML program. Response: Acceptable Risk

[Handwritten Signature]



[Handwritten Signature]

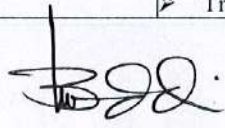
Annexure-B

KYC DOCUMENTATION

Customer type	Standard Identification document	document for verification of source of funds	Document or strategy for verification of address
Individuals	<ul style="list-style-type: none"> ➤ Passport ➤ National ID Card ➤ Birth Registration certificate (printed copy, with seal & signature from the registrar) ➤ Valid driving license (if any) ➤ Credit Card (if any) ➤ Any other document that satisfy to the bank. <p>NB: But in case of submitting the birth registration certificate, any other photo id (issued by a Government department or agency) of the person has to be supplied with it. If he does not have a photo id, then a certificate of identity by any renowned people has to be submitted according to the bank's requirement. That certificate must include a photo which is duly attested by the signing renowned person. 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 contract address and phone number.</p>	<ul style="list-style-type: none"> ➤ Salary certificate (for salaried person). ➤ Employed ID (for ascertaining level of employment). ➤ Self-declaration acceptable to the bank (commensurate with declared occupation) ➤ Document in support of beneficial owner's income (income of house wife, students etc.) ➤ Trade license if the customer declared to be a business person ➤ TIN (If any) ➤ Documents of property sale (if any) ➤ Other Bank statement (If any) ➤ Documents of FDR encashment (If any) ➤ Documents of foreign remittance (if any fund comes from outside the country) ➤ Documents of retirement benefit ➤ Bank loan 	<ul style="list-style-type: none"> ➤ Acknowledgement receipt of thanks letter through postal department. ➤ Proof of delivery of thanks letter through courier. ➤ Third party verification report of bank official ➤ 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 applicant or his/her parent's name. ➤ Residential 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
Joint Account	<ul style="list-style-type: none"> ➤ Passport ➤ National ID Card ➤ Birth Registration certificate (printed copy, with seal & signature from the registrar) ➤ Valid driving license (if any) ➤ Credit Card (if any) ➤ Any other document that satisfy to the bank. 	<ul style="list-style-type: none"> ➤ Salary certificate (for salaried person). ➤ Employed ID (for ascertaining level of employment). ➤ Self-declaration acceptable to the bank (commensurate with declared occupation) ➤ Document in support of beneficial owner's income (income of house wife, students etc.) ➤ Trade license if the customer declared to be a business person ➤ TIN (If any) ➤ Documents of property sale (if any) ➤ Other Bank statement (If any) ➤ Documents of FDR encashment (If any) ➤ Documents of foreign remittance (if any fund comes from outside the country) ➤ Documents of retirement benefit ➤ Bank loan 	<ul style="list-style-type: none"> ➤ Acknowledgement receipt of thanks letter through postal department. ➤ Proof of delivery of thanks letter through courier. ➤ Third party verification report of bank official ➤ 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 applicant or his/her parent's name. ➤ Residential 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
Sole Proprietorships or Individuals doing business	<ul style="list-style-type: none"> ➤ Passport ➤ National ID Card ➤ Birth Registration certificate (printed copy, with seal & signature from the registrar) ➤ Valid driving license (if any) ➤ Credit Card (if any) ➤ Rent receipt of the shop (if the shop in the rental) ➤ Ownership document of the shop (i.e purchase document of the shop or inheritance documents) ➤ Membership certificate of any association (Chamber of commerce, market association, trade association i.e.; hardware association, cloth merchant association, hawker's association etc.) ➤ Any other documents that satisfy to the bank. 	<ul style="list-style-type: none"> ➤ Trade license ➤ TIN (If any) ➤ 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) ➤ Documents of FDR encashment (If any fund injected by encashing personal FDR) ➤ Documents of foreign remittance (if any fund comes from outside the country) ➤ Bank Loan (if any) ➤ Personal Borrowing (if any) 	<ul style="list-style-type: none"> ➤ Acknowledgement receipt of thanks letter through postal department. ➤ Proof of delivery of thanks letter through courier. ➤ Third party verification report of bank official ➤ 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 applicant or his/her parent's name. ➤ Residential address appearing on an official document prepared by a Government agency.
Partnership	<ul style="list-style-type: none"> ➤ Partnership deed/ partnership letter ➤ Registration Partnership deed (if registered) ➤ Resolution of 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 in the rental) ➤ Ownership document of the shop (i.e purchase document of the shop or inheritance documents) ➤ Membership certificate of any association (Chamber of commerce, market association, trade association i.e.; hardware association, cloth merchant association, hawker's association etc.) ➤ Any other documents that satisfy to the bank. 	<ul style="list-style-type: none"> ➤ Trade license ➤ TIN (If any) ➤ Documents of property sale. (if injected any fund by selling personal property) ➤ Documents of FDR encashment (If any fund injected by encashing personal FDR) ➤ Documents of foreign remittance (if any fund comes from outside the country) ➤ Bank Loan (if any) ➤ Personal Borrowing (if any) 	<ul style="list-style-type: none"> ➤ Acknowledgement receipt of thanks letter through postal department. ➤ Proof of delivery of thanks letter through courier. ➤ Third party verification report of bank official ➤ 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 applicant or his/her parent's name. ➤ Residential address appearing on an official document prepared by a Government agency.
Private Limited Companies	<ul style="list-style-type: none"> ➤ Passport of all the directors ➤ National ID Card of all the directors ➤ Certificate of incorporation ➤ Memorandum and articles of association ➤ List of directors 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly authenticated by competent authority ➤ Other Bank statement ➤ Trade License 	




	<ul style="list-style-type: none"> ➤ Resolution of the board director of directors to open an account and identification of those who have authority to operate the account ➤ Power of attorney granted to its managers, official or employees to transact business on its behalf ➤ Nature of the company's business ➤ Expected monthly turnover ➤ Identify of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or instruction the signatories of the account act where such persons may not be a full time employee, officer or director of the company 	<ul style="list-style-type: none"> ➤ TIN ➤ VAT registration ➤ Bank loan 	
Public Limited Companies	<ul style="list-style-type: none"> ➤ Passport of all the directors ➤ 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 director of directors to open an account and identification of those who have authority to operate the account ➤ Power of attorney granted to its managers, official or employees to transact business on its behalf ➤ Nature of the company's business ➤ Expected monthly turnover ➤ Identify of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instruction the signatories of the account act where such persons may not be a full time employee, officer or director of the company. 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly authenticated by professional accountant. ➤ Other Bank statement (if any) ➤ Trade License ➤ TIN ➤ VAT registration ➤ Bank loan ➤ Any other genuine source 	
Government – owned entities	<ul style="list-style-type: none"> ➤ Statue of formation the entity ➤ Resolution of the board director of directors to open an account and identification of those who have authority to operate the account ➤ Passport of the operator (s) ➤ National ID Card of the operator (s) 	N/A	N/A

<p>NGO</p>	<ul style="list-style-type: none"> ➤ National ID Card of the operator (s) ➤ Passport of the operator (s) ➤ Resolution of the board director of directors to open an account and identification of those who have authority to operate the account ➤ Documents of nature of the NGO ➤ Certificate of registration issued by competent authority ➤ Bye-laws (certificate) ➤ List of Management Committee/ Director 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certificate by a professional accountant. ➤ Other Bank statement ➤ TIN ➤ Certificate of Grand/Aid 	
<p>Charities or Religious Organization</p>	<ul style="list-style-type: none"> ➤ National ID Card of the operator (s) ➤ 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 (certificate) ➤ List of Management Committee/ Director 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certificate by a professional accountant. ➤ Other Bank statement ➤ Certificate of Grand/Aid donation ➤ Any other legal source 	
<p>Clubs or Societies</p>	<ul style="list-style-type: none"> ➤ National ID Card of the operator (s) ➤ 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 (certificate) ➤ List of Management Committee/ Director 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certificate by a professional accountant. ➤ Other Bank statement ➤ Certificate of Grand/Aid Subscription ➤ If unregistered declaration of authorities person/body. 	
<p>Trusts Foundations or similar entities</p>	<ul style="list-style-type: none"> ➤ National ID Card of the operator (s) ➤ Passport of the operator (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 ➤ Certified true copy of the trust Deed ➤ Bye-laws (certificate) ➤ Power of attorney allowing transaction in the account. 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certificate by a professional accountant. ➤ Other Bank statement ➤ Donation 	
<p>Financial Institutions (NBFI)</p>	<ul style="list-style-type: none"> ➤ Passport of all the directors ➤ National ID Card of all the directors ➤ Certificate of incorporation ➤ Memorandum and articles of association 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certificate by a professional accountant. ➤ Other Bank statement ➤ Trade Licence ➤ TIN ➤ VAT registration 	

<ul style="list-style-type: none"> ➤ Certificate of commencement of business ➤ List of directors in form-XII ➤ Resolution of the board director of directors to open an account and identification of those who have authority to operate the account ➤ Power of attorney granted to its managers, official or employees to transact business on its behalf ➤ Nature of the company's business ➤ Expected monthly turnover <p>Identify of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instruction the signatories of the account act where such persons may not be a full time employee, officer or director of the company.</p>	<p>Cash flow statement</p>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------	--

Annexure-C

KYC PROFILE FROM FOR WALK-IN CUSTOMER & ONLINE TRANSACTION

Name	
Mobile No.	
Date of Birth	Nationality
Father's Name	
Mother's Name	
Present Address	
Permanent Address	
Identify Information (NID/Passport/Birth Registration Certificate)	
Type of ID.....	
ID No..... Expiry Date.....	
Weather Photocopy Obtained? Yes / No	
(According to instruction of BFIU Circular No. 26, Copy of Photo ID must have to be obtained for above Tk. 50,000/= (fifty thousand) up to Tk. 5, 00,000/= (five lac) online Transaction.	
Relation with Beneficiary/Account Holder	
Value of Transaction	
Reason of Transaction	

I/We solemnly declare that the information mentioned above is/are correct. I/We shall/will also submit any type of additional information/documents, if required.

Signature with date	
Customer's Full Name	

N.B: In case of issuing Pay Order/DD/TT name and full address of beneficiary must be obtained in application form.

For Bank Use Only

Collect Document Verified	Yes	No
---------------------------	-----	----

[Handwritten Signature]



Annexure-D

SUSPICIOUS TRANSACTION REPORT (STR) FORM

A. Reporting Institution:

- a. Name of the Bank:
- b. 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 of an date of pervious rep

C. Suspect Account Details:

- 1. Account Number:
- 2. Name of the Account:
- 3. Nature of the Account:
(Current/service/FDR/Loan/other. Pls. specify)
- 4. Nature of Ownership:
(Individual/Proprietorship/Partnership/Company/other, pls. specify)
- 4. Date of Opening Transaction:
- 5. Address:

D. Account holders 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. Place of Birth:
- 11. Passport No.
- 12. National Identification No.
- 13. Birth Registration no.
- 14. TIN:

[Handwritten Signature]


2. 1. Name of the Account Holder:

2. Relation with the account
Holder mention is SI, No D1

3. Address:

4. Profession:

5. Nationality:

6. Other Account(s) Number (if any):

7. Other business:

8. Father's Name:

9. Mother's Name:

10. Date of Birth:

11. Place of Birth:

12. Passport No.

13. National Identification No.

14. Birth Registration no.

15. TIN:

E. Introduce Details:

1. Name of introducer:

2. Account Number:

3. Relation with Account Holder:

4. Address:

5. Date of Opening:

6. Whether introduce is maintaining:
good relation with bank



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

- a. Identity of Clients
- b. Activity of 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. <input type="checkbox"/> Corruption and bribery | F. <input type="checkbox"/> Murder, Grievous physics injury | K. <input type="checkbox"/> Terrorism or Financing in terrorist activities |
| B. <input type="checkbox"/> Counterfeiting Currency | G. <input type="checkbox"/> Trafficking of women and children | L. <input type="checkbox"/> Adulteration or the Manufacture of goods through infringement of title |
| C. <input type="checkbox"/> Counterfeiting deeds and document | H. <input type="checkbox"/> Black Marketing | M. <input type="checkbox"/> Offences relating to the environment |
| D. <input type="checkbox"/> Extortion | I. <input type="checkbox"/> Smuggling of domestic and foreign Currency | N. <input type="checkbox"/> Sexual explanation |
| E. <input type="checkbox"/> Fraud | J. <input type="checkbox"/> Threat robbery privacy or hierarchy or aircraft | O. <input type="checkbox"/> Inside Trade and marketing |

[Handwritten signature]
