



Money Laundering & Terrorist Financing Risk Management Guideline-2025

Focus Group

Coordinator:

Mr. Mohammad Ziaul Hasan Molla, CAMS, CSAA
Deputy Managing Director-Channel Banking,
CAMLCO Bank Asia PLC, Corporate Office, Dhaka

Members:

Mr. Md. Rezaul Islam
EVP, DCAMLCO & Head of AML & CFT Division
Bank Asia PLC, Corporate Office, Dhaka

Mr. Nesar Ahmed
FVP, AML & CFT Division
Bank Asia PLC, Corporate Office, Dhaka

Mr. Md. Abdus Sabur Khan
FVP, AML & CFT Division
Bank Asia PLC, Corporate Office, Dhaka

Mr. Sharif Ahmed CDCS, CAMS
AVP, AML & CFT Division
Bank Asia PLC, Corporate Office, Dhaka

Mr. Md. Hashibul Alam CDCS, CAMS
FAVP, AML & CFT Division
Bank Asia PLC, Corporate Office, Dhaka

Preface

A bank should develop a thorough understanding and appropriate techniques to mitigate the inherent Money Laundering (ML) & Terrorist Financing (TF) & Proliferation financing (PF) risks. Policies and procedure for customer acceptance, due diligence and ongoing monitoring should be designed and implemented adequately to control those identified as well as inherent risks.

Bangladesh Bank as the major regulator of the financial system of the country plays a pivotal role to stabilize and enhance the efficiency of the financial system. Considering ML, TF and PF as one of the major threats to the stability and the integrity of the financial system, Bangladesh Financial Intelligence Unit (BFIU) has taken several initiatives including issuance of circulars/circular letters, Guidance Notes under Money Laundering prevention Act (MLPA) and Anti-terrorism Act (ATA). To keep pace with international initiatives MLPA, 2012 (Amendment 2015) and ATA 2009, (amendment 2012 & 2013) have been promulgated and be amended on course if necessary.

To comply with the requirement of Bangladesh Financial Intelligence Unit (BFIU) under the international initiatives, Bank Asia has prepared “Guidelines for Prevention of Money Laundering and Terrorist Financing-2025”. Bank Asia instructs the Branches/Divisions/Departments/SME Service Centers/Islamic Wings/Agent Banking to follow the guideline in order to mitigate Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks.

The purpose of this guidance is to build the legal and regulatory framework for anti-money laundering and combating financing on terrorism (AML & CFT) and thus the documents interpret the requirements of the relevant laws and regulations, and how they might be implemented in practice. It indicates good industry practices in AML and CFT procedures through proper guidance, assists the banks to design & implement the systems and controls necessary to mitigate the risks of the banks being used in connection with Money Laundering, Terrorist Financing and Proliferation Financing.

Table of Contents

Particulars			Page No.
CHAPTER I: BACKGROUND			
1.1		Preamble	1
1.2		Definition Money Laundering	1
1.3		The Economic and Social Consequences of Money Laundering	6
1.4		Stages of Money Laundering	8
1.5		Why Money Laundering is Done	9
1.6		Definition of Terrorist Financing	9
1.7		The Link Between Money Laundering and Terrorist Financing	12
1.8		Why We Must Combat Money Laundering and Terrorist Financing	12
1.9		How Financial Institutions can Combat Money Laundering	13
1.10		How Bank Asia Can Help in Combating Money Laundering, Terrorist Financing and Proliferation Financing	14
1.11		Targeted Financial Sanctions	14
CHAPTER II: INTERNATIONAL INITIATIVES			
2.1		International Initiatives	16
2.2		The United Nations	16
2.3		The Vienna Convention	16
2.4		The Palermo Convention	16
2.5		International Convention for the Suppression of the Financing of Terrorism	16
2.6		Security Council Resolution 1267 and Successors	17
2.7		Security Council Resolution 1373	17
2.8		Security Council Resolution 1540	17
2.9		The Counter-Terrorism Committee	17
2.10		Counter-Terrorism implementation Task Force (CTITF)	18
2.11		Global Program against Money Laundering	18
2.12		The Financial Action Task Force	18
2.13		FATF 40 Recommendations	18
2.14		FATF New Standards	18
	2.14.1	The FATF Recommendations	19
		A. AML & CFT Policies and Coordination	19
		B. Money Laundering and Confiscation	19
		C. Terrorist Financing And Financing of Proliferation	20
		D. Preventive Measures	21
		E. Transparency and Beneficial Ownership of Legal Persons and Arrangements	26
		F. Powers and Responsibilities of Competent Authorities, and Other Institutional Measures Regulation and Supervision	26
		G. International Cooperation	28
2.15		Monitoring Members Progress	28
2.16		The NCCT List	31
2.17		International Cooperation and Review Group (ICRG)	31
2.18		Asia Pacific Group on Money Laundering (APG)	31
2.19		The Egmont Group of Financial Intelligence Units	32
2.20		The Basel Committee on Banking Supervision	32
	2.20.1	Statement of Principles on Money Laundering	33
	2.20.2	Basel Core Principles for Banking	33
	2.20.3	Customer Due Diligence	33
2.21		International Organization of Securities Commissioner	33

CHAPTER III: NATIONAL INITIATIVES			
3.1		National Initiatives	34
3.2		Founding Member of APG	34
3.3		Legal Framework	34
3.4		Central and Regional Taskforces	34
3.5		Anti-Money Laundering Department	34
3.6		Bangladesh Financial Intelligence Unit	35
3.7		National Coordination Committee and Working Committee	35
3.8		National ML & TF Risk Assessment (NRA)	35
3.9		National Strategy for Preventing ML ,TF & PF	35
3.10		Chief Anti Money Laundering Compliance Officers (CAMLCO) Conference	36
3.11		Egmont Group Memberships	36
3.12		Anti-Militants and De-Radicalization Committee	36
3.13		Memorandum of Understanding (MOU) between ACC AND BFIU	36
3.14		NGO/NPO Sector Review	36
3.15		Implementation of TFS	37
3.16		Coordinated Effort on the implementation of the UNSCR	37
3.17		Risk Based Approach	37
3.18		Memorandum of Understanding (MOU) BFIU AND other FIUs	37
CHAPTER IV: VULNERABILITIES OF FINANCIAL INSTITUTIONS			
4.1		Vulnerabilities of the Financial System to Money Laundering	38
4.2		Vulnerabilities of Products and Services	39
	4.2.1	Lease/Term Loan	39
	4.2.2	Factoring	39
	4.2.3	Private Placement of Equity/Securitization of Assets	40
	4.2.4	Personal Loan/Car Loan/Home Loan	40
	4.2.5	SME/Women Entrepreneur	40
	4.2.6	Deposit Scheme	40
	4.2.7	Loan Backed Money Laundering	40
	4.2.8	Electronic Transfers of Funds	40
	4.2.9	Correspondent Banking	41
	4.2.10	Payable through accounts	41
	4.2.11	Crypto-Currencies	42
4.3		Hundi/Hawala	43
4.4		Structural Vulnerabilities	44
CHAPTER V: COMPLIANCE REQUIREMENTS UNDER THE LAW & CIRCULAR			45
5.1		Compliance Requirements Under the law	45
	5.1.1	Money Laundering Prevention Act 2012 (Amendment 2015)	45
	5.1.2	Anti-terrorism Act 2009 (Amendment 2012 & 2013)	48
5.2		Compliance Requirements under Circulars	51
	5.2.1	Policies for Prevention of Money Laundering and Terrorist Financing	51
5.3		Targeted Financial Sanctions	51
5.4		Self-Assessment	52
5.5		Independent Testing Procedure	53
	5.5.1	ICCD's obligations regarding Self-Assessment or Independent Testing Procedure	53
	5.5.2	AML & CFT Division's obligations regarding Self-Assessment or Independent Testing Procedure	53

CHAPTER VI: AML & CFT COMPLIANCE PROGRAM IN BANK ASIA			55
6.1		Bank Asia AML & CFT & CPF Compliance Program	55
6.2		Roles and Responsibilities of Board of Directors	55
6.3		Senior Management Role & Responsibilities	56
6.4		Statement of Commitment of President & Managing Director (MD)	57
6.5		Policy and Procedure	57
	6.5.1	Written AML & CFT Compliance Policy	58
	6.5.2	Procedure	58
6.6		Customer Acceptance Policy	59
6.7		ML & TF Risk Assessment	59
CHAPTER VII: ML & TF RISK ASSESMENT OF BANK ASIA			
7.1		Preamble	60
7.2		Risk	60
7.3		Risk Assessment	60
7.4		Risk Identification	60
7.5		Risk Assessment process	60
	7.5.1	Methodology of Risk Assessment	60
	7.5.1.1	Likelihood Scale	60
	7.5.1.2	Impact of Scale	61
7.6		Risk matrix and risk score	62
7.7		Risk Assessment and Management Exercise	
7.8		Risk Treatment	63
7.9		Monitoring and Review	63
CHAPTER VIII: ML & TF RISK MANAGEMENT OF BANK ASIA			
8.1		Risk Management	64
8.2		Risk management and mitigation	64
8.3		Which Risk do Banks Needs to Manage	64
	8.3.1	Business risk	64
	8.3.2	Regulatory risk	64
8.4		Risk Management Process	64
	8.4.1	Risk Identification	65
	8.4.1.1	Business Risks	65
	8.4.1.2	Regulatory Risks	66
8.5		Risk Management Strategies	66
8.6		Ongoing Risk Monitoring	67
8.7		Higher Risk Scenario	68
	8.7.1	Specific High Risk Elements and Recommendations for EDD	68
8.8		Low Risk Scenario	69
8.9		Risk Variables	70
8.10		Counter Measures for Risks	70
CHAPTER IX : COMPLIANCE STRUCTURE OF BANK ASIA			
9.1		Central Compliance Committee	71
9.2		Formation of Central Compliance Committee (CCC)	71
9.3		Responsibilities and Authorities of the CCC	72
9.4		Chief Anti Money Laundering Compliance Officer (CAMLCO)	73
9.5		Authorities and Responsibilities of CAMLCO	74
9.6		Branch Anti Money Laundering Compliance Officer (BAMLCO)	74

9.7		Responsibilities and Authorities of BAMLCO	75
9.8		Internal Control and Compliance	75
9.9		Employee Training and Awareness Program	79
CHAPTERX: CUSTOMER DUE DILIGENCE			
10.1		Preamble	81
10.2		Legal Obligations of CDD	82
10.3		General Rule of CDD	82
10.4		Timing of CDD	84
10.5		Transaction Monitoring	84
10.6		Exception when opening a bank account	85
10.7		In case where conducting the CDD measure is not possible	85
10.8		Customer Identification	86
10.9		Verification of Source of Funds	86
10.10		Verification of Address	86
10.11		Persons without Standard Identification Documentation	86
10.12		Walk-in/one off Customers	87
10.13		Non Face to Face Customers	87
10.14		Customer Unique Identification Code	87
10.15		Corresponding Banking	88
10.16		Politically Exposed Persons (PEPs), Influential Persons and Chief Executives or Top Level Officials of any International Organization	88
10.17		Wire Transfer	88
	10.17.1	Cross-Border Wire Transfers	89
	10.17.2	Domestic Wire Transfers	89
	10.17.3	Duties of Ordering, Intermediary and Beneficiary Bank in case of Wire Transfer	89
10.18		CDD for Beneficial Owner	90
10.19		Management of Legacy Accounts	90
CHAPTER XI : RECORD KEEPING			
11.1		Statutory Requirement	91
11.2		Legal Obligation	92
11.3		Obligations under Circulars	93
11.4		Records to be kept	93
11.5		Customer Information	93
11.6		Transactions	94
11.7		STR/SAR and Investigation	94
11.8		Internal & External Reports	94
11.9		Other Measures	94
11.10		Formats and Retrieval of Records	94
11.11		Training Records	94
CHAPTER XII: REPORTING TO BFIU			
12.1		Legal Obligations	96
12.2		Suspicious Transaction Reporting	96
12.3		Identified of STR/SAR	96
12.4		Tipping Off	99
12.5		Cash Transaction Report	99
12.6		Self-Assessment Report	99
12.7		Independent Testing Procedure	99
12.8		ICCD's obligations regarding Self-Assessment or Independent Testing Procedure	100
12.9		AML & CFT Division's obligations regarding Self-Assessment or Independent Testing	100

CHAPTER IX- Politically Exposed Persons (PEPs)			
13.1		Purpose	101
13.2		Politically Exposed Persons	101
	13.2.1	Who are Politically Exposed Persons (PEPs)	101
	13.2.2	Chief or similar high-ranking positions in an international organization.	102
	13.2.3	Who should be considered a family member of a PEP?	102
	13.2.4	Close associates' of a PEP	102
13.3		Various scenario related with PEPs/IPs	102
13.4		PEPs versus Risk	103
	13.4.1	Do all PEPs pose the same risk	103
	13.4.2	What are some indicators that a PEP might pose a lower risk	103
	13.4.3	What are indicators that a PEP might pose a higher risk	103
	13.4.4	What are some indicators that a PEP's family or known close associates pose a	104
	13.4.5	What are some indicators that a PEP's family or known close associates pose a	104
13.5	13.5.1	What are reporting organizations' obligations under the Regulations	104
	13.5.2	What measures may reporting organizations take in lower risk situations	105
	13.5.3	What measures may reporting organizations take in higher risk situations	105
	13.5.4	Long-term insurance contracts	105
	13.5.5	Beneficial owners of legal entities who are PEPs	106
13.6		Case Example	106
	13.6.1	A foreign national prosecuted in another country for bribery	106
	13.6.2	Proceed of corruption in one country traced as financial asset in another country	106
CHAPTER XIV : Beneficial Owner			
14.1		Legal Authority	107
14.2		Introduction	107
14.3		Who is a beneficial owner	108
14.4		Why is it important to identify the beneficial owner	108
14.5		Ways in which beneficial ownership information can be hidden/obscured	108
14.6		Ownership	109
14.7		Effective Control	111
14.8		Person on whose behalf a transaction is conducted	112
14.9		Beneficial owner of legal arrangements	113
14.10		Applying a risk based approach	113
14.11		Customer Due Diligence	114
14.12		Record Keeping	114
14.13		Example	115
14.14		Question/Answer	115
CHAPTER XI: e-KYC			
15.1		Introduction	118
	15.1.1	Background	118
	15.1.2	Scope	119
	15.1.3	Objective	120
15.2		e-KYC Process	121
	15.2.1	Definitions	121

	15.2.2	Process	121
	15.2.3	Applicability	121
15.3		Customer on Boarding-Simplified	124
	15.3.1	Customer on boarding models	124
	15.3.2	Customer on boarding by using fingerprint	124
	15.3.3	Customer on Boarding- by using face matching	127
15.4		Customer on boarding-regular measure	130
	15.4.1	Required Technology	131
	15.4.2	Sanctions and other screening	131
	15.4.3	Audit trail of customer profile	131
	15.4.4	Matching parameters	132
	15.4.5	Security measures	132
15.5		Other relevant issues	132
	15.5.1	Record Keeping	132
	15.5.2	Reliance on third parties	132
	15.5.3	Risk Assessment	133
	15.5.4	Implementation	133
	15.5.5	Transformation of existing clients CDD	133
15.6		e-KYC Profile- Simplified and Regular	
	15.6.1	Sample e-KYC output for simplified measures	134
	15.6.2	Sample e-KYC output for regular measures	135
	15.6.3	Customer Risk Grading Risk Grading Form	136
CHAPTERXVI: RECRUITMENT, TRAINING AND AWARENESS			
16.1		Obligations under Circular	138
16.2		Employee Screening	138
16.3		Know Your Employee (KYE)	138
16.4		Training for Employee	138
16.5		Awareness of Senior Management	139
16.6		Customer Awareness	139
16.7		Awareness of Mass People	139
CHAPTERXVII: TERRORIST FINANCING & PROLIFERATION FINANCING			
17.1		Preamble	143
17.2		Legal Obligations	143
17.3		Obligations under Circular	143
17.4		Necessity of Funds by Terrorist	143
17.5		Source of Fund/Raising of Fund	144
17.6		Movement of Terrorist Fund	144
	17.6.1	Formal Financial Sector	144
	17.6.2	Trade Sector	144
	17.6.2	Cash Couriers	144
	17.6.4	Use of Alternative remittance systems (ARS)	144
	17.6.5	Use of Charities and Non Profit Organizations	145
17.7		Targeted Financial Sanctions	145
	17.7.1	TFS related to terrorism and terrorist financing	145
	17.7.2	TFS related to Proliferation	145
		Automated Screening Mechanism of UNSCRs	145
		Responsibilities of Bank Officials for detection and Prevention of Financing	146
		Role of Bank Asia in Preventing TF & PF	147
		List of Abbreviations	148
		Risk Register	
		Annexure A: KYC Documentation	

CHAPTER I: BACKGROUND

1.1 Preamble:

Financial sector plays an indispensable role in the overall development of a country. The most important constituent of this sector is the financial institutions, which acts as a conduit for the transfer of resources from net savers to net borrowers. The financial institutions have traditionally been the major source of long term funds for the economy. FIs provide variety of financial products and services to fulfil the varied needs of the commercial sector.

Financial institutions may be unwittingly used as intermediaries for the transfer or deposit of funds derived from or associated with drug trafficking, terrorism and other criminal activity. Criminals and their associates use the financial system to make payments and transfers of funds from one account to another, to hide the source and beneficiary's ownership of money. These activities are commonly referred to as "money laundering."

The branches should put in place effective procedures to ensure that all persons conducting business with the Bank are properly identified; that transactions which do not appear to be legitimate are discouraged.

Money Laundering and Terrorist Financing have become very vital issue in recent years. Money laundering is employed by launderers worldwide to conceal the illicit money flow earned by unlawful activities. It may happen in almost every country in the world and the scheme typically involves transferring money through several countries in order to obscure its illicit origins. The rise of global financial markets makes money laundering easier than the imagination, making it possible to anonymously deposit "dirty" money in one country and then have it transferred to any other country for use.

After the most dreadful terrorist attack occurred on 11th September, 2001, combating money laundering and financing of terrorism got heightened focus and international response to protect these types of activities has been increased day by day.

It is widely acknowledged to be an essential component of terrorist activity as terrorists are able to facilitate their activities only if they have the financial resources to do so. The consequences of terrorist activities are terrific and devastating. So, prevention of ML & TF are very much essential for the economy and also for the security reason of our country. Recently another issue has come up and that is proliferation financing.

The process of ML, TF & PF is very much faster and ever evolving. The money launderers and terrorist financiers are inventing more and more complicated and sophisticated procedures as well as using new technology for ML and TF. To address these emerging challenges, the global community has taken various initiatives against ML, TF & PF. In accordance with international initiatives, Bangladesh has also acted on many fronts.

1.2 Definition of Money Laundering:

Money laundering can be defined in a number of ways. But the fundamental concept of Money Laundering refers to the methods criminals use to hide and disguise money constructing from crime or illegitimate source. If it is successful, then the identity of money can be disguised and ultimately appears to legitimate. The term "laundering" is used when criminals turn their "dirty" criminal money into 'clean' funds without arousing suspicion. Getting it into the financial system means that it becomes harder to trace and confiscate. Drug traffickers, terrorists, armed robbers, burglars and fraudsters all tend to launder the proceeds of their crimes through banking channels.

Illegal arms sales, smuggling and the activities of organized crime, including for example, drug trafficking and prostitution can generate huge funds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering. When a criminal activity generates substantial profits, the individual or group involvement must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where its trail can be

disguised. In summary, the money launderer wants to:

- place his/ her money in the financial system, without arising suspicion;
- move the money around, often in a series of complex transactions crossing multiple jurisdictions, so it becomes difficult to identify its original source; and
- then move the money back into the financial and business system, so that it appears as legitimate funds or assets.

Most countries subscribe to the following definition which was 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 offence, e.g. drug trafficking, or offences or from an act of participation in such offence or offences, 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 offence or offences to evade the legal consequences of his/her actions;
- The concealing or disguising the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences or from an act of participation in such an offence or offences, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offence or offences or from an act of participation in such offence or offences.

The Financial Action Task Force (FATF), which is recognized as the international standard setter for Anti Money Laundering (AML) efforts, defines the term "money laundering" succinctly as "the processing of criminal proceeds to disguise their illegal origin" in order to "legitimize" the ill-gotten gains of crime. It is notable that AML related definition which will be issued or Act be promulgated by our regulator in future be included in this guide book or manual is considered as approved.

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

"Money Laundering" means -

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

any offence(s) mentioned above;

"Property" has been defined in Section 2 (bb) of the Money Laundering Prevention Act 2012, (Amendment 2015) as –**"Property"** means –

- i) Any type of tangible, intangible, moveable, immoveable, property; or
- ii) cash, any deed or legal instrument of any form including electronic or digital form giving evidence of title or evidence of interest related to title in the property which is located within or outside the country.

"Predicate Offence" is defined in Section 2 (cc) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as follows:

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

01.	Corruption and bribery;	16.	Human Trafficking or obtaining money or trying to obtain money or valuable goods giving someone false
02.	Counterfeiting currency;	17.	Dowry;
03.	Counterfeiting deeds and documents;	18.	Smuggling and offences related to customs and excise duties;
04.	Extortion;	19.	Tax related offences;
05.	Fraud;	20.	Infringement of intellectual property rights;
06.	Forgery;	21.	Terrorism or financing in terrorist activities;
07.	Illegal trade of firearms;	22.	Adulteration or the manufacture of goods through
08.	Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;	23.	Offences relating to the environment;
09.	Illegal trade in stolen and other goods;	24.	Sexual exploitation;
10.	Kidnapping, illegal restrain and hostage taking;	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;
11.	Murder, grievous physical injury;	26.	Organized crime, and participation in organized criminal groups;
12.	Trafficking of women and children;	27.	Racketeering; and
13.	Black marketing ;	28.	Cyber Crime
14.	Smuggling of domestic and foreign currency;	29.	Pornography
15.	Theft or robbery or dacoity or piracy or hijacking of aircraft;	30.	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.

“Smuggling of fund or Property” has been defined in Section 2 (a) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as --**“Smuggling of money or Property”** means –

- i) Transfer or holding money or property outside the country in breach of the existing laws in the country; or
- ii) Refrain from repatriating money or property from abroad in which Bangladesh has an interest and was due to be repatriated; or
- iii) Not bringing into the country the actual dues from a foreign country, or paying to a foreign country in excess of the actual dues.

“Reporting Organization” has been defined in Section 2 (w) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as --**“Reporting Organization”** means

- i) Bank;
- ii) Financial institution;
- iii) Insurer;
- iv) Money changer;
- v) Any company or institution which remits or transfers money or money value;
- vi) Any other institution carrying out its business with the approval of Bangladesh Bank;
- vii) a. Stock dealer and stock broker,
b. Portfolio manager and merchant banker,
c. Securities Custodian Asset Manager;
- viii) a. Non-profit organization,
b. Non-Governmental Organization,
c. Cooperative Society
- ix) Real estate developer;
- x) Dealer in precious metals and/or stones;
- xi) Trust and Company Service Provider;
- xii) Lawyer, notary, other legal professionals and accountant;
- xiii) Any other institution which Bangladesh Financial Intelligence Unit (BFIU) may notify from time to time with the approval of the Government.

“Money value transferor” has been defined in section 2(b) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as - **“Money value transferor”** means a financial service in which the service provider receives currency, cheques, other financial instruments (electronic or otherwise) in one location and provides the beneficiary with the equal value in currency or financial instruments or any other means in a different location.

“Proceeds of crime” has been defined in section 2(c) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as -**“Proceeds of crime”** means any property obtained or derived, directly or indirectly, from a predicate offence or any such property retained or controlled by anybody.

“Cash” has been defined in section 2(m) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as – **“Cash”** means any currency recognized by a country as being the authorized currency for that country, including coins, paper currency, travelers’ cheque, postal notes, money orders, cheques, bank drafts, bearer bonds, letters of credit, bills of exchange, credit card, debit card or promissory notes.

“Foreign currency” has been defined in section 2(s) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as -**“Foreign currency”** means any foreign exchange defined under section 2 (d) of the Foreign Exchange Regulation Act, 1947 (Act No. VII of 1947).

“Bank” has been defined in section 2(t) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as – **“Bank”** means a **bank** company defined under section 5 (o) of the Bank Companies Act, 1991 (Act No. XIV of

1991) and it shall also include any other institution designated as a bank under any other law.

“Money Changer” has been defined in section 2(u) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as- “Money Changer” means any person or institution approved by Bangladesh Bank under section 3 of the Foreign Exchange **Regulation** Act, 1947 (Act No. VII of 1947) for dealing in foreign exchange transactions.

“Real estate developer” has been defined in **section 2(x)** of the Money Laundering Prevention Act, 2012 (Amendment 2015) as- “Real estate developer” means ---

- i. Any Real estate developer or its officers or employees defined under section 2(15) of Real Estate Development and Management Act, 2010(Act no 48 of 2010); or
- ii. Agents who are engaged in constructing and buying and selling of land, house, commercial buildings and flats etc.

“Entity” has been defined in section 2(y) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as- “Entity” means any kind of legal entity, statutory body, commercial or noncommercial organization, partnership firm, cooperative society or any organization comprising one or more than one person;

“Special Judge” has been defined in section 2 (dd) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as-“Special Judge” **means** the Special Judge appointed under section 3 of the Criminal Law Amendment Act, 1958 (Act No. XL of 1958).

“Stock Dealer and Stock Broker” has been defined in section 2 (ee) (1) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as – “Stock Dealer and Stock Broker” means an institution defined under rule 2(i) and (j) of the Securities and Exchange Commission (Stock Dealer, Stock Broker and Authorized Representative) Rules 2000.

“Portfolio Manager and Merchant Banker” has been defined in section 2 (ee) (2) of the Money Laundering Prevention Act 2012 (Amendment 2015) as – “Portfolio Manager and Merchant Banker” means institution defined under rule 2(f) and 2 (j) of the Securities and Exchange Commission (Merchant Banker and Portfolio Manager) Rules 1996.

“Securities Custodian” has been defined in section 2 (ee) (3) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as – “Securities Custodian” means an institution defined under rule 2(j) of the Securities and Exchange Commission (Security Custodial Service) Rules 2003.

“Asset Managers” has been defined in section 2(ee) (4) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as – “Asset Managers” means an **institution** defined under rule 2(s) of the Securities and Exchange Commission (Mutual Fund) Rules 2001.

1.3 The Economic and Social Consequences of Money Laundering

Money laundering has significant economic and social consequences, especially for developing countries and emerging markets. The easy passage of funds from one institution, or relatively facile systems that allows money to be placed without raising any questions, is fertile territory for money launderers. The upholding of legal, professional and ethical standards is critical to the integrity of financial markets. The potential macroeconomic consequences of unchecked money laundering include:

- a. **Increased Exposure to Organized Crime and Corruption:** Successful money laundering enhances the

profitable aspects of criminal activity. When a country is seen as a haven for money laundering, it will attract people who commit crime. If money laundering is prevalent, there is more likely to be corruption. In countries with weaker laws and enforcement, it is corruption that triggers money laundering. A comprehensive AML, CFT & CPF framework on the other hand helps curb criminal activities, eliminates profits from such activities, discourages criminals from operating in a country especially where law is enforced fully and proceeds from crime are confiscated.

- b. **Undermining the Legitimate Private Sector:** One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers are known to use front companies businesses that appear legitimate and engage in legitimate business but are in fact controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to hide the ill-gotten gains. By using front companies and other investments in legitimate companies, money laundering proceeds can be used to control whole industries or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxes, thus depriving the country of revenue.
- c. **Weakening Financial Institutions:** ML, TF and PF can harm the soundness of a country's financial sector. They can negatively affect the stability of individual banks or other financial institutions, such as securities firms and insurance companies. The establishment and maintenance of an effective AML, CFT & CPF program is usually part of a financial institution's charter to operate; non-compliance can result not only in significant civil money penalties, but also in the loss of its charter.
- d. **Dampening Effect on Foreign Investments:** Although developing economies cannot afford to be too selective about the sources of capital they attract, there is a dampening effect on foreign direct investment when a country's commercial and financial sectors are perceived to be compromised and subject to the influence of organized crime. To maintain a business-friendly environment these impedances have to be weeded out.
- e. **Loss of Control of, or Mistakes in, Decisions Regarding Economic Policy:** Due to the large amounts of money involved in the money laundering process, in some emerging market countries these illicit proceeds may dwarf government budgets. This can result in the loss of control of economic policy by governments or in policy mistakes due to measurement errors in macroeconomic statistics. Money laundering can adversely affect currencies and interest rates as launderers reinvest funds where their schemes are less likely to be detected, rather than where rates of return are higher. ML can increase the threat of monetary instability due to the misallocation of resources from artificial distortions in asset and commodity prices.
- f. **Economic Distortion and Instability:** Money launderers are not primarily interested in profit generation from their investments, but rather, in protecting their proceeds and hiding the illegal origin of the funds. Thus, they "invest" their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, to the extent that money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin, economic growth may suffer.
- g. **Loss of Tax Revenue:** ML diminishes government tax revenue and, therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case. A government revenue deficit is at the center of economic difficulties in many countries, and correcting it is the primary focus of most economic stabilization programs.
- h. **Risks to Privatization Efforts:** ML threatens the efforts of many states trying to introduce reforms into their economies through the privatization of state-owned properties such as land, resources, or enterprises.

Sometimes linked with corruption or inside deals, a government may award a state privatization tender to a criminal organization potentially at an economic loss to the public. Moreover, while privatization initiatives are often economically beneficial, they can also serve as a vehicle to launder funds.

- i. **Reputation Risk for the Country:** A reputation as a ML, TF & PF haven can harm development and economic growth in a country. It diminishes legitimate global opportunities because foreign financial institutions find the extra scrutiny involved in working with institutions in money laundering havens is too expensive. Once a country's financial reputation is damaged, reviving it is very difficult and requires significant resources to rectify a problem that could have been prevented with proper anti money laundering controls. Other effects include specific counter-measures that can be taken by international organizations and other countries, and reduced eligibility for governmental assistance.
- j. **Risk of International Sanctions:** In order to protect the financial system from ML, TF and PF the United States, the United Nations, the European Union, and other governing bodies may impose sanctions against foreign countries, entities or individuals, terrorists and terrorist groups, drug traffickers, and other security threats. FATF also maintains a list of jurisdictions identified as high-risk and non-cooperative, whose AML, CFT & CPF regimes have strategic deficiencies and are not at international standards. As a result, FATF calls on its members to implement counter-measures against the jurisdiction such as financial institutions applying enhanced due diligence to business relationships and transactions with natural and legal persons from the identified jurisdiction in an attempt to persuade the jurisdiction to improve its AML, CFT & CPF regime.
- k. **Social Costs:** Significant social costs and risks are associated with money laundering. It also enables drug traffickers, smugglers and other criminals to expand their operations. This drives up the cost of government expenses and budgets due to the need for increased law enforcement and other expenditures (for example, increased healthcare costs for treating drug addicts) to combat the serious consequences that result. Financial institutions that rely on the proceeds of crime face great challenges in adequately managing their assets, liabilities and operations, attracting legitimate clients.

1.4 Stages of Money Laundering

There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewelry) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). There are a number of crimes where the initial proceeds usually take the form of cash that needs to enter the financial system by some means. Bribery, extortion, robbery and street level purchases of drugs are almost always made with cash. These proceeds of crime have to enter the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated.

Despite the variety of methods employed, money laundering is not a single act but a process accomplished in 3 basic stages which are as follows:

- i. **Placement:** The physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international. Examples of placement transactions include:
 - Blending of funds: Comingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned restaurant.

- Foreign exchange: Purchasing of foreign exchange with illegal funds.
 - Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements.
 - Currency smuggling: Cross-border physical movement of cash or monetary instruments.
 - Loans: Repayment of legitimate loans using laundered cash.
 - Purchasing monetary instruments i.e. travelers' checks, payment orders.
 - Using cash to purchase expensive items that can be resold.
- ii. **Layering:** The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds. This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds. Examples of layering transactions include:
- Electronically moving funds from one country to another and dividing them into advanced financial options and or markets.
 - Moving funds from one financial institution to another or within accounts at the same institution.
 - Converting the cash placed into monetary instruments.
 - Reselling high value goods and prepaid access/stored value products.
 - Investing in real estate and other legitimate businesses.
 - Placing money in stocks, bonds or life insurance products.
 - Using shell companies to obscure the ultimate beneficial owner and assets.
 - Early surrender of an annuity without regard to penalties.
 - L/Cs with false invoices/bills of lading etc.
- iii. **Integration:** Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets. Examples of integration transactions include:
- a. Purchasing luxury assets like property, artwork, jewelry or high end automobiles.
 - b. Getting into financial arrangements or other ventures where investments can be made in business Enterprises.

1.5 Why Money Laundering is Done:

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

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

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

1.6 Definition of Terrorist Financing

Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. Financing of terrorism generally refers to carrying out transactions involving funds that may or may not be owned by terrorist, or that have been, or are intended to be, used to assist the commission of terrorism. Financing of Terrorism includes:

- i. providing or collecting property for carrying out an act of terrorism;
- ii. providing services for terrorism purposes;
- iii. arranging for retention or control of terrorist property; or
- iv. 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:

- a. '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 :
- b. 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
- c. 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.
- d. 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 6 of the Anti-Terrorism Act, 2009 (Amendment 2012 & 2013) of Bangladesh, terrorist activities means:

1. If any person, entity or foreigner-

- a. for the purposes of threatening the unity, integration, public security or sovereignty of Bangladesh by creating panic among the public or a section of the public with a view to compelling the Government or any entity or any person to do any act or preventing them from doing any act,-
 - i. kills, causes grievous hurt to, confines or kidnaps any person or attempts to do the same;
 - ii. conspires, abets or instigates any person to kill, injure seriously, confine or kidnap any person; or
 - iii. damages or tries to damage the property of any other person ,entity or the Republic ; or
 - iv. conspires or abets or instigates to damage the property of any other person, entity or the Republic; or
 - v. uses or keeps in possession any explosive substance, inflammable substance and arms for the purposes of sub-clauses (i),(ii), (iii) or (iv);
- b. with an intent to disrupt security of or to cause damage to the property of any foreign State, commits or attempts to commit or instigates or conspires or abets to commit an offence similar to the offences mentioned in sub-clauses (i),(ii),(iii),(iv) or (v) of clause (a);
- c. with a view to compelling any international organization to do any act or preventing it from doing any act, commits or attempts to commit or instigates or conspires or abets to commit an offence similar to the offences mentioned in sub-clauses (i),(ii),(iii),(iv) or (v) of clause (a);
- d. knowingly uses or possesses any terrorist property;
- e. abets, instigates, conspires to do or commits or attempts to commit an offence described in the United Nations conventions included in the Schedule 1 of this Act;

- f. commits any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an 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 any act; the person, entity or foreigner shall be deemed to have committed the offence of “terrorist activities”;

2. If any person or foreigner

- a. commits an offence under sub-clause (i) of clause(a) of sub- section(1), the person shall be punished with death or imprisonment for life and in addition to that a fine may also be imposed;
- b. commits an offence under sub-clause (ii) of clause (a) of sub-section (1), the person shall, if the offence is punishable with death, be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14(fourteen) years but not less than 4(four) years, and with fine;
- c. commits an offence under sub-clause (iii) of clause (a) of sub-section (1), the person shall be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14(fourteen) years but not less than 4(four) years, and with fine;
- d. commits an offence under sub-clause (iv) of clause (a) of sub-section(1), the person shall be punished with rigorous imprisonment for a term not exceeding 14(fourteen) years but not less than 4(four) years, and with fine;
- e. commits an offence under sub-clause (v) of clause (a) of sub- section (1), the person shall be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14 (fourteen) years but not less than 4(four) years, and with fine.
- f. If any person or foreigner commits an offence under clause (b), (c), (d), (e) or (f) of sub- section (1), the person shall be punished with **imprisonment** for life or rigorous imprisonment for a term not exceeding 14(fourteen) years but not less than 4(four) years and with fine.

3. If any entity commits the offence of terrorist activities

- a. steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of taka 50(fifty) lac, whichever is greater, may be imposed; and
- b. the head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20(twenty) years but not less than 4(four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20(twenty) lac, whichever is greater, may be imposed unless he is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

Offence of Terrorist Financing: -

1. If any person or entity willfully provides, receives, collects or makes arrangements for money, service or any other property, whether from legitimate or illegitimate source, by any means, directly or indirectly, with the intention that, it would, in full or in part, be used –
 - a. to carry out terrorist activity;
 - b. by a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.
2. Conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property mentioned in sub-section (1) was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act.

3. If any person is convicted of any of the offences mentioned in sub-section (1), the person shall be punished with rigorous imprisonment for a term not exceeding 20(twenty) years but not less than 4(four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or taka 10 (ten) lac, whichever is greater, may be imposed.
4. If any entity is convicted of any of the offences mentioned in the sub-section (1)-
 - a. steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of taka 50(fifty) lac, whichever is greater, may be imposed; and
 - b. the head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4(four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20(twenty) lac, whichever is greater, may be imposed unless he is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

1.7 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 of 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 to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

1.8 Why We Must Combat Money Laundering and Terrorist Financing:

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.

1.9 How Financial Institutions can Combat Money Laundering:

The prevention of laundering the proceeds of crime has become a major priority for all jurisdictions from which financial activities are carried out. One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. The adoption of procedures by which Banks and other Financial Institution's KYC is not only a principle of good business but is also an essential tool to avoid involvement in ML. For the purposes of these guidance notes the term Banks and other Financial Institutions refer to businesses carrying on relevant financial business as defined under the legislation.

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

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

In complying with the requirements of the Act and in following these Guidance Notes, Banks should at all times pay particular attention to the fundamental principle of good business practice - 'know your customer'. Having a sound knowledge of a customer's business and pattern of financial transactions and commitments is one of the best methods by which financial institutions and their staff will recognize attempts at money laundering.

1.10 How Bank Asia Can Help in Combating Money Laundering, Terrorist Financing and Proliferation Financing:

1. One of the best methods of preventing and combating ML, TF and PF is a sound knowledge of a customer's business and pattern of financial transactions and commitments. In this principle, Bank Asia has already adopted sound "Know Your Customer" procedure to record full and correct information of the customers. After obtaining information and documents from the customer, it should be verified from the independent & reliable source to avoid inadvertent involvement in ML, TF and PF. Thus **the** Bank's effort to combat ML, TF and PF largely focuses on the process where the launderer's activities are more susceptible to recognition and therefore concentrates to a large extent on the deposit taking procedures i.e., the placement stage.
2. Branches, SME Service Centers and Agent Banking Outlet must keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information of the people and organizations involved in laundering schemes.
3. AML & CFT Division and the Institute of Training and Development of Bank Asia also deal with employees training programs which are designed to make awareness about money laundering techniques and tools and so on to combat ML, TF and PF.
4. Branches, SME Service Centers and Agent Banking Outlet must maintain the regulatory requirement of record keeping procedure.
5. AML & CFT Division of Bank Asia conduct audit of our Branches, SME service centers those obtained "Marginal" rating on AML, CFT & CPF issues by Internal Control and Compliance Department (ICCD) in order to improve the rating of those Branches and SME Service Centers.
6. If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, Bank Asia own initiative shall send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to BFIU immediately.
7. Bank Asia shall maintain and update the listed individuals and entities in electronic form to run on regular basis a system checking at the website of United Nations for updated list. Bank Asia shall run regular check on the given parameters, including transactional review, to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.

1.11 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.

TFS related to terrorism and terrorist financing-

FATF recommendation 6 requires 'Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for

the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)'.

TFS related to Proliferation-

FATF recommendation 7 requires 'Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations'.

CHAPTER II: INTERNATIONAL INITIATIVES

2.1 International Initiatives

In response to the growing concern about money laundering, terrorist activities and proliferation financing, the international community has acted on many fronts. This part of this Guidance Notes discusses the various international organizations that are viewed as the international standard setters. It further describes the documents and instrumentalities that have been developed for AML, CFT and CPF purposes.

2.2 The United Nations

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

- 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, which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).
- Third, perhaps most importantly, 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.

2.3 The Vienna Convention

Due to growing concern about increased international drug trafficking and the tremendous amounts 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 party to the convention. The convention came into force on November 11, 1990.

2.4 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.

2.5 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.

2.6 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 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.

2.7 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 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 sharing information about planned terrorist acts.

2.8 Security Council Resolution 1540

UNSCR 1540 (2004) imposes binding obligations on all States to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery, and establish appropriate domestic controls over related materials to prevent their illicit trafficking. It also encourages enhanced international cooperation on such efforts. The resolution affirms support for the multilateral treaties whose aim is to eliminate or prevent the proliferation of WMDs (weapons of mass destructions) and the importance for all States to implement them fully; it reiterates that none of the obligations in resolution 1540 (2004) shall conflict with or alter the rights and obligations of States Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, the Chemical Weapons Convention, or the Biological Weapons Convention or alter the responsibilities of the International Atomic Energy Agency (IAEA) and Organization for the Prohibition of Chemical Weapons (OPCW).

2.9 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.

2.10 Counter-Terrorism Implementation Task Force (CTITF)

The Counter-Terrorism Implementation Task Force (CTITF) was established by the Secretary-General in 2005 and endorsed by the General Assembly through the United Nations Global Counter-Terrorism Strategy, which was adopted by consensus in 2006. The mandate of the CTITF is to enhance coordination and coherence of counter- terrorism efforts of the United Nations system. The Task Force consists of 36 international entities which by virtue of their work have, have a stake in multilateral counter-terrorism efforts. Each entity makes contributions consistent with its own mandate. While the primary responsibility for the implementation of the Global Strategy rests with Member States, CTITF ensures that the UN system is attuned to the needs of Member States, to provide them with the necessary policy support and spread in-depth knowledge of the Strategy, and wherever necessary, expedite delivery of technical assistance.

2.11 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.

2.12 The Financial Action Task Force (FATF)

The Financial Action Task Force (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 35 countries and territories and two regional organizations. There are also 31 associate members or observers of FATF (mostly international and regional organizations) that participate in its work.

2.13 FATF 40 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.

2.14. 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.

Table 1: Summary of new FATF 40 Standards

Group	Topic	Recommendations
1	Policies and Coordination	1-2
2	Money Laundering and Confiscation	3-4
3	Terrorist Financing and Financing of Proliferation	5-8
4	Preventive Measures	9-23
5	Transparency and Beneficial Ownership of Legal Persons and Arrangements	24-25
6	Power and Responsibilities of Competent Authorities and Other Institutional Measures.	26-35
7	International Co-operation	36-40

2.14.1 The FATF Recommendations

A. AML & CFT Policies and Coordination

1. Assessing risks and applying a risk-based approach

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the Anti-Money Laundering and countering the financing of terrorism (AML & CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML & CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

2. National cooperation and coordination

Countries should have national AML & CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate and where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing the financing of proliferation of weapons of mass destruction.

B. Money Laundering and Confiscation

3. Money laundering offence

Countries should criminalize money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties:

- a. property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations, or (d) property of corresponding value.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

C. Terrorist Financing And Financing of Proliferation

5. Terrorist financing offence

Countries should criminalize terrorist financing on the basis of the Terrorist Financing Convention and should criminalize not only the financing of terrorist acts but also the financing of terrorist organizations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing

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).

7. Targeted financial sanctions related to proliferation

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.

8. Non-profit organizations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:

- a. by terrorist organizations posing as legitimate entities;
- b. to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
- c. to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations

D. Preventive Measures

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Customer Due Diligence and Record-Keeping

10. Customer due diligence

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

- a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
- b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.
- c. Understanding and as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this

Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

12. Politically exposed persons

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

- a. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- b. obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- c. take reasonable measures to establish the source of wealth and source of funds; and
- d. Conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking

Correspondent banking the account of PEPs/Influential Person/Chief Executives or Top Level Officials of any international organization and their close

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

- a. gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- b. assess the respondent institution's AML & CFT controls;
- c. obtain approval from senior management before establishing new correspondent relationships;

- d. clearly understand the respective responsibilities of each institution; and
- e. With respect to “payable-through accounts”, be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTs) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTs without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTs provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTs provider and its agents operate. Countries should take measures to ensure that MVTs providers that use agents include them in their AML & CFT programs and monitor them for compliance with these programs.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

16. Wire transfers

Countries should ensure that financial institutions include required and accurate originator information and required beneficiary information, on wire transfers and related messages and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security

Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

Reliance, Controls and Financial Groups

17. Reliance on third parties

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

- a. A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.
- b. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
- c. The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.
- d. When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programs against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML & CFT programs is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML & CFT policies.

18. Internal controls and foreign branches and subsidiaries

Financial institutions should be required to implement programs against money laundering and terrorist financing. Financial groups should be required to implement group-wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML & CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML & CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programs against money laundering and terrorist financing.

19. Higher-risk countries

Financial institutions should be required to apply Enhanced Due Diligence (EDD) measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate counter measures when called upon to do so by the FATF. Countries should also be able to apply counter measures independently of any call by the FATF to do so. Such counter measures should be effective and proportionate to the risks.

Reporting of Suspicious Transactions

20. Reporting of suspicious transactions

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report immediately its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

- a. protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and
- b. prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

Designated Non-Financial Businesses and Professions

22. DNFBPs: Customer Due Diligence

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

- a. Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.
- b. Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.
- c. Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
- d. Lawyers, notaries, other independent legal professionals and accountants - when they prepare for or carry out transactions for their client concerning the following activities:
 - buying and selling of real estate;
 - managing of client money, securities or other assets;
 - management of bank, savings or securities accounts;
 - organization of contributions for the creation, operation or management of companies;
 - creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
- e. Trust and company service providers - when they prepare for or carry out transactions for a client concerning the following activities:
 - acting as a formation agent of legal persons;
 - acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
 - providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
 - acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
 - acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

- a. Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
- b. Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the

applicable designated threshold.

- c. Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. Transparency and Beneficial Ownership of Legal Persons and Arrangements

24. Transparency and beneficial ownership of legal persons

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and in time information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and in time information on express trusts, including information on the settlor, trustee and beneficiaries that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. Powers and Responsibilities of Competent Authorities, and Other Institutional Measures Regulation and Supervision

26. Regulation and supervision of financial institutions

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML & CFT purposes. This should include applying consolidated group supervision for AML & CFT purposes. Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML & CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML & CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing including the authority to conduct inspections. They should be authorized to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial

sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

- a. Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML & CFT measures. At a minimum:
 - Casinos should be licensed;
 - competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
 - Competent authorities should ensure that casinos are effectively supervised for compliance with AML & CFT requirements.
- b. Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML & CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML & CFT requirements.

Operational and Law Enforcement

29. Financial intelligence units

Countries should establish a financial intelligence unit (FIU) that serves as a national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML & CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialized in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate component authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

General Requirements

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML & CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23 that fail to comply with AML & CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

G. International Cooperation

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

- a. Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.
- b. Ensure that they have clear and efficient processes for the timely prioritization and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.
- c. Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
- d. Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.
- e. Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalize the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

- a. all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and
- b. a broad range of other powers and investigative techniques ;

these are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation

Countries should ensure that they have the authority to take expeditious action in response to , with requests to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organizations. In particular, countries should:

- ensure money laundering and terrorist financing are extraditable offences;
- ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritization where appropriate. To monitor progress of requests a case management system should be maintained;
- not place unreasonable or unduly restrictive conditions on the execution of requests; and
- ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalize the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorize their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritization and timely execution of requests, and for safeguarding the information received.

2.15 Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of FATF 40 recommendations is facilitated by a two-stage process: self-assessments and mutual evaluations. In the self-assessment stage, each member responds to a standard questionnaire, on an annual basis, regarding its implementation of FATF 40 recommendations. In the mutual evaluation stage, each member is examined and assessed by experts from other member countries in every five years. The first Mutual Evaluation (ME) of Bangladesh was conducted by a joint team of World Bank and International Monetary Fund in October, 2002 and the report thereof was adopted by the APG in September, 2003. The 2nd Mutual Evaluation of Bangladesh was conducted by an APG team in August, 2008 and 3rd round ME was conducted by APG team in October, 2015.

2.16 The NCCT List

FATF adopted a process of identifying those jurisdictions that serve as obstacles to international cooperation in implementing its recommendations. The process used 25 criteria, which was consistent with FATF 40 recommendations, to identify such non-cooperative countries and territories (NCCT's) and place them on a publicly available list. NCCT was a process of black listing of non-compliant country. Considering its massive impact on respective country, the FATF introduced new implementation mechanism known as International Cooperation and Review Group (ICRG).

2.17 International Cooperation 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.

2.18 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 40 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(Organization for Economic Cooperation and Development), United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units.

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(AML) and Counter Financing on Terrorism(CFT) 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.

2.19 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 worldwide.

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: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national regulation, in order to counter money laundering and terrorist financing."

Bangladesh has got the membership of prestigious Egmont Group, formed with Financial Intelligence Units of various countries which help get global support in fighting against money laundering, terrorist financing and other financial crimes. It will help stop money laundering and terrorist financing. It won't be easy now to launder money abroad through corruption.

2.20 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 Ten countries. Individual countries are 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. Three of the Basel Committee's supervisory standards and guidelines concern money laundering issues.

2.20.1 Statement of Principles on Money Laundering

In 1988, the Basel Committee issued its Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention). The Statement on Prevention outlines basic policies and procedures that managements of banks/FIs should undertake to assist in suppressing money laundering. There are essentially four principles contained in the Statement on Prevention:

- Proper customer identification;
- High ethical standards and compliance with laws;
- Cooperation with law enforcement authorities; and
- Policies and procedures to adhere to the statement.

2.20.2 Basel Core Principles for Banking

In 1997, the Basel Committee issued its Core Principles for Effective Banking Supervision (Core Principles), which provides a comprehensive blueprint for an effective bank supervisory system and covers a wide range of topics. Core Principle 15, one of the 25 Core Principles, deals with money laundering; it provides:

Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know your customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank from being used; intentionally or unintentionally, by criminal elements.

These "know your customer" or "KYC" policies and procedures are a crucial part of an effective institutional framework for every country.

In addition, the Basel Committee issued a "Core Principles Methodology" in 1999, which contains 11 specific criteria and five additional criteria to help assess the adequacy of KYC policies and procedures. These, additional criteria include specific reference to compliance with The Forty Recommendations.

2.20.3 Customer Due Diligence

In October, 2001, the Basel Committee issued an extensive paper on KYC principles, entitled Customer due diligence for banks/FIs (Customer Due Diligence). This paper was issued in response to noted deficiencies in KYC procedures on a world-wide basis. These KYC standards build upon and provide more specific information on the Statement on Prevention and Core Principle 15.

2.21 International Organization of Securities Commissioners

The International Organization of Securities Commissioners (IOSCO) is an organization of securities commissioners and administrators that have day-to-day responsibilities for securities regulation and the administration of securities laws in their respective countries. The current membership of IOSCO is comprised of regulatory bodies from 105 countries. With regard to money laundering, IOSCO passed a "Resolution on Money Laundering" in 1992. Like other international organizations of this type, IOSCO does not have law-making authority. Similar to the Basel Committee and International Association of Insurance Supervisors (IAIS), it relies on its members to implement its recommendations within their respective countries.

CHAPTER III: NATIONAL INITIATIVES

3.1 National Initiatives

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. Bangladesh hosted the 13th APG Typologies Workshop in 2010 and APG Annual Meeting of 2016.

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 & PF 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 & PF and other associated offences.

3.4 Central and Regional Taskforces

The Government of Bangladesh has formed a central and 7 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. The Deputy Governor of Bangladesh Bank and head of 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 (AMLDD) 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

As per the provision of MLPA, 2012 Bangladesh Financial Intelligence Unit (BFIU) has been established abolishing AMLD 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 AML, CFT & CPF 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.

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.

3.7 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 ACC, BFIU and 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 consider 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 & PF. 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, TF & PF

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 and Deputy Governor of Bangladesh Bank 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 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 tracing 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 NGO/NPO Sector Review

Bangladesh first assessed the ML, TF & PF risk associated with the NGO/NPO sector in 2008. As the sector was mainly depending on foreign donation, the report identified strategic deficiencies of supervision and control of the regulator. According to the requirement of FATF Recommendation 8, BFIU has conducted NGO/NPO sector review with the help from NGO Affairs Bureau, Microcredit Regulatory Authority, Department of Social Services and Research Department of Bangladesh Bank. The review report is a very comprehensive one that covers legal & institutional aspects, supervision mechanism, compliance requirements and risk & vulnerabilities relating to ML & TF.

3.15 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.

3.16 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.

3.17 Risk Based Approach

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on AML and CFT requires financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their ML & TF risks. This requirement is reflected in the Money Laundering Prevention Rules (MLPR) 2013. Rule 21 of MLPR 2013 states that every Reporting Organization-Financial Institution (RO-FI) shall conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. Rule 21 also states that RO-FI shall utilize this risk assessment report after having vetted by BFIU.

BFIU has issued a guidelines titled 'ML and TF Risk Assessment Guidelines for Banking Sector' in January, 2015 (Circular letter no. 01/2015) for providing the basic ideas of identifying, assessing and mitigating ML & TF risks that banks may encounter in doing their businesses. Banks were instructed to assess their own ML & TF risk considering their customers, products, delivery channels and geographical positions. They were also instructed to assess regulatory risk i.e. risk arises from non-compliance of AML & CFT measures. All the banks have submitted their ML & TF risk assessment reports to BFIU in complying with the instruction.

3.18 Memorandum of Understanding (MOU) BFIU and Other FIUs

To enhance the cooperation with foreign counterparts, BFIU signed Memorandum of Understanding (MoU) with other FIUs. BFIU has signed 80 (till June 23) MoU so far to exchange the information related to ML & TF with FIU of other countries.

CHAPTER IV: VULNERABILITIES OF FINANCIAL INSTITUTIONS

4.1 Vulnerability of the Financial System to Money Laundering

Money laundering is often thought to be associated solely with banks and money changers. All financial institutions, both banks and non-banks, are susceptible to money laundering activities. Whilst the traditional banking processes of deposit taking, money transfer systems and lending do offer a vital laundering mechanism, particularly in the initial conversion from cash, it should be recognized that products and services offered by other types of financial and non-financial sector businesses are also attractive to the launderer. The sophisticated launderer often involves many other unwitting accomplices such as currency exchange houses, stock brokerage houses, gold dealers, real estate dealers, insurance companies, trading companies and others selling high value commodities and luxury goods.

Certain points of vulnerability have been identified in the laundering process, which the money launderer finds difficult to avoid, and where his activities are therefore more susceptible to being recognized. These are:

- entry of cash into the financial system;
- cross-border flows of cash; and
- Transfers within and from the financial system.

Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their procedures with due regard to that risk.

Although it may not appear obvious that the products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that weaknesses cannot be exploited.

Banks and other Financial Institutions conducting relevant financial business in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. The liquidity of some products may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

All banks and non-banking financial institutions, as providers of a wide range of money transmission and lending services, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage.

Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

However, in addition, banks and non-banking financial institutions, as providers of a wide range of services, are vulnerable to being used in the layering and integration stages. Other loan accounts may be used as part of this process to create complex layers of transactions.

Some banks and non-banking financial institutions may additionally be susceptible to the attention of the more sophisticated criminal organizations and their “professional money launderers”. Such organizations, possibly under the disguise of front companies and nominees, may create large scale but false international trading activities in order to move their illicit money from one country to another. They may create the illusion of international trade using false/inflated invoices to generate apparently legitimate international wire transfers, and may use falsified/bogus letters of credit to confuse the trail further. Many of the front companies may even approach their bankers for credit to fund the business activity. Banks and non-banking financial institutions offering international trade services should be on their guard for laundering by these means.

4.2 Vulnerabilities of Products and Services

4.2.1 Lease/Term Loan Finance

Front company can take lease/term loan finance from a financial institution and repay the loan from illegal source, and thus bring illegal money in the formal financial system in absence of proper measures. The firm can also repay the loan amount even before maturity period if they are not asked about the sources of fund. In case of financial or capital lease, the asset purchased with FI's financing facility can be sold immediately after repayment of the loan through illegal money and sold proceeds can be shown as legal. So the money launderers and terrorist financier can use this financial instrument for placement and layering of their ill-gotten money.

4.2.2 Factoring

International factoring provides a simple solution of problems faced in case of open account trade regardless of whether the exporter is a small organization or a major corporation. The role of the factor/bank is to collect money owed from abroad by approaching importers in their own country, in their own language and in the locally accepted manner. A factor can also provide exporters with 100% protection against the importer's inability to pay. As international factoring lets exporters safely offer of competitive credit terms to their foreign customers, this international financing mechanism is now popular among both exporters and importers.

International factoring means the seller and buyer are in different countries. Over the years, international factoring has taken various forms due to varying needs of the exporters and security to the factors besides price bearing capacity of the former. These are (a) Direct Export Factoring (b) Direct Import Factoring (c) Back to Back Factoring.

- a. Direct Export Factoring: The direct export factoring is mostly used when handling exports to countries where the corresponding factoring network does not reach. This form of direct export factoring is often provided in combination with outside credit insurance scheme and the traditional services offered by a banking network.
 1. The exporter ships the goods to his importer/ debtor.
 2. The exporter assigns his invoices to the export factor.
 3. The export factor pays the seller the agreed advance.
 4. The export factor handles the accounts receivable in accordance with the sale contract between the exporter and the importer.
 5. The importer pays on the due date to export factor.
 6. The export factor settles the advance with the funds received and forwards the balance to the seller.
- b. Direct import factoring: Factors in an exporter's country are not sometimes perceived very active in marketing international factoring services. In that case, factors in importers' country offer their services directly to foreign suppliers. The exporter may also establish direct contact with factors in the importing country. The resultant arrangement will be of direct import factoring.
 1. The exporter ships the goods to his importer.
 2. The exporter assigns his invoices to the import factor, who assumes the credit risk, provided this has been agreed to beforehand.
 3. The import factor handles the accounts receivable in accordance with the sales contract between the exporter and the importer.
 4. The importer pays the import factor on the due date.
 5. The import factor forwards the payment to the exporter, possibly deducting the agent's commission.
- c. Back to back factoring: This is a highly specialized form of international factoring. It is used when the supplier sells his goods through his subsidiary to the importers/ debtors in the import factors' country. This is done to avoid large volumes of sales to a few importers/ debtors for whom it is difficult for the import factor to cover the credit risk. In such a case, import factor can sign a domestic factoring agreement with the

importer/ debtor. This agreement will facilitate to get debtors' receivables as security for the credit line as it has been asked to establish in favor of export factor.

1. The parent company ships goods to its subsidiary, which sells and ships the goods to the debtors in the import factor's country.
2. The seller assigns his invoices on the subsidiary via export factor to import factor.
3. The subsidiary assigns its receivables to the import factor with or without credit risk coverage.
4. The export factor pays the parent company the agreed advances.
5. The subsidiary's debtors pay the import factor.

The import factor distributes the funds according to the instructions from the export factor.

It is clear that in international factoring there is a provision that the two firms must be member of Factor Chain International or some association that can ensure the credit worthiness of the firms. In absence of this kind of private sector watchdog in the local factoring, the supplier and the buyer may ally together to legalize their proceeds of crime. Without conducting any bona fide transaction the supplier may get finance from FIs and FIs may get repayment from buyer. FIs may focus on getting repayment without considering the sources of fund which can be taken as an opportunity by the money launderer to place their ill-gotten money.

4.2.3 Private Placement of Equity/Securitization of Assets

Some FIs offer financing facilities to firms through private placement of equity and securitization of assets. FIs sell those financial instruments to private investors who may take this as an opportunity to make their money legal. Later the money launderers can sell these instruments and bring their money in the formal financial system.

4.2.4 Personal Loan/Car Loan/Home Loan

Any person can take personal loan from FIs and repay it by illegally earned money; thus he/she can launder money and bring it in the formal channel. After taking home loan or car loan, money launderers can repay those with their illegally earned money and later by selling that home/car, they can show the proceeds as legal money.

4.2.5 SME/Women Entrepreneur Loan

Small, medium and women entrepreneurs can take loan facilities from FIs and in many cases, repayment may be done by the illegally earned money. They even do so only to validate their money by even not utilizing the loan. This way they can bring the illegal money in the financial system.

4.2.6 Deposit Scheme

FIs can sell deposit products with at least a six months maturity period. However, the depositor can encash their deposit money prior to the maturity date with prior approval from Bangladesh Bank, foregoing interest income. This Deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong measures.

4.2.7 Loan Backed Money Laundering

In the "loan backed" money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a "loan or mortgage" back to the money laundering for the same amount with all the necessary "loan or mortgage" documentation. This creates an illusion that the trafficker's funds are legitimate. The scheme is reinforced through "legislatively" scheduled payments made on the loan by the money launderer.

4.2.8 Electronic Transfers of Funds

An electronic transfer of funds is any transfer of funds that is initiated by electronic means, such as an Automated Clearing House (ACH) computer, an automated teller machine (ATM), electronic terminals, mobile telephones,

telephones or magnetic tapes. It can happen within a country or across borders, and trillions of dollars are transferred in millions of transactions each day as it is one of the fastest ways to move money. As such, illicit fund transfers can be easily hidden among the millions of legitimate transfers that occur each day.

Money launderers also use electronic transfers of funds in the second stage of the laundering process, the layering stage. The goal is to move the funds from one account to another, from one bank to another, and from one jurisdiction to another with each layer of transactions –making it more difficult for law enforcement and investigative agencies to trace the origin of the funds. To avoid detection in either stage, the money launderer may take basic precautions such as varying the amounts sent, keeping them relatively small and under reporting thresholds, and, where possible, using reputable organizations.

The processes in place to verify the electronic transfer of funds have been tightened in recent years. Many transaction monitoring software providers have sophisticated algorithms to help detect or trigger alerts that may indicate money laundering or other suspicious activity using electronic transfers of funds.

4.2.9 Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). By establishing multiple correspondent relationships globally, banks can undertake international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence. Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks obtain a wide range of services through correspondent relationships, including cash management (for example, interest bearing accounts in a variety of currencies), international wire transfers of funds, check clearing, payable-through accounts and foreign exchange services.

The services offered by a correspondent bank to smaller, less well-known banks may be restricted to non-credit, cash management services.

Correspondent banking is vulnerable to money laundering for two main reasons:

- a. By their nature, correspondent banking relationships create a situation in which a financial institution carries out financial transactions on behalf of customers of another institution. This indirect relationship means that the correspondent bank provides services for individuals or entities for which it has neither verified the identities nor obtained any first-hand knowledge.
- b. The amount of money that flows through correspondent accounts can pose a significant threat to financial institutions, as they process large volumes of transactions for their customers’ customers. This makes it more difficult to identify suspect transactions, as the financial institution generally does not have the information on the actual parties conducting the transaction to know whether they are unusual.

4.2.10 Payable through Accounts

In some correspondent relationships, the respondent bank’s customers are permitted to conduct their own transactions — including sending wire transfers, making and withdrawing deposits and maintaining checking accounts through the respondent bank’s correspondent account without first clearing the transactions through the respondent bank. Those arrangements are called payable-through accounts (PTAs). In a traditional correspondent relationship, the respondent bank will take orders from their customers and pass them on to the correspondent bank. In these cases, the respondent bank has the ability to perform some level of oversight prior to executing the transaction.

PTAs differ from normal correspondent accounts in that the foreign bank’s customers have the ability to directly control funds at the correspondent bank. PTAs can have a virtually unlimited number of sub-account holders, including individuals, commercial businesses, finance companies, exchange houses or casas de cambio, and even other foreign banks. The services offered to subaccount holders and the terms of the PTAs are specified in the agreement signed by the correspondent and the respondent banks. PTAs held in the names of respondent banks often involve checks encoded with the bank’s account number and a numeric code to identify the sub-

account, which is the account of the respondent bank's customer. Sometimes, however, the sub-account holders are not identified to the correspondent bank.

Elements of a PTA relationship that can threaten the correspondent bank's money laundering defenses include:

- PTAs with foreign institutions licensed in offshore financial service centers with weak or nascent bank supervision and licensing laws.
- PTA arrangements where the correspondent bank regards the respondent bank as its sole customer and fails to apply its Customer Due Diligence policies and procedures to the customers of the respondent bank.
- PTA arrangements in which sub-account holders have currency deposit and withdrawal privileges.
- PTAs used in conjunction with a subsidiary, representative or other office of the respondent bank, which may enable the respondent bank to offer the same services as a branch without being subject to supervision.

4.2.11 Crypto-Currencies:

Crypto-currencies have no physical existence, but are best thought of as electronic accounting systems that keep track of people's transactions and hence remaining purchasing power. Crypto currencies are typically decentralized, with no central authority responsible for maintaining the ledger and no central authority responsible for maintaining the code used to implement the ledger system, unlike the ledgers maintained by commercial banks for example. As crypto-currencies are denominated in their own unit of account, they are like foreign currencies relative to traditional fiat currencies, such as dollars and pounds.

There are various Crypto-Currencies are traded in the market for example Binance Coin, Vechain, Tether, EOS, TRON, Bitcoin, Stellar, Ethereum, Ethereum Classic, Tezo5(Pre-Launch), NEO, Monero, Litecoin, Bitcoin Cash, RaiBlocks, IOTA, Dash, Cardano, Ripple, NEM etc.

The mechanics of Bitcoin – the original crypto-currency – to illustrate the fundamental elements of decentralized crypto-currencies. Transactions are implemented as messages that debit or credit account balances in duplicate ledgers. Programming protocols ensure that ledgers are synchronized, and agents are rewarded for updating and quality-assuring the ledgers with transaction data, which accumulate in 'blocks'. Cryptography is used to secure the transaction messages and the integrity of the ledgers containing account balances.

Crypto-currencies expand the mechanisms by which people can transact with each other, strengthening competitive pressures on payment systems providers. But, as noted by many international institutions and central banks, crypto-currencies facilitate a relatively small volume of transactions. These new payments mechanisms are unlikely to completely supplant traditional payments systems. People in different countries typically transact in their own local currency. Since most jurisdictions require tax obligations to be paid in domestic fiat currency, national currencies are likely to remain an important payment mechanism. Crypto-currencies are also unlikely to supplant financial institutions' role in providing credit. Banks and other financial institutions transform assets, manage risk, assess prospective creditors and monitor creditors' progress in meeting their obligations. Credit is largely incompatible with the (pseudo) anonymity that is a common element of crypto-currency design.

Ensuring price stability is likely to remain the pre-eminent monetary policy objective for central banks, an objective unchanged by the growth of crypto-currencies. As the 'licensed distributors' of fiat currency, central banks should remain able to set interest rates in their domestic fiat currency units. The introduction of crypto-currencies should not fundamentally disrupt central banks' use of interest rates to stabilize the inflation rates of their own fiat currencies.

Crypto-currencies also raise consumer protection, anti-money laundering, and counter-terrorism financing concerns. As niche payment systems, crypto-currencies do not currently pose material financial stability concerns, but

risks could increase in materiality if crypto-currencies become more popular and/or more integrated with the activities of traditional financial institutions. Crypto-currencies are extremely volatile, and there are significant risks associated with holding such assets. There is no certainty that specific crypto-currencies, such as Bitcoin, will continue to function and be valued by Trans actors, and there are non-trivial risks of loss and theft.

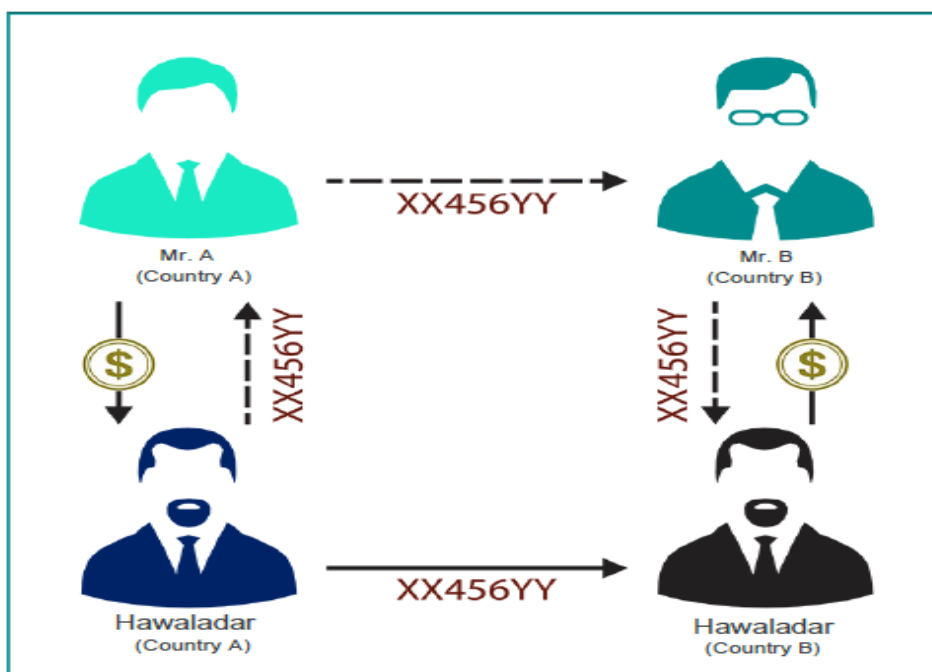
4.3 Hundi/Hawala

Hundi, also known as Hawala, is an informal and largely unregulated system of money transfer that is prevalent in many parts of the world, including Bangladesh. While it is used for various purposes, one significant context in which it operates is the remittance market. Remittances are an essential source of income for many Bangladeshi families, with millions of Bangladeshis working abroad and sending money back home.

How Hundi/Hawala Works?

Hundi is simply an underground money transfer services, this means it also has cross border corresponding transactions. In most cases, the physical money is not transferred to abroad rather two transaction occurred in two countries separately and the Hundi dealer in both end do the settlement in various means which include trade mis-invoicing, exchange or barter system, smuggling of goods etc. Generally, it operates outside of traditional banking and financial systems and relies on trust and the extensive network of Hawaladars (individuals or firms involved in the Hawala business).

Hawala transaction example



Ways to curb Hundi/Hawala:

Combating the challenges posed by Hundi/Hawala networks in Bangladesh requires a multifaceted approach that involves regulatory measures, law enforcement, education, and incentivizing the use of formal channels for remittances.

- Simplify documentation requirements for sending and receiving remittances, reducing paperwork and administrative hassles for user.
- Increase the number of remittance service providers, agents, and branches across the country, especially in rural areas, to make formal channels more accessible.

- Educate the citizen both in home and abroad about the benefits of using formal channels, including the security and legal protections offered to them.
- Conduct financial literacy programs and workshops to educate remittance senders and recipients on the advantages of using formal channel.
- Train bank staff and remittance agents to provide efficient and customer-friendly services, addressing any issues or concerns of customer promptly.

4.4 Structural Vulnerabilities

- FIs are yet to develop sufficient capacity to verify the identity and source of funds of their clients.
- The human resources are not skilled and trained enough to trace money laundering and terrorist financing activities.
- None of the FIs has Anti Money Laundering software to monitor and report transactions of a suspicious nature to the financial intelligence unit of the central bank.

CHAPTER V: COMPLIANCE REQUIREMENTS UNDER THE LAW & CIRCULAR

5.1 Compliance Requirements under the Laws

In Bangladesh, compliance requirements for FIs, as reporting organization, are based on Money Laundering Prevention Act 2012 (Amendment 2015), Anti-terrorism Act 2009, (Amendment 2012 & 2013) and circulars or instructions issued by BFIU.

5.1.1 Money Laundering Prevention Act 2012 (Amendment 2015)

Under the Section -

1. Offence of Money Laundering and Punishment (as per section 4 of MLP Act 2012 (Amendment 2015))

- (1) For the purposes of this Act, money laundering shall be deemed to be an offence.
- (2) Any person who commits or abets or conspires to commit the offence of money laundering shall be punished with imprisonment for a term of 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) lacs, whichever is greater. However, in case of failure of the payment of the fine in due time, the court may issue an order of extra imprisonment considering the amount of the unpaid fine.
- (3) 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 or related with money laundering or any predicate offence.
- (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) lacs, 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.
- (5) It shall not be a prerequisite to charge or punish for money laundering to be convicted or sentenced for any predicate offence.

2. Punishment for violation of a freezing or attachment order – (as per section 5 of MLP Act 2012 (Amendment 2015))

Any person who violates a freezing or attachment order issued under this Act shall be punished with imprisonment for a term not exceeding 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or with both.

3. Punishment for divulging information – (as per section 6 of MLP Act 2012 (Amendment 2015))

- (1) No person shall, with an ill motive, divulge any information relating to the investigation or any other related information, to any person, organization or news media.
- (2) Any person, institution or agent empowered under this Act shall refrain from using or divulging any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purpose of this Act.
- (3) Any person who contravenes the provisions contained in sub-sections (1) and (2) shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine, not exceeding Tk. 50 (fifty) thousand or with both.

4. Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information – (as per section 7 of MLP Act 2012 (Amendment 2015))

- (1) Any person who, under this Act ---
 - a. Obstructs or declines to cooperate with any investigation officer for carrying out the investigation; or
 - b. Declines to supply information or submit a report being requested without any reasonable ground; shall be deemed to have committed an offence under this Act.
- (2) Any person who is convicted under sub-section (1) shall be punished with imprisonment for a term not exceeding 1 (one) year or with a fine not exceeding Tk. 25 (twenty five) thousand or with both.

5. Punishment for providing false information (as per section 8 of MLP Act 2012 (Amendment 2015))

- (1) No person shall knowingly provide false information in any manner regarding the source of fund or self-identity or the identity of an account holder or the beneficiary or nominee of an account.
- (2) Any person who violates the provisions of sub-section (1) shall be punished with imprisonment for a term not exceeding (three) years or a fine not exceeding Tk. 50 (fifty) thousand or both.

6. Powers and Responsibilities of BFIU in Preventing and Restraining the Offence of Money Laundering – (as per section 23 of MLP Act 2012 (Amendment 2015))

- (1) For the purposes of this Act Bangladesh Financial Intelligence Unit (BFIU) shall have the following powers and responsibilities:
 - a. To analyze or review information related to cash transactions and suspicious transactions received from any reporting organizations and information obtained through any other sources and to collect necessary additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data and information on the same and, and investigating agency or the relevant law enforcement agencies for taking the necessary actions;
 - b. Notwithstanding anything contained in any other law, obtain necessary information or report from reporting organizations.
 - c. Issue an order to any reporting organization to suspend or freeze transactions of any account for maximum of 7(seven) times by 30 (thirty) days each if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing an offence or money of an account has been or might be used to commit a crime/an offence:
 Provided that such order may be extended for additional period of a maximum of 6 (six) months by of 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account;
 - d. Issue from time to time, any directions necessary for the prevention of money laundering to the reporting organizations;
 - e. Conduct on-site inspections on the reporting organizations, if necessary.
 - f. Arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by Bangladesh Financial Intelligence Unit (BFIU);
 - g. Carry out any other functions including monitoring activities of the reporting organizations necessary for the purpose of this Act.
- (2) If any investigation agency makes a request to provide it with any information in any investigation relating to money laundering or suspicious transaction, then Bangladesh Financial Intelligence Unit (BFIU) shall provide with such information where no obligation for it is under any existing law or for any other reason.
- (3) If any reporting organization fails to provide with the requested information timely under this section

pursuant to this Section, Bangladesh Financial Intelligence Unit (BFIU) may impose a fine on such organization which may extend to a maximum of taka 5(five) lakhs at the rate of taka 10 (ten) thousand per day and if any organization is fined more than 3(three) times in 1(one) financial year, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

- (4) If any reporting organization provides false information or statement requested under this Section, BFIU may impose a fine on such organization not less than taka 20 (twenty) thousand but not exceeding taka 5 (five) lacs and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Financial Intelligence Unit (BFIU) may suspend the registration or license of the organization or any of its branches/service centers/booths/agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.
- (5) If any reporting organization fails to comply with any instruction given by Bangladesh Financial Intelligence Unit (BFIU) under this Act, BFIU may impose a fine on such organization which may extend to a maximum of taka 5(five) lacs at the rate of taka 10 (ten) thousand per day for each of such noncompliance and if any organization is fined more than 3(three) times in 1(one) financial year, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.
- (6) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Financial Intelligence Unit (BFIU) under clause (c) of sub-section (1), BFIU may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.
- (7) If any person or entity or reporting organization fails to pay any fine imposed by BFIU under sections 23 and 25 of this Act, Bangladesh Financial Intelligence Unit (BFIU) shall inform Bangladesh Bank and BFIU may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh and in this regard if any amount of the fine remains unrealized Bangladesh Financial Intelligence Unit (BFIU) may, if necessary, make an application before the court for recovery and the court may pass such order which it deems fit.
- (7a) while conducting enquiry and investigation of the offences under this Act an investigation agency may obtain documents and information related to the customer of a bank or financial institution through an order by the competent court or through Bangladesh Financial Intelligence Unit.
- (8) If any reporting organization is imposed fine under sub-section (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit (BFIU) may also impose a fine not less than taka 10(ten) thousand but not exceeding taka 5 (five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

7. Responsibilities of Reporting Organizations in Preventing the Offence of Money Laundering – (as per section 25 of MLP Act 2012 (Amendment 2015))

- (1) Reporting Organizations shall have the following duties and responsibilities including other duties and responsibilities specified by rules in the prevention of money laundering:
 - a. maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
 - b. in case of closed account of any customer, keep previous records of transactions of such account and its transactions for at least 5(five) years from the date of closure;
 - c. provide the information maintained under sub-sections (a) and (b) to Bangladesh Financial Intelligence Unit (BFIU) from time to time, as requested;
 - d. if any doubtful transaction or attempt of such transaction as defined under 2(n) is observed by reporting organization, it shall be reported as Suspicious Transaction Report (STR) to the Bangladesh Financial Intelligence Unit (BFIU) proactively and immediately.
- (2) If any reporting organization violates the provisions contained in sub-section (1), Bangladesh Financial Intelligence Unit (BFIU) or regulatory/controlling authority of the reporting organization:
 - a. Impose a fine on the said reporting organization of a minimum of Tk. 50 (fifty) thousand and up to a maximum of Tk. 25 (twenty-five) lacs; and
 - b. Cancel the license or the authorization for carrying out commercial activities of the said Organization or any of its branches/service centers/booths/agents, in addition to the fine mentioned in clause (a), and where appropriate, shall inform the registration or licensing or authority about the subject matter so that the relevant authority may take appropriate action against the said Organization.
- (3) Bangladesh Bank shall collect the sum of fine received under sub-section (2) under manner determined by it and the sum received shall be deposited into the State Treasury.

8. Offences Committed by an Entity – (as per section 27 of MLP Act 2012 (Amendment 2015))

- (1) If any offence under this Act is committed by an entity, every proprietor, director, manager, secretary or any other officer, staff or representative of the said entity who is directly involved in the offence shall be deemed to be guilty of the offence, unless he is able to prove that the said offence has been committed without his knowledge or he took steps to prevent the commission of the said offence.

Explanation – In this section “Director” means any partner or the Board of Directors, by whatever name it is called; it also means its member.

5.1.2 Anti-terrorism Act 2009 (Amendment 2012 & 2013)

Under the Section-

1. Offences relating to financing for terrorist activities – {(as per section 7 of ATA 2009 (Amendment 2013))}

- (1) If any person or entity willfully provides, receives, collects or makes arrangements for money, service or any other property, whether from legitimate or illegitimate source, by any means, directly or indirectly, with the intention that, it would, in full or in part, be used-
 - a. to carry out terrorist activity;
 - b. by a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.
 - c. Conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property mentioned in sub-section (1) was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act.
- (2) If any person is convicted of any of the offences mentioned in sub-section (1), the person shall be

punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or taka 10(ten) lac, whichever is greater, may be imposed.

(3) If any entity is convicted of any of the offences mentioned in the sub-section (1) –

- a. steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is greater, may be imposed; and (b) the head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20 (twenty) lac, whichever is greater, may be imposed unless he is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

2. Powers of BFIU – {as per section 15 of ATA 2009 (Amendment 2013)}

(1) BFIU may take necessary steps to prevent and identify any transaction carried out by any reporting agency with intent to commit an offence under this Act and for this purpose it shall have the following powers and authority, namely:-

- a. to call for a report relating to any suspicious transaction from any reporting agency, analyze or review the same and to collect additional information relating thereto for the purpose of analyzing or reviewing the same and maintain record or database of them and, as the case may be, provide with the said information or report to the police or other concerned law enforcement agencies for taking necessary actions;
- b. if there is reasonable ground to suspect that a transaction is connected to terrorist activities, to issue a written order to the respective reporting agency to suspend or freeze transactions of that relevant account for a period not exceeding 30 (thirty) days and, if it appears necessary to reveal correct information relating to transactions of the said account, such suspension or freezing order may be extended for an additional term not exceeding 6 (six) months by 30 (thirty) days at a time;
- c. to monitor and supervise the activities of the reporting agencies;
- d. to give directions to the reporting agencies to take preventive steps to prevent financing of terrorist activities and proliferation of weapons of mass destructions (WMD);
- e. to monitor the compliance of the reporting agencies and to carry out on-site inspection of the reporting agencies for carrying out any purpose of this Act; and
- f. to provide training to the officers and employees of the reporting agencies for the purpose of identification of suspicious transactions and prevention of financing of terrorist activities. BFIU, on identification of a reporting agency or any of its customers as being involved in a suspicious transaction connected to financing of terrorist activities, shall inform the same to the police or the appropriate law enforcement agency and provide all necessary cooperation to facilitate their inquiries and investigations into the matter.

(2) Bangladesh Bank, on identification of a reporting agency or any of its customers as being involved in a suspicious transaction connected to financing of terrorist activities, shall inform the same to the police or the appropriate law enforcement agency and provide all necessary cooperation to facilitate their inquiries and investigations into the matter.

(3) If the offence is committed in another country or the trial of an offence is pending in another country, BFIU shall take steps to seize the accounts of any person or entity upon request of the foreign state or pursuant to any international, regional or bilateral agreement, United Nations conventions ratified by the Government of Bangladesh or respective resolutions adopted by the United Nations Security Council.

(4) The fund seized under sub-section (3) shall be subject to disposal by the concerned court or

pursuant to the concerned agreements, conventions or resolutions adopted by the United Nations Security Council.

- (5) The power and responsibilities of BFIU under the provisions of this Act shall be exercised by BFIU, and if BFIU requests to provide with any information under this Act, all the governmental, semi-governmental or autonomous bodies, or any other relevant institutions or organizations shall, on such request or, as the case may be, spontaneously provide it with such information.
- (6) Bangladesh Financial Intelligence Unit shall, on request or, as the cases may be, spontaneously provide the financial intelligence units of other countries or any other similar foreign counterparts with any information relating to terrorist activities or financing of terrorist activities.
- (7) For the interest of investigation relating to financing of terrorist activities, the law enforcement agencies shall have the right to access any document or file of any bank under the following conditions, namely:-
 - a. according to an order passed by a competent court or special tribunal; or
 - b. with the approval of the BFIU.
- (8) If any reporting agency fails to comply with the directions issued by BFIU under this section or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine, determined and directed by BFIU, not exceeding taka 25 (twenty five) lac, and BFIU may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.
- (9) If any reporting agency fails to pay or does not pay any fine imposed by BFIU according to sub-section (8), BFIU may recover the amount from the reporting agency by debiting its accounts maintained in any other bank or financial institution or in BFIU and in case of any unrealized or unpaid amount, BFIU may, if necessary, apply before the concerned court for recovery.

3. Duties of Reporting Organizations – {as per section 16 of ATA 2009 (Amendment 2013)}

- (1) Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through it which is connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to BFIU without any delay.
- (2) The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by BFIU under section 15, which are applicable to the reporting agency, have been complied with or not.
- (3) 2[(3) If any reporting agency fails to comply with the provision under sub-section (1), the said reporting agency shall be liable to pay a fine, determined and directed by BFIU, not exceeding taka 25 (twenty five) lac and BFIU may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.
- (4) If the Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of any reporting organization fails to comply with the provision of sub-section (2), the Chairman of the Board of Directors, or the Chief Executive Officer, as the case may be, shall be liable to pay a fine, determined and directed by Bangladesh Bank, not exceeding taka 25 (twenty five) lac, and BFIU may remove the said person from his office or, as the case may be, shall inform the competent authority about the subject matter to take appropriate action against the person.

- (5) If any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank under sub-section (3), or if the Chairman of the Board of Directors, or the Chief Executive Officer, by whatever name called, fails to pay or does not pay any fine imposed by Bangladesh Bank under sub-section (4), Bangladesh Bank may recover the amount from the reporting agency or from the account of the concerned person by debiting any account maintained by him in any bank or financial institution or in Bangladesh Bank, and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

5.2 Compliance Requirements under Circulars

5.2.1 Policies for Prevention of Money Laundering and Terrorist Financing

In pursuance of section 16(2) of Anti-terrorism Act, 2009 (Amendment 2012), and section 1.1 of BFIU circular no. 26 dated 16.06.2020, Bank Asia has its own policy manual approved by their Board of Directors/topmost committee to prevent money laundering, combating financing on terrorism and financing of proliferation of weapons of mass destruction offences. This policy manual has developed in conformity with international standard and laws and regulations in force in Bangladesh. Bank Asia will review this manual time to time and confirm the meticulous compliance of the circulars, guidelines & instruction issued by Bangladesh Financial Intelligence Unit (BFIU).

To implement the policy manual and compliance instructions of Bangladesh Financial Intelligence Unit (BFIU), Bank Asia has designated Deputy Managing Director ((Not below the two tier of President & Managing Director) as Chief Anti Money Laundering Compliance Officer (CAMLCO) in the Central Compliance Committee (CCC) and two officers as Branch Anti Money Laundering Compliance Officer (BAMLCO) & Branch Anti Money Laundering Officer (BAMLO) in the branch level.

5.3 Targeted Financial Sanctions

BFIU has instructed all banks and FIs to take necessary action on UNSCR (targeted financial sanctions). To comply with this direction Bank should consult the UN sanction list regularly and if find any account with it, bank should inform BFIU immediately.

Automated Screening Mechanism of UNSCRs

As per advice from Bangladesh Financial Intelligence Unit (BFIU), for effective implementation of TFS relating to TF & PF Bank Asia has already been started automated screening mechanism that prohibit any listed individuals or entities to enter into the banking channel. The bank is operating the system for detecting any listed individuals or entities prior to establish any relationship with them. In particular, bank need to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individuals or entities could not use the formal financial channel. In a word, bank shall ensure that screening has done before-

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

In Bank Asia, Risk Fraud & Transaction Monitoring Platform (software developed by AML & CFT division in collaboration with ICT division) is used for screening sanction list while opening of any account or establishing relationship with customer. Without screening any account cannot be opened through AML solution. Bank Asia has purchased sanction screening software titled “nSCREEN” purchased from Nazdaq Technologies for sanction screening of foreign trade related transaction. Screening of sanctioned lists of UNSCRs, OFAC, UN, EU and so on for all types of foreign trade related transactions is one of the important issue of our regulatory requirement. Operation of automated & real time screening of sanctioned lists before conducting foreign trade transactions is the prime function of our Authorized Dealers(ADs) and International Division is the supervisor of ADs as well. Without screening any transaction cannot be done as per regulatory requirement.

For proper implementation of UN sanction list, all officials of Bank Asia must have enough knowledge about-

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

Besides screening the parties to transaction, such as the seller of the goods, the shipping company, any agents or third parties present in the transaction, and know the ports of call of the **vessel** for the particular transaction flow (origin port, destination port) where possible.

5.4 Self-Assessment

Banking system in Bangladesh is mainly based on branch banking. The branches of the banks are in every corner of the country and they have an active role in stimulating the economic growth of the country. It is very difficult for the AML & CFT Division or ICC to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFIU has established a Self-Assessment Reporting system for the branches.

According to the instructions of BFIU, branches of bank need to conduct the Self-Assessment to evaluate them on a half yearly basis. Self-Assessment has to be done through a checklist that is circulated by BFIU circular no. 26, dated June 16, 2020. Before finalizing the evaluation report, there shall have to be a meeting presided over by the Head of Branch/BAMLCO with all concerned officials of the branch. In that meeting, there shall be a discussion on the branch evaluation report; if the identified problems according that report are possible to solve at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations shall have to be jotted down. In the subsequent quarterly meetings on preventing ML, TF & PF, the progress of the related matters should be discussed.

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

Each branch will assess its AML & CFT activities covering the following areas on half yearly basis:

- The percentage of officers/employees that received official training on AML & CFT;
- Training, experiences and activities of BAMLCO;
- The awareness of the officers/employees about the internal AML & CFT policies, procedures and programs, and Bangladesh Bank's instructions and guidelines;
- The arrangement of AML & CFT related meeting on regular interval;
- The effectiveness of the customer identification & source of fund verification during opening an account;
- The risk categorization of customers by the branch;
- Regular update of KYC profile as per BFIU circular;
- KYC procedure for walk-in-customer, online customer etc.
- The monitoring of customers' transactions with their declared TP after categorizing the customers based on risk or transactions over specific limit;
- UN sanction screening mechanism;

- Identification of Suspicious Transaction Reports (STRs);
- Identification of Structuring;
- Cash transaction reporting;
- The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees;
- The measures taken by the branch during opening of account of PEPs, Influential person, High Official of International Organization;
- Mobile financial services or wire transfer;
- Compliance related to Head Office, BFIU and Bangladesh Bank audit;
- Transaction monitoring related to inward and outward remittance;

5.5 Independent Testing Procedure

The audit must be independent (i.e. performed by people not involved with the branch's AML & CFT compliance). Audit is a kind of assessment of checking of a planned activity. Independent testing has to be done through a checklist that is provided by BFIU Circular No. 26 dated June 16, 2020 and circulated by Bank Asia under Bank Asia AML & CFT Division instruction circular no. 08/20; dated June 22, 2020.

The individuals conducting the audit should report directly to the Board of Directors/Senior Management. Audit function shall be done by the ICCD. At the same time external auditors could be appointed (if possible) to review the adequacy of the program.

In order to comply the section 6 of Money Laundering Prevention Act 2012(amendment 2015) i.e. the information collected, received and retrieved by the bank, may be audited/inspected to check whether the task of AML & CFT Division are in order. The team comprising by one or more officials of Audit Wing of AML & CFT Division (who are out of the said desk) may be appointed to review the adequacy of the task in order to maintain the confidentiality/ secrecy of the Division as per MLPA.

5.5.1 ICCD's obligations regarding Self-Assessment or Independent Testing Procedure

The ICCD shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the AMLD.

While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the ICCD should examine the AML & CFT activities of the concerned branch using the specified checklists (attached with instruction circular 08/20 dated 22.06.2020) for the Independent Testing Procedure. The ICCD should send a copy of the report with the rating of the branches inspected/audited by the ICCD to the AML & CFT Division of the bank. Besides these ICCD should audit additional 10% (ten percent) of branches as per section

8.2 (2) of BFIU circular no. 26 dated June 16, 2020. The audit team of ICCD should examine the AML & CFT related activities & determine the score of the branch and send a copy of the report to the AML & CFT Division.

5.5.2 AML & CFT Division's obligations regarding Self-Assessment or Independent Testing Procedure

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

- a. Total number of branch and number of Self-Assessment Report received from the branches;
- b. The number of branches inspected/audited by the ICCD at the time of reporting and the status of the branches (branch wise achieved number);

- c. Same kinds of irregularities that have been seen in maximum number of branches according to the received Self-Assessment Report and measures taken by the AML & CFT Division to prevent those irregularities.
- d. The general and special irregularities mentioned in the report submitted by the ICCD and the measures taken by the AML & CFT Division to prevent those irregularities; and
- e. Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as 'unsatisfactory' and 'marginal' in the received report.

CHAPTER VI: AML & CFT COMPLIANCE PROGRAM IN BANK ASIA

Banking sector is one of the most vulnerable sectors for the ML, TF & PF among the financial sectors due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership. Bank Asia Ltd has been considering the Money Laundering & TF risks as one of the indispensable segment in its risk management strategies. The Board & Senior Management set the tone from the top by openly voicing their commitment to the AML & CFT program.

Bank can play a vital role in preventing ML, TF & PF and in this regard their roles and responsibilities are defined in MLP Act 2012 (amendment 2015), ATA, 2009 (amendment 2012 & 2013) and rules and instructions issued under this legal framework by BFIU. To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU, Bank Asia has developed and maintained an effective AML, CFT and CPF compliance program. This covers senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

6.1 Bank Asia AML, CFT & CPF Compliance Program

In the process of developing the compliance program, Bank Asia has paid special attention to size and range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by Bank Asia. The program includes-

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

6.2 Roles and Responsibilities of Board of Directors

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

- shall understand their roles and responsibilities in managing ML, TF & PF risks faced by the bank as reporting institution;
- must be aware of the ML, TF & PF risks associated with business strategies, delivery channels and geographical coverage of its business products and services;
- understand the AML & CFT measures required by the laws including the MLPA, 2012 (amendment 2015) & ATA, 2009 (amendment 2012 & 2013) and the industry's standards and best practices as well as the importance of implementing AML, CFT & CPF measures to prevent the bank from being abused by money launderers and financiers of terrorism;
- establish appropriate mechanisms to ensure the AML, CFT & CPF policies are periodically reviewed and assessed in line with changes and developments in the bank's products and services, technology as well as trends in ML, TF & PF;
- assess the implementation of the approved AML, CFT & CPF policies through regular reporting and

updates by the Senior Management and Audit Committee; and

- define the lines of authority and responsibility for implementing the AML, CFT & CPF measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;
- maintain accountability and oversight for establishing AML, CFT & CPF policies and minimum standards;
- approve policies regarding AML, CFT & CPF measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;
- establish an effective internal control system for AML, CFT & CPF and maintain adequate oversight of the overall AML, CFT & CPF measures undertaken by the bank;
- ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML, TF & PF;
- establish MIS that is reflective of the nature of the bank's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered as well as geographical coverage.

■ **Communication Of Compliance Program**

Bank Asia to communicate their compliance program immediately after the approval from the board of directors or from the highest authority to all of its employees, member of the board of the directors and other relevant stakeholders at home and abroad. The bank should select the proper channel that is the best suited to them to communicate with the compliance program. The bank also should upload the compliance program in their website for their customers or other stakeholders.

6.3 Senior Management Role & Responsibilities

The Senior Management have the following roles and responsibilities:

- be aware of and understand the ML, TF & PF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;
- introduce proper mechanisms and formulate procedures to effectively implement AML, CFT & CPF policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;
- formulate AML, CFT & CPF policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the bank and its geographical coverage;
- provide periodic reporting on time to the Board on the level of ML, TF & PF risks facing the bank, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML, CFT & CPF which may have an impact on the bank;
- convey a clear signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service;
- Communicate clearly to all employees on an annual basis by a statement from the CEO or Managing Director that clearly sets forth its policy against ML, TF & PF 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 bank to comply with all laws and regulations designed to combat money laundering, terrorist financing and proliferation financing;
- assign adequate resources to effectively implement and administer AML, CFT & CPF compliance

- programs that are reflective of the size and complexity of the bank's operations and risk profiles;
- appoint a chief anti-money laundering compliance officer (CAMLCO) at management level at Head Office/Corporate Office and designate a compliance officer at management level at each branch or subsidiary;
- provide appropriate level of AML, CFT & CPF training for employees at all levels throughout the bank;
- Senior management of Bank Asia shall advise Human Resources Division (HRD) for inclusion of AML, CFT & CPF compliance in their manual as well as employee screening process and punishment regarding involvement of ML, TF & PF activities so that it helps to adopt HR or Human Resources Policy for ensuring the compliance of AML, CFT & CPF measures by the employees of the bank.

Senior Management shall also instruct HRD to develop following issues for proper implementation of AML, CFT & CPF measures:-

- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML, CFT & CPF measures;
- Proper weight in the annual performance evaluation of employees for extra ordinary preventive action vis a vis for non-compliance;
- Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;

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

6.4 Statement of Commitment of Managing Director (MD)

At the beginning of new year AML & CFT Division communicates the latest Managing Director message regarding AML & CFT to all employees of the bank that clearly sets forth Bank Asia's policy against ML, TF & PF and any activity which facilitates to prevent Money Laundering or the funding of terrorist or criminal activities.

- ❖ Use of Risk based Approach;
- ❖ Know Your Customer and Beneficial owner information
- ❖ Support Electronic & Digital Payment Option
- ❖ Review Existing Transaction Monitoring Scenarios.
- ❖ Trade Based Money Laundering.
- ❖ All Employees to be watchful to detect suspicious transactions/activities.
- ❖ Be more cautious on Adverse Media report.

As per BFIU Circular 26 dated June 16, 2020 "the account of PEPs/Influential Person/Chief Executives or Top Level Officials of any international organization and their close family members or close associates account where necessary may take approval from Chief Anti Money laundering Compliance Officer (CAMLCO).

6.5 Policies and Procedures

An AML & CFT policy usually includes the 4 (four) key elements; they are -

- ❖ High level summary of key controls;
- ❖ Objective of the policy (e.g. to protect the reputation of the institution);
- ❖ Scope of the policy (A statement confirming that the AML/CFT policy applies to all areas of the

business); and

- ❖ Waivers and exceptions- procedures for obtaining exemptions from any aspects of the policy should be carefully controlled; and Operational controls.

6.5.1 Written AML & CFT Compliance Policy

At a minimum, the board of directors or the management committee of Bank Asia develop, administer, and maintain an AML & CFT compliance policy that ensures and monitors compliance with the Acts, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes.

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

The Policies should be tailored to the bank and would have to be based upon an assessment of the money laundering and terrorist financing risks, taking into account the bank's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering and terrorist financing.

It should include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures should address its Know Your Customer ("KYC") policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transactions, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness.

It should also include a description of the roles the AML&CFT Compliance Officers(s)/Unit and other appropriate personnel will play in monitoring compliance with and effectiveness of AML&CFT policies and procedures. It should develop and implement screening programs to ensure high standards when hiring employees. It should also implement standards for employees who consistently fail to perform in accordance with an AML&CFT framework. It should incorporate AML&CFT compliance into job descriptions and performance evaluations of appropriate personnel. It should have the arrangements for program continuity despite changes in management or employee composition or structure.

The AML&CFT policies should be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing AML&CFT related rules and regulations or business.

In addition the policy should emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and should set forth the consequence of non-compliance with the applicable laws and the institution's policy including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any bank with money laundering and terrorist financing activity.

6.5.2 Procedures

The standard operating procedures are often designed at a lower level in the organization and modified as needed to reflect the changes in products, personnel and promotions, and other day to day operating procedures. The

procedure will be more detailed than policies. Standard operating procedures translate policy into an acceptable and working practice. In addition to policies and procedures, there should also be a process to support and facilitate effective implementation of procedures and that should be reviewed and updated regularly.

6.6 Customer Acceptance Policy.

Bank Asia has developed a clear Customer Acceptance Policy which was approved by the board.

6.7 ML & TF Risk Assessment

Assessing AML & CFT risk is, therefore one of the most important steps in creating a good AML & CFT compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk – whether low, medium or high- must be identified and mitigated by the application of controls, such as verification of customer identity, customer due diligence policies, suspicious activity monitoring and sanctions screening. Money Laundering and Terrorist Financing risks vary across jurisdictions, geographical regions, customers, products and services, delivery channels, and over time. Bank Asia develops systems and procedures to detect, monitoring and report the riskier customers and transactions. Considering the issues, Branch can assess their risk level and the action taken against mitigation of risk. Bank Asia has developed ML & TF risk assessment procedure including the risk register which is mentioned in our ML & TF Risk Management guideline.

CHAPTER VII: ML & TF RISK ASSESMENT OF BANK ASIA

7.1 Preamble

The regulatory framework for combating money laundering and terrorist financing is applicable in the form of AML & CFT Regulations as amended from time to time. Keeping in view of growing sensitivities on domestic and international front, there is need to focus on the areas where related risks are relatively high in order to allocate resources in the most effective way. Accordingly, following guidelines are aimed at providing enabling environment for effective implementation of risk based approach considering banks' internal policies, procedures and risk parameters etc.

7.2 Risk

Risk can be defined as the combination of the probability of an event and its consequences. In simple term, risks can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur.

7.3 Assessing Risk

Banks should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks for customers, countries or geographic areas, products, services and transactions or delivery channels. They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities.

7.4 Risk Identification

7.5 Risk Assessment process

Having identified the risks involved, they need to be assessed or measured in terms of the chance (likelihood) they will occur and the severity or amount of loss or damage (impact) which may result if they do occur. The risk associated with an event is a combination of the chance (likelihood) that the event will occur and the seriousness of the damage (impact) it may do.

7.5.1 Methodology of Risk Assessment

Money Laundering and Terrorist Financing Risk Assessment Committee of Bank Asia PLC. has rated each risk element by-

- the chance of the risk happening – 'likelihood'
- the amount of loss or damage if the risk happened – 'impact' (consequence).

7.5.1.1 Likelihood Scale

A likelihood scale refers to the potential of an ML & TF risk occurring in the business for the particular risk being assessed. Three levels of risk are shown in the following Table, but the Bank can have as many as they believe are necessary:

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: Likelihood Scale

7.5.1.2 Impact of Scale

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen.

In assessing the possible impact or consequences, the assessment can be made from several viewpoints. It does not cover everything and it is not prescriptive. Impact of an ML & TF risk could, depending on individual business circumstances, be rated or looked at from the point of view of:

- how it may affect the business (if through not dealing with risks properly the entity suffer a financial loss from either a crime or through fines from the regulator)
- the risk that a particular transaction may result in the loss of life or property through a terrorist act
- the risk that a particular transaction may result in funds being used for any of the following: corruption, bribery, smuggling of goods/workers/immigrants, banking offences, narcotics offences, psychotropic substance offences, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud, forgery, extortion, smuggling of domestic and foreign currency, black marketing.
- the risk that a particular transaction may cause suffering due to the financing of illegal drugs
- reputational risk – how it may affect the business if it is found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being shunned by the community of customers
- how it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the business.

Three levels of Impact are shown in the following table, but the branch/department can have as many as they believe are necessary:

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	Minor or negligible consequences or effects.

Table: Impact of Scale

7.6 Risk matrix and risk score

A risk matrix has been developed combining of LIKELIHOOD and IMPACT in order to obtain risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk. How the risk score is derived can be seen from the risk matrix and risk score table shown below. Four levels of risk or score are shown in the following figure and table, but the bank can have as many as they believe are necessary.

Very Likely	Medium 2	High 3	Extreme 4
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2
What is the chance it will happen	Minor	Moderate	Major

Table: Risk Matrix and Score

Four levels of score have been shown in the matrix. The implication of each score is as follows:

Rating/Score	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.

7.7 Risk Assessment and Management Exercise

From the above discussion, the banks will have an idea to calculate risk score by blending likelihood and impact, the risk matrix and risk score and can assess the risks of individual customer, product/service, delivery channel and risks related to geographic region by using the simplified risk management worksheet. It can also fix up its necessary actions against the particulars outcomes of risks. All the exercises done by the banks would be called together "Risk Register" (Discussed in the chapter VII).

7.8 Risk Treatment

Manage the business risks by -

- ◆ minimizing and managing the risks; and
- ◆ applying strategies, policies and procedures

Manage the regulatory risks by -

- ◆ putting in place systems and controls; and
- ◆ carrying out the risk plan and AML & CFT program

This stage is about identifying and testing methods to manage the risks the bank may have identified and

assessed in the previous process. In doing this they will need to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk. Examples of a risk reduction or treatment step are:

- setting transaction limits for high-risk products;
- having a management approval process for higher-risk products;
- process to place customers in different risk categories and apply different identification and verification methods;
- not accepting customers who wish to transact with a high-risk country

7.9 Monitoring 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.

CHAPTER VIII: ML & TF RISK MANAGEMENT OF BANK ASIA

8.1 Risk Management

Risk management is a systematic process of recognizing risk and developing methods to both minimize and manage the risk. This requires the development of a method to identify, prioritize, treat (deal with), control and monitor risk exposures. In risk management, a process is followed where the risks are assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

8.2 Risk management and mitigation

Banks should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures must be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

Higherrisk - Where higher risks are identified banks should be required to take enhanced measures to manage and mitigate the risks.

Lowerrisk - Where lower risks are identified, countries may allow banks to take simplified measures to manage and mitigate those risks.

8.3 Which Risk do Banks Needs to Manage?

For the ML & TF aspects, BFIU expects a risk management practice to address two main risks: business risk and regulatory risk.

8.3.1 Business risk

Business risk is the risk that your business may be used for ML&TF. The banks must assess the following risks in particular:

- **customer risks** - Identifying risk determinants while establishing relationships with customer;
- **products or services risks** - Predicting risk attributes resulting from customer's need for financial services and appropriate controls;
- **business practices and/or delivery method risks**- Identifying risks associated with delivery channels which may vary from customer to customer depending on their needs;
- **country or jurisdictional risks** - Risks resulting from customer geographic presence and jurisdiction in which the customer is operating.

8.3.2 Regulatory risk

Regulatory risk is associated with not meeting all obligations of banks under the Money Laundering Prevention Act, 2012(amendment 2015), Anti Terrorism Act, 2009 (amendment 2012 & 2013) (including all amendments), the respective Rules issued under these two acts and instructions issued by BFIU. Examples of regulatory obligations are failure to report STR/SAR, unable or inappropriately verification of customers and lacking of AML & CFT program (how a business identifies and manages the ML & TF risk it may face) etc.

It is unrealistic that a bank would operate in a completely ML & TF risk-free environment. Therefore, it is suggested that a bank shall identifies the ML&TF risk it faces, and then works out the best ways to reduce and manage that risk.

8.4 Risk Management Process

In assessing and mitigating ML & TF risk, the bank should consider a wide range of financial products and services, which are associated with different ML & TF risks.

8.4.1 Risk Identification

The first step is to identify what ML & TF risks exist in a bank when providing designated services. Some examples of ML & TF risks associated with different banking activities:

Retail banking: provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services.

Corporate banking: where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions

Wealth management: culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.

Investment banking: layering and integration transfer of assets between parties in exchange for cash or other assets, global nature of markets.

Correspondent banking: high value transactions, limited information about the remitter and source of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

8.4.1.1 Business Risks

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

Customers

Followings are some indicators (but not limited to) to identify ML & TF risk arises from customers of a bank:

- a new customer;
- a new customer who wants to carry out a large transaction;
- a customer or a group of customers making lots of transactions to the same individual or group;
- a customer who has a business which involves large amounts of cash;
- a customer whose identification is difficult to check;
- a customer who brings in large amounts of used notes and/or small denominations;
- customers conducting their business relationship or transactions in unusual circumstances, such as:
 - significant and unexplained geographic distance between the institution and the location of the customer,
 - frequent and unexplained movement of accounts to different institutions,
 - frequent and unexplained movement of funds between institutions in various geographic locations;
- a non- resident customer;
- a corporate customer whose ownership structure is unusual and excessively complex;
- customers that are Politically Exposed Persons (PEPs) or Influential Persons (IPs) or Head of international organizations and their family members and close associates;
- customers submits account documentation showing an unclear ownership structure;
- customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income.

Products and services

- private banking i.e., prioritized or privileged banking;
- credit card;
- anonymous transaction;
- non face to face business relationship or transaction;
- payment received from unknown or unrelated third parties;
- any new product & service developed;
- service to walk-in customers;
- mobile banking.

Business practices/delivery methods

- direct to the customer;
- online/internet;
- phone;
- Fax;
- Email;
- third-party agent or broker.

Channels/Countries it does business in/with (jurisdictions)

- any country which is unidentified by credible sources as having significant level of corruption and criminal activity;
- any country subject to economic or trade sanctions;
- any country known to be a tax haven and unidentified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country;
- any country unidentified by FATF or FATF Style Regional Body (FSRBs) as not having adequate AML & CFT system;
- any country identified as destination of illicit financial flow.

8.4.1.2 Regulatory Risks

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

- customer/beneficial owner identification and verification not done properly;
- failure to keep record properly;
- failure to scrutinize staffs properly;
- failure to train staff adequately;
- not having an AML & CFT program;
- failure to report suspicious transactions or activities;
- not submitting 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, BB;
- not submitting accurate information or statement requested by BFIU, BB.

8.5 Risk Management Strategies

The banks may adopt the following components (where appropriate to the nature, size and complexity of its business), among others, as part of its risk management strategy:

- reviews at senior management level of the bank's progress towards implementing stated ML & TF risk management objectives;
- clearly defined management responsibilities and accountabilities regarding ML & TF risk management;
- adequate staff resources to undertake functions associated with ML & TF risk management
- specified staff reporting lines from ML & TF risk management system level to board or senior management level, with direct access to the board member(s) or senior manager(s) responsible for overseeing the system;
- procedural controls relevant to particular designated services;
- documentation of all ML & TF risk management policies;
- a system, whether technology based or manual, for monitoring the bank's compliance with relevant controls;
- policies to resolve identified non-compliance;
- appropriate training program(s) for staff to develop expertise in the identification of ML & TF risk(s) across the bank's designated services;
- an effective information management system which should:
 - produce detailed and accurate financial, operational and compliance data relevant to ML & TF risk management;
 - incorporate market information relevant to the global AML & CFT environment which may assist the banks to make decisions regarding its risk management strategy;
 - enable relevant, accurate and timely information to be available to a relevant officer (for example, the AML & CFT Compliance Officer) within the banks;
 - allow the banks to identify, quantify, assess and monitor business activities relevant to ML & TF risk(s);
 - allow the banks to monitor the effectiveness of and compliance with its internal AML & CFT systems and procedures;
 - allow the banks to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.

8.6 Ongoing Risk Monitoring

A bank's ongoing monitoring of its risk management procedures and controls may also alert the bank to any potential failures including (but not limited to):

- failure to include all mandatory legislative components;
- failure to gain board and/or executive approval of the AML & CFT program;
- insufficient or inappropriate employee due diligence;
- frequency and level of risk awareness training not aligned with potential exposure to ML & TF risk(s);
- changes in business functions which are not reflected in the AML & CFT program (for example, the introduction of a new product or distribution channel);
- failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML & CFT program;
- legislation incorrectly interpreted and applied in relation to a customer identification procedure;
- customer identification and monitoring systems, policies and procedures that fail to:
 - prompt, if appropriate, for further identification and/or verification when the ML & TF risk posed by a customer increases;
 - detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;
 - take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;
 - take appropriate action where the identification document provided is neither an original nor a certified copy;

- recognize foreign identification documentation issued by a high risk jurisdiction
- record comprehensive details of identification documents, for example, the date of issue;
- consult appropriate resources in order to identify high-risk customers;
- identify when an expired or old identification document (for example, a driver's license) has been used;
- collect any other name(s) by which the customer is known;
- lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers;
- lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:
 - customer identification policies, procedures and systems;
 - identifying potential ML & TF risks
- acceptance of documentation that may not be readily verifiable.

8.7 Higher Risk Scenario

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations include the following:

a. Customer risk factors

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer);
- Non-resident customers;
- Legal persons or arrangements that are personal asset-holding vehicles;
- Companies that have nominee shareholders or shares in bearer form;
- Business that are cash-intensive;
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

b. Country or geographic risk factors

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML & CFT systems;
- Countries subject to sanctions, embargos or similar measures;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity;
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

c. Product, service, transaction or delivery channel risk factors

- Private banking;
- Anonymous transactions (which may include cash);
- Non-face-to-face business relationships or transactions;
- Payment received from unknown or un-associated third parties.

8.7.1 Specific High Risk Elements and Recommendations for EDD

Some of the relatively high risk elements identified by AMLD and recommended actions for EDD may be as under:

S.No.	Customers	Recommendations for EDD
01	NPOs/NGOs/Charities, Trusts, Clubs, Societies, and Associations etc.	In relation to these customers, branches may: <ol style="list-style-type: none"> obtain a declaration from Governing Body / Board of Trustees / Executive Committee / sponsors on ultimate control, purpose and source of funds etc; obtain an undertaking from Governing Body/Board of Trustees/Executive Committee /sponsors to inform the bank about any change of control or ownership during operation of the
		account; and <ol style="list-style-type: none"> obtain a fresh Resolution of the Governing Body/Executive Committee of the entity in case of change in person(s) authorized to operate the account.
02.	Housewife accounts	In relation to housewife accounts, branches may- <ol style="list-style-type: none"> Obtain a self-declaration for source of fund. Besides this branch may obtain beneficial ownership information; Update details of funds providers, if any along with customer's profile; and Identify and verify funds providers if monthly credit turnover exceeds an appropriate threshold to be decided by banks.
03.	Landlords	In relation to such customers, branches may apply any recommend methods for assessment of source of funds/income e.g. collecting rent agreement copy etc.
04.	PEPs/IPs	In relation to such customers, branches may apply CDD as well as EDD process as this is a High Risk Account.
05.	Student Account	In relation to such customers, branches should- <ol style="list-style-type: none"> Obtain purpose of opening account; Source of fund; Beneficial owner information, if needed. Regular monitoring of transaction.
	Products & Services	Recommendations for EDD
01.	Online transactions	In relation to online transactions, Branches should pay special attention to geographical factors / locations for movement funds.
	Delivery Channels	Recommendations for EDD
01.	Wire transfers	In relation to wire transfers, branches may: <ol style="list-style-type: none"> monitor such transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and Ensure that funds transfers which are out of character/ inconsistent with the history, pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.

8.8 Low Risk Scenario

There are circumstances where the risk of money laundering or terrorist financing may be lower. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

a. Customer risk factors

- ◆ Banks – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements;

- ◆ Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- ◆ Public administrations or enterprises.

b. Product, service, transaction or delivery channel risk factors

- ◆ Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

c. Country risk factors

- ◆ Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML&CFT systems;
- ◆ Countries identified by credible sources as having a low level of corruption or other criminal activity. In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

Note that having a lower money laundering and terrorist financing risk for identification and verification purposes does not necessarily mean that the same customer poses lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

8.9 Risk Variables

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a bank should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- ◆ The purpose of an account or relationship;
- ◆ The level of assets to be deposited by a customer or the size of transactions undertaken;
- ◆ The regularity or duration of the business relationship.

8.10 Counter Measures for Risks

- a. Enhanced due diligence measures
- b. Simplified CDD measures
- c. Ongoing Due Diligence

(The above mentioned points are specified in the paragraph 9.3 of Chapter IX of this guidelines)

CHAPTER IX: COMPLIANCE STRUCTURE OF BANK ASIA

Compliance structure of Bank Asia is an organizational setup that deals with AML, CFT & CPF compliance of the bank and the reporting procedure. This includes-

- ❖ Central Compliance Committee (CCC),
- ❖ Chief Anti Money Laundering Compliance Officer (CAMLCO),
- ❖ Branch Anti Money Laundering Compliance Officer (BAMLCO),
- ❖ Branch Anti Money Laundering Officer (BAMLO)
- ❖ Departmental/Divisional Anti Money Laundering Compliance Officer (DAMLCO)

9.1 Central Compliance Committee

Under the obligation of BFIU Circular No. 26 dated June 16, 2020, "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 issued instructions time to time by BFIU, every bank must set up a Central Compliance Committee (CCC) will report directly to the Managing Director or the Chief Executive Officer of the bank." [Para 1.3,1 (ka) of BFIU Circular No. 26].

As per guideline of BFIU, the central compliance unit shall be headed by a high official, who will be known as the Chief Anti Money Laundering Compliance Officer (CAMLCO). In this case, 'High official' will be considered as an official not below than the 02 (two) tier of the Managing Director/Chief Executive Officer. In line with the BFIU guideline, Bank Asia has nominated Deputy Managing Director as CAMLCO. Before assigning the CAMLCO to other duties of the Bank, the management has to ensure that the AML, CFT & CPF activities of the bank will not be hampered for it.

As per guideline of BFIU, Bank can also nominate one or more Deputy of the CAMLCO, who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO). The DCAMLCO will be not below the rank of 'Deputy General Manager' or 'Senior Vice President' or 'Equivalent' of the bank. In line with the BFIU guideline, Bank Asia has designated both the CAMLCO and DCAMLCO who 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 & PF.

The AML & CFT Division shall issue instructions for the branches, where transaction monitoring system, internal control system, policies and techniques will be included to prevent Money Laundering and Terrorist Financing as and when required. The AML & CFT Division will report to BFIU without any delay in case of any account/business relationship found with any person/entity whose name/names appeared to the mass media (TV/News Paper) regarding ML, TF, PF or any predicate offences under MLPA, 2012 (Amendment, 2015). The CCC can also make a Suspicious Transaction Report (STR) or Suspicious Activity report (SAR) directly to BFIU in this regard.

9.2 Formation of Central Compliance Committee, Corporate Office (CCC)

Central Compliance Committee at Corporate Office of Bank Asia Ltd shall be constructed by the Heads of Division/ Department & Officials of different Division/Department including CAMLCO and DCAMLCO excluding the **officials of Internal Audit Department** under the directives of BFIU. For ensuring the independent audit function Internal Audit Department is not included in CCC of Bank Asia Ltd. CCC has been constructed by comprising the following:

1.	Deputy Managing Director & CAMLCO	Chairman
2.	Head of AML & CFT & DCAMLCO	Member Secretary

and as member, the Head of (Corporate Assets & Loan Liabilities, Human Resources Division, Retail Banking, Channel Banking, Islamic Banking, SME, CRM, ID, FRD, BOD, LSSD, CARDS, and so on)

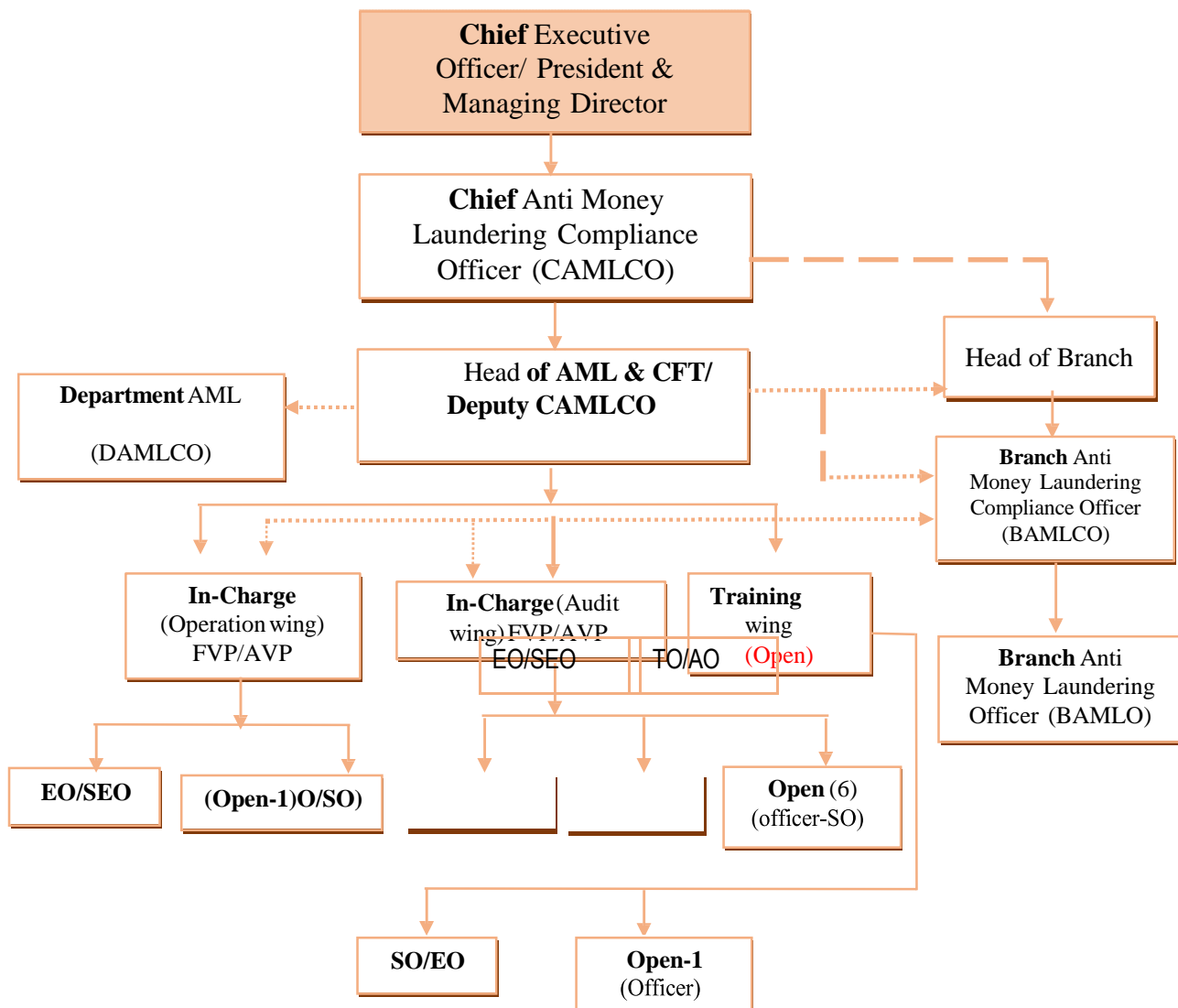
9.3 Responsibilities and Authorities of the CCC:

CCC is the prime mover of the Bank Asia for ensuring the compliance of AML, CFT & CPF measures. Its main responsibilities are to—

- i. develop the bank's policy, procedure and strategies in preventing ML, TF & PF;
- ii. coordinate bank AML & CFT compliance initiatives;
- iii. coordinate the ML & TF risk assessment of the bank and review thereon;
- iv. present the compliance status with recommendations before the President & Managing Director on half yearly basis;
- v. forward STR/SAR and CTR to BFIU in time and in proper manner;
- vi. report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner;
- vii. impart training, workshop, seminar related to AML, CFT & CPF for the employee of the bank;
- viii. take required measures to submit information, report or documents in time.

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

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

Organogram of the AML & CFT Division:**9.4 Chief Anti Money Laundering Compliance Officer (CAMLCO)**

Bank Asia has designated Chief Anti Money Laundering Compliance Officer (CAMLCO) at its Corporate Office with sufficient authority to implement and enforce corporate wide AML, CFT & CPF policies, procedures and measures and who will report directly to President & Managing Director. This provides evidence of senior management's commitment to efforts to combat money laundering and terrorist financing and, more importantly, provides added assurance that the officer will have sufficient influence to enquire about potentially suspicious activities. The CAMLCO is responsible for oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering and terrorist financing.

The designated CAMLCO, directly or through the CCC, is the central point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML, CFT & CPF program.

All staffs engaged in the Bank Asia at all levels must be aware of the identity of the CAMLCO, DCAMLCO and the Officials of AMLD and branch/SME Service Center/Islamic Wing level AML, CFT & CPF compliance officers, and the procedure to follow when making a suspicious transaction/activity report. All relevant staffs must be aware of the chain through which suspicious transaction/activity reports should be passed to the CAMLCO.

As the CAMLCO is responsible for the oversight of all aspects of the bank's AML, CFT & CPF activities and is the focal point for all activity within the bank relating to ML & TF his/her job description should clearly set out the extent of the responsibilities given to him/her. The CAMLCO will need to be involved in establishing the basis on which a risk-based approach to the prevention of ML, TF & PF is put into practice.

9.5 Authorities and Responsibilities of CAMLCO

Authorities-	Responsibilities-
<ul style="list-style-type: none"> i. CAMLCO shall act on his own authority; ii. He/she shall not take mandatorily any permission or consultation from/with the Managing Director before submission of STR/SAR and any document or information to BFIU; iii. He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU; iv. He/she must have access to any information of the bank; v. He/she shall ensure his/her continuing competence 	<ul style="list-style-type: none"> i. CAMLCO must ensure overall AML, CFT & CPF compliance of the bank; ii. oversee the submission of STR/SAR or any document or information to BFIU in time; iii. maintain the day-to-day operation of the bank' iv. AML, CFT & CPF compliance; v. CAMLCO will inform to Managing Director or Board of Director for proper functioning of CCC/AML & CFT Division ; vi. CAMLCO shall review and update ML, TF & PF risk assessment of the bank; vii. Corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.

9.6 Role of Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO):

- Deputy CAMLCO is the first point of contact for any AML/CFT/KYC/CDD issues of BAP
- Deputy CAMLCO is Responsible for overseeing the compliance function.
- Act as principal interface between the internal stake holders and compliance resources.
- Ensure day to day compliance with applicable money laundering prevention laws, rules and regulations.
- Coordinate with BFIU, Other Regulatory bodies and law enforcement agencies in respect of suspicious activity reporting, Cash Transaction Report and any other issues as required.
- Develop and maintain ongoing relationships with regulatory authorities, Government agencies external & internal audit teams and Head of Branches.
- Supervise Transaction Monitoring and Sanction Screening;
- Respond to AML & CFT questionnaire of different foreign corresponding Banks;
- Development, update and enforcement of Money Laundering & Terrorist Financing Risk Management Guideline, Guideline for prevention of Money laundering & Terrorist Financing and Customer Acceptance Policy etc;
- Evaluating self-assessment reports received from the branches and AML Audit report from ICCD and Prepare Half yearly report on AML/CFT activities for submission to Triple C, MD & CEO & BFIU;
- Evaluate and investigate suspicious activity/transactions reports and recommend to CAMLCO for filling TSR/SAR to BFIU and arrange to preserve all such SAR/STR reports;
- Prepare AML-CFT Training calendar and arrange & conduct training on AML-CFT for all levels employees in collaboration with BAITD and HRD;
- Maintain an effective communication with across the bank through prudent reporting and escalation of serious risk vulnerabilities, control gaps of failures to Triple C.

9.7 Branch Anti Money Laundering Compliance Officer (BAMLCO)

Under the obligation of BFIU Circular No.26 dated June 16,2020 “for the implementation of all existing acts, rules, BFIU’s instructions and bank’s own policies on preventing ML TF & PF, bank shall nominate Head of Branch or Manager Operation of the Branch or even Experienced General Banking Official as Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch.”

In Bank Asia, under the directive of BFIU, the Manager Operations of the Branch/SME Service Center/Islamic Wing will be nominated as the “BAMLCO”. Bank Asia is desire to maintain the highest level of AML, CFT & CPF compliance, Branch will also nominate another official as “Branch Anti Money Laundering Officer (BAMLO)”.

Both BAMLCO and BAMLO have to have sufficient knowledge in the existing acts, rules and regulations, BFIU's instructions (circulars, circular letters, etc.) and our own policies on preventing Money Laundering, Terrorist Financing and Proliferation Financing.

BAMLO will assist BAMLCO to do the job successful and effective regarding AML, CFT & CPF issues. In absence of BAMLCO, BAMLO will act as BAMLCO to mitigate the AML, CFT & CPF matters.

9.8 Responsibilities and Authorities of BAMLCO

AML & CFT Division has circulated different Instruction Circulars time to time. AML & CFT Division, Corporate Office instruction circular no. 05/16 dated 02.06.2016, instruction circular no. 07/15 dated March 22, 2015, Interoffice Memorandum No- 96/12 dated May 07, 2012, Interoffice Memorandum No-107/09 dated 04.11.2009, Instruction circular no-INFO/2007/ID-20 dated 14.06.2007, and Instr/2007/ICCD-03/18 dated 04.07.2007 regarding assignment of BAMLCO and BAMLO in branches for monitoring and supervising AML, CFT & CPF issues. Hence, BAMLCO & BAMLO will be responsible to monitor & supervise all AML & CFT issues/matters as per Acts and Circulars of BFIU, Bangladesh Bank.

Responsibilities of BAMLCO

BAMLCO will perform the following responsibilities:

Knowledge on AML, CFT & CPF issues:

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

Branch Compliance Program:

1. Implement all instructions of AML & CFT Division/CCC regarding AML & CFT issues time to time.

Sanctions Screening:

1. 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.
2. Reviews suspected matches and reports valid matches to the AML & CFT Division/CCC, Corporate Office for onward submission to regulatory authority

Customer Due Diligence:

1. Identify and verify the identity of the customer information and documents obtained from the reliable source.
2. Ensure the KYC of all customers have done properly.
3. Ensure the update of KYC of the customer have done timely.
4. Ensure due diligence while establishing relationship with the new customer and also while conducting financial transaction with the existing customer.
5. Ensure due diligence when there is a suspicion of ML, TF & PF.
6. Ensure due diligence of walk-in customer, online customers and depositor or withdrawer other than account holder.
7. Identify the beneficial owner of the account and conduct due diligence of the beneficial owners.
8. 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):

1. Obtain CAMLCO approval where necessary of for establishing or continuing existing business relationship with PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates as per circular no. 26 dated June 16, 2020.
2. Confirm EDD of PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates.
3. Comply Enhance Due Diligence (EDD) for the high risk customer and obtain additional information/documents.
4. 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:

1. Introduce self-auditing, self-assessment and independent testing procedure in the branch and report to ICCD & AML & CFT Division in time.
2. Ensure regular transaction monitoring to find out any unusual transaction. Records of all transaction monitoring should be kept in the file.
3. Review cash transaction to find out any structuring;
4. Ensure monitoring of account transaction as per instruction of BFIU as well as AML & CFT Division.

Risk Grading of Customer:

1. Ensure proper risk grading of the customer with compare to his occupation, product/services, source of fund, transaction profile (TP), delivery channel and geographical location of the customer.
2. Detect high risk customer using subjective/objective judgment and ensure proper filing.

Update Customer Information and TP & KYC:

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

Arrangement of AML & CFT Meeting:

1. BAMLCO shall arrange quarterly meeting regarding AML, CFT & CPF issues as per instruction of BFIU circular no. 26 dated 16.06.2020 in the branch level and confirm all the employees are present in the meeting.
2. BAMLCO shall take effective measures on the following matters after reviewing the compliance of the existing rules, acts to prevent ML, TF and PF: a) KYC, b) Transaction Monitoring, c) Identification of STR/SAR and reporting, d) Record Keeping, and e) Training.

Report Submission to AML & CFT Division:

1. Review Monthly Cash Transaction Report (CTR), Quarterly (Meeting Minutes), Half-yearly (Self-Assessment) statements and send these to AML & CFT Division within the stipulated time period without any fail. Conduct meeting before finalization of Self-Assessment report.
2. Review information and documents before submitting those reports to AML & CFT Division for onward submission to BFIU.

STR/SAR Identification and Reporting:

1. Report STR/SAR by monitoring and analyzing transaction.
2. Review the CTR of each month and find out STR/SAR and send it to AML & CFT Division.
3. Ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
4. Analyze the Cash Transactions immediate below the CTR threshold limit to identify structuring.
5. Monitor customer unusual behavior and unusual transaction pattern.
6. 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:

1. Keep records of customer's identification and transactions at least five years after the termination of relationships with the customers.
2. Ensure that the branch is maintaining AML, CFT & CPF files properly and record keeping is done as per the requirements.
3. Ensure confidentiality of the records preserved.

Training of employees:

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

Others responsibilities:

1. Ensure all the required information and document are submitted properly to CCC/AML & CFT Division and any freeze order or stop payment order are implemented properly and without delay;
2. 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;
3. Create awareness regarding AML, CFT & CPF among the customer of the branch.
4. Ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.
5. 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. Any other responsibility assigned by the CCC/ AML & CFT Division.

Authorities of BAMLCO

For shouldering these responsibilities and preventing ML, TF & PF in the branch, Bank Asia will consider to give the following authority to

BAMLCO:

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

Branch AML Officer (BAMLO) will be reliever of BAMLCO at the time of absence and all responsibilities then will be applicable upon BAMLO.

DAMLCO: In addition, Bank Asia has assigned a Departmental/Divisional AML Compliance Officer (DAMLCO) under the Instruction of Bangladesh Bank Money Laundering & Risk Management Guideline 2015 para 43 to perform the departmental/divisional AML, CFT & CPF related compliance program smoothly.

DAMLCO will perform the following responsibilities:

- ❖ Timely respond to AML & CFT Queries
- ❖ Take proper initiative to mitigate to ML, TF & CPF.
- ❖ Ensure that corrective actions have taken by the department to prevent ML & TF.
- ❖ If suspicious activity or transaction is detected promptly report it to AML & CFT division.

9.9 Internal Control and Compliance

Under the obligation of 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 the Internal Audit Department 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 Report received from the branches and to execute the Independent Testing Procedure appropriately.”

Internal Control & Compliance Department (ICCD) of Bank Asia shall have an important role for ensuring proper implementation of bank’s AML, CFT & CPF Compliance Program. ICCD of Bank Asia is equipped

with enough manpower and autonomy to look after the prevention of ML, TF & PF. The ICCD has to oversee the implementation of the AML, CFT & CPF compliance program of the bank and has to review the 'Self-Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

To ensure the effectiveness of the AML, CFT & CPF compliance program, bank should assess the program regularly and look for new risk factors. FATF recommendation 18 suggests that-

Financial institutions should be required to implement programs against money laundering and terrorist financing. Financial groups should be required to implement group wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML, CFT & CPF purposes. Financial institutions should be required to ensure that their foreign branches and majority owned subsidiaries apply AML, CFT & CPF measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programs against money laundering and terrorist financing'.

An institution's 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 audit must-

- ❖ understand ML, TF & PF risk of the bank and check the adequacy of the mitigating measures;
- ❖ examine the overall integrity and effectiveness of the AML, CFT & CPF 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 & CPF 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;
- ❖ assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- ❖ determine when assessing the training program and materials:
 - the importance of the board and the senior management place on ongoing education, training and compliance,
 - employee accountability for ensuring AML, CFT & CPF 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.

9.10 Employee Training and Awareness Program

A formal AML, CFT & CPF compliance program should include an ongoing employee training program. The importance of a successful training and awareness program cannot be overstated. Employees in different

business functions need to understand how the financial institution's policy, procedures, and controls affect them in their day to day activities which has been narrated under FATF recommendation 18. As per AML circular, each financial institution shall arrange suitable training for their officials to ensure proper compliance of ML and TF prevention activities.

CHAPTER X : CUSTOMER DUE DILIGENCE OF BANK ASIA

10.1 Preamble

A sound Customer Due Diligence (CDD) program is one of the best ways to prevent money laundering and other financial crime. The more you know about its customers, the greater chance of preventing money laundering abuses.

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.

The CDD obligations on banks under legislation and regulation are designed to make it more difficult to abuse the banking industry for money laundering or terrorist financing. The CDD obligations compel banks to understand who their customers are to guard against the risk of committing offences under MLP Act 2012, (amendment, 2015) including 'Predicate Offences' and the relevant offences under ATA, 2009 (amendment 2012 & 2013).

Therefore, Bank Asia demonstrate supervisory authority to put in place, implement adequate CDD measures considering the risks of money laundering and terrorist financing. Such risk sensitive CDD measures 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 Know Your Customer (KYC) program is an essential part of financial institutions' risk management policies. Having sufficiently verified/corrected information about customers - "Knowing Your Customer" (KYC) - and making use of that information underpins all AML & CFT efforts, and is the most effective defense against being used to launder the proceeds of crime.

Bank with inadequate KYC program may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the Bank's overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences. Bank Asia therefore, need to carry out customer due diligence for two broad reasons:

- to help the organization, at the time due diligence is carried out, to be reasonably satisfied to those customers who they say about, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government or international sanctions) to provide them with the product or service requested; and
- to enable the organization in investigation, law enforcement by providing available information about customers in due process.

It may be appropriate for the bank to know more about the customer by being aware of the nature of the customer's business in order to assess the extent to which his transactions and activity undertaken with or through the bank is consistent with that business.

10.2 Legal Obligations of CDD

Under the obligation of MLPA, 2012, "The branch shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to Bangladesh Bank"

According to MLP Act 2012, SRO No. 357-Law/2013 dt. 21/11/2013, part-vi, sec-17(3) under MLP rules 2013, the bank shall identify the customer (whether permanent or occasional, and whether natural or legal person or legal

arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data). The verification of identity of a customer or a beneficial owner should include a series of independent checks and inquiries and not rely only on documents provided by the customer or beneficial owner. The bank shall verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person.

The bank shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the bank is satisfied that it knows who the beneficial owner is.

The bank shall understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship. The bank shall also conduct ongoing due diligence on the business relationship.

(6)(a) The bank shall scrutinize the transactions undertaken by a customer throughout the relationship with the customer to ensure that the transactions are consistent with the nature, business and risk profile of the customer, including where necessary, with the source of funds.

(6)(b) The bank shall keep up-to-date documents, data, information and so on collected under CDD process and review the existing records, particularly for high risk categories customers with utmost care and need to mitigate any sort of risk.

10.3 General Rule of CDD

Completeness and Accuracy of the customer information

Branch must take customer's identity and underlying purpose of establishing relationship with the branch, and should collect sufficient information up to its satisfaction. "Satisfaction of the bank" means satisfaction of the appropriate authority that is necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

It is an obligation for branches to maintain complete and accurate information of their customer and person acting on behalf of a customer. Complete refers to combination of all information for verifying the identity of the person or entity. For example: name and detail address of the person, profession, source of funds, Passport/National Identity Card/Birth Registration Certificate with acceptable ID card with photo, phone/mobile number etc., Accurate refers to such complete information that has been verified for accuracy.

KYC procedures refer knowing a customer physically and financially. This means to conduct an effective KYC, it is essential to accumulate complete and accurate information about the prospective customer.

Branch should verify this information using reliable, independently sourced documents and data. Documentary verification procedures include:

- Confirming the identity from an unexpired official document that bears a photograph of the customer.
- Confirming the validity of the official documentation (like NID checking through software provided by Election Commission).
- Confirming the residential address (by obtaining Utility Bill/physical verification/sending thanks letter).

If the Branch is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, unable to identify the beneficial owner taking reasonable measures, unable to obtain information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer. **Annexure-A (KYC Documentation)** provides an example of collection of documents and verification process of customer before opening account or conducting any transaction.

Ongoing CDD measures (Review and update)

Branches should take necessary measures to review and update the KYC of the customer after a certain interval. This procedure shall have to be conducted in every two years in case of low risk customers. Furthermore, this procedure shall have to be conducted in every year in case of high risk customers. But, branches should update the changes in any information on the KYC as soon as branch gets to be informed. Moreover, branches should update KYC information anytime if there is any particular necessity realized. Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay.

Branch should collect the Transaction Profile of customer account in the specified form. After reviewing the nature of the customer, the source of money/fund in the account and the nature of transaction, branch should again collect the Transaction Profile along with the amendments in it from the customer by reviewing the transactions of the customer within 6 (six) months of establishing business relation and assessing the effectiveness with a logical consideration.

Enhanced CDD measures for high risk customer

Branches should conduct Enhanced CDD measures, when necessary, in addition to normal CDD measures. Branch should conduct Enhanced Due Diligence (EDD) under the following circumstances in line with BFIU:

- ❖ Individuals or legal entities scored with high risk;
- ❖ Individuals who are identified as Politically Exposed Persons (PEPs), Influential Persons and Chief Executives or Top level officials of any international organization;
- ❖ Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes;
- ❖ 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 and terrorism financing (such as the countries and territories enlisted as High-Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force's Public Statement).

Higher risk customers and their transactions should be reviewed even more closely at account opening and more frequently during their account relationships. Branch should consider obtaining additional information from high risk customers such as:

- ❖ Source of funds and wealth
- ❖ Identifying information on individuals with control over the account, such as signatories or guarantors
- ❖ Occupation or type of business
- ❖ Financial statements
- ❖ Reference checking
- ❖ Domicile/Residence
- ❖ Proximity of the customer's residence, place of employment, or place of business
- ❖ Description of the customer's primary trade area and whether international transactions are expected to be routine.
- ❖ Description of the business operations, the anticipated volume of currency and total sales, and list of major customers and suppliers.
- ❖ Explanation of changes of account activity.

Simplified CDD measures

Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is

appropriate where there is little opportunity or risk of the services or customer becoming involved in money laundering or terrorist financing. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). The possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

10.4 Timing of CDD

A branch must apply CDD measures when it does any of the following:

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

10.5 Transaction Monitoring

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

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

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

10.6 Exception when opening a bank account with Bank Asia

The verification of the documents of account holder may take place after the account has been opened, provided that there are adequate safeguards in place to ensure that, before verification has been completed

- a) the account is not closed;

- b) transaction is not carried out by or on behalf of the account holder (including any payment from the account to the account holder)

10.7 In case where conducting the CDD measure is not possible

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

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

Branch should always consider whether an inability to apply CDD measures is caused by the customer. In this case, the branch should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the branch should consider whether there are any circumstances which give grounds for making a report to BFIU.

If the branch concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be sent to the BFIU. The branch must then retain the funds until consent has been given to return the funds to the source from which they came.

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

10.8 Customer Identification

Customer identification is an essential part of CDD measures. For the purposes of this Guidance Notes, a customer includes:

- ❖ the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);
- ❖ the beneficiaries of transactions conducted by professional intermediaries; and
- ❖ any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for branches to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware of any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

Whenever the opening of an account or business relationship is being considered, or a one-off transaction or series of linked transactions is to be undertaken, identification procedures must be followed. Identity

must also be verified in all cases where money laundering is known, or suspected.

Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken. Records must be maintained as set out Chapter VII (Record Keeping), and information should be updated or reviewed as appropriate.

10.9 Verification of Source of Funds

Branch should collect and verify the document supporting source of fund of the person at the time of establishing any business relationship or while conducting CDD. The document could include present employment identity, salary certificate/copy/advice, pension book, financial statement, income tax return, business documents or any other documents that could satisfy the branch. The branch should request the person to produce E-TIN (Electronic Tax Identification Number) certificate which declares taxable income.

10.10 Verification of Address

Branch should verify the address of the person at the time of establishing any business relationship or while conducting CDD. This could be done through the physical verification by the branch or by standard mail or courier service correspondence. The branch could collect any other document (recent utility bill mentioning the name and address of the customer) as per their satisfaction.

Verification of the information obtained must be based on reliable and independent sources – which might either be a document or documents produced by the customer, or electronically by the branch, or by a combination of both. Where business is conducted face-to-face, branch should see original of any documents involved in the verification.

10.11 Persons without Standard Identification Documentation

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

Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address. A Head of Branch may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

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

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

10.12 Walk-in/one off Customers

Branch should collect complete and accurate information while serving Walk-in customer, i.e. a customer without having account. Branch should know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT.

Branch must collect complete and accurate information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit, branch should identify sources of funds as well.

10.13 NonFaceToFaceCustomers

Non face to face customer refers to "the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the premises of bank branch". To avoid money laundering and terrorist financing risks while providing service to non-face to face customer, branch should apply one or more of the following measures of control:

- a) Ensuring that the customer's identity is established by additional ID documents, information provided by the Government Department or agency should be verified.
- b) Certified true copy of Passport/NID must be collected, where there is a non face to face contract.

10.14 Customer Unique Identification Code

Branch should use unique identification code for any customer maintaining more than one account or availing more than one facilities from our bank. Such unique identification system could facilitate banks to avoid redundancy, and saves time and resources. This mechanism also enables banks to monitor customer transactions effectively.

10.15 Corresponding Banking

Cross Border Correspondent banking shall refer to "providing banking services to another bank (respondent) by a bank (correspondent). These kinds of banking services shall refer to credit, deposit, collection, clearing, payment, cash management, international wire transfer, drawing arrangement for demand draft or other similar services.

Bank should establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank through collection of information as per BFIU Circular No. 26 dated June 16, 2020. The Bank should also obtain approval from its senior management before establishing and continuing any correspondent relationship. The Bank must be sure about the effective supervision of that foreign bank by the relevant regulatory authority. Bank should not establish or maintain any correspondent relationship with any shell bank and not to establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank.

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

The bank will not allow third parties use its correspondent bank account(s) i.e. in the form of "Payable through account".

10.16 Politically Exposed Persons (PEPs), Influential Persons and Chief Executives or Top Level Officials of any International Organization

All Clients must be subject to an assessment to determine whether they are PEP's or Influential Persons or chief executives or top level officials of any international organization and their linked entities. These customers pose a higher risk of money laundering, bribery, corruption and reputational risk to the bank due to their current or former position of political power or influence, which makes them more vulnerable to corruption. Relationships with these customers may increase the risk to the bank due to the

possibility of that individuals holding such positions may misuse their power and influence for personal gain or advantage or for the personal gain or advantage of their Close Family Members and Close Associates. The person's status (PEPs, Influential Persons and chief executives or top level officials of any international organization) itself does not incriminate individuals or entities. It does, however, put a prospective or existing Client into a higher risk category.

Branch will send copy of Account Opening Form (AOF) of PEPs, Influential Person, Higher Management employees of International Organization and their close family members and close associates to Anti Money Laundering & Combating Financing on Terrorism Department (AML & CFT Division). After scrutinizing the said AOF, AML & CFT Division will obtain approval from Chief Anti Money Laundering Compliance Officer (CAMLCO), if found in order. The management of the said branch (es) is hereby instructed to closely monitor them.

10.17 Wire Transfer

"Wire transfer" refers to such financial transactions that are carried out on behalf of an originator (person or institution) through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution.

10.18 Cross-Border Wire Transfers

Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all cross-border wire transfers involving an amount equivalent to USD.1000.00 and above are accompanied by the following information before transmitting the same to Intermediary/Beneficiary Banks:

Collected&preservedthecompleteandaccurateoriginator/applicantinformationsuchas:

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

Collected&preservedthemeaningfulbeneficiaryinformationsuchas:

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

Furthermore, for cross-border wire transfers, below the threshold (USD.1000.00) full and meaningful originator information has to be preserved. For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved.

Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file has to contain required and accurate originator information, and full beneficiary information. In addition, bank should include the account number of the originator.

10.19 Domestic Wire Transfers

In case of threshold domestic wire transfers of at least BDT 25,000/- (twenty five thousands), complete and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank/institutions. Furthermore, for domestic wire transfers below the threshold full and meaningful originator information has to be preserved. For providing money of domestic wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved. Mobile financial services providing department should use KYC format provided time to time by Payment System Department, Bangladesh Bank, in addition to aforesaid instructions. In case of wire transfer by using debit or credit card (except buying goods and services), similar information as above has to be preserved in the payment related message/instructions.

10.20 Duties of Ordering, Intermediary and Beneficiary Bank in case of Wire Transfer

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

Intermediary Bank:

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

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

Beneficiary Bank:

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

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

10.18 CDD for Beneficial Owner

Branch should apply CDD obligations for the beneficial owners of the accounts before or during the course of establishing a business relationship or conducting occasional transactions. In doing so, banks should put in place appropriate measures to identify beneficial owner. Branch, upon its own satisfaction ensure CDD of beneficial ownership by collecting information and documents from independent and reliable sources that includes publicly available information, information from customer or information from other reliable sources. Banks should consider following aspects while identifying beneficial ownership includes:

- Any natural person operating accounts on behalf of customer;
- Any person (whether acting alone or together) who has controlling interest or ownership

interest on a customer who might be legal entity or legal arrangements. Where there is any doubt identifying controlling interest, the banks should consider other means to determine controlling interest or ownership of a legal entity or arrangements. In addition to that bank should also consider reasonable measures to verify the identity of the relevant natural person who hold senior management position;

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

Where, a natural or legal persons who holds controlling interest, listed on a stock exchange and subjects to disclosure requirements or majority owned subsidiaries of such listed companies may exempted from identifying or verifying beneficial ownership requirements.

10.19 Management of Legacy Accounts

Legacy accounts refers those accounts opened before 30 April, 2002 and yet to update KYC procedures. These legacy accounts should be treated as "Dormant". No withdrawal should be permitted in those accounts; however, deposit can be permitted. These accounts will be fully functional only after conducting proper CDD measures. Central Compliance Unit should preserve data of such accounts at their end.

CHAPTER XI : 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.

Branch 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.

11.1 Statutory Requirement

The requirement contained in Section 25 (1) of Money Laundering Prevention Act 2012 (Amendment 2015) to retain correct and full records of customers' identification and transactions while operating an account of a customer, and to retain the records of customers' identification and transactions at least for five years after closing of relationships with the customers are essential/important constituents of the audit trail that the law seeks to establish.

FATF recommendation 11 states that financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

The records prepared and maintained by any FI on its customer relationship and transactions should be such that:

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

Records relating to verification of identity will generally comprise:

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

Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. pertaining to:
 - i. the customer;
 - ii. the beneficial owner of the account or product;
 - iii. the non-account holder conducting any significant one-off transaction;
 - iv. any counter-party;
- Details of transaction including:
 - i. nature of such transactions;

- ii. volume of transactions customer's instruction(s) and authority(ies);
- iii. source(s) of funds;
- iv. destination(s) of funds;
- v. book entries;
- vi. custody of documentation;
- vii. date of the transaction;
- viii. form in which funds are offered and paid out;
- ix. parties to the transaction;
- x. Identity of the person who conducted the transaction on behalf of the customer.

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

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

Under the obligation of MLP Rules, 2013, 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.

11.2 Legal Obligations

Under the obligation of 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 Bangladesh Bank"

Under the obligation of MLP Rules, 2013, 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.

11.3 Obligations under Circulars

Under the obligations of BFIU Circular No. 26 dated June 16, 2020–

1. All necessary information/ documents of customer's domestic and foreign transactions has to be preserved for at least 5(five) years after closing the account.
2. All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved for at least 5(five) years after closing the account.
3. All necessary information/documents of a walk-in Customer's transactions has to be preserved for at least 5 (five) years from the date of transaction.
4. Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence.
5. Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU.

11.4 Records to be kept

The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that a bank meets its obligations and that, in so far as is practicable, in any subsequent investigation the bank can provide the authorities with its section of the audit trail. The records shall cover:

- customer information
- transactions
- internal and external suspicion reports
- report from AML & CFT Division/CAMLCO
- training and compliance monitoring
- information about the effectiveness of training

11.5 Customer Information

In relation to the evidence of a customer's identity, branch must keep a copy of or the references to, the evidence of the customer's identity obtained during the application of CDD measures. Where a branch has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. A branch may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. The date when the relationship with the customer ends is the date:

- an occasional transaction, or the last in a series of linked transactions, is carried out; or
- The business relationship ended, i.e. the closing of the account or accounts.

11.6 Transactions

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the branch's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques should be maintained in a system from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed.

11.7 STR/SAR and Investigation

Where a FI has submitted a report of suspicious transaction to BFIU or where it is known that a customer or any transaction is under investigation, it should not destroy any records related to the customer or transaction without the consent of the BFIU or conclusion of the case even though the five-year limit may have been elapsed. To ensure the preservation of such records the financial institutions should maintain a register or tabular records of all investigations and inspection made by the investigating authority and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

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

11.8 Internal and External Reports

A branch should make and retain:

- records of actions taken under the internal and external reporting requirements; and
- When the nominated officer has considered information or other material concerning possible money laundering but has not made a report to BFIU, a record of the other material that was considered.

In addition, copies of any STRs made to the BFIU should be retained for five years. Records of all internal and external reports should be retained for five years from the date the report was made.

11.9 Other Measures

Bank's records should include:

- (a) in relation to training:
 - dates AML training was given;
 - the nature of the training;
 - the names of the staff who received training; and
 - the results of the tests undertaken by staff, where appropriate.
- (b) in relation to compliance monitoring
 - reports to senior management; and
 - records of consideration of those reports and of any action taken as a consequence.

11.10 Formats and Retrieval of Records

To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of a bank, provided that they have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form and that can be reproduced and recollected without undue delay.

It is not always necessary to retain documents in their original hard copy form, provided that the bank has reliable procedures for keeping records in electronic form, as appropriate, and that these can be reproduced without undue delay.

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

place and in what form.

11.11 Training Records

Financial institutions will comply with the regulations concerning staff training, they shall maintain training records which include:-

- i. details of the content of the training programs provided;
- ii. the names of staff who have received the training;
- iii. the date/duration of training;
- iv. the results of any testing carried out to measure staffs understanding of the requirements;
and
- v. an on-going training plan.

CHAPTER XII : REPORTING TO BFIU

12.1 Legal Obligations

Under the obligations of MLPA, 2012 (amendment 2015), “The reporting organizations shall have to report any suspicious transaction (defined in Section 2(Z) of MLPA, 2012(amendment 2015) and Section 2(16) of ATA, 2009(amendment 2013)) to the BFIU immediately on its own accord”

Under the obligations of MLP Rules 2013, “Every bank is obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self-assessment, independent testing procedure etc.) to BFIU without any delay or in due time. Besides they have to produce any document that is sought by BFIU.”

12.2 Suspicious Transaction Reporting

Money Laundering Prevention Act, 2012 (amendment 2015) defines suspicious transaction as follows-

„Suspicious Transaction• means such transactions –

- that deviates from usual transactions;
- with regards to any transaction, there is ground to suspect that,
 - the property is the proceeds of an offence,
 - it is financing to any terrorist activity, a terrorist group or an individual terrorist;
- Any transaction or attempted transaction that are delineated in the instructions issued by Bangladesh bank from time to time for the purpose of this act.

Anti Terrorism Act, 2009 (Amendment 2013) defines suspicious transaction as follows-

„Suspicious Transaction• means such transactions –

- which is different 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;
- which is any other transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.

The final output of an AML & CFT compliance program is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the AML & CFT risk for branch. Therefore it is necessary for the safety and soundness of the branch. 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 activities or the transactions are not seems to be usual manner. Such report is to be identified by the branch and send to AML & CFT Division for onward submission to the competent authorities i.e. to BFIU. Suspicion basically involves a personal and subjective assessment. The branch has to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

12.3 Identified 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 unusual transactions/activities may something be sourced as follows:

- Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable

explanation;

- By monitoring customer transactions;
- By using red flag indicators (**Annexure B**).

A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile 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.

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-

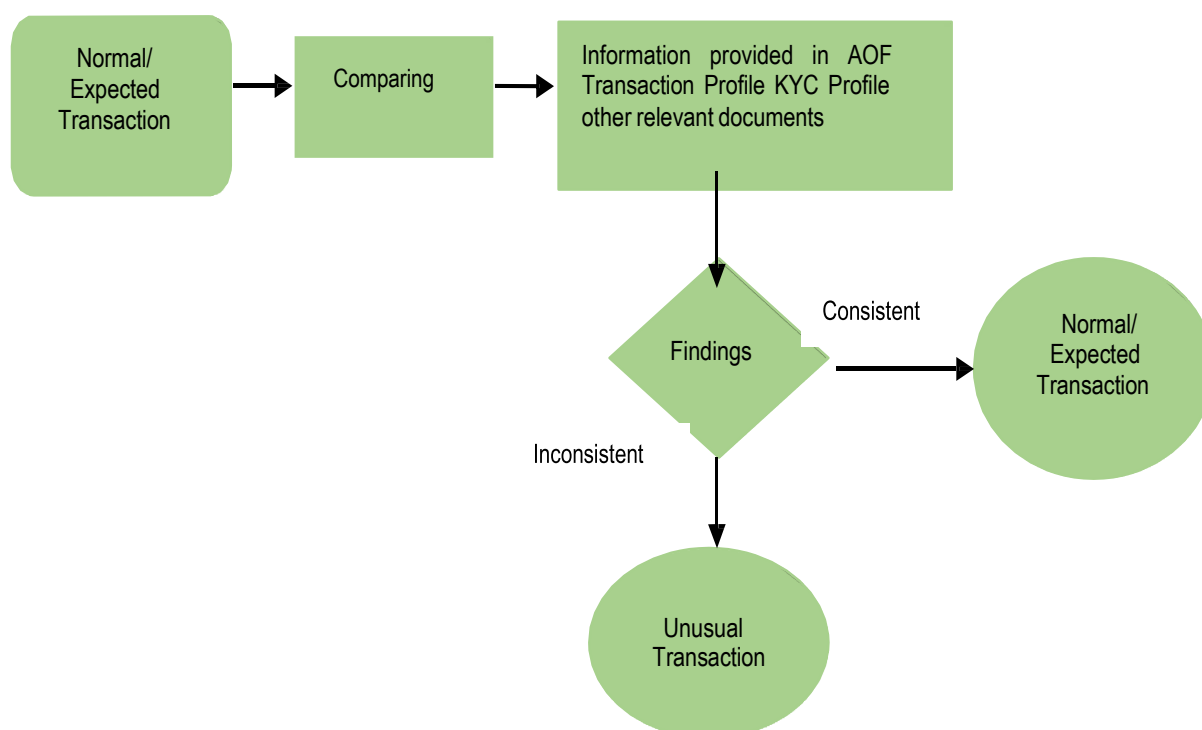


Figure: Identification of STR/SAR

As discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, branch should conduct the following 3 stages:

a) Identification

This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of financial institutions monitoring of unusual transactions may be automated, manually or both. Some financial institutions use specialized software to detect unusual transactions or activities, however, the use of such software can only be complemented managerial oversight and not be replaced the need for constant monitoring of activity of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution and supported by adequate information systems to alert management and other appropriate staff (e.g., the compliance officer) of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should always be an ongoing activity.

b) Evaluation

These problems must be in place at Branch level and AML & CFT Division. After identification of STR/SAR, at Branch level BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage concerned BAMLCO must be tactful considering the tipping off provision of the acts. If BAMLCO is not satisfied, he should forward the report to CCC. After receiving report from Branch, CCC should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stages of evaluation (whether reported to BFIU or not) bank/branch should keep records with proper manner.

c) Disclosure

This is the final stage and AML & CFT Division should submit STR/SAR to BFIU if it is still suspicious. For simplification the flow chart in following page shows STR/SAR identification and reporting procedures:

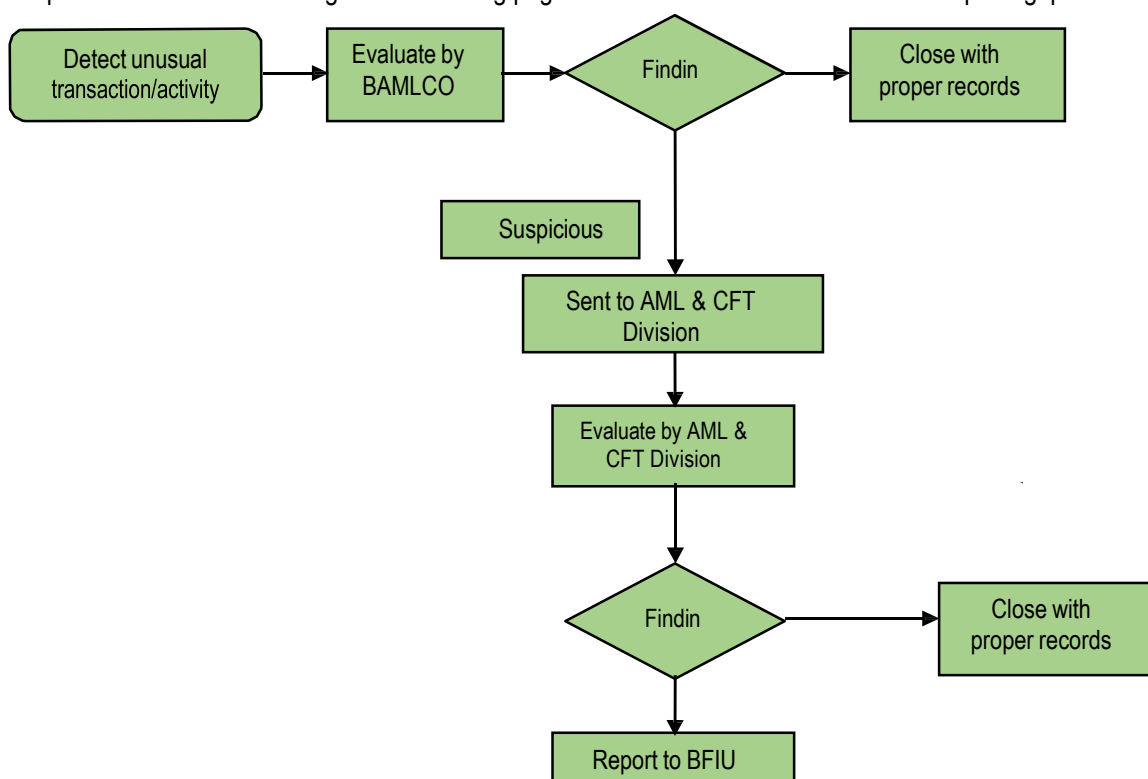


Figure: STR/SAR identification and reporting procedures

12.4 Tipping Off

Bank officials need to consider the confidentiality of the reporting of STR/SAR. They should not make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious.

12.5 Cash Transaction Report

CTR process of bank is fully automated in our bank. Every branch will download CTR through the system and monitor all transactions in due time. If any branch has not any such transaction, branch should report it to the AML & CFT Division, Corporate Office as ,there is no reportable CTR*. Simultaneously, branches need to identify suspicious transaction while reviewing the cash transactions and preserve the evidence regarding monitoring. If any suspicious transaction is found, the branch will submit it as ,Suspicious Transaction Report to the AML & CFT Division. If no such transaction is identified, Branch will inform to the CCC as ,No suspicious transaction has been found*. Besides, every branch needs to preserve its CTR in their branch/SME Service Centers/Islamic Window.

AML & CFT Division will also review all transactions under CTR of all branches and search for suspicious transaction. If any suspicious transaction is found report it to BFIU through goAML web. AML & CFT Division must ensure the accuracy and timeliness while reporting CTR to BFIU. AML & CFT Division has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR. Moreover, CCC must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

12.6 Self-Assessment Report

Banking system in Bangladesh is mainly based on branch banking. The branches of the banks are in every corner of the country and they have an active role in stimulating the economic growth of the country. It is very difficult for the AML & CFT Division or ICC to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFIU has established a Self-Assessment Reporting system for the branches.

According to the instructions of BFIU, branches of bank need to conduct the Self-Assessment to evaluate them on a half yearly basis. Self-Assessment has to be done through a checklist that is circulated by BFIU Circular No. 26 dated June 16, 2020. Before finalizing the evaluation report, there shall have to be a meeting presided over by the branch manager with all concerned officials of the branch. In that meeting, there shall be a discussion on the branch evaluation report; if the identified problems according that report are possible to solve at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations shall have to be jotted down. In the subsequent quarterly meetings on preventing money laundering and terrorist financing, the progress of the related matters should be discussed. After the end of every half year, the branch evaluation report along with the measures taken by the branch in this regard and adopted recommendations regarding the issue should be submitted to the Internal Audit Department or ICCD of the Head Office and the Central Compliance Unit within the 15th of the next month.

12.7 Independent Testing Procedure

The audit must be independent (i.e. performed by people not involved with the branch's AML & CFT compliance). Audit is a kind of assessment of checking of a planned activity. Independent testing has to be done through a checklist that is circulated by BFIU Circular No. 26 dated June 16, 2020.

The individuals conducting the audit should report directly to the board of directors/senior management. Audit function shall be done by the ICCD. At the same time external auditors could be appointed (if possible) to review the adequacy of the program.

12.8 ICCD's obligations regarding Self-Assessment or Independent Testing Procedure

The ICCD shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the AML & CFT Division.

While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the ICCD should examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure. The ICCD should send a copy of the report with the rating of the branches inspected/audited by the ICCD to the AML & CFT Division of the bank.

12.9 AML & CFT Division's obligations regarding Self-Assessment or Independent Testing Procedure

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

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

CHAPTER XIII- Politically Exposed Persons (PEPs)

13.1 Purpose

This chapter termed as “Guidance note on Politically Exposed Persons (PEPs)” is issued as per power conferred in section 23(1)(d) of Money Laundering Prevention Act, 2012 and in section 15(1)(d) of Anti-Terrorism Act, 2009 for all the reporting organizations (as per section 2 (W) of Money Laundering Prevention Act 2012 and section 2 (20) of Anti-Terrorism Act 2009) operating in Bangladesh.

The purpose of this chapter is to assist the branches to obtain an explicit overview of the obligations under the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regime of Bangladesh for Politically Exposed Persons (PEPs).

This chapter is intended to provide the branches/service centers with guidance on the application of customer due diligence requirements associated with PEPs in adherence to the Financial Action Task Force (FATF) recommendations and international best practices.

13.2 Politically Exposed Persons (PEPs)

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

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

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

13.2.1 Who are Politically Exposed Persons (PEPs)?

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

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

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

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

The definition of PEPs is not intend to cover middle ranking and more junior individuals as mentioned in 2.1 and 2.2.

13.2.3 Who should be considered a family member of a PEP?

Family members of a PEP shall include:

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

However, this is not an exhaustive list. Reporting organizations should take a proportionate and risk- based approach to the treatment of family members who do not fall into this definition. A corrupt PEP may use members of his/her wider family to launder the proceeds of corruption on his/her behalf.

It may be appropriate to include a wider circle of family members (such as aunts and uncles) in cases where a reporting organization assessed a PEP to pose a higher risk. This would not apply in relation to lower risk PEPs. In low-risk situations, a reporting organization should not apply any EDD measures to someone who is not within the definition above and should apply normal customer due diligence measures. A family member of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

13.2.4 Close associates' of a PEP

A „known close associate“ of a PEP is defined as:

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

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

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

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

13.6.1 PEPs versus Risk

13.5.1 Do all PEPs pose the same risk?

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

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

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

13.5.2 What are some indicators that a PEP might pose a lower risk?

The following indicators suggest a PEP poses a lower risk:

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

13.4.3 What are indicators that a PEP might pose a higher risk?

The following indicators suggest a PEP poses a higher risk:

a) Higher risk indicator – product

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

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

- associated with high levels of corruption
- political instability
- weak state institutions
- weak anti-money laundering defence
- armed conflict
- non-democratic forms of government
- widespread organized criminality
- a political economy dominated by a small number of people/entities with close links to the state
- lacking a free press and where legal or other measures constrain journalistic investigation
- a criminal justice system vulnerable to political interference

- lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector
- law and culture antagonistic to the interests of whistleblowers
- weaknesses in the transparency of registries of ownership for companies, land and equities
- human rights abuses

c) Higher risk indicators – personal and professional The following characteristics might suggest a PEP poses higher risk:

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

13.4.4 What are some indicators that a PEP's family or known close associates pose a lower risk?

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

13.4.5 What are some indicators that a PEP's family or known close associates pose a higher risk?

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

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

13.5 What are reporting organizations' obligations under the Regulations?

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

- obtain senior management approval for establishing or continuing business relationships with such persons
- take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons
- conduct enhanced, ongoing monitoring of those business relationships

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

13.5.2 What measures may reporting organizations take in lower risk situations?

In lower risk situations a reporting organization may take the following measures:

- Conduct enquiries about a PEP's family or known close associates in a flexible manner except those required to establish whether such a relationship does exist.
- take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP. It is necessary to seek source of wealth information but in all lower risk cases, especially when dealing with products that carry a lower risk of laundering the proceeds of corruption, reporting organizations should minimize the amount of information they collect and how they verify the information provided (for example, via information sources it has available).
- oversight and approval of the relationship takes place at a lower level of senior management.
- a business relationship with a PEP or a PEP's family and close associates is subject to less frequent formal review than it was considered high risk

13.5.3 What measures may reporting organizations take in higher risk situations?

In higher risk situations a reporting organization may take the following measures:

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

13.5.4 Long-term insurance contracts

In relation to life insurance policies, reporting organizations should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiaries, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, reporting organizations should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

13.5.5 Beneficial owners of legal entities who are PEPs

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

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

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

13.6 Case Example:

13.6.1 A foreign national prosecuted in another country for bribery

An foreign suspect was convicted in the "Country U" for bribery offences which took place in a third country (Country A).

The suspect was employed in Country A by an inter-governmental organization which received more than USD 260 million of aid from the Country U's donor agency. The suspect's employer worked closely with both the "Country U" and "Country A" governments to construct hospitals, schools and other facilities.

It was alleged that over a three month period while in Country A, the suspect solicited a bribe for awarding sub-contracts funded by the Country U's donor agency. The suspect allegedly solicited a cash payment of USD 190,000 to allow a sub-contractor in Country A to continue working on projects. The suspect was arrested and charged with receiving a bribe as an agent of an organization which received Country U's government funds.

The suspect pleaded guilty to seeking USD 190,000 in bribes and sentenced to 22 months imprisonment.

13.6.2 Proceed of corruption in one country traced as financial asset in another country.

A governor of a province in Country B was alleged to take approximately USD 1.5 million in bribes. The proceed of bribe were then used to purchase 17 (seventeen) properties in Country B and 6 (six) in Country C. The governor was subsequently removed from office following charges of corruption.

CHAPTER XIV : Beneficial Owner

14.1. Legal Authority

1. This guideline is issued pursuant to section 25 of Money Laundering Prevention Act, 2012 and section 3.3(3) of BFIU circular No-19/2017.

14.2. Introduction

2. It is crucial to know who the beneficial owner(s) are so that one can make appropriate decisions about the level of money laundering and terrorist financing risk associated with customer. Some criminal enterprises deliberately try to hide the true owners and controllers of their business and its assets. Sometimes identifying and verifying who customers' beneficial owner(s) are can be difficult to do. This could be because the ownership structure is complex but legitimate. However, someone should remain alert to the possibility that it may be because there is an attempt to conceal the beneficial owner(s).

3. This guideline on Beneficial Ownership applies primarily to customers who are legal persons or arrangements. The guideline provides information on how to determine beneficial ownership by identifying the individual(s) that own more than 20 percent of ownership, those with effective control on a customer, and persons on whose behalf a transaction is conducted.

4. Acting on behalf of a customer is not part of the beneficial ownership definition. However, the reporting entities should identify and verify those persons. Information on 'acting on behalf' is included to help reporting entities understand the distinction between a beneficial owner and a person acting on behalf of a customer.

5. A risk-based approach will allow some flexibility in the measures to verify the identity of the customer's beneficial owners. Generally, simplified customer due diligence relates to customers that are already subject to transparency and public disclosure. Thus, simplified customer due diligence, which in effect means there is no requirement to check beneficial ownership.

6. Examples provided in this guideline are suggestions to assist meeting obligations but are not intended as exhaustive examples. After reading this guideline, if still do not understand any of the obligations one should seek legal advice, or contact BFIU for further clarification.

14.3. Who is a beneficial owner?1

7. The definition of beneficial owner means the individual who –

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

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

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

9. 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.

14.4. Why is it important to identify the beneficial owner?

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

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

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

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

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

a) Use of shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions,

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

b) Complex ownership and control structures involving many layers of ownership, sometimes in the name of other legal persons and sometimes using a chain of ownership that is spread across several jurisdictions,

c) Bearer shares and bearer share warrants,

d) Use of legal persons as directors,

e) Formal nominee shareholders and directors where the identity of the nominator is undisclosed,

f) Informal nominee shareholders and directors, such as close associates and family,

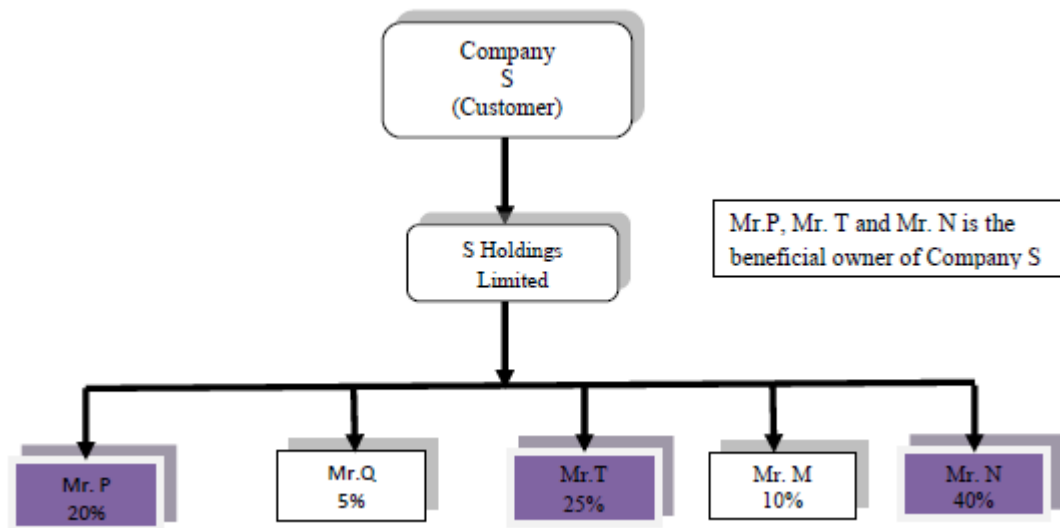
g) Trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,

h) Use of intermediaries in forming legal persons², including professional intermediaries such as accountants, lawyers, notaries, trust and company service providers.

14.6. Ownership

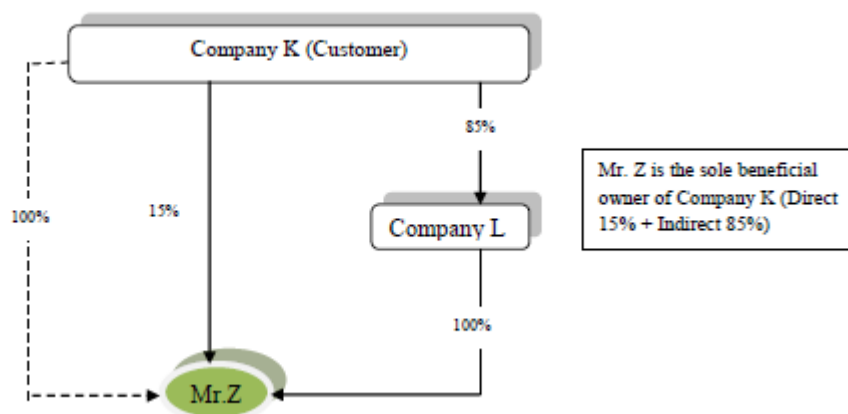
13. The reporting entities should understand the ownership and control structure of the customers. The threshold for controlling interest owns 20% or more of the customer. The ownership can be simple and complex in nature. Few examples are as follows:

a) Simple ownership

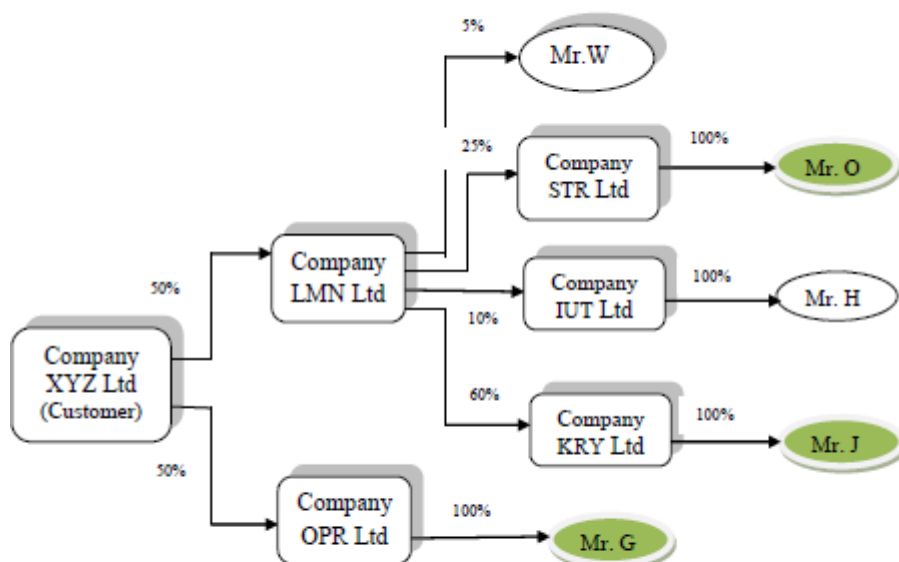


As per MLPR 2019 Legal person means any entity other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundation, installations, partnerships or associations and other relevantly similar entities,

b) Simple (Direct and Indirect) ownership



c) Complex (Multi level Indirect) ownership



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

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

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

14.7. Effective Control

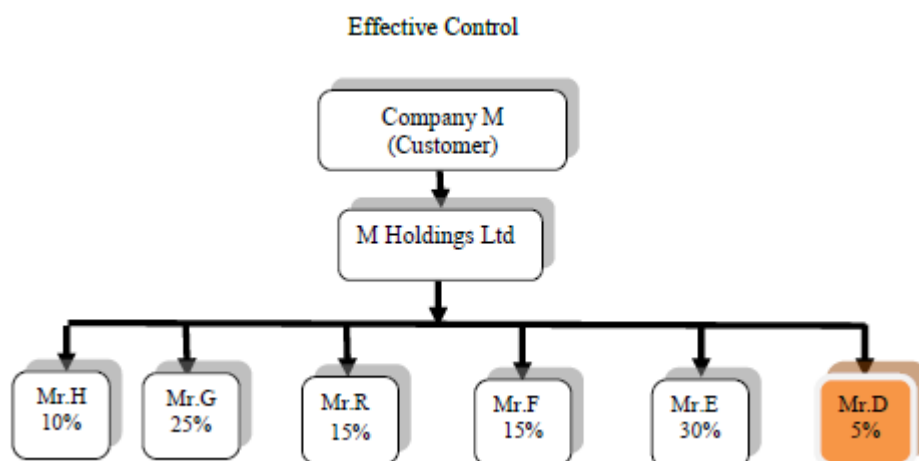
16. It is essential to understand the customer's governance structure as an aid in identifying those persons that exercise effective control over the customer. In deciding the effective controller(s) in relation to a customer, reporting entities should consider:

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

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

- a) Personal connections to persons in positions such as Executive Directors/ CEOs/ Managing Director or that possess ownership;
- b) Significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person;
- c) Control without ownership by participating in the financing of the enterprise, or because of close family relationships, historical or contractual associations, or if a company defaults on certain payments;

d) Use, enjoyment or benefiting from the assets owned by the legal person even if control is never exercised.



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

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

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

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

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

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

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

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

is noted as the beneficial owner due to their position as a member of a managing body, this does not mean that they receive monetary income from the company or that the company operates in their personal interests.

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

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

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

14.8. Person on whose behalf a transaction is conducted

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

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

14.9. Beneficial owner of legal arrangements

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

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

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

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

Example: Person 'B' is the author of a trust for the benefit of his child. The trustee seeks to establish a relationship with a financial institution to help manage the assets of the trust. Even though the trustee is the controller of the

assets of the trust he may not be the ultimate beneficial owner and the main focus of CDD should include person 'B' as well.

14.10. Applying a risk-based approach

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

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

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

Example: A local business

Stage one-gather information

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

Stage two-identify beneficial owners

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

Stage three

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

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

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

14.11. Customer Due Diligence

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

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

14.12. Record keeping

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

14.13. Example

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

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

In this example, Reporting entities be required to record:

- The ownership of the Company - shared by Mr. A (25% of the shares) and BC Company Ltd. (75% of the shares);
- The ownership structure of the entity - ABC Company Ltd. is a privately traded.
- The identification of all members the Board of Directors (Mr. S's Family) as they are having effective control;
- Identification of Mr. A as he is having more than 20% of ownership
- Identification of all of the individuals who own or control, directly or indirectly, 20% or more of the shares of BC Company Ltd since it owns 75% of the shares, it also exercises control. However, in a case like this, the reporting entity must research further to determine whether any individual owns enough shares of BC Company Ltd. that would constitute 20% of ABC Company Ltd., or until the reporting entity determine that there is no such individual;
- The manner in which the reporting entity obtained this information; and
- The measures taken to verify accuracy of information.

36. Example 2 Record for ownership and control structure of partnership

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

In this example the reporting entity is required to record:

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

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

14.14. Question/Answer

37. Who is required to submit data to the reporting entity in supporting beneficial ownership?

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

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

- apartment association;
- building association;
- a company listed on the regulated market to which disclosure rules complying with Bangladeshi law or similar international standards are applied, which ensure the sufficient transparency of the data of owners;
- a foundation the goal of whose economic activities is safekeeping or collecting assets in the interests of the beneficiaries or group of persons specified in the articles of association and that has no other economic activity.
- As gardening associations are ordinary non-profit associations within the legal meaning, then the obligation to submit the data of the beneficial owner applies to them.

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

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

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

- Companies listed on the stock exchange do not have to submit the data of beneficial owners, but the subsidiaries belonging to their groups of companies must do it. The same principles that apply to ordinary companies apply here as well: if there are no natural persons among the shareholders of a listed company whose shareholding in

the company exceeds 20%, the members of the controlling body of the listed company, i.e. the management board and the supervisory board, are noted as the beneficial owners.

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

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

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

CHAPTER XV : e-KYC

15.1 Introduction

15.1.1 Background

The concept of Know Your Customer (KYC) within the financial sector and Designated Non -Financial Business and Professions (DNFBPs) started only few decades back. It has got momentum when FATF came forward with a set of recommendations for prevention of money laundering and financing of terrorism. Within the FATF standards KYC had been emerged as one of the main preventive measures or tools to protect financial institutions abusing from criminal activities.

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

- (a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
- (b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, as such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.
- (c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- (d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their

business and risk profile, including, where necessary, the source of fund. The Financial institutions should be required to apply each of the CDD measures and should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation. The relevant identification data may be obtained from a public register, from the customer or from other reliable and independent sources.

In 2017, the FATF provided a specific supplement to the 2013 Guidance on AML/CFT Measures and financial inclusion, focusing specifically on CDD and financial inclusion. The Guideline highlights risk mitigation measures that Financial Institutions' should apply commensurate with the nature and level of risks identified, to mitigate the risks. It also presents different CDD approaches which can be implemented to facilitate financial inclusion and remove obstacles linked to the verification of the customer's identity, either a broad understanding of the reliable and independent source of information or simplified due diligence measures. Where the risks of ML and TF are lower, one or more of the digital ID system's basic processes, may be less reliable (i.e., have a lower assurance level) would still satisfy the requirements of Recommendation 10.

FATF standards are applicable for both traditional and digital financial services. The digital financial services cover financial products and services, including payments, transfers, savings, credit, insurance and securities. They are delivered via digital/electronic technology such as e-money (initiated either online or on a mobile phone), payment cards and regular bank accounts.

In Bangladesh, section 25 of Money Laundering Prevention Act (MLPA), 2012 requires financial institutions to collect complete and correct identity of customer while establishing business relationship with its potential customer. The Rule 6 to 12 of the Money Laundering Prevention (MLP) Rules 2019 provides a detail framework to conduct customer due diligence for the financial institutions, where Rule no. 10 provides the legal basis to adopt risk based approach in case of customer due diligence, i.e. application of

simplified measures for lower risk scenario and vis-à-vis enhanced measures for higher risk scenario. With the spirit of those laws, Bangladesh Financial Intelligence Unit (BFIU) has issued several circulars and circular letters instructing the financial institutions' to conduct know your customer programs, which starts from customer onboarding.

Digital financial products and services, and digital identity solutions have developed significantly over the last several years and have major potential to facilitate access to basic services for unserved and underserved people and businesses, especially in emerging and developing countries. The development of branchless banking channels through non-bank agents (e.g. computer shops, mobile phone shops, commission agent business, grocery stores etc.), combined with mobile phone solutions, and e-money accounts have helped to reach vast groups of citizen and offer them basic, but regulated financial services.

In several countries, the expansion of digital financial services has been supported by the implementation of a tiered KYC approach. However, in Bangladesh for lower threshold of transaction and limited wallet size and considering proven low risk, BFIU directed for Simplified Due Diligence (SDD) for mobile financial services, digital financial services and other low or limited risks banking, insurance and securities products. The scope of the applicable measures of SDD is limited and it applies only when the products or service are assessed low risk.

The lower ML/TF risk situations may permit the use of digital ID systems for the purposes of simplified due diligence, for example, when the ML/TF risks of potential customers are lower, a digital ID system for identity proofing may be appropriate. Conversely, for higher ML/TF risk situations, financial institutions may adopt additional independent means of reliable information to verify customers' identity details. It is also observed in several countries that several low risk accounts are being created and ultimately controlled by one bad actor. Therefore, additional measures are required to ensure that this type of ML/TF risk is mitigated, for example, putting restrictions on the use of the account.

In Bangladesh, Election Commission of Bangladesh holds the citizens (18 years and above) identity data with their biometrics has higher level of assurance and authenticity, where, the financial institutions' can have access to check the authenticity of customer provided identity data and bio-metrics by using this database. Therefore, this e-KYC Guideline is based on the national ID card and the bio-metrics data stored against each NID card.

This e-KYC guideline contains a set of instructions for the financial institutions to enable them to conduct customer due diligence in a digital means.

15.1.2 Scope

This Guideline shall be known as Electronic Know Your Customer (e-KYC) Guidelines which deals with electronic customer onboarding, identification and verification of customer identity, creating of customer digital KYC profile as well as risk grading of customer in a digital means. The scope of this Guideline will be as follows:

- (a) The provisions of this Guideline shall be applicable only for natural person;
- (b) The requirements of this guideline shall be applicable based on the risk exposures of the customers of the financial institutions. For example, for an assessed low risk customer, financial institution shall be required to

conduct simplified e-KYC which includes electronic customer onboarding, verify customer identity and preserve customer profile digitally, whereas, financial institution shall be required to conduct regular and enhanced e-KYC which includes electronic customer onboarding, verify customer identity, preserve KYC and risk grading in a digital manner for a customer with a regular and higher risks scenario;

(c) The e-KYC requirement of this Guideline is based on the biometric verification; therefore, a client whose status is legal person or legal arrangement excluded from the obligation of this Guideline. In this case, KYC and CDD norms for the legal person or legal arrangement shall be undertaken as per the provisions of the MLPA 2012, Anti-Terrorism Act

(ATA), 2009, the MLP Rules, 2019, Anti Terrorism (AT) Rules 2013; and instructions contained in the circulars and guidelines issued the BFIU time to time.

(d) Where e-KYC attempts failed due to any technical reason, the traditional KYC approach should be followed for the natural person.

15.1.3 Objectives

The key objective of promoting e-KYC is that it can provide an ample scope of quick onboarding of customer by verifying customer identity through digital means which can leverage saving of time and provide ease both for the client and service providers. Additionally, e-KYC can save institutional cost as well as foster growth of customer base compare to the traditional growth. Therefore, the basic objectives of implementing e-KYC are as follows:

- Establish good governance within the financial industry;
- Enhancing the growth of financial inclusion;
- Protect financial sector from abuse of criminal activities;
- Ensure integrity and stability of the financial sector;
- Manage ML/TF risks;
- Reduction of cost related to customer on boarding and managing CDD;
- Promote fintech services; and
- Participate in the national level well-being.

2. E-KYC Process

15.2.1 Definitions E-KYC is a combination of paperless customer onboarding, promptly identifying and verifying customer identity, maintaining KYC profile in a digital form and determining customer risk grading through digital means. It is a faster process of doing KYC of customer verifying his/her identity document or bio-metric data.

The e-KYC module can be divided into following two types¹ based on the customer's risk exposures:

¹ This guideline suggested two types of biometrics i.e. fingerprint and face matching, however, if the infrastructure permit Financial Institution can introduce other type of biometric for example iris. ² The EDD measures should include collection of additional information, monitoring of account activity and approval from Chief AML/CFT Compliance officer

(a) **Simplified e-KYC:** Where a customer can be onboarded and verifying customer identity electronically using simplified digital KYC form in case of proven lower risk scenario. No risk grading will be required while onboarding of customer. However, sanction screening should be undertaken and KYC review shall be done every five years; and

(b) **Regular e-KYC:** Where a customer can be onboarded and verifying customer identity electronically, a prescribed digital KYC required to be filled in and stored as well as a risk grading exercise required to be

documented. However, based on the risk grading exercise where customer rated as high risk or some specific scenarios (for example. PEPs), some Enhanced Customer Due Diligence (EDD)² required to be undertaken as per provided sample in the section 6.2 of this Guideline.

15.2.2 Process

The traditional KYC process requires to be filled in the KYC form and collect photo ID and signature of the customers along with required documents. All the way it's a manual process. However, e-KYC is a digital process where financial institutions can open a customer account by filling up a digital form, taking photograph on the spot, and authenticate the customer's identification data (ID No., biometric information, address proof) instantaneously. Such bio metric information or digital signatures or electronic signatures may be used for transaction authentication as well. The customer onboarding process may undertake via followings means:

- (a) **Assisted customer onboarding:** Where a financial institution or its nominated agent or third-party visit customer or customer visit financial institution or its nominated agent or third party's premises and open account with the direct assistance of financial institution or its nominated agent or third party; and
- (b) **Self check- in:** Where customer can on board at his own by using kiosk, smart phone, computer or other digital means abiding by the norms of this e-KYC Guidelines. Self check in shall be allowed for face matching model only as described section 3.3 of this Guideline.

15.2.3 Applicability

e-KYC shall only be applicable for natural person who have valid NID document. Natural person without NID and a legal entity or arrangement has to follow the KYC norms as prescribed by the BFIU from time to time. Therefore, 'simplified' and 'regular' e-KYC norms shall be applicable based on threshold and risk mentioned in this Guideline. As such this Guideline applicable for the Bank, Non- Bank Financial Institutions, Insurance Companies, Capital Market Intermediaries and the other companies licensed by the Bangladesh Bank, herein after in this Guideline will be referred as financial institutions. The threshold mentioned in this Guideline may be changed from time to time by the BFIU. The financial institutions shall conduct paper based customer onboarding and simplified or regular KYC and CDD measures if any customer unable to onboard with this e-KYC mechanism.

15.2.3.1. Simplified e-KYC

The scope of simplified e-KYC covers the followings which may be revised by the BFIU based on identified risk and consultation with relevant stakeholders from time to time:

a) Digital Financial services

- Mobile Financial Services (MFS) approved by Bangladesh Bank;
- Payment Service Providers (PSPs) approved by Bangladesh Bank;
- Payment Services Operators (PSO) approved by Bangladesh Bank; and
- Fintech Companies with a proven low risk scenario.

b) Financial inclusion products

- Subsidy and allowances paid by the Government under its safety net programs (G2P);
- All receipt by the government (P2G);
- Existing financial inclusion products.

c) Agent banking products:

- Existing agent banking products within the transaction limits set by the Bangladesh Bank time to time

d) Banking products:

- Deposit or Withdrawal not exceeding BDT 1,00,000 per month in a checking account;
- Term Deposit upto. BDT 10,00,000;
- Special deposit scheme with maturity value upto exceeding BDT 10,00,000

e) Non-Bank Financial institutions Products:

- Any type of NBFi products not exceeding BDT 10,00,000;

f) Securities Market Products³:

- Deposit to the BO account up to BDT 15,00,000;

g) Insurance Products⁴:

- **Life Insurance:** The sum assured within the range of BDT 3,00,000 - 20,00,000 with an annual premium shall not be exceeds BDT 2,50,000.
- **Non-Life Insurance:** Any sum premium not exceeding BDT 20,000 -250,000.

This includes customer initial deposit plus amount transferred through link account. ⁴Any sum insured lower than BDT 3,00,000 for life insurance and any sum premium lower than BDT 20,000 will be given flexibility to follow this e-KYC regulation. However, it is encouraged to use digital onboarding in such case by using at least a photo ID document.

15.2.3.2 Regular e-KYC

The scope of regular e-KYC covers the followings:

a) Agent banking accounts:

- When agent banking customer performed transaction with the branch as a regular customer;

b) Banking products:

- Other banking products except the banking products mentioned in section 2.3.1(d);

c) Non-Bank Financial institutions Products:

- Any type of NBFi products exceeding BDT 10,00,000;

d) Securities Market Products:

- Deposit to the BO account exceeds BDT 15,00,000;

e) Insurance Products:

- **Life Insurance:** Any sum assured exceeds BDT 3,00,000 - 20, 00,000 and/or any annual premium exceeds BDT 2, 50,000.
- **Non-Life Insurance:** Any sum premium exceeds BDT 20,000 -250,000.

15.3. Customer Onboarding-Simplified

15.3.1 Customer onboarding models

The financial institutions' are allowed to follow customer boarding under this Guidance which is based on national identification document, information stored within a specific NID plus any one of the bio-metric verification out of fingerprint matching, face matching, voice matching and iris matching⁵. The customer onboarding should also be covered self check-in, check in with assistance of service providers and other relevant means as required necessary. An electronic customer onboarding involves multiple activities. An efficient customer onboarding starts from clients' identity information and can be segmented into following steps:

5 The financial institutions are free to choose any model based on their preparation and infrastructure.

- a) Data capture and generation;
- b) Identity verification;
- c) Sanction and other screening;
- d) Account opening;
- e) Customer profiling (e-KYC Profile); and
- f) Customer risk grading (as applicable).

For the purpose of undertaking e-KYC, this guideline suggests initially following two bio-metric based models of customer onboarding which are as follows: (a) Customer onboarding by using fingerprint; and (b) Customer onboarding by matching face.

However, other two models i.e. voice matching and iris matching can also be used if there are sufficient infrastructural and logistics facilities available. Moreover, financial institutions can also introduce other innovative models using biometric beyond these four models having prior approval from BFIU.


15.3.2 Customer onboarding by using fingerprint

The customer onboarding by using fingerprint matching is one of the commonly used methods where customer fingerprint will be used as a main identifier of a person's identity. The minimum generic approach for this model will be as follows:

(a) Step-one


In this step, a customer approaches to a financial institution or its agent or a financial institution or its agent approaches to a customer for account opening or BO account opening or policy opening process using e-KYC. Then, the customer will provide his or her NID. The financial institution or its agent inserts NID number and Date of Birth (DOB) into the specified template and also collects fingerprint, then press Next button. Once the financial institution or its agent presses Next button the information of NID number, DOB and fingerprint data will be matched with NID database, if the data is matched, then next template will be appeared.

(b) Step-two⁶

Applicant's Name:		
Mother's Name:		
Father's Name:		
Spouse Name:		
Gender (M/F/T):		
Profession:		
Mobile Phone Number:		
Present Address:		
Permanent Address:		
Nominee:	Relation:	Photograph: Next 


In step two, financial institutions or its agent will insert or punch customer's personal information data as far as possible. It is encouraged that Financial institution use the technology that enable data fetching from the NID and wherever required insert rest other information manually. On completion of personal information, the financial institution or agent will press Next option.

(c) Step-Three

Photograph:	Next 
-------------------	-------------------------------------------------------------------------------------------------

In step three, financial institution or its agent or client will capture or upload customer's photograph. However, when there is self check in occurs, then live selfie with proper light and camera frame is required⁷; then press Next option.

(d) Step-Four⁸

Client wet signature or electronic signature or digital signature or PIN.....	Next 
-------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------

In step four, customer wet signature (signature using pen) or customer electronic signatures (signature using devices) or digital signature or personal identification number (PIN) is required to be preserved for future reference.

(e) Step-Five

Account Opening Notification

⁶ This template given here is the minimum information. The financial institutions may add few more fields where necessary (especially for insurance and capital market intermediaries). Where necessary, financial institutions may add additional fields for additional nominee(s) and/ or where additional guardian information required for the minor account. ⁷ There should a mechanism that system only captured real persons' picture only. ⁸ Where necessary, the financial institutions may collect physical signature at the later stage and preserve it digitally for further future use.

In step five, after completion of all the processes, system will generate a notification of account opening in process. After completion of necessary sanction and other screening, account opening confirmation notification should be sent to the customer.

The simplified customer onboarding process will be completed once the client gets notification from the financial institution. However, at any point of relationship, the financial institution may ask for additional information from customer and will preserve it in the digital KYC profile of customer.

In case of joint customer (more than one) onboarding the similar process need to be followed. All the field mentioned in step- two is the minimum requirement, however, financial institution especially banks, MFS and non-bank financial institutions may add few fields where necessary. On the other hand, the capital market intermediaries and the insurance companies may add necessary relevant fields as per CDBL requirement and policy proposal form respectively.

15.3.2.1 Required technology

The electronic customer onboarding and e-KYC process requires technology platform. Therefore, based on the simplified e-KYC model at a minimum, following technology and instruments may be used to complete the process;

- (a) Software/App/Program compatible to the above process;
- (b) Internet connection;
- (c) Online connection to the NID verification server⁹;
- (d) Fingerprint capturing devices;
- (e) Electronic signature capturing devices (where necessary) etc.

15.3.2.2 Sanction and other screening

The full-fledged account procedures will be completed by completion of sanction and other necessary screening which includes as follows:

- (a) UNSCRs screening;
- (b) Adverse media screening (where necessary); and
- (c) Internal or external exit list (where necessary).

15.3.2.3 Audit trail of customer profile

To maintain an audit trail, a Financial institution or their nominated third parties required to preserve a digital KYC profile and relevant logbook, even for low risk or financial inclusion products, which should include the followings:

- (a) Customer details (name, contact, address, etc) with photograph;
- (b) Customer ID image (both side);
- (c) Customer signature (where necessary);
- (d) Customer risk review process (once in 5 years);
- (e) Transaction pattern etc; and
- (f) Others information as deemed necessary to complete customer KYC.

⁹ Means NID database either hold by NID Wing of Election Commission and/or Government established any other Authority for identity verification.

The financial institution should maintain a digital log for all successful and unsuccessful client onboarding, matching parameters etc. for further work and audit trail. All the data should be preserved and stored digitally for further both for internal and external audit purposes. The sample e-KYC profile, at a minimum, should be look like as per 6.1.

15.3.2.4 Matching parameters¹⁰

As the electronic onboarding requires matching customer's ID stored data with the national identification database, the following elements or information required to be matched as per described percentile:


Particulars	Matching Percentage
Applicants' Name	≥ 80%
Date of Birth	100%
Fingerprint	≥ 80%
NID number	100%
Fathers' Name	≥ 80%
Mothers' Name	≥ 80%

15.3.2.5. Security measures

The financial institution may use additional security measures in the customer onboarding process which may contains checking the phone number by generating PIN codes and other measures as deemed necessary. Additionally, security of data recorded and preserved under this e-KYC should be maintained properly by the Financial institution so that no customer data to be hacked or compromised. This Guideline also suggest to preserved customer data locally hosted server or cloud sever and put in place necessary data protection and data security measures as prescribed by the prudential and self regulators and/or by the government of Bangladesh.

15.3.3 Customer onboarding by using face matching The financial institution may adopt customer onboarding using face matching model where customer face biometrics will be used as a main identifier of a person's identity along with the national ID number. Following steps will be required for onboarding of a customer by using face matching model:

(a) Step-one¹¹

<ul style="list-style-type: none"> • Taking picture of customer NID (original copy)-front page • Taking picture of customer NID (original copy)-back page 	Next 
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------

Applicant's name, parent name filled may be left as editable form for correction of spelling mistake, however, date of birth, NID number should be kept in un-editable form.

In this step, a customer approaches to a financial institution or its agent or a financial institution or its agent approaches to a customer or customer engaged in self check-in for account opening, or BO account opening or insurance policy opening process by using e-KYC procedures. Then, it requires to capture photograph or scanning front page of the customer NID followed by the back page. An optical character recognition (OCR) should be used to capture the NID data both in Bangla and English. In the back end all NID data will be preserved within specific format.

(b) Step-two¹²

<ul style="list-style-type: none"> • Taking picture of customer face 	Next →
-------------------------------------------------------------------------------------	--------

In step two, financial institution or its agent or client will take an appropriate photograph of the customer's face by using high resolution camera or webcam. While taking picture agent or client required to be tactful enough to take the face only of the customer as well as visible quality of the photograph.

(c) Step-Three¹³

Applicant's Name:	
Mother's Name:	
Father's Name:	
Spouse Name:	
Gender (M/F/T):	
Profession:	
Mobile Phone Number:	
Present Address:	
Permanent Address:	
Nominee: Relation: Photograph:	Next →

In step three, all necessary information will be fetched up in the above digital format. Furthermore, additional input may be punched to fulfill the whole template.

(d) Step-Four¹⁴

Client wet signature or electronic signature or digital signature or PIN.....	Next →
-------------------------------------------------------------------------------	--------

In step four, customer wet signature (signature using pen) or customer electronic signatures (signature using devices) or digital signature or personal identification number (PIN) is required to be preserved for future reference.

(e) Step-Five

Account Opening Notification

¹¹ System should be capable enough to capture front page of NID first, then followed by back page. ¹² There should a mechanism that system only captured real persons' picture only.

¹³ This template given here is the minimum information. The financial institutions may add few more fields where necessary (especially for insurance and capital market intermediaries). Where necessary, reporting entities may add additional fields for additional nominee(s) and/ or where additional guardian information required for the minor account. ¹⁴ Where necessary, the reporting entity may collect physical signature at the later stage and preserve it digitally for further future use.

In step five, after completion of all the processes, system will generate a notification of account opening in process. After completion of necessary sanctions and other screening, account opening confirmation notification should be sent to the customer. The simplified customer onboarding process will be completed once the client gets notification from the financial institution. However, at any point of relationship, the financial institution may ask for additional information from customer and will preserve it in the digital KYC profile of customer. In case of joint customer (more than one) onboarding, the similar process required to be followed. All the field mentioned in step- two is the minimum requirement, however, financial institutions especially banks, MFS and non-bank financial institutions may add few fields where necessary. On the other hand, the capital market intermediaries and the insurance companies may add necessary relevant fields as per CDBL requirement and policy proposal form respectively.

15.3.3.1. Require technology

At a minimum, the customer onboarding via face matching model requires to use the following technology to complete the whole customer onboarding process;

- (a) Software/App/Program compatible to the above process;
- (b) Internet connection;
- (c) Smart phone or desktop computer with high resolution webcam;
- (d) Online connection to the NID verification server¹⁵;
- (e) Electronic signature capturing devices (where necessary) etc.

15.3.3.2 Sanctions and other screening

The full-fledged account procedures will be completed by completion of sanction and other necessary screening which includes as follows:

- (a) UNSCRs screening;
- (b) Adverse media screening (where necessary); and
- (c) Internal or external exit list (where necessary).

15.3.3.3. Audit trail of customer profile

To maintain an audit trail a financial institution or their nominated third parties are required to preserve a digital KYC profile and relevant logbook, even for low risk or financial inclusion products, which should include the followings:

- (a) Customer details (name, contact, address, etc) with photograph;
- (b) Customer ID image (both side);
- (c) Customer signature (where necessary);
- (d) Customer risk review process (once in 5 years);
- (e) Transaction pattern etc; and
- (f) Others information as deemed necessary to complete customer KYC.

The financial institution should maintain a digital log for all successful and unsuccessful clients onboarding, matching parameters etc. for further use and audit trail. All the technology data should be preserved and stored digitally for further both internal and external audit purposes. The sample e-KYC profile, at a minimum, should be look like as per annex -1.

¹⁵ Means NID database either hold by NID Wing of Election Commission and/or Government established any other Authority for identity verification.

15.3.3.4. Matching parameters¹⁶

As the electronic onboarding requires matching customer's ID stored data with the national identification database, the following elements or information required to be matched as per described percentile:

Particulars	Matching Percentage
Applicants' Name	≥ 80%
Date of Birth	100%
Fingerprint	≥ 80%
NID number	100%
Fathers' Name	≥ 80%
Mothers' Name	≥ 80%

15.3.3.5. Security measures

The financial institution may use additional security measures in the customer onboarding process which may contains checking the phone number by generating PIN codes and other measures as deemed necessary. Additionally, security of the data recorded and preserved under this e-KYC should be maintained properly by the financial institution so that no customer data to be hacked or compromised. This Guideline also suggest to preserved customer data locally hosted server or cloud sever and put in place necessary data protection and data security measures as prescribed by the prudential and self regulators and/or by the government of Bangladesh.

15.4. Customer onboarding- Regular measure

The financial institutions are encouraged to use electronic onboarding and e-KYC procedures for the products and services which are not fall under proven low risk or limited risks as well. This means electronic onboarding and e-KYC procedures are also applicable for any sorts of financial products. Both the technology-based model i.e. fingerprints and faces matching technologies are applicable for regular onboarding and managing KYC. Similarly, such onboarding process only applicable for natural person who have valid NID.

Initially onboarding process for the regular e-KYC is similar, however, it requires few modes of additional information and conduct additional customer due diligence compared to the simplified method. The reporting entities are required to create digital customer KYC profile and risk grading exercise digitally during the regular e-KYC. This means similar step by step¹⁷ procedures have to be followed in case of different models (fingerprint and face matching) as discussed above to complete the regular e-KYC procedures. Therefore, the component of regular e-KYC includes the following elements:

- A digital template with more information compared to simplified e-KYC;
- A more stringent KYC profile of the customer;
- Screening of customer other than UN Sanctions (for example: PEPs/IPs, Beneficial Owner, Adverse Media, Internal External list checking etc.); and
- Risk grading exercise

¹⁶ Applicant's name, parent name filled may be left as editable form, however, date of birth, NID number should be kept in un-editable form.

¹⁷ All steps mentioned in this Guideline are generic; the financial institution may reorganize this step by step process where necessary.

Along with the process of digital onboarding already discussed above, the digital information template at a minimum required for regular e-KYC would be as follows:

Account Name.....	Account Type.....
Account Number.....	Unique Account Number.....
Applicant's Name:	
Mother's Name:	
Father's Name:	
Spouse Name :	
Gender (M/F/T).....	Date of Birth.....
Profession.....	Monthly income..... Sources of Fund.....
Mobile Phone Number:.....	
Present Address:	Nationality.....
Permanent Address:	
Nominee:.....	Date of Birth..... Relation..... Photograph.....
<p>NB: a) Incorporate 'add' button of similar field if there is more than one applicant; b) Incorporate 'add' button of similar field if there is more than one nominee; c) If applicant is minor then they should proceed for traditional methods of account opening; d) Incorporate 'add' the following field if nominee is 'Minor' i) Name of minor nominee... ii) Name of Guardian... iii) Address.... iv) Relation.... v) NID of Guardian..... vi) Photograph of Guardian.....</p>	

The customer onboarding process and instructions as discussed above for the simplified measures will be similar for regular e-KYC. After opening account financial institution may collect additional information and customer wet signature to create full digital profile of the client.

15.4.1. Required technology

The same technologies mentioned in this Guideline for simplified e-KYC also be applicable for regular e-KYC.

15.4.2. Sanctions and other screening

The screening mechanism for regular e-KYC is quite stringent compare to the simplified one. The full-fledged account procedures will be completed by completion of sanctions and other necessary screening which includes as follows:

- (a) UNSCRs screening;
- (b) PEPs/IPs Screening;
- (c) Identification of beneficial ownership (if any);
- (d) Adverse media screening;
- (e) Risk grading of customer;
- (f) Customer Due Diligence template;
- (g) Enhanced Due Diligence (if needed).

15.4.3. Audit trail of customer profile

To maintain an audit trail a financial institution or their nominated third parties are required to preserve a digital KYC profile and relevant log book or data which should include the followings:

- (a) Customer details (Name, contact, address, etc) with photograph;
- (b) Customer ID image (both side);
- (c) Customer signature (where necessary);
- (d) Risk grading of customer (where necessary);
- (e) Customer Due Diligence template (where necessary)
- (f) Customer transaction pattern; and
- (g) Others information as deemed necessary to complete customer KYC.

The financial institution should maintain a digital log for all successful and unsuccessful e-KYC onboarding process for further work and audit trail. All the technology data should be preserved and stored digitally for further audit purposes. The sample e-KYC profile, at a minimum, should look like as per 6.2.

15.4.4. Matching parameters

The similar matching parameters mentioned in the simplified e-KYC will be applicable for regular e-KYC.

15.4.5. Security measures

The financial institution may use additional security measures in the customer onboarding process which may contains checking the phone number by generating pin codes and other measures as deemed necessary. Additionally, security of the data recorded and preserved under this e-KYC should be maintained properly by the financial institution so that no customer data to be hacked or compromised. This Guideline also suggest to preserved customer data locally hosted server or cloud sever and put in place necessary data protection and data security measures as prescribed by the prudential and self regulators and/or by the government of Bangladesh.

15.5. Other relevant issues

15.5.1. Record Keeping

The financial institution should maintain all sorts of digital data and log until five years after the closure of the account or business relationship. The digital data shall contain customer onboarding, customer identity verification, KYC profile, risk grading exercise; transaction related data and their analysis; all sorts of correspondence with customer; data collected later for CDD purposes; and all other relevant files.

Digital footprint and log should contain but not limited to information collected during clients' identity verifications and other relevant information related to the screening measures also required to be preserved. The financial institutions also may collect other complementary data (such as, geo location, IP addresses, etc.) which could also support ongoing due diligence.

15.5.2. Reliance on third parties

To implement the e-KYC, the financial institution may rely on the third-party technology providers either full or part to implement e-KYC. Though a financial institution may be engaged with third party, the ultimate responsibility still lies with them. This means financial institution may rely on another entity or technology providers that satisfies the criteria described above to conduct customer due diligence which covers (i) customer identification and verification data from independent and reliable sources; (ii) identify and understand who the beneficial owner(s) is; and (iii) identify the purpose and intended nature of business and relevant CDD measures in a digital manner. Yet, the financial institution itself should ensure the reliability and authenticity of the data collected. The following condition may apply while engaging with any third party for the financial Institutions:

- Immediately obtain the necessary information concerning the identity of the customer as mentioned in (i) –(iii) in the above.
- Take adequate steps to satisfy itself that the third party will make available copies of identity evidence or other appropriate forms of access to the data or digital log as mentioned (i) –(iii) in the above and in this Guideline without delay.
- The activities of the third party shall be regulated under this e-KYC Guidance and will be monitored by the financial institutions.

- Third party shall ensure customer and financial institutions' data protection according to the IT security policy of Bangladesh Government and the respective prudential and self regulators.

- Both the third party and the financial institution covered under this guidance shall ensure the customer data collected under this guidance shall not digitally transmitted or transferred outside Bangladesh without prior approval of the prudential regulators and/or BFIU. In this case, BFIU Circular No. 23 dated 31/01/2019 will be applicable.

15.5.3 Risk Assessment

The financial institution shall have to conduct a risk assessment of new technology based electronic KYC mechanism to understand how it may be abused and put in place appropriate measures to prevent such abuse as per the circulars and Guidance issued by BFIU. The financial institution also required to conduct customer risk assessment as mentioned in 6.3 of this Guideline.

15.5.4 Implementation

The financial institutions should implement this regulation by December 2020 as the timeline set out in the National Strategy Paper for preventing ML/TF 2019-2021 published by the Government People's Republic of Bangladesh.

15.5.5 Transformation of existing clients CDD

The financial institution may transform their existing clients CDD related documents into digital form following above mentioned procedures where applicable.

6. e-KYC Profile- Simplified and Regular

6.1 Sample output of the simplified e-KYC¹⁸

<div style="border: 1px solid black; width: 100px; height: 100px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> Photo Customer </div>	<div style="border: 1px solid black; width: 100px; height: 100px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> Photo Others </div>
Applicant's Name:	
Mother's Name:	
Father's Name :	
Spouse Name.....	
Date of Birth Gender (M/F/T).....	
Profession.....	
Mobile Phone Number.....	
Present Address:	
Permanent Address:	
Nominee:: Relation..... Photograph.....	
Specimen signature/digital signature (where necessary)	
<div style="border: 1px solid black; width: 150px; height: 50px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> Front side of NID </div>	<div style="border: 1px solid black; width: 150px; height: 50px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> Back side of NID </div>
<ol style="list-style-type: none"> 1. Has UNSCRs check done? (Yes) (No) 2. Has review of customer profile done (existing customer)? if so, date of review 3. What is the average range of customer transaction (over 6/12 months)?..... 4. Any other relevant field may be add here 	

Photo Others' shall include the photograph of nominee(s), beneficial owner(s), joint account holder(s), minor(s) their guardian(s) as applicable.

6.2. Sample output of regular e-KYC

	Photo Customer		Photo Others	
--	-------------------	--	-----------------	--

Applicant's Name:.....

Account number:..... Unique account number.....

Mother's Name:

Father's Name :

Spouse Name:

Date of Birth Gender (M/F/T).....

Profession:..... Monthly income Sources of Fund.....

Mobile Phone Number:..... Nationality..... TIN (if any):

Present Address:

Permanent Address:.....

Nominee:.....: Relation..... Photograph.....

Specimen signature.....

Front side of NID	Back side of NID
-------------------	------------------

5. Has UNSCRs check done? (Yes) (No)
6. Has risk grading done? If assessed risk high then conduct EDD as per BFIU circular.

Risk Type	Overall Score
Regular (< 15)	
High (≥15)	

7. Is the customer is IPs/PEPs? If client is PEPs or IPs with higher risk, then conduct EDD as per BFIU circular.
8. Is there any adverse media news against the customer? If any then conduct EDD.
9. Has the source of und verified/justified? (Yes) (No)
10. Has the beneficial ownership checked? If there any beneficial owner found, then conduct CDD on beneficial owner. If beneficial owner is PEPs, then conduct EDD.
11. Are any other documents obtained.....?
12. Nominee details:.....
13. Has review of customer profile done (existing customer)? if so, date of review.....
14. What is the average range and usual pattern of customer transaction (over 6/12 months)?....
15. Any other relevant field may be add here.....

6.3 Form for Customer Risk Grading:

1. Type of On-boarding			
Branch/Relationship Manager	2		
Direct Sales Agent	2		
Walk-in	3		
Internet/Self check-in/Other non Face to Face	5		
2. Geographic Risks:		Score	
Client is–			
Resident Bangladeshi	1		
Non-resident Bangladeshi	2		
Foreign Citizen	3		
For Foreigners:			
Risk classification of country of origin			
Does client's country of citizenship feature in FATF/EU/OFAC/UN Black List/Grey List?			
No	0		
Yes	5		
3. Type of Customer:		Score	
Is client a PEP/Chief or High Official of International Organization, as per BFTU Circular?			
No	0		
Yes	5		
Is client's family/close associates related to PEP/Chief or High Official of International Organization?			
No	0		
Yes	5		
Is client a IP? or his family/close associates related to IP?			
No	1		
Yes (based on assessed risk)	5		
4. Product and Channel Risk:		Score	
Type of Product			
Savings account	1		
Current account	4		
FDR	3		
Deposit Scheme upto 12 lac	1		
Deposit Scheme above 12 lac	3		
Forex account	5		
S.N.D.	3		
R.F.C.D.	5		
5. Business and Activity Risk		Score	
(a) Business			
Please pick Applicable from Annexure and put the relevant score in the next column		
(b) Profession			
Please pick Applicable from Annexure and put the relevant score in the next column		
6. Transactional Risks:		Score	
What is the client's Average Yearly Transactions Worth?			
<BDT 1 million	1		
From BDT 1 million to 5 million	2		
From BDT 5 million to 50 million (5 crores)	3		
More than BDT 50 million (5 crores)	5		
7. Transparency Risk		Score	
Has client has Provided credible source of funds?			
No	5		
Yes	1		

Annexure: Select Business or Profession (for 6.3 item no.5)

<i>Client Business</i>	<i>Score</i>	<i>Client Profession</i>	<i>Score</i>
<i>Jeweller/Gold/Valuable Metals Business</i>	5	<i>Pilot/Flight Attendant</i>	5
<i>Money Changer/Courier Service/Mobile Banking Agent</i>	5	<i>Trustee</i>	5
<i>Real Estate Developer/Agent</i>	5	<i>Professional (Journalist, Lawyer, Doctor, Engineer, Chartered Accountant, etc.)</i>	4
<i>Promoter/Contractor: Construction Projects</i>	5	<i>Director (Private/Public Limited Company)</i>	4
<i>Art and Antiquities Dealer</i>	5	<i>High Official of Multinational Company (MNC)</i>	4
<i>Restaurant/Bar/Night Club/Parlour/Hotel</i>	5	<i>Homemaker</i>	4
<i>Export/Import</i>	5	<i>Information Technology (IT) sector employee</i>	4
<i>Manpower export</i>	5	<i>Athlete/Media Celebrity/Producer/Director</i>	4
<i>Firearms</i>	5	<i>Freelance Software Developer</i>	4
<i>RMG/Garments Accessories/Buying House</i>	5	<i>Government service</i>	3
<i>Share/Stocks Investor</i>	5	<i>Landlord/Homeowner</i>	3
<i>Software/Information and Technology Business</i>	5	<i>Private Service: Managerial</i>	3
<i>Travel Agent</i>	4	<i>Teacher (Public/Private/Autonomous Educational Institution)</i>	2
<i>Merchant with over 10 million takas invested in business</i>	4	<i>Private Sector Employee</i>	2
<i>Freight/Shipping/Cargo Agent</i>	4	<i>Self-employed Professional</i>	2
<i>Automobiles business (New or Reconditioned)</i>	4	<i>Student</i>	2
<i>Leather/Leather goods Business</i>	4	<i>Retiree</i>	1
<i>Construction Materials Trader</i>	4	<i>Farmer/Fisherman/Labourer</i>	1
<i>Business Agent</i>	3	<i>Others: (Please State Below and circle numerical score as needed)</i>	
<i>Thread/"Jhut" Merchant</i>	3		1..2..3..4 ..5
<i>Transport Operator</i>	3		
<i>Tobacco and Cigarettes Business</i>	3		
<i>Amusement Park/Entertainment Provider</i>	3		
<i>Motor Parts Trader/Workshop</i>	3		
<i>Small Business (Investment below BDT 5 million)</i>	2		
<i>Computer/Mobile Phone Dealer</i>	2		
<i>Manufacturer (except, weapons)</i>	2		
<i>Others: (Please State Below and circle numerical score as needed)</i>			
	1..2..3.. 4..5		

CHAPTER XVI : RECRUITMENT, TRAINING AND AWARENESS

16.1 Obligations under Circular

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

16.2 Employee Screening

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

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

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

16.3 Know Your Employee (KYE)

Know-your-customer, an essential precaution, must be coupled with know-your-employees. There are a lot of instances that highlight the involvement of employees in fraudulent transactions and in most cases in association with customers. This therefore brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables. Policies, procedures, job descriptions, internal controls, approval levels, levels of authority, compliance with personnel laws and regulations, code of conduct/ethics, accountability, dual control, and other deterrents should be firmly in place. And the auditor should be conversant with these and other requirements, and see that they are constantly and uniformly updated. Background screening of prospective and current employees, especially for criminal history, is essential to keep out unwanted employees and identifying those to be removed. It can be an effective risk management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. It can be used effectively, the pre-employment background checks/examines may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. KYE requirements should be included in the banks HR policy.

16.4 Training for Employee

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

AML & CFT basic training should cover the following-

- an overview of AML & CFT initiatives;

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

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

16.5 Awareness of Senior Management

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

16.6 Customer Awareness Program

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

16.7 Awareness of Mass People

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

The Need for Staff Awareness

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

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

Education and Training Programs

All relevant staff should be educated in the process of the “Know Your Customer” requirements for ML and TF prevention purposes. The training in this respect should cover not only the need to know the true identity

Of the customer but also, where a business relationship is being established, the need to know enough about the

type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the institution itself. Some sorts of high-level general awareness raising training are, therefore, also suggested.

General Training

A general training program should include the following:

- General information on the risks of money laundering, terrorist financing and proliferation financing schemes, methodologies, and typologies;
- Legal framework, how AML & CFT related laws apply to banks and their employees;
- Institution's policies and systems with regard to customer identification and verification, due diligence, monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

The person responsible for designing the training must identify which, if any, of these topics relate to the target audience. Effective training should present real life money laundering schemes, preferably cases that have occurred at the institution or at similar institutions, including, where applicable, how the pattern of activity was first detected and its ultimate impact on the institution.

Job Specific Training

The nature of responsibilities/activities performed by the staff of a financial institution is different from one another. So their training on AML, CFT & CPF issues should also be different for each category. Job specific AML, CFT & CPF trainings are as under:

i. New Employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so. The new or fresh employee may be trained up within a year.

ii. Customer Service/Relationship Managers

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to the organization's strategy in the fight against money laundering, terrorist financing and proliferation financing. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with non-regular (walk-in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

iii. Processing (Back Office) Staff

The staffs, who receive completed Account Opening, FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training in the processing and verification

procedures. The staffs, who are in a position to deal with account opening, or to accept new customers, must receive the training given to relationship managers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the organization's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML & CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

iv. Credit Officers

Training should reflect an understanding of the credit function. Judgments about collateral and credit require awareness and vigilance toward possible laundering and funding terrorists. Indirect lending programs and lease financing also call for KYC efforts and sensitivity to laundering risks.

v. Foreign Trade Officers

Foreign Trade officials involved in day to day trade processes role based training also be included. Objective behind such training should be to impart training to them on TBML specific risks and responsibilities.

vi. Cash Officers:

Anti-Money Laundering (AML) training is a critical component of the professional development for Cash Officers and Tellers. As key personnel involved in financial transactions, both positions play a vital role in preventing money laundering and other financial crimes within the bank or financial institution. The AML training should be thorough, comprehensive, and up-to-date to ensure compliance with local and international regulations. To ensure that Cash Officers and Tellers are adequately equipped to perform their roles efficiently and accurately, comprehensive training programs are essential.

vii. Audit and compliance staff

These are the people charged with overseeing, monitoring and testing AML, CFT & CPF controls, and they should be trained about changes in regulation, ML, TF and PF methods and enforcement, and their impact on the institution.

viii. Senior Management/Operations Supervisors and Managers

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

ix. Senior Management and Board of Directors

ML, TF and PF issues and dangers should be regularly and thoroughly communicated to the board. It is important that the Compliance Division has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering and terrorist financing poses to the institution. Major AML, CFT & CPF compliance related circulars/circular letters issued by BFIU should be placed to the board to bring it to the notice of the Board members.

x. AML & CFT Compliance Officer

The CAMLCO, DCAMLCO, and AML & CFT Compliance Officer should receive in depth training on all aspects of the ML, TF & PF Prevention Legislation, BFIU directives and internal policies and standards.

In addition, the CAMLCO, DCAMLCO and AML & CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

xi. Training Procedures

The trainers can take the following steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick “why are they here” assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.
- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file.

xii. Refresher Training

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

Training should be conducted ongoing basis, incorporating trends and developments in an institution's business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions/unusual activity.

9.11 External Auditor

External auditor shall play an essential part in reviewing the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External audit should focus their audit programs on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits, to the financial sector supervisors.

External auditor of Bank Asia will review the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report.

CHAPTER XVII: TERRORIST FINANCING & PROLIFERATION FINANCING

17.1 Preamble

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

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

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

17.2 Legal Obligations

Under obligations of ATA 2009 (amendment 2012 & 2013), “Every Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009(amendment 2012 & 2013) and if any suspicious transaction is identified, the agency shall spontaneously report it to 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(amendment 2012 & 2013); which are applicable to the bank, have been complied with or not.”

17.3 Obligations under Circular

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

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

17.4 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.

17.5 Source 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.

17.6 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.

17.7.1 Formal Financial Sector

Financial institutions and other regulated financial service providers' services and products available through the formal financial sector serve as vehicles for moving funds that support terrorist 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.

17.7.2 Trade Sector

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

17.7.3 Cash Couriers

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

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

17.7.4 Use of Alternative remittance systems (ARS)

Alternative remittance systems (ARS) are used by terrorist organizations for convenience and access. ARS have the additional attraction of weaker and/or less opaque record-keeping and in many locations may be subject to

generally less stringent regulatory oversight. Although FATF standards call for significantly strengthened controls over such service providers, the level of anonymity and the rapidity that such systems offer have served to make them a favored mechanism for terrorists.

17.7.5 Use of Charities and Non-Profit Organizations

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

17.7 Targeted Financial Sanctions

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

17.7.1 TFS related to terrorism and terrorist financing

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

17.7.2 TFS related to Proliferation

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

17.8 Automated Screening Mechanism of UNSCRs

As per advise from Bangladesh Financial Intelligence Unit (BFIU), for effective implementation of TFS relating to TF & PF Bank Asia has already been started automated screening mechanism that prohibit any listed individuals or entities to enter into the banking channel. The bank is operating the system for detecting any listed individuals or entities prior to establish any relationship with them. In particular, bank need to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individuals or entities could not use the formal financial channel. In a word, bank shall ensure that screening has done before-

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

For proper implementation of sanction list screening (OFAC, EU, UN, etc.), all officials of Bank Asia must have

enough knowledge about-

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

17.9 Responsibilities of Bank Officials for detection and Prevention of Financing on Terrorism and Financing in proliferation

Bank Asia establish clear lines of internal accountability, responsibility, and reporting system. Duties and responsibilities of the Bank officials/divisions/departments/units in detecting and preventing financing on terrorism and financing in proliferation of weapons of mass destruction are details as under:

Bank officials/divisions/ departments/units	Role/Responsibilities
Officials responsible for Account Opening	Screening of sanction lists and local black list before account opening. Perform due diligence on prospective clients prior to opening account. Obtain documents perfectly. Be diligent regarding the identification (s) of account holder and the transactions relating to the account. Complete the KYC/CDD for new customer.
Operations Officer	Obtain source of large deposits and preserve the record. Ensure that all control points are completed prior to allowing transaction in the account. Update customer transaction profiles in the system as and when required.
Teller	Obtain identity documents of walk-in customer while receiving or paying cash including online transaction. Duly checked the signature of signatories before payment of any cheque.
Credit/Foreign Exchange/SME officials of the Branch	Confirm risk assessment of customer's business. Must screen of sanction lists and local black list before processing any loan proposal. Implementation of BFIU instructions.
HOB/MOB/ BAMLCO	Confirm the transaction monitoring process. Circulate and upgrade all employees of the branch regarding internal circular and BFIU circular of AML & CFT. Confirm sanction lists and local black list checking is done. Confirm AML & CFT training of all the employees of the branch. Confirm KYC/CDD/EDD of the customers of the branch.

International Division	Confirm that the respondent bank is not under sanction list. Confirm screening of customer information with sanction lists. Confirm the regulatory rules and regulation is maintained perfectly.
	Confirm that the applicant and beneficiary of foreign trade are not involved in financing on terrorism and financing in proliferation.
FRD Division	Confirm the source of fund of the remittance. Ensure the screening of the beneficiary or those who are involved in the transaction of the remittance.
ICT Department	Confirm that system will generate report as per requirement of BFIU and AML & CFT Division. Update the system time to time in line with AML & CFT Division and BFIU
Credit Risk Management Division	Confirm that borrowers are not involve with terrorist financing and proliferation financing of weapons of mass destruction. Screening of customer information with sanction lists.
ICCD	Confirm the implementation status of combating terrorist financing and proliferation financing as per requirement of BFIU.
Card Division	Confirm screening of new customer and existing customer information with sanction lists and local black list. Confirm KYC/CDD of the customer before issuing cards.
Treasury Department	Release of remittance after checking confirmation of sanction list from the branch/department.
Central Compliance Unit (CCC)	Take appropriate initiative for combating terrorist financing and proliferation financing. Confirm of implementation of BFIU guidelines, circulars and internal circulars of the bank. Monitoring of all Branches/SME Service Centers/Islamic Wings.
CAMLCO	Take necessary initiative to comply the guidelines regarding terrorist financing and proliferation financing. Ensure that Bank has an effective system in place for combating terrorist financing and proliferation financing.
Managing Director	Provide all kinds of necessary support for implementation of guidelines, circulars for combating terrorist financing and proliferation financing

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

17.10 Role of Bank Asia in Preventing TF & PF Risk

- ❖ Bank Asia discussed a procedure for detection and prevention of financing of terrorism and financing in proliferation of weapons of mass destruction, issued instructions about the duties of Bank officials in the point 10.9 and it will review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.
- ❖ Bank shall take necessary measures, with appropriate caution and responsibility, to prevent and identify

financial transactions through which it is connected to any offence under ATA, 2009 (amendment 2012 & 2013) and if any suspicious transaction is identified, the agency shall spontaneously report it to Bangladesh Bank without any delay.

- ❖ If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, bank shall send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to BFIU immediately.
- ❖ The bank shall maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. Bank shall run regular check on the given parameters, including transactional review, to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.
- ❖ The bank shall run a check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009, (amendment 2012 & 2013); individuals or entities owned or controlled directly or indirectly by such persons or entities, as well as persons and entities acting on behalf of, or at the direction of, individuals or entities listed or scheduled under the Act are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.

KYC documentation

KYC documentation

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Individual	<ul style="list-style-type: none"> • Photograph of applicant (attested by the introducer) and nominee (attested by the applicant) • Passport/ National Id Card/ Birth Certificate + other photo ID (acceptable by the Bank) • Valid driving license (if any) • Credit Card (if any) • Any other documents that satisfy the bank. <p><i>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</i></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) • Documents in support of beneficial owner's income (income of house wife, students etc.) • Trade License if the customer declared to be a business person • E-TIN (if any) • Documents of property sale. (subject to necessity) • Other Bank statement (if any) • Document of FDR encashment (if any) • Document of foreign remittance (if any fund comes from outside the country) • Document of retirement benefit. • Bank loan. 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). • Residential address appearing on an official document prepared by a Government Agency

	<i>indicate his/her position or capacity on it together with a contact address and phone number.</i>		
Minor Account	<ul style="list-style-type: none"> • Photograph of applicant & guardian (attested by the introducer) and nominee (attested by the applicant) • Birth Certificate/Passport • Any Other certificate attaching the photo ID like ID card/registration card (educational), etc. which is acceptable. • Nominee & Guardian information • Nominee & Guardian identity certificate. • Information of beneficial owner (if any) 	<ul style="list-style-type: none"> • Supporting documents of profession of guardian. • Supporting documents of profession of beneficial owner. 	<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. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old).
Joint Account	<ul style="list-style-type: none"> • Photograph of applicants (attested by the introducer) and nominee (attested by the applicant) • Passport/National Id Card/ Birth Certificate + other photo ID (acceptable by the Bank) • Valid driving license (if any) • Credit Card (if any) 	<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) • Documents in support of beneficial owner's income (income of house wife, students etc.) • Trade License if the customer declared to be a business person • E-TIN (if any) • Documents of property sale.(if any) • Other Bank statement (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. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). • Residential address appearing on an official document prepared by a Government Agency

		<ul style="list-style-type: none"> • Document of FDR encashment (if any) • Document of foreign remittance (if any fund comes from outside the country) • Document of retirement benefit. • Bank loan. 	
Sole Proprietorships or Individuals doing business	<ul style="list-style-type: none"> • Photograph of the account holder duly attested by the introducer. • Passport/National Id Card/ Birth Certificate + other photo ID (acceptable by the Bank) • Valid driving license (if any) • Credit Card (if any) • Rent receipt of the shop (if the shop is rental) • Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents) • 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 (update) • E-TIN • Self-declaration acceptable to the bank. (commensurate with nature and volume of business) • Documents of property sale. (if injected any fund by selling personal property) • Other Bank statement (if any) • Document of FDR encashment (if any fund injected by encashing personal FDR) • Document 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. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). • Residential address appearing on an official document prepared by a Government Agency

Partnerships	<ul style="list-style-type: none"> • Photograph of the partners (attested by the introducer). • Partnership deed • Registered partnership deed (if registered) • Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. • Passport of partners/ National ID Card of partners/ Birth Certificate + other photo ID (acceptable by the Bank) • Valid driving license of partners (if any) • Credit Card of partners (if any) • Rent receipt of the shop (if the shop is rental) • Ownership documents of the shop (i.e. purchase documents 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 (update) • E-TIN • Documents of property sale. (if injected any fund by selling personal property of a partner) • Other Bank statement (if any) • Document of FDR encashment (if any partner injected capital by enashing Personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan • 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. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). • Residential address appearing on an official document prepared by a Government Agency
Private Limited Companies	<ul style="list-style-type: none"> • Photograph of the all Directors (attested by the introducer) • Passport of all the directors/National ID Card of all the directors/ Birth Certificate + other photo ID (acceptable by the Bank) • Certificate of 	<ul style="list-style-type: none"> • A copy of last available financial statements duly authenticated by competent authority • Other Bank statement • Trade License • E-TIN • VAT registration • Bank loan 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Physical verification, if necessary.

	<ul style="list-style-type: none"> incorporation • Memorandum and Articles of Association • List of directors • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials, or Employees to transact business on its behalf. • Nature of the company's business. • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company. 		
Public Limited Companies	<ul style="list-style-type: none"> • Photograph of the signatories/directors • Passport of all the directors/National ID Card of all the directors/ Birth Certificate + other photo ID (acceptable by the Bank) • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business 	<ul style="list-style-type: none"> • A copy of last available financial statements duly authenticated by competent authority • Other Bank statement • Trade License • E-TIN • Cash flow statement • VAT registration • Bank loan • Any other genuine source 	N/A

	<ul style="list-style-type: none"> • List of directors in form - XII • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials, or Employees to transact business on its behalf. • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company. 		
Government-Owned entities	<ul style="list-style-type: none"> • Photograph of the signatories. • Statue of formation of the entity • Resolution of the board 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)/ Birth Certificate + other photo ID (acceptable by the Bank) 	N/A	N/A
NGO	<ul style="list-style-type: none"> • Photograph of the signatory (s) (attested by the introducer) 	<ul style="list-style-type: none"> • A copy of last available financial statements duly 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department.

	<ul style="list-style-type: none"> • National ID Card of the operator (s)/ Passport of the operator (s)/ Birth Certificate + other photo ID (acceptable by the Bank) • Resolution of the board 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 (certified) • List of Management Committee/ Directors 	<p>authenticated by competent authority</p> <ul style="list-style-type: none"> • Other Bank statement • Trade License • E-TIN • Certificate of Grand/ Aid 	<ul style="list-style-type: none"> • Proof of delivery of thanks letter through courier.
Charities or Religious Organizations	<ul style="list-style-type: none"> • Photograph of the signatory (s) (attested by the introducer) • National ID Card of the operator (s)/ Passport of the operator (s)/ Birth Certificate + other photo ID (acceptable by the Bank) • Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the Organizations • Certificate of registration issued by competent authority (if any) • Bye-laws (certified) • List of Management Committee/ Directors 	<ul style="list-style-type: none"> • A copy of last available financial statements duly authenticated by competent authority • Other Bank statement • Certificate of Grand/ Aid/ donation • Any other legal source 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.

Clubs or Societies	<ul style="list-style-type: none"> • Photograph of the signatory(s) (attested by the introducer) • National ID Card of the operator (s)/ Passport of the operator (s)/ Birth Certificate + other photo ID (acceptable by the Bank) • Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the Organizations • Certificate of registration issued by competent authority (if any) • Bye-laws (certified) • List of Management Committee/ Directors 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by a professional (if registered) • Other Bank statement • Certificate of Grand/ Aid • Subscription • If unregistered declaration of authorized person/ body 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Physical verification, if necessary.
Trusts, Foundations or similar entities	<ul style="list-style-type: none"> • Photograph of the signatory(s) (attested by the introducer) • National ID Card of the trustee (s)/ Passport of the trustee (s)/ Birth Certificate + other photo ID (acceptable by the Bank) • 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 (certified) • Power of attorney allowing transaction in the account. 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by a professional (if registered) • Other Bank statement • Donation 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Physical verification, if necessary.

Financial Institutions (NBFI)	<ul style="list-style-type: none"> • Photograph of all the directors(attested by the introducer) • Passport of all the directors/ National ID Card of all the directors/ Birth Certificate + other photo ID (acceptable by the Bank) • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form - XII • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials, or Employees to transact business on its behalf. • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by professional accountant. • Other Bank statement • Trade License • E-TIN • Cash flow statement • VAT registration 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.
-------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	company		
Embassies	<ul style="list-style-type: none"> • Photograph of the signatory(s) (attested by the introducer) • Valid Passport with visa of the authorized official • Clearance of the foreign ministry • Other relevant documents in support of opening account 		<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.
Foreign National (Individual)	<ul style="list-style-type: none"> • Passport along with visa page. • Identity of nominee(s), beneficial owner(if any) • Photograph of applicant (attested by the introducer) and nominee(s) (attested by the applicant) • Valid driving license (if any) • Credit card (if any) • Any other documents that satisfy the bank • Documents in support to stay in Bangladesh • Documents in support to source of fund or profession. 	<ul style="list-style-type: none"> • Work permit • Employment certificate • Documents of foreign remittance • Other bank statement (if any) 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.
Foreign National Firm/Company/ Joint Venture Contracting	<ul style="list-style-type: none"> • Copy of registration in Bangladesh with Board of investment/ Bangladesh Bank for Foreign/ Joint Venture Firm/Company • Memorandum and Article of Association duly certified by RJSC. • Copy of partnership deed • Copy of Bye-laws • Copy of service contact/ appointment letter/ work permit if any for 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by professional accountant. • Other Bank statement • Certificate of grant/aid • Any other documents of legal source. 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.

	<p>operation of the account</p> <ul style="list-style-type: none"> • Resolution of governing body to open account and authorization of operation. • List of authorized signatories and members of the governing body. • Copies of the relevant pages of passport • In case of foreign signatory(s) passport with visa page and work permit. • In case of Bangladesh signatory(s) NID/ Passport/ Birth Certificate + other photo ID (acceptable by the Bank) • E-TIN (if any) • Supporting documents of sources of fund of the signatory(s). • Photographs of the signatories duly attested by the introducer. 		
Non Resident Bangladeshi (NRB) Account	<ul style="list-style-type: none"> • Photocopy of relevant pages of the passport duly attested by the competent authority. • Work/resident permit • Supporting documents of the nominee (NID/ Passport/ Birth Certificate + any other photo ID acceptable by the bank officials) • Documents of beneficial owner (if any) • Photograph of applicant (attested by the introducer) and nominee(s) (attested by the applicant) 	<ul style="list-style-type: none"> • Employee ID • Documents for foreign remittance • Employee certificate 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.

	<ul style="list-style-type: none"> Supporting document of source of fund/profession. 		
--	-----------------------------------------------------------------------------------------------------	--	--

Note:

- a. If any customer want to authorize any person to operate an account on behalf of his/her then duly singed the mandate form to be obtained by the branch official. Mandate Form should be filled up mentioning the purpose of mandate and duration of this mandate. Branch official must be obtain accurate and complete information of mandatee.
- b. If there is one or more beneficial owners have been found then branch official must obtain supporting document of profession and identity.
- c. AML declaration form must be signed by the customer.
- d. SBS form must filled up and duly singed by the branch officials.
- e. If a person is US person as per FATCA, branch officials must obtain declaration and supporting documents as per requirement.

RISK REGISTER
ML & TF Risk Register for Customers

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer	Very Likely	Minor	Medium 2	a) Sanction list must be checked before opening account. b) Comply CDD. c) Complete KYC perfectly. d) Input TP as per authentication of the source of fund of the client. e) Physical verification is required.
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	Very Likely	Moderate	High 3	a) Sanction list must be checked before opening account. b) Confirm the source of fund. c) Identify beneficial owner, if any. d) Input TP as per nature of
				business and source of fund. e) Obtain supporting document against the large transaction. f) Complete CDD accurately.
Walk-in customer (beneficiary is government/semi government/ autonomous body/ bank & NBFIs) in case of issuing PO,DD, etc.	Very Likely	Minor	Medium 2	a) Check Sanction list. b) Ensure the purpose of transaction and source of fund of the applicant. c) Complete the KYC of the applicant perfectly.
Walk-in customer (beneficiary is other than government/semi government/ autonomous body/ bank & NBFIs)	Very Likely	Moderate	High 3	a) Check Sanction list. b) Identify the reason of transaction. c) Complete and accurate information of the applicant and beneficiary.
Non-resident customer (Bangladeshi)	Very Likely	Moderate	High 3	a) Sanction list must be checked before opening account. b) Maintain proper documentation as per Foreign Exchange guideline and circulars issued by regulatory authority. c) Complete KYC accurately.

A customer making series of transactions to the same individual or entity	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Monitoring the TP of the client. b) Justify the source of fund. c) Generate the statement and review the transactions. d) Monitoring the online transactions exceeding the limits declared in their TPs. e) Justify the link between the two parties.
Customer involved in outsourcing business	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Monitoring the inward remittance in favor of the client. b) Confirm the work area of outsourcing income. c) Monitoring the transaction on regular basis. d) Comply the CDD. e) Collect the information of KYCC. f) Monitoring the countries/jurisdiction from which the fund comes/receives.

Customer appears to do structuring to avoid reporting threshold	Likely	Major	High 3	<ul style="list-style-type: none"> a) Monitoring the cash transaction on regular basis. b) Obtain justification of transaction. c) If found any suspicious then report as STR.
Customer appears to have accounts with several banks in the same area	Likely	Major	High 3	<ul style="list-style-type: none"> a) Confirm the source of fund of the client. b) Monitoring transaction pattern. c) Obtain justification from the customer regarding maintains of several accounts. d) Complete CDD and EDD perfectly.
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Monitoring the nature of business of the client. b) Monitoring the nature of transaction. c) If found any suspicious then report as SAR.
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Likely	Major	High 3	<ul style="list-style-type: none"> a) Update the KYC. b) Regular monitoring of the client transaction. c) Take necessary steps as per court order against the client (if any).
Negative news about the customers' activities/business in media or from other reliable sources	Likely	Major	High 3	<ul style="list-style-type: none"> a) Inform CCC immediately. b) Update KYC. c) Regular monitor transaction. d) If seems to be suspicious Submit STR to CCC for onward submission to BFIU.
Customer is secretive and reluctant to meet in person	Unlikely	Major	Medium 2	<ul style="list-style-type: none"> a) Visit customer address and try to communicate. b) Regular monitoring of transaction. c) If found suspicious then submit STR.
Customer is a mandate who is operating account on behalf of another person/ company.	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Proper CDD of the mandatee. b) Relationship between the account holder and mandate. c) Proper KYC of the mandate. d) Find out the reason for providing mandate. e) Duration of mandate. f) Monitoring of transaction.

Large deposits in the account of customer with low income	Likely	Major	High 2	a) Request to client for submitting supporting document regarding the large transaction. b) If failed to submit the document take necessary steps for STR.
Customers about whom BFIU seeks information (individual)	Very Likely	Moderate	High 3	a) Regular monitor of the client. b) Update KYC. c) Check whether there is any negative information about the customer in media. d) If suspicious found then submit STR.
A customer whose identification is difficult to check	Likely	Major	High 3	a) Verify the identity of the customer through bank officials. b) For new account if identification not possible then do not open account. c) If existing account then close the account prior notice to customer.
Significant and unexplained geographic distance between the bank and the location of the customer	Likely	Major	High 3	a) Purpose of account opening. b) Complete the CDD. c) Keep transaction especially online transaction under monitoring.
Customer is a foreigner	Likely	Major	High 3	a) Check the Sanction list before opening the account. b) Purpose of opening account in Bangladesh. c) Apply EDD. d) Follow the instruction of Foreign Exchange guideline and circulars of FEPS.
Customer is a minor	Very Likely	Minor	Medium 2	a) Obtain birth certificate. b) Complete the CDD of guardian and the minor. c) Reason for opening minor account. d) Identify the beneficial ownership.
Customer is Housewife doing small transaction	Very Likely	Minor	Medium 2	a) Confirm source of fund. b) Reason for opening account. c) TP will be low. d) Monitoring of transaction on regular basis.
Customer is Housewife doing large transaction	Likely	Major	High 3	a) Confirm source of fund. b) Obtain supporting document against

				<p>the large transaction.</p> <p>c) Identify the beneficial owner.</p> <p>d) Obtain KYC of beneficial owner.</p> <p>e) Monitoring of transaction on regular basis.</p>
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	High 3	<p>a) Obtain CAMLCO approval for establishing or continuing existing business relationship.</p> <p>b) Check whether the source of fund commensurate with the designation.</p> <p>c) Complete the EDD.</p> <p>d) Follow the instruction of Foreign Exchange guideline and FEPD circulars.</p>
Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Likely	Major	High 3	<p>a) Confirm of the source of fund.</p> <p>b) Monitor the transactions.</p> <p>c) Find out the beneficial owner.</p> <p>d) Complete KYC of customer and beneficial owner.</p> <p>e) Perform CDD of customer and beneficial owner.</p>
Customers doing significant volume of transactions with higher-risk geographic locations.	Likely	Major	High 3	<p>a) Reason for opening account.</p> <p>b) Regular monitoring of online transaction.</p> <p>c) Install TP as per source of fund of the client.</p> <p>d) Find out the Reason by supporting documents.</p>
A customer who brings in large amounts of used notes and/or small denominations	Likely	Moderate	Medium 2	<p>a) Justification of nature of business.</p> <p>b) Whether the nature of business consistence with this condition or not.</p>
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	High 3	<p>a) Obtain source of fund with supporting documents.</p> <p>b) Obtain customer's customer (KYCC).</p> <p>c) Regular monitoring of transaction on regular basis.</p> <p>d) Obtain the membership certificate issued from relevant trade body i.e. membership of jewelry Association in case of jewelry business.</p>

Customer is a money changer/ courier service agent / travel agent	Likely	Major	High 3	<ul style="list-style-type: none"> a) Obtain correct and complete information regarding business. b) Follow the instruction of Foreign Exchange guideline and FEPD circulars (if needed). c) Identify the source of fund with supporting documents. d) Obtain license from competent authority.
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Likely	Major	High 3	<ul style="list-style-type: none"> a) Complete CDD as well as EDD. b) Obtain information about necessary documents with respect to nature of business. c) Regular monitoring on regular basis.
Customer is involved in Manpower Export Business	Likely	Major	High 3	<ul style="list-style-type: none"> a) Obtain supporting documents as a source of fund regarding their nature of business. b) Complete proper CDD. c) Check license issued by Ministry of Expatriates Welfare and Overseas employment and membership certificate. d) Monitoring of Transaction. e) Check Sanction list. f) Keep in touch with media regarding the customer. g) Perform EDD
Customer has been refused to provide banking facilities by another bank	Likely	Major	High 3	<ul style="list-style-type: none"> a) Check the genuineness of NID/Passport etc. with recent photograph. b) Complete CDD as well as EDD. c) Try to know the reason of refusal. d) Check additional ID like driving license, E-TIN, Utility bill, etc.
Accounts opened before 30 April, 2002	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Update KYC profile. b) Obtain recent photograph. c) Obtain photo ID d) If KYC not possible mark as dormant. e) Monitor transaction regularly.

Customers with complex accounting and huge transaction	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Monitor transaction regularly and justify whether it commensurate with source of fund. b) Obtain supporting documents of income like sales proceeds, balance sheet, etc. c) If suspicious, then perorated as STR.
Receipt of donor fund , fund from foreign source by micro finance institute (MFI)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Check Sanction list of the donor. b) Obtain supporting documents (approval from appropriate authority). c) Monitor transaction. d) Identification of beneficial owner. e) If suspicious, then perorated as STR.
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	Unlikely	Moderate	Low 1	<ul style="list-style-type: none"> a) Obtain declaration whether the organization follow the instruction of MLP guideline. b) Complete the CDD of the customer properly. c) Monitor the transactions.
Wholesale Banking Customer				
Entity customer having operations in multiple locations	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Obtain information regarding their operation in multiple locations. b) Monitor the transactions regularly. c) Check their balance sheet. d) If suspicious, then perorated as STR.
Customers about whom BFIU seeks information (large corporate)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Try to know the reason of seeking information by BFIU from reliable source or media. b) Monitoring of transaction. c) Obtain update KYC of the customer. d) Perform EDD
Owner of the entity that are Influential Persons (IPs) and their family members and Regular associates	Likely	Major	High 3	<ul style="list-style-type: none"> a) Obtain CAMLCO approval for establishing or continuing existing business relationship. b) Obtain CDD as well as EDD. c) Regularly monitoring of transaction.

A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Obtain information regarding source of fund with supporting documents. b) Identify the beneficial owner. c) Check whether TP of customer Commensurate with nature of business and transaction pattern. d) Check TP. e) Check cash flow statement and sales register. f) Verify the business address of the customer.
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Obtain information of KYCC. b) Check TP. c) Check online transaction. d) Obtain justification of such transaction. e) Review of Statement regular basis.
A customer whose identification is difficult to check.	Unlikely	Major	Medium 2	<ul style="list-style-type: none"> a) Personally visit the place and try to identify the customer. b) If not satisfied don't open the account. c) In case of existing customer close the account prior notice to customer. d) Obtain information regarding the customer from other reliable sources.
Owner of the entity that are Politically Exposed Persons (PEPs) or chief / senior officials of International Organizations and their family members and close associates	likely	Major	High 3	<ul style="list-style-type: none"> a) Obtain CAMLCO approval for establishing or continuing existing business relationship. b) Complete Enhance Due Diligence. c) Follow the instruction of Foreign Exchange guideline and FEPD circulars.
Charities or NPOs (especially operating in less privileged areas).	likely	Major	High 3	<ul style="list-style-type: none"> a) Identification of beneficial owner. b) Complete CDD. c) Monitoring of transactions. d) Identification of source of fund from reliable sources. e) Obtain the permission/ license required by customer from competent authority. f) Perform EDD

Credit Card Customer				
Customer who changes static data frequently	Likely	Major	High 3	a) Obtain supporting documents for changing information. b) Obtain customer acknowledgement by sending letter to old and new address. c) Monitoring of transactions.
Credit Card customer	Very Likely	Moderate	High 3	a) Check Sanction list before providing the credit card. b) Collect required documents as per PPG and Bank Policy. c) Obtain KYC. d) Verify the address and contact number. e) Obtain CIB report. f) Confirm that whether the client is using other card or not. g) Regular monitoring of transaction.
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	Very Likely	Moderate	High 3	a) Monitoring of transaction. b) Justification of transaction with his income. c) If found suspicious then submit STR.
Prepaid Card customer	Very Likely	Moderate	High 3	a) Check Sanction list. b) Collect CIB report. c) Obtain KYC. d) Verify the address and contact number. e) Collect required document as per PPG and bank policy. f) Check whether customer already availing bank card. g) Monitoring of transaction.
Customer doing frequently online cash transaction in a same time from credit card but declined	Very Likely	Moderate	High 3	a) Talk with the client immediately and confirm whether he is doing transaction or not. b) If found anything wrong then take necessary steps. c) Regular monitoring of transaction.
International Trade Customer				
A new customer (Outward	Likely	Moderate	Medium	a) Check Sanction lists.

remittance-through SWIFT)			2	<ul style="list-style-type: none"> b) Purpose of the remittance. c) Collect supporting documents. d) Obtain KYC. e) Follow the instruction of Foreign Exchange guideline and FEPD circular.
A new customer (Import/Export)	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Screening against Sanction List. b) Obtain CDD. c) Old customer of other bank: Obtain certificate from previous bank on "no overdue bill of entry" d) New Customer: Confirm that all relevant documents including IRC/ERC are in place. e) Follow the instruction of foreign exchange guideline and FEPD circulars. f) Physical verification, where necessary.
A new customer (Inward remittance-through SWIFT)	Very Likely	Minor	Medium 2	<ul style="list-style-type: none"> a) Check the SANCTION list. b) Obtain KYC/CDD of the beneficiary. c) Purpose of the remittance with supporting documents. d) Collect "Form C" where applicable. e) Follow the instruction of Foreign Exchange guideline and other circulars.
A new customer who wants to carry out a large transaction (Import/Export)	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Obtain CDD. b) Obtain respective IRC/ERC issued mentioning bank. c) If customer is old for other bank then collect "no overdue bill of entry". d) Follow the instruction of foreign exchange guideline and FEPD circulars.
A new customer who wants to carry out a large transaction (Inward/outward remittance)	Unlikely	Major	Medium 2	<ul style="list-style-type: none"> a) Obtain KYC/CDD of the client. b) Obtain information regarding the transaction related to his/her nature of business. c) Follow the instruction of foreign

				Exchange guideline and FEPD circulars.
A customer wants to conduct business beyond its line of business (import/export/ remittance)	Unlikely	Major	Medium 2	a) Obtain KYC of the customer. b) Obtain information regarding the diversification of the business. c) Check the justification of diversification of business. d) If suspicious, then perorated as STR.
Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	Likely	Major	High 3	a) Check the Sanction List and local black list issued by competent authority. b) Obtain Enhanced Due Diligence (EDD). c) Obtain CAMLCO approval for establishing or continuing existing business relationship. d) Regular monitoring of transaction. e) Check whether the source of fund commensurate with the
Correspondent Banks	Likely	Major	High 3	a) Follow the instruction of the master circular BFIU Circular No. 26 at the time of establish relationship. b) Obtain information regarding nature of business of the correspondence/ respondent bank. c) Update KYC on regular basis
Money services businesses (remittance houses, exchange houses)	Likely	Major	High 3	a) Follow the instruction of the master circular BFIU Circular No. 26. b) Obtain information regarding the correspondence/ respondent bank. c) Update KYC on regular basis.

a. ML & TF Risk Register for Products & Services

A comprehensive ML & TF risk assessment must take into account the potential risks arising from the transactions, products and services that the Bank Asia offers to its customers and the way these products and services are delivered to the customer. The Branch should pay particular attention to ML & TF risk which may arise from the application of new technologies. In identifying the risks of transactions, products, and services, the following factors are some example of ML & TF risk that Bank may face and the possible ways to reduce and manage those risks:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)	Likely	Major	High 3	a) Obtain purpose of opening account with supporting document if needed. b) If student is a minor then collect birth certificate and collect guardian information with documents. c) Obtain information regarding the beneficial owner. d) Obtain the reason behind the large transaction. e) Obtain TP related with the source of fund.
Locker Service	Likely	Major	High 3	a) Make sure customer have maintained account with us. b) Obtain KYC of the client. c) Confirm the source of fund. d) Update KYC periodically. e) Monitor customer's activity when he/she is using locker.
Foreign currency endorsement in Passport	Very Likely	Moderate	High 3	a) Check the visa of the customer. b) Follow the instruction of foreign exchange guideline and circulars regarding endorsement. c) Complete the TM form with duly signed by the customer.
Large transaction in the account of under privileged people	Unlikely	Major	Medium 2	a) Obtain CDD of the customer. b) Obtain documents regarding source of fund. c) Justification from the customer regarding the purpose of transaction.
FDR (less than 2 million)	Very Likely	Minor	High 3	a) Obtain CDD of the customer. b) Obtain information regarding the source of fund.
FDR (2 million and above)	Likely	Moderate	Medium 2	a) Obtain CDD of the customer. b) Obtain information regarding the source of fund. c) If source of fund is not provided by the customer.

				d) Check customer has other FDR maintaining with the bank.
Special scheme deposit accounts opened with big installment and small tenure	Very Likely	Moderate	High 3	a) Obtain KYC. b) Obtain supporting documents regarding source of fund.
Multiple deposit scheme accounts opened by same customer in a branch	Very Likely	Minor	Medium 2	a) Obtain KYC. b) Obtain supporting documents regarding source of fund.
Multiple deposit scheme accounts opened by same customer from different location	Likely	Moderate	Medium 2	a) Obtain KYC. b) Obtain supporting documents regarding source of fund. c) Obtain justification regarding opening of multiple deposit scheme in different locations. d) Monitoring of online transactions
Open DPS in the name of family member or Installments paid from the account other than the customer's account	Very Likely	Moderate	High 3	a) Obtain written documents mentioning the reason of this kind of transaction. b) Obtain information of beneficial owner. c) Regular monitoring of transaction.
Early encashment of FDR, special scheme etc.	Very Likely	Minor	Medium 2	a) Collect information regarding early encashment.
Non face to face business relationship /transaction	Likely	Major	High 3	a) Collect information from the relationship officer. b) Collection of data other reliable sources. c) Justification of source of data. d) Check the relationship of the client and banker.
Payment received from unrelated/un-associated third parties	Likely	Major	High 3	a) Obtain evidence of actual relationship or reason for such receipt. b) Perform EDD. c) If anything suspicious report as SAR. d) Don't allow transaction until risk is reduced.
SME Banking Product				
Want to open FDR where source of fund is not clear	Likely	Major	Extreme 4	a) Obtain CDD. b) Obtain supporting documents regarding source of fund.

				c) If not satisfied don't open FDR.
Early encashment of FDR	Very Likely	Minor	Medium 2	a) Collect information regarding early encashment.
Repayment of loan EMI from source that is not clear	Likely	Moderate	Medium 2	a) Obtain information of source of fund. b) Monitor transaction.
Repayment of full loan amount before maturity	Likely	Moderate	Medium 2	a) Ensure source of fund of repayment before early adjustment of loan. b) Obtain reason behind early adjustment of loan.
Loan amount utilized in sector other than the sector specified during availing the loan	likely	Major	High 3	a) Monitor the utilization loan. b) If found suspicious, then send STR.
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	likely	Major	High 3	a) Obtain information of repayment of loan. b) If found suspicious, then send STR.
Source of fund used as security not clear at the time of availing loan	Unlikely	Moderate	Medium 2	a) Collect information and confirm the security. b) If found clear then provide sanction.
Wholesale Banking Product				
Development of new product & service of bank	Likely	Moderate	Medium 2	a) Identify feasibility of the product & service. b) Identify the ML & TF risk of the product & service.
Payment received from unrelated third parties	Unlikely	Moderate	Medium 2	a) Obtain relationship of the parties. b) Complete short KYC of depositor. c) Received payment only from the distributors, agents and suppliers of the customer. d) Monitoring the transaction regularly.
High Value FDR	Very Likely	Minor	Medium 2	a) Obtain CDD. b) Obtain supporting documents regarding source of fund.
Term loan, SOD(FO), SOD(G-work order), SOD(Garment), SOD(PO), Loan General, Lease finance, Packing Credit, BTB L/C	Likely	Minor	Medium 2	a) Obtain CDD. b) Analysis the credit worthiness of the customer. c) Visit customer's office, factory and mortgaged properties. d) Monitor the transaction.

BG (bid bond), BG(PG), BG (APG)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Verify the work order from the concern authority. b) Ensure assignment of bill from the concerned authority. c) Perform CDD. d) Obtain margin. e) Obtain sufficient collateral.
L/C Subsequent term loan, DP L/C	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Obtain certificate from the respective countries chamber of commerce. b) Ensure proper verification of the price of the imported items from the international market/website. c) Obtain undertaking from the customer regarding the fair price.
SOD (Earnest Money), STL	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Check the work order. b) Verify the tender notice. c) Follow up the client whether the client get the work order or not. d) Verify other sources of income of the customer.
OBU	Unlikely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Confirm Enhance Due Diligence. b) Obtain information about the customer from the media, International market, web, etc. c) Obtain credit report of the customer. d) Preserve the permission obtained by the customer from competent authority. e) Confirm that advance is allowed considering the category.
Syndication Financing	Likely	Major	High 3	<ul style="list-style-type: none"> a) Perform CDD of the customer. b) Verify the value of plants, machinery and imported items. c) Obtain certificate from the respective chamber of commerce. d) Obtain information from lead bank regarding payment system. e) Physical verification.

Credit Card				
Supplementary Credit Card Issue	Very Likely	Major	Extreme 4	a) Obtain required documents as per Product Program Guideline (PPG) and bank's policy. b) Collect relationship of supplementary card holder with customer. c) Obtain KYC of supplementary cardholder. d) Collect CIB report. e) Keep transaction under monitoring. f) Check the Sanction list. g) Check whether customer is already availing Bank Credit card.
Frequent use of Card Cheque	Very Likely	Major	Extreme 4	a) Update KYC. b) Obtain the purpose of the transaction. c) The account where the fund is transferred. d) Monitoring of transaction.
Credit card issuance against ERQ and RFCD accounts	Likely	Major	High 3	a) Check SANCTION LIST. b) Collect CIB report of the customer. c) Verification of address of the client. d) Obtain KYC. e) Check the customer is availing the other bank credit card. f) Confirm that transactions are conducted as per foreign exchange guideline and FEPD circulars. g) Collect required documents as per PPG and Bank's policy.
International Trade				
Line of business mismatch (import/export/remittance)	Likely	Major	High 3	a) Perform EDD of the customer. b) Check the diversification of business. c) If found suspicious then send for STR.
Under / Over invoicing (import/export/remittance)	Very Likely	Major	Extreme 4	a) Perform EDD. b) Check the unit price of the product intended for import and export with the present international market

				price through internet. c) If found suspicious then send for STR.
Retirement of import bills in cash import / export/ remittance)	Very Likely	Major	Extreme 4	a) Check the size of the transaction with the cash flow. b) Background checking of Beneficial owner. c) Confirm EDD.
Wire transfer	Very Likely	Moderate	High 3	a) Follow the instruction of the BFIU Circular No. 26 before conducting the transaction. b) Obtain information of applicant and beneficiary as per BFIU Circular No. 26.
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)	Likely	Moderate	Medium 2	a) Confirm the purpose of the remittance with supporting documents. b) Collect information of applicant and beneficiary as per BFIU Circular No. 26. c) If found suspicious then send for STR.

a. ML & TF Risk Register for Business practices/delivery methods or channels

These are some example of ML & TF risk in terms of business practices/delivery methods or channels that Bank may face and the possible ways to reduce and manage those risks:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Online (multiple small transaction through different branch)	Very Likely	Moderate	High 3	a) Obtain justification regarding the transaction pattern from the customer. b) Obtain KYC of the bearer as per BFIU Circular No. 26. c) Monitor online transaction. d) If found any suspicious then send for STR.
BEFTN/RTGS	Very Likely	Minor	Medium 2	a) Obtain information regarding the purpose of the transaction. b) Obtain information regarding

				relationship of the customer and beneficiary. c) Monitor transaction pattern. d) Update TP.
BACH	Likely	Moderate	Medium 2	a) Check the four corners of Cheque. b) Check the amount of cheque. c) Check the cheque number. d) Check TP of the client. e) Check the signature card of the client.
IDBP (Inland Documentary Bill Purchase)	Very Likely	Minor	Medium 2	a) Confirm CDD. b) Check the genuineness of LC and acceptance from BB dashboard.
Agent Banking				
Savings account	Very Likely	Minor	Medium 2	a) Check Sanction List. b) Open through biometric and capture other related documents in the system along with attaching hard copy with AOF. c) Confirm the source of the agent client d) Strictly follow CDD process. e) Confirm the dual control in Account approval and internal verification over phone. f) Confirm the Limited Cash withdrawal limit.
Current Account	Likely	Moderate	Medium 2	a) Check Sanction List. b) Open through biometric and capture other related documents in the system along with attaching hard copy with AOF. c) Confirm the source of the agent client d) Strictly follow CDD process. e) Confirm the dual control in Account approval and internal verification over phone. f) Confirm the Limited Cash withdrawal limit.
Term Deposit Scheme	Likely	Moderate	Medium 2	a) Only Savings/Current account holder can open the account. b) No walking customer is allowed to

				open the account. c) TDS account open by debiting linked account and also credit the linked account after maturity or pre-mature tenure.
DPS	Very Likely	Minor	Medium 2	a) Only Savings/Current account holder can open the account. b) No walking customer is allowed to open the account. c) DPS account open by debiting linked account and also credit the linked account after maturity or pre-mature tenure.
Mobile Banking	Likely	Moderate	Medium 2	a) Obtain KYC. b) Confirm CDD & EDD. c) Monitor transaction regularly. d) Check NID/ Passport/ Birth Certificate along with photo. e) Check additional documents
Credit Card				
New Merchant sign up	Unlikely	Minor	Low 1	a) Confirm KYC of merchant. b) Visit merchant physically. c) Collect documents as per PPG and bank's policy.
High volume transaction through POS	Very Likely	Moderate	High 3	a) Check merchant product & price and match with POS transactions. b) Check transaction profile of the merchant. c) Obtain justification from
Alternate Delivery Channel				
Large amount withdrawn from ATMs	Likely	Moderate	Medium 2	a) Check the timing of transaction. b) Obtain justification of transaction. c) If found any suspicious send
Larger amount transaction from different location and different time(mid night) through ATM	Likely	Major	High 3	a) Check the timing of transaction. b) Obtain justification of transaction. c) If found any suspicious send
Huge fund transfer through	Likely	Major	High	a) Check the transaction limit

internet			3	number through internet banking. b) Generate report regarding high value of transaction through internet from the system. c) Monitor transaction.
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Very Likely	Moderate	High 3	a) Check the Sanction list of the parties involved with this transaction. b) Confirm whether the transaction meets the central bank circulars or guideline. c) Obtain purpose of the remittance. d) Confirm the KYC. e) Obtain information as per BFIU Circular No. 26.
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103).	Very Likely	Major	Extreme 4	a) Obtain documents related to this transaction. b) Obtain Form C from the client before release the remittance.

a. ML & TF Risk Register for Country/jurisdiction

Country or geographical risk may arise because of the location of a customer, the origin of destination of transactions of the customer, but also because of the business activities of the Bank itself, its location and the location of its organizational units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to money laundering and terrorism financing.

There is no general definition based on which particular countries or geographical areas can be categorized as low, medium or high risk. The factors which may define if a specific country or geographical area is more vulnerable to money laundering and terrorism financing, may include different criteria. These are some example of ML & TF risk that Bank may face and the possible ways to reduce and manage those risks:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Import and export from/to sanction country	Very likely	Major	Extreme 4	a) Inform AML & CFT Division immediately and take the opinion. b) Check the Sanction List. c) Inform BFIU through AML & CFT Division without delay.

Transshipments, container, flag vessel etc. under global sanction	Very likely	Major	Extreme 4	a) Inform AML & CFT Division immediately and take the opinion. b) Check the Sanction list. c) Inform BFIU through AML & CFT Division without delay.
Establishing correspondent relationship with sanction bank and/or country	Very likely	Major	Extreme 4	a) Inform AML & CFT Division immediately and take the opinion. b) Check the Sanction list. c) Inform BFIU through AML & CFT Division without delay.
Establishing correspondent relationship with poor AML & CFT practice country	Very likely	Major	Extreme 4	a) Confirm the EDD before establishing relationship with the correspondent bank. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the correspondent bank.
Customer belongs to higher - risk geographic locations such as High Intensity Financial Crime Areas	Very likely	Major	Extreme 4	a) Confirm the EDD before establishing relationship with the correspondent bank. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the correspondent bank.
Customer belongs to countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.	Very likely	Major	Extreme 4	a) Confirm the EDD before establishing relationship with the correspondent bank. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the correspondent bank.
Customer belongs to High Risk ranking countries of the Basel AML index.	Very likely	Major	Extreme 4	a) Confirm the EDD before establishing relationship. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the bank/entity.
Customer belongs to the countries identified by the bank as higher -risk because of its prior experiences or other factors.	Likely	Major	High 3	a) Confirm the specific reason of transaction. b) Obtain EDD of the customer.

Any country identified by FATF or FSRBs-(FATF Style Regional Body) as not having adequate AML & CFT systems	Very Likely	Major	Extreme 4	a) Don't accept as a customer.
Any country identified as destination of illicit financial flow	Likely	Major	High 3	a) Confirm Customer Due Diligence and Enhanced Due Diligence.
Border Area	Likely	Major	High 3	a) Update KYC of the account holder periodically. b) Confirm EDD if needed. c) Monitor cash deposit and online transaction. d) Monitor high risk customer on regular basis.
Countries subject to UN embargo/ sanctions	Very Likely	Major	Extreme 4	a) If there is any existing customer stop the transaction immediately and inform BFIU through AML & CFT Division.

7.1.1 Register for Regulatory Risk

Regulatory risk is associated with not meeting all the obligations of Bank under the Money Laundering Prevention Act 2012 (Amendment 2015), Anti Terrorism Act 2009, (amendment 2012 & 2013). Following are some example of ML & TF risk the Bank may face in terms of noncompliance of regulations and the possible ways to reduce and manage those risks.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML & CFT guideline	Likely	Major	High 3	a) Develop AML & CFT guideline. b) Update guideline time to time.
Not forming a Central Compliance Committee (CCC)	Likely	Major	High 3	a) Formation of Central Compliance Committee as per BFIU Circular No. 26.
Not having an AML & CFT Compliance Officer	Likely	Moderate	Medium 2	a) Nominate the compliance officer name as per requirement of BFIU Circular No. 26.
Not having Branch Anti Money Laundering Compliance Officer	Likely	Moderate	Medium 2	a) Central Compliance Committee (CCC) will nominate Branch Anti Money Laundering Compliance Officer (BAMLCO) at branch level mentioning details scope of works

				and responsibilities of BAMLCO as per BFIU Circular no. 26 dated 16.06.2020
Not having an AML & CFT program	Likely	Major	High 3	a) Develop AML & CFT program. b) Update program time to time.
No senior management commitment to comply with MLP and AT Act.	Likely	Moderate	Medium 2	a) Provision of commitment of senior management to be included in the AML & CFT policy guideline.
Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	Likely	Major	High 3	a) Follow the AMLD & BFIU circulars, circular letters, instruction issued from time to time.
Unique account opening form not followed while opening account	Likely	Moderate	Medium 2	a) Circular No. 26. Develop the unique account opening form while opening new account as per BFIU
Non screening of new and existing customers against UNSCR and OFAC lists	Likely	Major	High 3	a) Before establishing any kind of relationship with customer must check SANCTION LIST sanction and OFAC lists.
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Likely	Major	High 3	a) Must follow the instruction of Foreign Exchange Regulation Act 1947 while dealing with NRB accounts.
Complete and accurate information of customer not obtained	Likely	Major	High 3	a) Follow the instruction of BFIU Circular No. 26 regarding complete and accurate information of the customer. b) Update KYC periodically. c) If fails to update then close the account prior notice to customer.
Failure to verify the identity proof document and address of the customer	Likely	Major	High 3	a) Verify (business unit) the identity proof document and address of the customer b) Verify the ID from the competent authority. c) Verify the address by collecting other documents like utility bill, phone bill, etc.
Beneficial owner identification and verification not done properly	Likely	Major	High 3	a) Monitor transaction and find out the beneficial owner of the account. b) Collect KYC of beneficial owner.
Customer Due Diligence (CDD) not practiced properly	Likely	Major	High 3	a) Perform CDD of the customer as per BFIU Circular No. 26.
Failure to perform Enhanced	Likely	Major	High	a) Perform EDD for the high risk

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.)			3	customer. b) Obtain CAMLCO approval for establishing or continuing existing business relationship.
Failure to complete KYC of customer including walk in customer	Likely	Major	High 3	a) Complete KYC of customer including walk in customer as per BFIU Circular No. 26
Failure to update TP and KYC of customer	Likely	Major	High 3	a) Update TP & KYC as per BFIU Circular No. 26.
Keep the legacy accounts operative without completing KYC	Unlikely	Major	Medium 2	a) Update the KYC of the legacy accounts. b) If failed then follow the instruction of the BFIU Circular No. 26.
Failure to assess the ML & TF risk of a product or service before launching	Unlikely	Major	Medium 2	a) Assess the ML and TF risk of a product or service before launching.
Failure to complete the KYC of Correspondent Bank	Likely	Major	High 3	a) Complete the KYC of correspondent Bank reciprocally. b) Update KYC of correspondent bank time to time.
Senior Management approval not obtained before entering into a Correspondent Banking relationship	Unlikely	Major	Medium 2	a) Obtain Chief Anti Money Laundering Compliance Officer approval before entering into a Correspondent Banking relationship.
Failure to comply with the instruction of BFIU by bank Foreign subsidiary	Likely	Moderate	Medium 2	a) Obtain confirmation from the subsidiary on compliance. b) Monitor the AML & CFT activity of subsidiary.
Failure to keep record properly	Likely	Major	High 3	a) Follow the instruction of BFIU Circular No. 26 regarding record keeping.
Failure to report complete and accurate CTR on time	likely	Major	High 3	a) Rectify the irregularities of the information in CBS and FIU software module. b) Branch and AML & CFT Division will monitor the CTR transaction. c) Send the CTR through goAML software and FIU software (CD copy).

Failure to review CTR	Likely	Moderate	Medium 2	a) Generate the CTR from CBS. b) Monitor transaction report by both AML & CFT Division and Branch on monthly basis.
Failure to identify and monitor structuring	Likely	Major	High 3	a) Set up a mechanism for finding out structuring and generate report from CBS. b) Identity & Monitor structuring report regular basis.
Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Likely	Major	High 3	a) Monitor structuring report, high value transaction report, TP changing report and identify STR. b) Develop monitoring system to identify STR.
Failure to conduct quarterly meeting properly	likely	Moderate	Medium 2	a) Conduct meeting on quarterly basis and discuss regarding the recent circulars, laws and guideline of AML & CFT matters and its implementation. b) Send the meeting minutes to AML & CFT Division on quarterly basis.
Failure to report suspicious transactions (STR)	Very Likely	Major	Extreme 4	a) Both Branch and AML & CFT Division will monitor monthly CTR report at the time of finding suspicious transaction. b) Monitor other transaction and activity of the customer at the time of finding
Failure to conduct self-assessment properly	Likely	Major	High 3	a) Branch will mention the actual position of strength and weakness of the branch. b) Cross check with the Independent Testing Report and Inspection Report.
Failure to submit statement/report to BFIU on time	likely	Major	High 3	a) Submit all the statements and reports to BFIU on time.
Submit erroneous statement/report to BFIU	Likely	Major	High 3	a) Statement/report must be checked carefully before sending to BFIU.
Not complying with any order for freezing or suspension of transaction issued by BFIU or	Very Likely	Major	Extreme 4	a) Must comply with any order for freezing or suspension of transaction issued by BFIU or BB timely.

BB				b) AML & CFT Division will check the order for freezing or suspension of transaction.
Not submitting accurate information or statement sought by BFIU or BB.	Likely	Major	High 3	a) Must submit accurate information or statement to BFIU or BB on time.
Not submitting required report to senior management regularly	likely	Moderate	Medium 2	a) Submit the respective report to senior management on regular basis.
Failure to rectify the objections raised by BFIU or bank inspection teams on time	Very Likely	Major	Extreme 4	a) Must regularized the objections raised by the BFIU or Bank inspection teams timely. b) AML & CFT Division will follow up the irregularities.
Failure to obtain information during wire transfer	Likely	Major	High 3	a) Must obtain information during wire transfer as per BFIU Circular No. 26. b) Inspection team will check the compliance regarding wire transfer.
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely	Major	High 3	a) Comply with the responsibilities of ordering, intermediary and beneficiary bank perfectly.
Failure to scrutinize staff properly	Unlikely	Major	Medium 2	a) HRD must scrutinize the background of the newly recruited employees properly. b) Must conduct reference check.
Failure to circulate BFIU guidelines and circulars to branches	Likely	Major	High 3	a) AML & CFT Division must circulate all the circulars and guidelines issued by BFIU to branches on time.
Inadequate training/workshop arranged on AML & CFT	Unlikely	Major	Medium 2	a) Workshop regarding AML & CFT matters on regular basis to build up the knowledge of all employees. b) Conduct the evaluation test at the time of training. c) Maintain the database of training list of employees.

No independent audit function to test the AML program	likely	Major	High 3	a) ICCD will inspect the AML program and conduct the Independent Testing Procedure.
-------------------------------------------------------	--------	-------	-----------	-------------------------------------------------------------------------------------

Red Flags pointing to Money Laundering

- ✓ The client cannot provide satisfactory evidence of identity.
- ✓ Situations where it is very difficult to verify customer information.
- ✓ Situations where the source of funds cannot be easily verified.
- ✓ Transactions in countries in which the parties are non-residents and their only purpose is a capital investment (they are not interested in living at the property they are buying).
- ✓ Frequent change of ownership of same property in unusually short time periods with no apparent business, economic or other legitimate reason and between related persons.
- ✓ Client wants to re-sell Property shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.
- ✓ Client wishes to form or purchase a company whose corporate objective is irrelevant to the client's normal profession or activities, without a reasonable explanation.
- ✓ The client sets up shell companies with nominee shareholders and/or directors.
- ✓ Client repeatedly changes Attorneys within a short period of time without any reasonable explanation.
- ✓ Client purchases property in names of other persons or uses different names on offers to purchase, closing documents and deposit receipts.
- ✓ Client deposits a large amount of cash with you to make payments which are outside of the client's profile.
- ✓ Client negotiates a purchase but wants to record a lower value on documents, paying the difference "under the table", (inadequate consideration).
- ✓ Client's documents such as identification, statement of income or employment details are provided by an intermediary who has no apparent reason to be involved, (the intermediary may be the real client).
- ✓ Transaction involves legal entities and there is no relationship seen between the transaction and the business activity of the buying company, or the company has no business activity.
- ✓ Client requests the firm to act as his agent in obtaining high sum bankers' drafts, cashiers' cheques and other cash equivalent or near cash monetary instruments or in making wire transfers to and from other banks or financial institutions, (anonymity).
- ✓ Divergence from the type, volume or frequency of transactions expected in the course of the business relationship.
- ✓ Client gives power of attorney to a non-relative to conduct large transactions (same as above).
- ✓ Use of letters of credit to move money between those countries, where such trade would not normally occur and / or is not consistent with the customer's usual business activity. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.
- ✓ The method of payment requested by the client appears inconsistent with the risk characteristics of the transaction. For example receipt of an advance payment for a shipment from a new seller in a high-risk jurisdiction.
- ✓ The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or that includes changes in regard to the beneficiary or location of payment without any apparent reason.
- ✓ Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction of same business entity are indicators for TBML. In this regard the study of foreign exchange remittances may help detect the offence.
- ✓ The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities or sensitive / non co-operative jurisdictions.
- ✓ The commodity is transshipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.

- ✓ Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense.
- ✓ Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- ✓ Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.
- ✓ Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management.

Red Flags pointing to Financing of Terrorism

Behavioural Indicators:

- ✓ The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- ✓ Use of false corporations, including shell-companies.
- ✓ Inclusion of the individual or entity in the United Nations 1267 Sanctions list.
- ✓ Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
- ✓ Beneficial owner of the account not properly identified.
- ✓ Use of nominees, trusts, family members or third party accounts.
- ✓ Use of false identification.
- ✓ Abuse of non-profit organization.

Indicators linked to the financial transactions:

- ✓ The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
- ✓ The transaction is not economically justified considering the account holder's business or profession.
- ✓ A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
- ✓ Transactions which are inconsistent with the account's normal activity.
- ✓ Deposits were structured below the reporting requirements to avoid detection.
- ✓ Multiple cash deposits and withdrawals with suspicious references.
- ✓ Frequent domestic and international ATM activity.
- ✓ No business rationale or economic justification for the transaction.
- ✓ Unusual cash activity in foreign bank accounts.
- ✓ Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- ✓ Use of multiple, foreign bank accounts.