

Money Laundering & Terrorist Financing Risk Management Guidelines

RISK



LOW



Janata Bank Limited
your committed partner in progress

Money Laundering & Terrorist Financing Risk Management Guidelines

July, 2021



JANATA BANK LIMITED

ML & TF Prevention Department

Head Office: 110, Motijheel C/A, Dhaka-1000, Phone: +88-02-9558386, 55110024 SWIFT: JANBDDH,
E-mail: aml@janatabank-bd.com, <http://www.jb.com.bd>, PABX: 9560000, 9560039, 9566020, 9556245-49, 9560027-30, Ext: 549,205

Focus Group

- Advisor** : **Md. Abdus Salam Azad**
MD & CEO
- Chairman** : **Md. Ismail Hossain**
Deputy Managing Director & CAMLCO (Ex.)
- Member** : **Md. Jashim Uddin**
Deputy Managing Director & Ex. CAMLCO
- Sk. Md. Zaminur Rahman**
General Manager (Ex.), ICT Division
- Md. Ahsan Ullah**
General Manager, Human Resources Division
- Md. Quamruzzaman Khan**
General Manager, Treasury & Foreign Trade Division
- Md. Mahbubor Rahman**
General Manager & Ex. CAMLCO
- Md. Asaduzzaman**
General Manager, Risk Management Division
- Shyamal Krishna Saha**
General Manager & CAMLCO
- Mashfiul Bari**
General Manager, Credit Division
- Compiled by** : **Most. Altafun Nessa**
Deputy General Manager & DCAMLCO
- Morjina Khatun**
Senior Principal Officer
- Sayed Shafiul Maznabin**
Officer-IT

Preface

Money laundering and terrorist financing have major impacts on a country's economy as a whole, impeding the social, economic, political and cultural development of a society. Both money laundering and terrorist financing can weaken individual financial institution and are threats to the reputation of a country's overall financial sector. Combating money laundering and terrorist financing assists in promoting a strong, sound and stable financial sector.

To maintain stability and integrity of international financial system, the Financial Action Task force (FATF), an inter-governmental body established by G-7 in 1989, has set 40 recommendations for preventing money laundering and combating terrorist financing. As per recommendations of FATF, every financial institution (FI) and designated non-financial business and profession (DNFBP) must identify, assess and take effective actions to mitigate Money Laundering and Terrorist Financing risks. These requirements are reflected in Money Laundering Prevention Rules (MLPR) 2019.

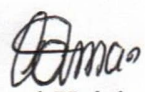
Bangladesh Financial Intelligence Unit (BFIU) vide their Circular Letter No. 01/2015 dated 08 January 2015 instructed that every schedule bank would prepare their own "Money Laundering and Terrorist Financing Risk Management Guidelines".

In view of above perspectives, Janata Bank Limited formulates its own guidelines to portray the basic ideas to detect, evaluate and manage money laundering and terrorist financing risks. These risks may arise out from the business elements such as customers, products, delivery methods and countries/jurisdictions. Once identified, bank/branch will assess the magnitude of risk by blending the chance and impact of the risks.


Important to mention that this is a humble attempt to update the previous guidelines where aspects of Money Laundering and Terrorist Financing Risk are delineated and discussed. These Guidelines are updated on the basis of existing laws & rules of the government and policies, guidelines & circulars of BFIU which have been issued recently. It is an ongoing process and will be updated or revised as and when required.

The Guidelines are intended to provide general advice to the employees of Janata Bank Limited. It should never be relied on as a substitute for Money Laundering Prevention Act, 2012; Money Laundering Prevention (Amendment) Act, 2015; Anti-Terrorism Act, 2009; Anti-Terrorism (Amendment) Act, 2013; and BFIU Guidelines.

These Guidelines have been duly approved by the Board of Directors in its 673th meeting on 13 July 2021.



(Shyamal Krishna Saha)
GM & CAMLCO



(Md. Abdus Salam Azad)
MD & CEO

Contact Point: Deputy General Manager & DCAMLCO
Janata Bank Limited
ML & TF Prevention Department
Head Office: Janata Bank Bhaban,
110, Motijheel C/A (19th Floor),
Dhaka-1000, Bangladesh
Phone: +88-02-223388386, +88-02-55110024.
e-mail: aml@janatabank-bd.com
website: https://www.jb.com.bd/about_us/aml

TABLE OF CONTENTS

CHAPTER		Page No.
Table of Contents		7-12
List of Abbreviations		13
An Overview of Money Laundering and Terrorist Financing Risk Management Guidelines		14-18
A.	Overview and Objective	14
B.	Scope	15
C.	Roles and Responsibilities about formation and Implementation of this policy Guidelines	15
i)	The Board of Directors	15
ii)	Risk Management Committee	16
iii)	MD & CEO	16
iv)	ML & TF Prevention Department	16
v)	Operation Divisions (All Credit Division, Foreign Trade & Treasury Division ICT Division)	17
vi)	Internal Audit Division	17
vii)	Human Resources Division	18
viii)	Other Divisions including the Executives /Officers and Staff of Head Office, Divisional Office, Area Office and branches	18
D.	Implementation	18
Chapter: 1	INTRODUCTION	19-24
	1.1 Defining Money Laundering	19
	1.2 Stages of Money Laundering	20
	1.3 Why Money Laundering is Done	20
	1.4 Defining Terrorist Financing	21
	1.5 The Link Between Money Laundering and Terrorist Financing	22
	1.6 Why We Must Combat ML & TF	22
	1.7 Targeted Financial Sanctions	23
Chapter: 2	INTERNATIONAL INITIATIVES ON ML AND TF	25-31
	2.1 Introduction	25
	2.2 The United Nations	25
	2.2.1 The Vienna Convention	25
	2.2.2 The Palermo Convention	25
	2.2.3 International Convention for The Suppression of The Financing of Terrorism	26
	2.2.4 Security Council Resolution 1267 And Successors	26
	2.2.5 Security Council Resolution 1373	26
	2.2.6 Security Council Resolution 1540	27
	2.2.7 The Counter-Terrorism Committee	27
	2.2.8 Counter-Terrorism Implementation Task Force (CTITF)	27
	2.2.9 Global Program Against Money Laundering	27
	2.3 The Financial Action Task Force	28
	2.3.1 FATF 40+9 Recommendations	28
	2.3.2 FATF New Standards	28
	2.3.3 Monitoring Members Progress	28
	2.3.4 The NCCT List	29

CHAPTER			Page No.
	2.3.5	International Cooperation and Review Group (ICRG)	29
	2.4	Asia Pacific Group on Money Laundering (APG)	29
	2.5	The Egmont Group of Financial Intelligence Units	30
	2.6	The Basel Committee on Banking Supervision	31
	2.6.1	Statement of Principles on Money Laundering	31
	2.6.2	Basel Core Principles for Banking	31
	2.6.3	Customer Due Diligence	31
Chapter: 3	MAJOR NATIONAL AML & CFT INITIATIVES		32-36
	3.1	Introduction	32
	3.2	Founding Member Of APG	32
	3.3	Legal Framework	32
	3.4	Central and Regional Taskforces	32
	3.5	Anti-Money Laundering Department	33
	3.6	Bangladesh Financial Intelligence Unit (BFIU)	33
	3.7	National Coordination Committee and Working Committee	33
	3.8	National ML & TF Risk Assessment (NRA)	33
	3.9	National Strategy for Preventing ML and TF	34
	3.10	Chief Anti-Money Laundering Compliance Officers (CAMLCO) Conference	34
	3.11	Egmont Group Memberships	34
	3.12	Anti-Militants and De-Radicalization Committee	35
	3.13	Memorandum of Understanding (MoU) Between ACC and BFIU	35
	3.14	NGO/NPO Sector Review	35
	3.15	Implementation of TFs	35
	3.16	Coordinated Effort on The Implementation of the UNSCR	36
	3.17	Risk Based Approach	36
	3.18	Memorandum of Understanding (MoU) BFIU And Other FIUs	36
Chapter: 4	AML & CFT COMPLIANCE PROGRAM OF JANATA BANK LIMITED		37-44
	4.1	Introduction	37
	4.2	Component of AML & CFT Compliance Program	37
	4.3	Development of AML & CFT Compliance Program	37
	4.4	Communication of Compliance Program	38
	4.5	Senior Management Role	38
	4.5.1	Role of Senior Management	38
	4.5.2	Statement of Commitment of CEO & MD	39
	4.6	Policies and Procedures	42
	4.6.1	Written AML & CFT Compliance Policy	42
	4.7	Customer Acceptance Policy	43
Chapter: 5	COMPLIANCE STRUCTURE OF THE BANK		45-54
	5.1	Anti-Money Laundering Organogram of Janata Bank Limited	45
	5.2	Central Compliance Committee	45
	5.2.1	Formation of CCC	46
	5.2.2	Authorities and Responsibilities of the CCC	46
	5.2.3	Separation of CCC From Internal Control & Compliance	46
	5.3	Chief Anti Money Laundering Compliance Officer (CAMLCO)	47
	5.3.1	Authorities and Responsibilities of CAMLCO	47

CHAPTER			Page No.
	5.4	Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)	48
	5.4.1	The authorities & Responsibilities of DCAMLCO	48
	5.5	ML & TF Prevention Department	48
	5.5.1	Functions of ML & TF Prevention Department:	49
	5.6	Division Level Organization Structure	49
	5.6.1	Responsibilities of DAMLCO	49
	5.7	Area Level Organization Structure	50
	5.7.1	Responsibilities of AAMLCO	50
	5.8	Branch Level Organization Structure	51
	5.8.1	Formation of Branch Anti-Money Laundering Compliance Committee (BAMLCC)	51
	5.8.2	Responsibilities of BAMLCC	51
	5.8.3	Branch Anti Money Laundering Compliance Officer (BAMLCO)	52
	5.8.4	Nomination of BAMLCO	52
	5.8.5	Authorities and Responsibilities of BAMLCO	52
	5.9	Internal Control and Compliance	53
	5.10	External Auditor	54
Chapter: 6		CUSTOMER DUE DILIGENCE	55-80
	6.1	Introduction	55
	6.2	General Rule of CDD	55
	6.2.1	Completeness and Accuracy	55
	6.2.2	Ongoing CDD measures (Review and update)	56
	6.2.3	Enhanced CDD measures	57
	6.3	Timing of CDD	57
	6.4	Transaction Monitoring	57
	6.5	Exception When Opening A Bank Account	58
	6.6	In Case Where Conducting the CDD Measure is Not Possible	58
	6.7	Customer Identification	58
	6.8	Verification of Source of Funds	59
	6.9	Verification of Address	59
	6.10	Persons Without Standard Identification Documentation	59
	6.11	Walk-In/ One Off Customers	60
	6.12	Non-Face to Face Customers	60
	6.13	Customer Unique Identification Code	60
	6.14	Correspondent Banking	61
	6.15	Politically Exposed Persons (PEPs)	61
	6.15.1	Definition of PEPs	62
	6.15.2	Chief or Similar High-Ranking Positions in An International Organization	62
	6.15.3	Family Members of PEPs	62
	6.15.4	Close Associates of PEPs	63
	6.15.5	Various Scenario Related with PEPs/IPs	63
	6.15.6	Risk Related with PEPs	63
	6.15.7	Obligations Under the Regulations	65
	6.16	Wire Transfer	67
	6.16.1	Cross-Border Wire Transfers	67
	6.16.2	Domestic Wire Transfers	68

CHAPTER			Page No.
6.16.3	Duties of Ordering, Intermediary and Beneficiary Bank in Case of Wire Transfer	68	
6.17	Beneficial Ownership and Control	69	
6.17.1	Definition	69	
6.17.2	Importance to identify the beneficial owner	69	
6.17.3	Ownership	70	
6.17.4	Effective Control	71	
6.17.5	Person on whose behalf a transaction is conducted	72	
6.17.6	Beneficial owner of legal arrangements	72	
6.17.7	Ways in which beneficial ownership information can be hidden/obscured	73	
6.17.8	Identification of Beneficial Owner	73	
6.17.9	Applying a risk-based approach	74	
6.17.10	Record keeping	75	
6.17.11	Who is required to submit data to the Branch in supporting beneficial ownership?	76	
6.17.12	Who are not obliged to submit data of the beneficial owner?	76	
6.17.13	Does a branch of a foreign company have to submit the data of the beneficial owner?	77	
6.17.14	The beneficial owner in the case of a company whose parent company is a company listed on a regulated market	77	
6.17.15	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)	77	
6.17.16	General instruction while identifying beneficial ownership	78	
6.18	Reliance on Third Party	78	
6.19	Management of Legacy Accounts	78	
6.20	Management of Foreign Currency Account	79	
6.20.1	NRB Foreign Currency (FC) Account	79	
6.20.2	Non-Resident Foreign Currency Deposit (NFCD) Account	79	
6.20.3	Resident Foreign Currency Deposit (RFCD) Account	80	
6.20.4	KYC Documentation to opening NRBFC/NFCD/RFCD Accounts	80	
Chapter: 7	RECORD KEEPING	81-83	
7.1	Introduction	81	
7.2	Legal Obligations	81	
7.3	Records to be Kept	81	
7.4	Records to be kept by Branch	82	
7.5	Customers' Information	82	
7.6	Transactions	82	
7.7	Internal and External Reports	83	
7.8	Other Measures	83	
7.9	Formats and Retrieval of Records	83	
Chapter: 8	REPORTING TO BFIU	84-90	
8.1	Legal Obligations	84	
8.2	Definition of Suspicious Transaction	84	
8.3	Reporting Process	84	
8.3.1	Identification of STR/SAR	85	
8.3.2	Evaluation	86	

CHAPTER			Page No.
	8.3.3	Disclosure	86
	8.4	Documenting Reporting Decisions	87
	8.5	Some Special Scenarios for Reporting	87
	8.6	Tipping Off	88
	8.7	Penalty	88
	8.7.1	Penalty of not reporting	88
	8.7.2	Penalty of Tipping Off	88
	8.8	Cash Transaction Report (CTR)	89
	8.9	Self-Assessment Report	89
	8.10	Independent Testing Procedure	89
	8.11	Internal Audit Department's or ICC's Obligations Regarding Self-Assessment or Independent Testing Procedure	90
	8.12	Central Compliance Committee's Obligations Regarding Self-Assessment or Independent Testing Procedure	90
Chapter: 9	TRANSACTIONS MONITORING		91-93
	9.1	Transaction Profile (TP)	91
	9.2	Transaction Monitoring Process	92
	9.2.1	Review of TP violation report	92
	9.2.2	Review of Structuring	92
	9.2.3	Review of Placement and Layering	92
	9.2.4	Reporting of STR to ML & TF Prevention Department	93
	9.3	Maintaining Secrecy	93
Chapter:10	TERRORIST FINANCING & PROLIFERATION FINANCING		94-98
	10.1	Introduction	94
	10.2	Legal Obligations	94
	10.3	Obligations Under Circular	94
	10.4	Necessity of Funds by Terrorist	94
	10.5	Sources of Fund/Raising of Fund	95
	10.6	Movement of Terrorist Fund	95
	10.6.1	Formal Financial Sector	95
	10.6.2	Trade Sector	95
	10.6.3	Cash Couriers	95
	10.6.4	Use of Alternative Remittance Systems (ARS)	96
	10.6.5	Use of Charities and Non-Profit Organizations	96
	10.7	Targeted Financial Sanctions	96
	10.8	Automated Screening Mechanism of UNSCRS	97
	10.9	Role of The Bank in Preventing TF & PF	97
	10.10	Flow-Chart for Implementation of TFs By Banks	98
Chapter:11	TRADE BASED MONEY LAUNDERING		99-102
	11.1	Definition of Trade Based Money Laundering	99
	11.2	Techniques of Trade-based Money Laundering	99
	11.2.1	Trade description fraud	99
	11.2.2	Other types of Trade-based Money Laundering	100
	11.2.2.1	Related party transactions	100
	11.2.2.2	High-risk jurisdictions	100
	11.3	Role of Financial Institutions in the Settlement of Trade Transactions	100

CHAPTER			Page No.
	11.4	Trade-Based Money Laundering “Red Flag” Indicators	100
	11.5	Response of Janata Bank Limited to Combat Trade Based Money Laundering	101
	11.6	Trade Related CDD Requirements at Branch Level	101
Chapter: 12	RECRUITMENT, TRAINING AND AWARENESS		103-104
	12.1	Recruitment	103
	12.2	Employee Screening	103
	12.3	Know Your Employee (KYE)	103
	12.4	Training for Employee	103
	12.5	Awareness of Senior Management	104
	12.6	Customer Awareness	104
	12.7	Awareness of Mass People	104
Conclusion			105
Annexure A: Calculation of Risk			106
Annexure B: Risk Register			107-132
Annexure C: KYC Documentation			133-141
Annexure D: Suspicious Transaction Report (STR) Form			142-144
Annexure E: Common Indicators of Suspicious Transactions			145-149
Annexure F: KYC for Walk-in/One-off Customers			150
Annexure G: BAMLCO Nomination Form			151
Annexure H: Glossary			152-155

LIST OF ABBREVIATIONS

AD	Authorized Dealer
AML	Anti-Money Laundering
AMLDD	Anti-Money Laundering Department
APG	Asia Pacific Group on Money Laundering
ARS	Alternative Remittance System
ATA	Anti-Terrorism Act
BAMLCO	Branch Anti-Money Laundering Compliance Officer
BB	Bangladesh Bank
BDT	Bangladeshi Taka
BFIU	Bangladesh Financial Intelligence Unit
BoD	Board of Directors
CAMLCO	Chief Anti-Money Laundering Compliance Officer
CAP	Customer Acceptance Policy
CBS	Core Banking Solution
CCC	Central Compliance Committee
CDD	Customer Due Diligence
CEO	Chief Executive officer
CFT	Combating the Financing of Terrorism
CSR	Corporate Social Responsibility
DCAMLCO	Deputy Chief Anti Money Laundering Compliance Officer
DD	Demand Draft
DNFBPs	Designated Non-Financial Business and Professions
CTR	Cash Transaction Report
EDD	Enhanced Due Diligence
EU	European Union
FATF	Financial Actions Task Force
FC	Foreign Currency
FI	Financial Institution
FIU	Financial Intelligence Unit
FMJ	Foreign Money and Jewellery
GBP	Great British Pound (British pound sterling)
HR	Human Resource
IP	Influential Person
KYC	Know Your Customer
KYE	Know Your Employee
ME	Mutual Evaluation
MER	Mutual Evaluation Report
ML	Money Laundering
MLPA	Money Laundering Prevention Act
MLPR	Money Laundering Prevention Rules
MoU	Memorandum of understanding
NFCD	Non-Resident Foreign Currency Deposit
NRA	National Risk ML & TF risk assessment
NRB	Non-Resident Bangladesh
PEP	Politically Exposed Persons
PF	Proliferation Financing
RFCD	Resident Foreign Currency Deposit
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
TP	Transaction Profile
UN	United Nations
US	United States
USD	United States Dollar
UNSCR	United Nations Security Council Resolution

AN OVERVIEW OF MONEY LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT GUIDELINES

A. Overview and Objective

Money Laundering is committed by launderers worldwide to conceal the proceeds earned from criminal activities. It happens in almost every country in the world, and a single scheme typically involves transferring money through several countries in order to obscure its origins. And the rise of global financial markets makes money laundering easier than ever, making it possible to anonymously deposit proceeds of crime in one country and then have it transferred to any other country for use.

Money laundering has a major impact on a country's economy as a whole, impeding the social, economic, political, and cultural development of a society. Both money laundering and terrorist financing can weaken individual financial institution, and they are also threatening to a country's overall financial sector reputation. Combating money laundering and terrorist financing is, therefore, a key element in promoting a strong, sound and stable financial sector.

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

Governments of Bangladesh is committed to prevent money laundering and terrorist financing according to international best practice. As a 2nd largest & state-owned commercial bank of Bangladesh Janata Bank Limited (the bank) also committed to implement Govt's commitments. Showing zero tolerance to money laundering and terrorist financing the bank develop this ***Money Laundering and Terrorist Financing Risk Management Guidelines*** in line with the existing Money Laundering Prevention Act, 2012 (amendment-2015), Anti-Terrorism Act, 2009 ((amendment 2013), Anti-Terrorism rules, 2013, Money Laundering Prevention Rules 2019, Money Laundering & Terrorist Financing Risk Management Guideline & circulars issued by Bangladesh Financial Intelligence Unit (BFIU).

Additionally, the bank considers Financial Action Task Force (FATF) Recommendations and the international best practices to prevent the Money Laundering (ML), Terrorist Financing (TF) and Proliferation of weapons of mass destruction (WMD) as well as United Nations Security Council sanctions while designing this Guidelines.

The bank expects all its Executives & Officers, Members and counterparties, including its consultants, contractors, and customers to observe the highest standards of ethics and to provide the bank with any help, information and support in combating ML & TF.

This Guidelines are designed -

- to assist the bank in complying with the Anti Money Laundering and Combating Terrorist Financing regulations of Bangladesh,

- to enable the bank in assessing the adequacy of the internal controls, policies and procedures to combat money laundering and terrorist financing subject to its supervision;
- to develop a risk-based approach to managing compliance in accordance with the guidance of BFIU and uses a combination of risk assessments and risk models to drive its risk-based approach.
- to perform a formal anti- money laundering risk assessment periodically. This risk assessment is performed to identify and assess, in certain key risk categories those situations most vulnerable to money laundering activities.
- to develop, maintain and consistently apply effective controls to prevent at all levels according to its policies and international best practice;
- to measure residual risk associate with the Customer, Product & Services, Business Practice/Delivery Channel or Methods, Country/ Jurisdiction and Regulator considering mitigating controls and to devote the resources for additional risk mitigation where appropriate
- to controls and to devote the resources for additional risk mitigation where appropriate.
- to create awarnesses among the all Executives & Officers of the bank and stakeholders regarding the risk arising out due ML & TF and to pay proper attention to this Guidelines while conducting relevant financial business and be vigilant for practicing suitable procedures while discharging their duties to avoid risks of the bank including financial sanctions from BFIU.
- to establish policies, procedures and systems that facilitate all stakeholders and employees to detection and prevention of ML & TF and other illegitimate/ immoral activities that are harmful for the bank; which may be revised from time to time;
- develop an environment that encourage reporting any suspicious transaction/ suspicious activity that is detrimental to the image of the bank;
- review systems and procedures to prevent ML, TF & PF.

B. Scope

Specifically, the Guidelines is centered on Preventing money laundering and terrorist financing activities by

- detecting accounts and transactions that may relate to money laundering or terrorist activities;
- ongoing transaction monitoring on risk-based approach (RBA) of trade transaction, all foreign remittance including web-based money transfer, SWIFT transfer etc.;

C. Roles and Responsibilities about formation and Implementation of this Guidelines

i) The Board of Directors

- Approve the Guidelines and any revisions there to;
- Delegate to the Risk Management Committee (RMC) authority to monitor and implement the Guidelines and operational procedures for preventing and combating prohibited practices and money laundering/terrorism financing transactions, which are stipulated in the Guidelines.

ii) Risk Management Committee

- Review the Guidelines and submit it to the Board approval;
- Monitor the implementation of the Policies and operational procedures;
- Review and approve the case investigation report of prohibited practice and AML work report;
- Review the implementation of AML upon receipt of report on major issues related to AML, and review the improvement efforts for defects identified in AML work; and
- Review the functioning of the Whistleblower mechanism.

iii) MD & CEO

- Review and discuss the formulation and implementation of the Guidelines with the Compliance Division, put forward corresponding opinions and suggestions for the Risk Management Committee in a timely manner, and supervise the effective implementation of the policies and procedures.
- Review the case investigation report of prohibited practice, discuss with the Internal Audit Division, Legal Division and Compliance Division on potential internal control issues and external legal implication, and evaluate the effect on the risk management of the Bank.

iv) ML & TF Prevention Department

- Maintain and update the Guidelines on bi annual basis for submission to RMC's review;
- Advise on questions raised by Bank staff related to the Guidelines, including its applicability and potential violations;
- Prepare divisional guidelines to lay down procedures of the Guidelines, assist and provide advice on the implementation of divisional guidelines;
- Investigate complaints of prohibited practice as per the process prescribed under the Whistleblower Procedures;
- Conduct reviews to identify potential areas of vulnerability in the Bank's operations; evolve intelligence mechanisms to detect actual/potential violations and develop appropriate response;
- Review the AML work report of the Bank and propose improvement measures;
- Submit AML work report to the RMC according to the internal reporting requirements of the Bank;
- Ensure that suitable KYC procedures are implemented. Review and approve documents required for sensitive accounts and any other accounts that require special approval during client identification;
- Compile and maintain a list of clients/external counterparties which are subject to sanction by the Bank;
- Control to ensure approval of any deviations from the Guidelines;
- Provide training to the staff and senior management from time to time on the laws and regulations of anti-corruption, anti-fraud and Anti Bribery as well as Bank policies and procedures of AML jointly with Janata Bank Staff College;

- Report to the CAMLCO, CEO & MD of the Bank and RMC about major issues identified;
- Ensure that the norms of the bank are communicated to external stakeholders where necessary;
- after getting report from BAMLCOs of the branches analyze and escalate the potential suspicious report to BFIU as per Janata Bank's instruction circular no 965 dated 12/07/2020 circulated in line with BFIU Circular no-26 dated 16/06/2020;
- Other responsibilities as authorized by the CEO & MD of the Bank or his delegate DMD & CAMLCO from time to time when considered necessary.

v) Operation Divisions (All Credit Division, Foreign Trade & Treasury Division ICT Division)

- Ensure proper implementation of this Guidelines in their respective Division, for ensuring the integrity of the assets of the bank;
- Ensure regular control and risk self-assessments, that suitable controls to prevent and ML & TF are in place;
- Monitor effectiveness of the Guidelines by regularly reviewing and assessing key risk indicators and qualitative factors;
- Perform integrity due diligence as per internal procedures;
- Perform ongoing monitoring on the true purpose, end use of disbursed funds and capital source/use of transactions with clients and counterparties;
- Perform ongoing monitoring on trade transactions, inward foreign remittance;
- Perform ongoing monitoring on SWIFT and all Web based transaction;
- Collect KYC and review the AML/CFT Guidelines and compliance of the Correspondent Bank/ RMA/Exchange House annually and report to ML&TFPD;
- Perform ongoing monitoring for cyber fraud and wire fraud by ICTD;
- Co-operate with the ML&TFPD to carry out AML work;
- Escalate Report to the ML&TFPD if identified any suspicious transactions;
- Perform ongoing monitoring through automated monitoring tools of all web-based spot cash transaction done by the branches to Walk-in Customer by Foreign Remittance Department;
- Assist the ML&TFPD, and cooperate with the work of investigation personnel; and
- Other responsibilities as authorized by the CEO & MD of the Bank or his delegate DMD from time to time when considered necessary.

vi) Internal Audit Division

- Record reports of prohibited practice, analyze the evidence and initiate investigation if necessary as per the Whistleblower Procedures;
- Discuss with the ML&TFPD during investigation if needed;
- Report to the RMC on the investigation findings;
- Evaluate the effectiveness of the policies and procedures AML & CFT and put forward improvement measures against internal control deficiencies observed in the case of audit and investigations;

- Inform the Human Resources Division on any sanctions related to the Bank staff pursuant to the investigation, if any, carried out by the Internal Audit Division under the provisions of this Guidelines;
- Keep proper record of all reports and investigation, and maintain confidentiality of such information; and
- Other responsibilities as authorized by the CEO & MD of the Bank or his authorized delegate under this Guidelines from time to time when considered necessary.

vii) Human Resources Division

- Assist the ML & TFPD on arrangement with training;
- Execute the disciplinary actions/sanctions to the Bank Executives/ Officers and staff; and
- Other responsibilities as authorized by the CEO & MD of the Bank or his delegate DMD from time to time when considered necessary.

viii) Other Divisions including the Executives /Officers and Staff of Head Office, Divisional Office, Area Office and branches

- Understand the requirements on policies, procedures and guidelines of the bank to the extent required by their duties;
- Participate in trainings organized by the ML&TFPD of the bank according to their duty requirements; and
- Obtaining and recording customer identification and other customer information as required under the law;
- Report to the head of their division and the ML&TFPD when they become aware of or have doubt about any suspicious activities.
- Report to the head of branches if Executives /Officers and Staff of the branches become aware of or have doubt about any suspicious activities.
- BAMLCO's of the branches after getting report from Executives /Officers and Staff of the branches analyze and escalate the potential suspicious report to ML&TFPD.

D. Implementation

The implementation of this Guidelines will commence immediately after its approval by the Board of Directors.

Chapter: 1

INTRODUCTION

1.1 Defining Money Laundering

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

- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;
- The 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 offense or offenses or from an act of participation in such an offense or offenses, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

The Financial Action Task Force (FATF), the international standard setter for anti-money laundering (AML) and combating financing of terrorism (CFT) efforts, recommends that money laundering should be criminalized in line with the Vienna Convention and Palermo Convention. Like other countries of the world, Bangladesh has criminalized money laundering in line with those conventions. Moreover, Bangladesh also considers some domestic concerns like ‘smuggling of money or property from Bangladesh’ in criminalizing money laundering.

Section 2 (v) of Money Laundering Prevention Act (MLPA), 2012 of Bangladesh defines money laundering as follows:

‘Money laundering’ means –

- i. knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:
 - 1) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime;
 - or
 - 2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
- ii. smuggling money or property earned through legal or illegal means to a foreign country;
- iii. knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or

- iv. concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
- v. converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
- vi. acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
- vii. performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
- viii. Participating in, associating with, conspiring, attempting, abetting, instigating or counseling to commit any offences mentioned above.

Money laundering is a criminal offence under section 4(1) of MLPA, 2012 and penalties for money laundering are-

1. Any person who commits or abets or conspires to commit the offence of money laundering, will be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lacks, whichever is greater.
2. In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved in or related with money laundering or any predicate offence.
3. Any entity which commits an offence under this section will be punished with a fine of not less than twice of the value of the property or taka 20 (twenty) lacks, whichever is greater and in addition to this the registration of the said entity will be liable to be cancelled.

1.2 Stages of Money Laundering

Obviously, there is no single way of laundering money or other property. It can range from the simple method of using it in the form in which it is acquired to highly complex schemes involving a web of international businesses and investments. Traditionally it has been accepted that the money laundering process comprises three stages:

Placement: Placement is the first stage of the money laundering process, in which illegal funds or assets are brought first into the financial system directly or indirectly.

Layering: Layering is the second stage of the money laundering process, in which illegal funds or assets are moved, dispersed and disguised to conceal their origin. Funds can be hidden in the financial system through a web of complicated transactions.

Integration: Integration is the third stage of the money laundering process, in which the illegal funds or assets are successfully cleansed and appeared legitimate in the financial system.

1.3 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.

1.4 Defining Terrorist Financing

Terrorist financing can simply be defined as financial support, in any form, of terrorism or of those who encourage, plan or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF as follows:

1. If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used in full or in part, in order to carry out:
 - a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below¹; or
 - b) Any other act intended to cause death or serious bodily injury to a civilian or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing an act
2. For an act to constitute an offense set forth in the preceding paragraph 1, it will not be necessary that the funds were actually used to carry out an offense referred to said in paragraph 1, subparagraph (a) or (b).

Bangladesh has ratified this convention and criminalized terrorism or terrorist activities under section 6(1) of Anti-Terrorism Act, 2009 in line with the requirement set out in 9 (nine) conventions and protocols that were annexed in the convention.

Section 7(1) of Anti-Terrorism Act (ATA), 2009, defines terrorist financing as follows-

If any person or entity willfully provides, receives, collects or decides 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 will be deemed to have committed the offence of terrorist financing.

Moreover, according to Anti-Terrorism Act (ATA), 2009 conviction for terrorist financing will not depend on any requirement that the fund, service or any other property was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act. The penalties for the offences for money laundering are-

1. In case of a TF offence made by a person, he/she will 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.

2. In case of a TF offence made by an entity, the Government may list the entity in the Schedule or proscribe and listed the entity in the Schedule, by notification in the official Gazette 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. Moreover, the head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, will 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/she 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.

1.5 The Link Between Money Laundering and Terrorist Financing

The techniques used to launder money are essentially the same as those used to conceal the sources of and uses for terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets of organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

1.6 Why We Must Combat ML & TF

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

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

Money laundering distorts assets and commodity prices and leads to misallocation of resources. For the bank 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 the bank and the underlying criminal activities like fraud, counterfeiting, narcotics trafficking, and corruption weaken the reputation and standing of the bank. Actions taken by the bank to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. The bank 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.

If a money launderer uses the bank for making his/her money legitimate, the business of the bank may hamper. If the money launderer withdraws his/her deposited money from the bank before maturity, the bank will face liquidity crisis if the amount is big enough. Moreover, if it is found that bank used for ML & TF activities, and it did not take proper action against that ML & TF as per the laws of the country, the bank will have to face legal risk. Finally, the reputation of the bank 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 the bank, it's 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.

1.7 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: 2

INTERNATIONAL INITIATIVES ON ML AND TF

2.1 Introduction

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

2.2 The United Nations

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

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

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

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

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

2.2.1 The Vienna Convention

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

2.2.2 The Palermo Convention

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

- Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;

- Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;

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

2.2.3 International Convention for The Suppression of The Financing of Terrorism

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

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

2.2.4 Security Council Resolution 1267 And Successors

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

2.2.5 Security Council Resolution 1373

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

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

2.2.6 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 and the importance for all States to implement them fully; it reiterates that none of the obligations in resolution 1540 (2004) will 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).

2.2.7 The Counter-Terrorism Committee

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

2.2.8 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.

2.2.9 Global Program Against Money Laundering

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

2.3 The Financial Action Task Force

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. There are currently 39 members of the FATF; 37 jurisdictions and 2 regional organizations (the Gulf Cooperation Council and the European Commission). These 39 Members are at the core of global efforts to combat money laundering and terrorist financing. There are also 31 international and regional organizations which are Associate Members or Observers of the FATF and participate in its work.

2.3.1 FATF 40+9 Recommendations

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

2.3.2 FATF New Standards

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

Summary of new FATF 40 Standards:

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

2.3.3 Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of 40+9 recommendations is facilitated by a two-stage process: self-assessments and mutual

evaluations. In the self-assessment stage, each member country responds to a standard questionnaire, on an annual basis, regarding its implementation of 40+9 recommendations. In the mutual evaluation stage, each member country 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 (ME) of Bangladesh was conducted by an APG team in August, 2008 and 3rd round Mutual Evaluation (ME) of Bangladesh was conducted by an APG team in September, 2016.

In 2019 a follow-up report (FUR) analyses the progress of Bangladesh in addressing the technical compliance deficiencies identified in its MER. Technical compliance re-ratings are given where sufficient progress has been made. In addition to technical compliance with the five recommendations requested by Bangladesh, this report analyses progress made in implementing new requirements relating to FATF Recommendations which have changed since the MER was adopted: 2, 5, 7, 8, 18 and 21.

2.3.4 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 were consistent with 40+9 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).

2.3.5 International Cooperation and Review Group (ICRG)

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

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

2.4 Asia Pacific Group on Money Laundering (APG)

The Asia Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 41 members and a

number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units. APG is the FATF style regional body (FSRB) for the Asia Pacific region.

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

The APG has five key roles:

- to assess compliance by APG members with the global standards through a robust mutual evaluation program;
- to coordinate bi-lateral and donor-agency technical assistance and training in the Asia/Pacific region in order to improve compliance by APG members with the global standards;
- to participate in, and co-operate with, the international anti-money laundering network primarily with the FATF and with other regional anti-money laundering groups;
- to conduct research and analysis into money laundering and terrorist financing trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities; and
- to contribute to the global policy development of anti-money laundering and counter terrorism financing standards by active Associate Membership status in the FATF.

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

2.5 The Egmont Group of Financial Intelligence Units

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

The mission of the Egmont Group has been expanded in 2004 to include specifically financial intelligence on terrorist financing. To be a member of the Egmont Group, a country's FIU must first meet the Egmont FIU definition, which is-

A central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information:

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

2.6 The Basel Committee on Banking Supervision

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

2.6.1 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.

2.6.2 Basel Core Principles for Banking

In 1997, the Basel Committee issued its Core Principles for Effective Banking Supervision (Core Principles), which provide a comprehensive blueprint for an effective bank supervisory system and covers a wide range of topics. These Core Principles were reviewed in September 2012 and adopted 29 Core Principles. The 29th principle deals with money laundering; it provides that-

'The supervisor determines that banks have adequate policies and processes, including strict customer due diligence rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities.'

2.6.3 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.

Chapter: 3

MAJOR NATIONAL AML & CFT INITIATIVES

3.1 Introduction

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

3.2 Founding Member of APG

Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40 recommendations. Bangladesh has formally endorsed by the APG Membership out-of-session in September 2014 as the Co-Chair for 2018-2020. Bangladesh hosted the 13th APG Typologies Workshop in 2010.

3.3 Legal Framework

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

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

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

3.4 Central and Regional Taskforces

The Government of Bangladesh has formed a central and 7 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 BB 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 (AMLD) was established in Bangladesh Bank in June, 2002 which worked as the FIU of Bangladesh. It was the authority for receiving, analyzing and disseminating Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs).

3.6 Bangladesh Financial Intelligence Unit (BFIU)

As per the provision of MLPA, 2012 Bangladesh Financial Intelligence Unit (BFIU) has been established abolishing 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 money laundering, combating financing of terrorism and proliferation of weapons of mass destruction and it has been bestowed with operational independence. BFIU has also achieved the membership of Egmont Group in July, 2013.

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

3.7 National Coordination Committee and Working Committee

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

3.8 National ML & TF Risk Assessment (NRA)

Bangladesh first conducted National ML & TF Risk Assessment (NRA) in 2011-2012. The methodology used for NRA was developed by 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 considers the output of institutional, sectoral, geographical risk assessment. It covers all the sectors of the economy, legal and institutional framework. The report identifies some high-risk areas for Bangladesh that are corruption, fraud-forgery, drug trafficking, gold smuggling and human trafficking. Banks, non-banks financial institutions, real estate developers and jewelers were identified as most vulnerable sectors for ML & TF. The foreign donation receiving NGO/NPO working in the coastal or border area was identified as vulnerable for TF incidence.

3.9 National Strategy for Preventing ML and TF

National Strategy for Preventing Money Laundering and Combating Financing of Terrorism, 2011-2013 was adopted by the NCC in April 2011. Bangladesh has completed all the action items under the 12(twelve) strategies during that time. A high-level committee headed by the Head of BFIU 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.
- 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.
- 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.
- discouraging illicit fund transfer by increasing pace of stolen assets recovery initiatives and or recovering the evaded tax.
- enhancing the capacity of BFIU in identifying and analyzing emerging ML & TF cases including ML&TF risks arising from the use of new technologies.
- enhancing compliance of all reporting agencies with special focus on new reporting agencies like NGOs/NPOs and DNFBPs.
- expanding investigative capacity and improving the quality of investigation and prosecution of ML & TF cases to deter the criminals.
- establishing identification and tracking out mechanism of TF&PF and fully implementation of targeted financial sanctions related to TF & PF effectively.
- boosting national and international coordination both at policy and operational levels.
- developing a transparent, accountable and inclusive financial system in Bangladesh.

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

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

3.11 Egmont Group Memberships

BFIU has achieved the membership of Egmont group in the Egmont plenary on July, 2013 in Sun City, South Africa. Through Egmont membership, BFIU has achieved access to a wider

global platform and this will help to establish relationship with other FIUs of different countries to get benefit by exchanging views, experiences and information via Egmont Secure Web.

3.12 Anti Militants and De-Radicalization Committee

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

3.13 Memorandum of Understanding (MoU) Between ACC and BFIU

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

3.14 NGO/NPO Sector Review

Bangladesh first assessed the ML & TF 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 Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) requires 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. 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) will conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. Rule 21 also states that RO-FI will utilize this risk assessment report after having vetted by BFIU.

BFIU has issued a guideline titled ‘Money Laundering and Terrorist Financing 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. To make the risk assessment report of respective bank more comprehensive an indicative risk register is enclosed as Annexure-A. Banks are advised to compare their own risk register with the Annexure-A if they find any addition area to cover then amends their risk registers accordingly.

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 77 (till date) MoU so far to exchange the information related to ML&TF with FIU of other countries.

Chapter: 4

AML & CFT COMPLIANCE PROGRAM OF JANATA BANK LIMITED

4.1 Introduction

National ML & TF risk assessment suggests that banking sector is one of the most vulnerable sectors for the ML & TF among the financial sectors due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership. Banks can play a vital role in preventing ML, TF & PF and in this regard their roles and responsibilities are delineated in MLPA, 2012, ATA, 2009 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, the bank develops and maintains its own AML and CFT 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.

4.2 Component of AML & CFT Compliance Program

In developing an AML&CFT compliance program, attention has been given to the size and range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by our bank. The AML & CFT compliance program of the bank includes:

- 1) Senior Management Role and commitment to prevent ML, TF & PF;
- 2) Internal Policies, Procedures and Controls - includes 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);
- 4) Independent audit function- includes the role and responsibilities of internal audit on AML & CFT compliance and external audit functions;
- 5) Awareness building program includes training, workshop, seminar for bank's employees, member of the board of directors, owners and above all for the customers on AML & CFT issues.

4.3 Development of AML & CFT Compliance Program

In developing AML & CFT compliance program, the bank considers relevant laws, regulations, and guidelines relating to AML & CFT and also the practices related to corporate governance. In drafting the compliance program, all relevant departments like general banking, credit, foreign trade, information & communication technology, overseas banking department internal audit and compliance and above all central compliance unit are involved. Proper attention has been given to the size and range of activities, complexity of operations, customer base, use of technology, diversity of product, delivery channel, external linkage, geographic location and the output of ML & TF risk assessment of the bank.

4.4 Communication of Compliance Program

Bank communicates the compliance program after the approval from the board of directors to all employees, member of the board of the directors and other relevant stakeholders at home and abroad. The bank also uploads the compliance program in the website for customers or other stakeholders.

4.5 Senior Management Role

For the purposes of preventing ML, TF & PF, senior management includes members of the board of directors, or the member of the highest management committee in absence of the board of directors and the CEO & Managing Director.

As per instruction from Anti-Terrorism Act (ATA), 2009, The Board of Directors, or in the absence of the Board of Directors, the CEO & Managing Director of the bank will approve and issue directions regarding the duties of its officers, and will ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, which are applicable to the reporting agency, have been complied with or not.

According to BFIU Circular 26 dated 16 June 2020 the bank must have own policy manual that must conform international standards, laws and regulations in force in Bangladesh and instructions of BFIU on preventing money laundering and terrorist financing, and this policy manual must be approved by the Board of Directors or by the highest management committee, where applicable. This policy manual will be communicated to all concerned persons. Banks will conduct review of the policy manual from time to time and will amend/change where necessary.

The CEO & Managing Director of the bank will announce effective and specific commitment, give the necessary instructions to fulfill the commitments in preventing ML & TF to all the employees of all branches, agent offices, regional offices and the head office and will ensure the implementation of the commitments. This statement of commitment will be issued in every year.

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

4.5.1 Role of Senior Management

Board of Directors (BoD) will -

- Approve AML & CFT compliance program and ensure its implementation;
- Issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- Take reasonable measures through analyzing self-assessment report and independent testing report summary;
- Understand ML & TF risk of the bank, take measures to mitigate those risk;
- CEO and MD will issue statement of commitment to prevent ML, TF & PF;
- Ensure compliance of AML & CFT program;

- Allocate enough human and other logistics to effective implementation of AML & CFT compliance program.

As part of its AML&CFT policy bank communicates clearly to all employees on an annual basis by a statement from the CEO & MD 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 and its senior management to comply with all laws and regulations designed to combat money laundering and terrorist financing.

4.5.2 Statement of Commitment of CEO & MD

Statement of commitment of CEO & MD of the bank will include the followings-

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

Senior management must need to ensure the adequacy of the human and other resources devoted to AML & CFT. Moreover, they need to ensure the autonomy of the designated officials related to AML & CFT. Senior management will take the report from the Central Compliance Committee (CCC) into consideration which will assess the operation and effectiveness of the bank's systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner.

Senior management of the bank will adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the bank which includes following issues for proper implementation of AML &CFT measures:

- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- Proper weight will be given 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;
- Other measures that will be taken in case of non-compliance by the bank.

In line with above measures, the bank has been added weight in the Annual Confidential Report (ACR) of its employees and the following clause to “জনতা ব্যাংক লিমিটেড চাকুরি শ্রবিধানমালা ২০২০” (HR policy)-

Quoted from HR Policy	Translation Vetted from Law Department
৫৬। আচরণ সংক্রান্ত অন্যান্য বিধিবিধানের প্রযোজ্যতা:	56. Applicability of other rules/regulations regarding Code of Conduct:

(ক) যদি কোনো কর্মচারী মানিলান্ডিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ পরিপালনের বিষয়ে অবহেলার দায়ে দোষী হন অথবা বাংলাদেশ ব্যাংকের BFIU কর্তৃক কোনো আর্থিক জরিমানা আরোপ করা হয় অথবা সংশ্লিষ্ট কর্মচারীর প্রশাসনিক ক্ষমতা রহিতকরণ বা নিয়ন্ত্রণের শর্ত আরোপ করা হয়, তাহা হইলে বাংলাদেশ ব্যাংকের BFIU কর্তৃক আরোপিত আর্থিক জরিমানা আদায়যোগ্য অথবা প্রশাসনিক ক্ষমতা রহিতকরণ বা অন্যবিধ সিদ্ধান্ত আরোপযোগ্য;

(খ) এ ছাড়াও বাংলাদেশ ব্যাংক কর্তৃক জারিকৃত ইউনিফর্ম কোড অব কন্ডাক্ট- এর বিধিবিধান প্রযোজ্য হইবে এবং আচরণ সংক্রান্ত কোনো বিধান এই প্রবিধানমালায় বর্ণিত না হইলে সরকারি কর্মচারীগণের জন্য প্রযোজ্য বিধিবিধান প্রযোজ্য হইবে;

(গ) প্রবিধি ৩৪ (ড) এবং ৪৪ হইতে ৫৬ পর্যন্ত আচরণবিধির পরিপন্থী কার্যকলাপ অসদাচরণ বলিয়া গণ্য হইবে।

৫৭। দণ্ডের ভিত্তি:

কর্তৃপক্ষের মতে যদি কোনো কর্মচারী-

- (ক) অসদাচরণের দায়ে দোষী হন; অথবা
(খ) অননুমোদিত অনুপস্থিতি বা পলায়নের দায়ে দোষী হন; অথবা
(গ) (১) তিনি বা তাহার উপর নির্ভরশীল অথবা অন্য যেকোনো ব্যক্তি তাহার মাধ্যমে বা তাহার পক্ষে যদি তাহার জ্ঞাত আয়ের উৎসের সহিত অসামঞ্জস্যপূর্ণ কোনো অর্থ-সম্পদ বা অন্য কোনো সম্পত্তির (যাহার যুক্তিসংগত হিসাব দিতে তিনি অক্ষম) অধিকারী হন, অথবা
(২) তিনি প্রকাশ্য আয়ের সহিত সঙ্গতিবিহীন জীবন-যাপন করেন; অথবা

(ঘ) দুর্নীতিপরায়ণ হন অথবা নিম্নবর্ণিত কারণে দুর্নীতিপরায়ণ বলিয়া যুক্তিসংগতভাবে বিবেচিত হন, যথা-

- (১) তিনি বা তাহার উপর নির্ভরশীল অথবা অন্য যেকোনো ব্যক্তি তাহার মাধ্যমে বা তাহার পক্ষে যদি তাহার জ্ঞাত আয়ের উৎসের সহিত অসামঞ্জস্যপূর্ণ কোনো অর্থ-সম্পদ বা অন্য কোনো সম্পত্তির (যাহার যুক্তিসংগত হিসাব দিতে তিনি অক্ষম) অধিকারী হন, অথবা

(ka) If any employee is found guilty of negligence in carrying out prevention of money laundering and combating terrorist financing program or any fine is imposed or the administrative power of the concerned employee is ceased or any restriction in exercise of such power is imposed by the BFIU of Bangladesh Bank, the fine will be recoverable or cessation of administrative power or other decision will be conferrable;

(kha) In addition, the provisions of the Uniform Code of Conduct issued by the Bangladesh Bank shall apply and if any provision relating to conduct is not mentioned in these regulations, the rules applicable to government employees shall apply;

(ga) Any act contrary to Rules 34 (da) and 44 to 56 shall be deemed to be misconduct.

57. Grounds for Penalty:

Where an employee, in the option of the authority-

- (ka) is guilty of misconduct; or
(kha) is guilty of unauthorized absence or desertion; or
(ga) i) is inefficient by reason of infirmity of mind or body of willfully fails to perform his duties vested on him or neglects in performing his duties or is inefficient or has ceased to be efficient and is not likely to recover his efficiency.
ii) Is otherwise inefficient or has ceased to be efficient and is not likely to recover his efficiency; or
(gha) is corrupt or may reasonably be considered corrupt, because-
i) he is or any of his dependents or any other person through him or on his behalf is, in possession (for which he cannot reasonably account) of pecuniary resources or of property disproportionate to his own sources of income; or

<p>(২) তিনি প্রকাশ্য আয়ের সহিত সংগতিবিহীন জীবনযাপন করেন; অথবা</p> <p>(৩) তাহার বিরুদ্ধে দুর্নীতিপরায়ণতার অব্যাহত কুখ্যাতি থাকে; অথবা</p> <p>(ঙ) চুরি, আত্মসাৎ, তহবিল তহরুফ, জাল-জালিয়াতি, বিশ্বাসভঙ্গ বা প্রতারণার দায়ে দোষী হন; অথবা</p> <p>(চ) অনৈতিক কোনো কর্মকাণ্ডে জড়িত হন; অথবা</p> <p>(ছ) সত্য গোপন বা মিথ্যার আশ্রয় গ্রহণের দায়ে দোষী হন; অথবা</p> <p>(জ) অপিত ক্ষমতা বহির্ভূত কার্যক্রম পরিচালনার দায়ে দোষী হন; অথবা</p> <p>(ঝ) নাশকতামূলক কর্মে লিপ্ত হন বা লিপ্ত রহিয়াছেন বলিয়া সন্দেহ করিবার যুক্তিসংগত কারণ থাকে অথবা নাশকতামূলক কাজে লিপ্ত অন্যান্য ব্যক্তির সহিত জড়িত রহিয়াছেন বলিয়া সন্দেহ করিবার যুক্তিসংগত কারণ থাকে, এবং সেই কারণে তাহাকে চাকুরিতে রাখা জাতীয়/ব্যাংকের নিরাপত্তার জন্য হানিকর বলিয়া বিবেচিত হয়;</p> <p>তাহা হইলে নিয়োগকারী কর্তৃপক্ষ এতৎসংক্রান্ত বিধান অনুসরণক্রমে কোনো কর্মচারীর বিরুদ্ধে বিভাগীয় কার্যধারা রুজু ও পরিচালনা করিয়া উক্ত কর্মচারীর উপর এক বা একাধিক দণ্ড আরোপ করিতে পারে, যাহা এই প্রবিধানমালার বিধি দ্বারা নিয়ন্ত্রিত হইবে।</p> <p>৫৮। দণ্ড আরোপের ক্ষেত্র:</p> <p>(ক) অসদাচরণের জন্য যেকোনো দণ্ড;</p> <p>(খ) অননুমোদিত অনুপস্থিতি বা পলায়নের জন্য তিরস্কার ব্যতীত যেকোনো দণ্ড;</p> <p>(গ) উপপ্রবিধি ৫৭ (গ) (১)- এ বর্ণিত অদক্ষতার জন্য তিরস্কার এবং চাকুরি হইতে বরখাস্ত ব্যতীত যেকোনো দণ্ড;</p> <p>(ঘ) উপপ্রবিধি ৫৭ (গ) (২)- এ বর্ণিত অদক্ষতার জন্য বরখাস্ত ব্যতীত যেকোনো দণ্ড;</p> <p>(ঙ) দুর্নীতির জন্য যেকোনো গুরুদণ্ড, তবে উক্ত অপরাধের পুনরাবৃত্তির ক্ষেত্রে নিম্নপদ বা নিম্ন বেতন গ্রেডে অবনমিতকরণ ব্যতীত যেকোনো গুরুদণ্ড;</p> <p>(চ) উপপ্রবিধি ৫৭ (ঙ)- এ বর্ণিত অপরাধের জন্য তিরস্কার ব্যতীত যেকোনো দণ্ড;</p>	<p>ii) he has assumed a style of living beyond his ostensible means; or</p> <p>iii) he has a persistent reputation of being corrupt; or</p> <p>(uma) is guilty of theft, embezzlement, defalcation, forgery, breach of trust or fraud; or</p> <p>(cha) engages himself in any immoral activity; or</p> <p>(chha) is guilty of concealing the truth or falsehood; or</p> <p>(ja) is guilty of conducting activities beyond the powers vested to him; or</p> <p>(jha) is engaged or is reasonably suspected of being engaged, in subversive activities or is reasonably suspected of being associated with others engaged in subversive activities and on that ground his retention in service is considered prejudicial to national/bank security;</p> <p>The appointing authority may, subject to comply with the procedures prescribed in these Rules (Regulation), initiate and conduct departmental proceedings against him and may impose on him one or more penalties.</p> <p>58. Scope for Imposition of Penalty:</p> <p>(ka) for misconduct any penalty;</p> <p>(kha) for unauthorized absence or desertion any penalty except censure;</p> <p>(ga) for inefficiency in sub-rule 57 (ga) (i) any penalty except censure and dismissal from service;</p> <p>(gha) for inefficiency in sub-rule 57 (ga) (ii) any penalty except dismissal from service;</p> <p>(uma) for corruption any penalty, but for repetition of the offence, any major penalty except reduction to lower post or lower grade of pay scale;</p>
--	--

<p>(ছ) উপপ্রবিধি ৫৭ (চ)- এ বর্ণিত অপরাধের জন্য যেকোনো দণ্ড;</p> <p>(জ) উপপ্রবিধি ৫৭ (ছ)- এ বর্ণিত অপরাধের জন্য তিরস্কার ব্যতীত যেকোনো দণ্ড;</p> <p>(ঝ) উপপ্রবিধি ৫৭ (জ)- এ বর্ণিত অপরাধের জন্য তিরস্কার ব্যতীত যেকোনো দণ্ড;</p> <p>(ঞ) উপপ্রবিধি ৫৭ (ঝ)- এ বর্ণিত অপরাধের জন্য উপপ্রবিধি ৫৯ (ক)(২)- এর (অ)(আ)(ই) ব্যতীত যেকোনো গুরুদণ্ড;"</p>	<p>(cha) for an offense as make down in sub-rule 57 (uma) any penalty except censure;</p> <p>(chha) for an offense as make down in sub-rule 57 (cha) any penalty;</p> <p>(ja) for an offense as make down in sub-rule 57 (chha) any penalty except censure;</p> <p>(jha) for an offense as make down in sub-rule 57 (ja) any penalty except censure;</p> <p>(neo) for an offense as make down in sub-rule 57 (jha) any major penalty except the penalties mentioned in clauses (a), (aa), (e) of sub rule 59(ka)(2);</p>
---	--

The revised HR policy has been duly approved by the Board of Directors in its 618th meeting held on 18 June 2020.

Senior management must 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; this implies that decisions on entering or maintaining high-risk business relationships must be escalated to senior management.

4.6 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.

4.6.1 Written AML & CFT Compliance Policy

The AML & CFT compliance policy must be written and be approved by the board of directors which will ensure and monitor compliance with the Acts, including record keeping and reporting requirements.

The written AML&CFT compliance policy has established clear responsibilities and accountabilities within the organization 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 compliance with the obligations under the law.

The AML&CFT compliance policy includes standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. It is addressed in the policy:

- Know Your Customer (“KYC”) before opening new accounts;
- Monitoring existing accounts for unusual or suspicious activities;
- Reporting suspicious transactions,
- Hiring and training employees
- A separate audit or internal control function to regularly test the program’s effectiveness.
- Description of the roles the AML&CFT Compliance Officers(s)/Committee and other appropriate personnel
- Screening programs to ensure high standards when hiring employees

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

4.7 Customer Acceptance Policy

The bank has developed a clear Customer Acceptance Policy ensures that explicit guidelines are in place to set-up any kind of business relationship with the bank which have been incorporated to design the policy towards comprehensive coverage and implementation of customer acceptance in the Bank. We have developed that policy for our Bank in line with the recommendations of Money Laundering & Terrorist Financing Risk Management Guidelines of Bangladesh Financial Intelligence Unit (BFIU). The Policy has been duly approved by the Board of Directors in its 534th meeting held on 8 August 2018.

A concrete Customer Acceptance Policy is very important so that inadequate understanding of a customer’s background and purpose for utilizing a bank account or any other banking product/service may not expose the Bank to risks. Accordance with this view we have been developed that policy in Bengali language for its easy implementation which has been duly approved by the Board of Directors in its 554th meeting held on 14 January 2019. The primary objectives of that Customer Acceptance Policy are –

1. to manage any risk that the services provided by the Bank may be exposed to;
2. to prevent the Bank from being used, intentionally or unintentionally, for ML/TF purposes; and
3. to identify customers who are likely to pose a higher than average risk.

The bank accepts only those customers whose appropriate identity is established by conducting due diligence to the risk profile of the client. Parameters of risk perception must be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to enable categorization of customers into different risk grade.

The bank does not open an account where it is unable to apply appropriate customer due diligence measures i.e. if the bank is unable to verify the identity and/or obtain documents required as per with the risk categorization due to non-cooperation of the customer and does not allow withdrawal of money. Decision is taken to close an account by the bank after giving due notice to the customer explaining the reasons for such decision.

Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of banking as

there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

Necessary checks should be made before opening a new account so that the bank can ensure the identity of the customer does not match with any person with known criminal background or with proscribed entities such as individual terrorists or terrorist organizations etc.

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

- 1) No account in anonymous or fictitious name or account only with numbers will be opened;
- 2) No account in the name of any person or entity listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance adopted under Chapter VII of the Charter of UN on suspicion of involvement in terrorism or terrorist financing activities and proscribed or enlisted by Bangladesh Government will be opened or operated;
- 3) No banking relationship will be established with a Shell Bank or a Shell Company;
- 4) In addition, instructions given by BFIU from time to time regarding customer acceptance will be followed.

Chapter: 5

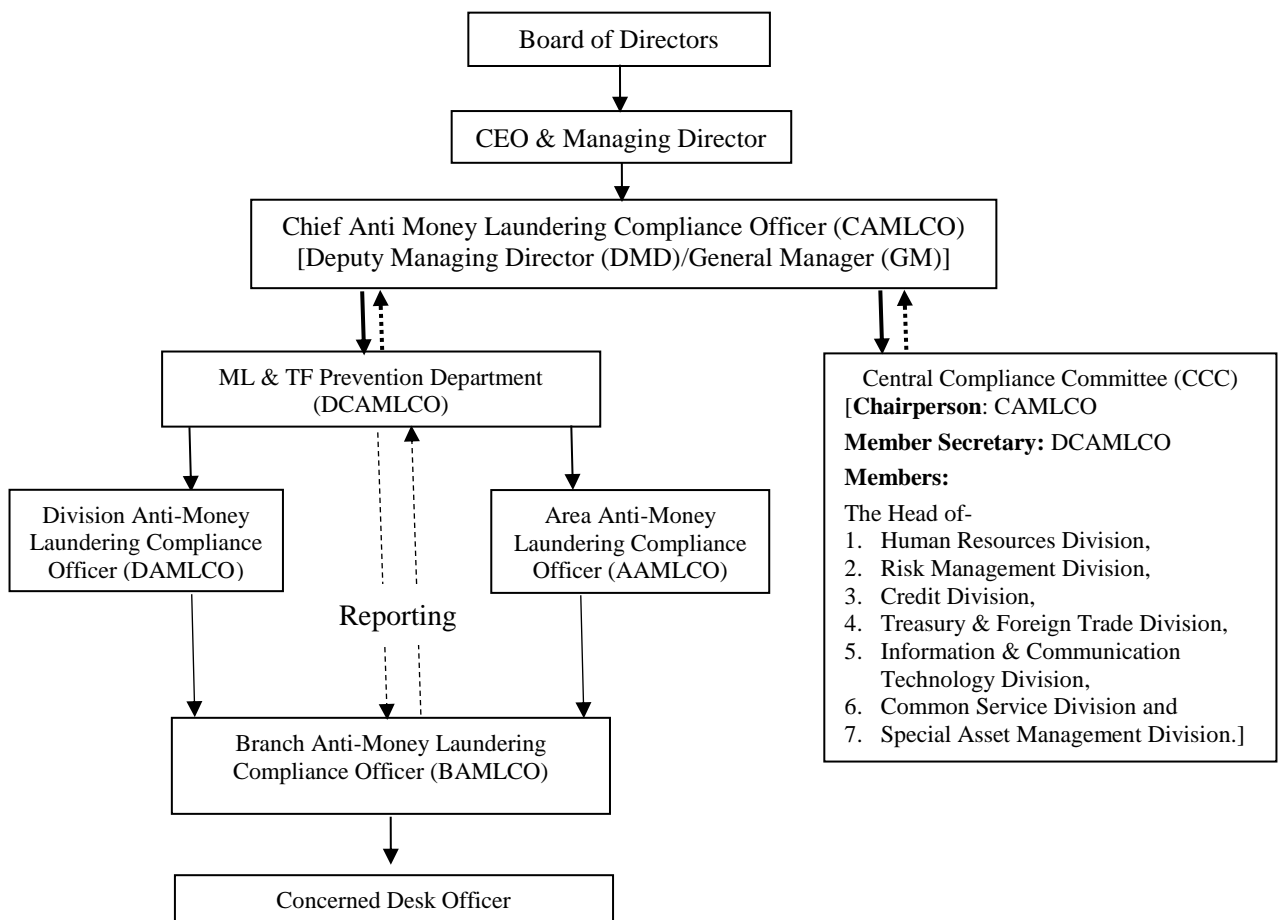
COMPLIANCE STRUCTURE OF THE BANK

5.1 Anti-Money Laundering Organogram of Janata Bank Limited

Compliance structure of the bank is an organizational setup that deals with AML & CFT 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).

Anti-Money Laundering Organogram of the bank is given below:



5.2 Central Compliance Committee

According to BFIU Circular-26 dated 16 June 2020, the bank will set up a Central Compliance Committee (CCC) that will be directly monitored by the CEO & MD of the bank.

The central compliance Committee is 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 up to 2 (two) steps below of the CEO & MD. If the CAMLCO is changed, it should be informed to BFIU without delay. Before assigning the CAMLCO to other duties of the bank, the management has to ensure that the AML & CFT activities of the bank will not be hampered.

5.2.1 Formation of CCC

The Bank constitutes a Central Compliance Committee (CCC) headed by the Chief Anti Money Laundering Compliance Officer (CAMLCO) to develop, administer and maintain monitoring and compliances regarding Money Laundering and Terrorist Financing prevention.

Members of the Central Compliance Committee:

1. Deputy Managing Director/General Manager (CAMLCO)- President
2. Head of Risk Management Division- Member
3. Head of Credit Division- Member
4. Head of Information Technology Division- Member
5. Head of Human Resources Division - Member
6. Head of Treasury & Foreign Trade Division- Member
7. Head of Common Services Division- Member
8. Head of ML & TF Prevention Department (DCAMLCO)- Member Secretary

5.2.2 Authorities and Responsibilities of the CCC

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

- develop banks policy, procedure and strategies in preventing ML, TF & PF;
- coordinate banks AML & CFT compliance initiatives;
- coordinate the ML & TF risk assessment of the bank and review thereon;
- present the compliance status with recommendations before the CEO & MD on half yearly basis;
- forward STR/SAR and CTR to BFIU in time and in proper manner;
- report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner;
- impart training, workshop, seminar related to AML & CFT for the employees of the bank;
- take required measures to submit information, report or documents in time.

For shouldering these responsibilities bank authority has considered the following authority to CCC-

- appointment of BAMLCO and assign their specific job responsibilities;
- requisition of human resources and logistic supports for ML and TF prevention Department;
- make suggestion or administrative sanction for non-compliance by the employees.
- send any account information to BFIU as per request

5.2.3 Separation of CCC From Internal Control & Compliance

For ensuring the independent audit function in the bank CCC will be completely separated from internal audit or compliance and control (ICC). In this regard ICC also examines the performance of CCC and the bank's AML & CFT compliance program. To ensure this autonomy there will not be any member from ICC to CCC and vis-a-vis; but there should be enough co-ordination and co-operation in performing their responsibilities and information exchange. There will not be any impediment to transfer employee from ICC to CCC and vis-à-vis but no one will be posted in these 2 (two) departments/units at the same time.

5.3 Chief Anti Money Laundering Compliance Officer (CAMLCO)

The bank will designate a Chief Anti Money Laundering Compliance Officer (CAMLCO) at its head office who has sufficient authority to implement and enforce corporate wide AML&CFT policies, procedures and measures and who reports directly to CEO & MD. 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 has 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 position within the organization of the person appointed as CAMLCO is sufficiently senior to command the necessary authority and is not below the 2 steps below the CEO & MD.

CAMLCO, directly or through the CCC is the pivotal point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML&CFT program. CAMLCO may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions.

All staffs engaged in the bank at all levels must be made aware of the identity of the CAMLCO, his deputy and the staff and branch/unit level AML&CFT 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 will be passed to the CAMLCO.

As the CAMLCO is responsible for the oversight of all aspects of the bank's AML&CFT activities and is the focal point for all activity within the bank relating to ML & TF his/her job description will 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 money laundering/terrorist financing is put into practice.

5.3.1 Authorities and Responsibilities of CAMLCO

Authorities-

- CAMLCO should be able to act on his own authority;
- He/she should not take any permission or consultation from/with the CEO & MD before submission of STR/SAR and any document or information to BFIU;
- He/she will maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU
- He/she must have access to any information of the bank;
- He/she will ensure his/her continuing competence.

Responsibilities-

- CAMLCO must ensure overall AML&CFT compliance of the bank;
- Oversee the submission of STR/SAR or any document or information to BFIU in time;
- Maintain the day-to-day operation of the bank's AML&CFT compliance;
- CAMLCO will be liable to CEO & MD or BoD for proper functioning of CCC;
- CAMLCO will review and update ML & TF risk assessment of the bank;
- Ensure that corrective actions have taken by the bank to address the deficiency identified by the BFIU.

5.4 Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)

The bank will 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 at least in the rank of ‘Deputy General Manager’ of the bank. The CAMLCO and DCAMLCO have to have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML & TF. The DCAMLCO is responsible for the oversight of all aspects of the bank’s AML/CFT activities and is the focal point for all activity within the bank relating to ML & TF after CAMLCO. He/she should have vast knowledge & experience on general banking, investment/credit and foreign exchange business of the bank.

5.4.1 The Authorities & Responsibilities of DCAMLCO

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

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

5.5 ML & TF Prevention Department

To Implement the decision of CCC and to monitoring the overall activities of AML and CFT, the Bank has constituted a separate department named Money Laundering and Terrorist

Financing Prevention Department (AMLD) at its Head Office. The department work under supervision of CCC. ML & TF prevention department will implement and enforce corporate-wide anti-money laundering policies, procedures and measures of the Bank and will report directly to Chief Anti-Money Laundering Compliance Officer (CAMLCO).

5.5.1 Functions of ML & TF Prevention Department:

- Formulate, monitor, review and enforce the Bank's Anti-Money Laundering/CFT Policy.
- Formulate, monitor, review and enforce the Bank's Know Your Customer (KYC) policy and identification procedure for detection of suspicious transaction/account activities.
- Issue anti-money laundering circulars, instructions and circulate BFIU circulars and policy guidelines to the branches and concerned officers of the Bank.
- Ensure timely anti-money laundering reporting and compliance to BFIU, including CTR, STR, KYC Update, Taskforce Data & other data required by BFIU
- Monitor the Bank's Self-Assessment and Independent Testing Procedures for AML compliance and any corrective action.
- Conduct inspection on branches and concerned controlling offices regarding anti-money laundering compliance.
- Respond queries of and issue necessary instructions to the branches so as to money laundering apprehensions.
- Develop and conduct training courses and will collaborate Janata Bank Staff College (JBSC) for AML, CTF & TBML related courses to raise the level of awareness of compliance in the Bank.
- Place Memorandum before the Board of Directors at least once a year regarding the status of the anti-money laundering activities undertaken by the Bank.
- Extend all out cooperation to BFIU, Bangladesh Bank Inspection Team, Internal Audit Team and External Audit Team and other law enforcement Agencies as and when required.
- 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. The CCC could also make a Suspicious Transaction Report (STR) or Suspicious Activity report (SAR) directly to BFIU in this regard.

5.6 Division Level Organization Structure

To strengthening our emphasis towards prevention of Money Laundering campaign every divisional office will form a Division Anti Money Laundering Compliance Committee (DAMLCC) headed by DGM/AGM. The head of DAMLCC will be designated as Division Anti Money Laundering Compliance Officer (DAMLCO). The committee will act under direct supervision of Divisional Head (General Manager).

5.6.1 Responsibilities of DAMLCO:

- Monitoring the overall activities of AML and CFT for Corporate-1 and Corporate-2 Branches.

- He/She will monitor and supervise the activities of Area Anti Money Laundering Compliance Committee.
- Division Anti-Money Laundering Compliance Officer (DAMLCO) will have sufficient authority to implement and enforce anti-money laundering policies, procedures and measures and can report directly to ML & TF Prevention Department at Head Office regarding all the anti-money laundering matters.
- DAMLCO will have overall supervision ensuring that the AML program is effective within all of the branches.
- Provide on the job AML training to Branch employees.
- Ensure timely anti-money laundering reporting and compliance to ML & TF Prevention Department at Head Office, including CTR, STR, KYC Update, Account Information & Other Data required by Head Office.
- To develop the compliance knowledge of all staff, especially the compliance personnel of Divisional Office, Area Offices and Branches, will arrange coordination meeting at own office and send recommendation for training for employees who haven't got training in this regard;
- To monitor the activities through self-testing for AML/CFT compliance and take any required corrective action;
- Conduct inspection on branches and concerned area offices regarding anti-money laundering compliance.
- Will inform update AML policy, circulars, laws and regulations to all employees of controlling offices and branches.
- Perform AML Risk Assessment for the branch.
- Perform periodic Quality Assurance on the AML program in the branch.
- Perform Self-Assessment on AML performance of the branch and ensure compliance and any corrective action.
- Ensure that the required reports and systems are in place to maintain an effective AML program.
- Preserve all circulars & instructions issued from BFIU and Head Office, circulate the copies among all the officers for necessary information acquaintances.
- Getting AML tasks done by Branch Officers;

5.7 Area Level Organization Structure

To ensure the successful compliance of bank's AML/CFT program every Area Office will form an Area Anti Money Laundering Compliance Committee (AAMLCC) headed by AGM. The head of AAMLCC will be designated as Area Anti Money Laundering Compliance Officer (AAMLCO). The committee will act under direct supervision of Area head and will be monitored by DAMLCC.

5.7.1 Responsibilities of AAMLCO:

The authorities & responsibilities of AAMLCO will be same as the authorities & responsibilities of DAMLCO but it will be work for grade-1 to grade-4 branches. The important responsibilities of AAMLCO are to:

- Monitoring the overall activities of AML and CFT for grade-1 to grade-4 Branches.

- The BAMLCC will review Anti-Money Laundering activities of the branches under their supervision at the end of each quarter and preserve minutes of the meeting.
- AAMLCO will have sufficient authority to implement and enforce anti-money laundering policies, procedures and measures and can report directly to ML & TF Prevention Department at Head Office regarding all the anti-money laundering matters.
- AAMLCO will have overall supervision ensuring that the AML program is effective within all of the branches.
- Provide on the job AML training to Branch employees.
- Ensure timely reporting and compliance to ML & TF Prevention Department at Head Office, including CTR, STR, KYC Update, Account Information & Other Data required by Head Office.
- To develop the compliance knowledge of all staff, especially the compliance personnel of Area Offices and Branches, will attend coordination meeting arranged by DAMLCO at Divisional office and send recommendation for training for employees who haven't got training in this regard;
- To monitor the activities through self-testing for AML/CFT compliance and take any required corrective action;
- Conduct inspection on branches regarding anti-money laundering compliance.
- Perform AML Risk Assessment for the branch.
- Perform Self-Assessment on AML performance of the branch and ensure compliance and any corrective action.
- Ensure that the required reports and systems are in place to maintain an effective AML program.
- Preserve all circulars & instructions issued from BFIU and Head Office, circulate the copies among all the officers for necessary information acquaintances.

5.8 Branch Level Organization Structure

Branches need to be organized adequately in accordance with the Bangladesh Financial Intelligence Unit Guidance Notes on Prevention of Money Laundering within the framework of Managing Core Risk in Banking and internal circulars to strengthen our emphasis towards prevention of Money Laundering campaign.

5.8.1 Formation of Branch Anti-Money Laundering Compliance Committee (BAMLCC)

Every branch will establish a BAMLCC consisting of the following members:

- a) Branch Manager
- b) BAMLCO;
- c) In charge, GBD/Deposit;
- d) In charge, Foreign Exchange (For AD Branches);
- e) In charge, Credit/Advance;
- f) Officer, A/C Opening;

5.8.2 Responsibilities of BAMLCC

BAMLCC will review Anti-Money Laundering activities of the branch at the end of each quarter and preserve minutes of the meeting. The main responsibilities of BAMLCC are as follows:

- Ensure implementation of all instructions of this Guideline;
- Be familiar with laws, regulations, policies, guidelines related to AML/CFT;
- Inform all other officers & executives about laws, regulations, policies, guidelines related to AML/CFT;
- Verify the compliance to open a new account i.e. KYC, TP, risk grading and proper documentation;
- Ensure all account's TP & KYC profile are updated;
- Monitor High risk account;
- Monitor the foreign remittance transaction;
- Review cash transaction to find out structuring;
- Ensure regular transaction monitoring to find out suspicious transactions;
- Ensure improvement of branch rating and confirm branch rating never go below than "fair".
- Perform any other responsibilities as instructed by BFIU and Head Office from time to time.

5.8.3 Branch Anti Money Laundering Compliance Officer (BAMLCO)

According to BFIU Circular-26, dated 16 June, 2020- The manager, the second officer of the branch or a high official experienced in general banking/foreign exchange/Credit will be nominated as the BAMLCO. The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and bank's own policies on preventing Money Laundering and Terrorist Financing & proliferation financing. Clear job descriptions and responsibilities of BAMLCO will be mentioned in his/her appointment letter.

5.8.4 Nomination of BAMLCO

In the Bank, 1 (one) of the following persons may be nominated as BAMLCO depending on the type of branches:

- a) AGM, GBD (For Local Office & Janata Bhaban Corporate Branch);
- b) AGM/In charge, GBD (For Corporate-1 Branches);
- c) Assistant Branch Manager (2nd Officer) (For Corporate-2 Branches);
- d) Branch Manager (For Grade-1, 2, 3 & 4 Branches);

Each branch will nominate an officer as BAMLCO considering the above criteria by a letter to ML & TF Prevention Department for onward submission to CAMLCO. CAMLCO will issue office order describing the duties and responsibilities of BAMLCO for all branches.

5.8.5 Authorities and Responsibilities of BAMLCO

Branch Anti-Money Laundering Compliance Officer (BAMLCO) will have sufficient authority to implement and enforce anti-money laundering policies, procedures and measures and can report directly to ML & TF Prevention Department at Head Office regarding all the anti-money laundering matters. Branch Manager will have overall supervision ensuring that the AML program is effective within the branch.

BAMLCO will arrange AML & CFT meeting with BAMLCC and other concerned important officials of the branch quarterly and will take effective measures on the following matters after reviewing the compliance of the existing acts, rules and regulations, BFIU's instructions on preventing Money Laundering & Terrorist Financing:

- Know Your Customer,
- Transaction monitoring,
- Identifying and reporting of Suspicious Transactions,
- Record keeping,
- Training.

For preventing ML, TF & PF in the branch, the BAMLCO will perform the following responsibilities:

- ensure that the KYC of all customers have done properly and for the new customer KYC is being done properly;
- ensure that the UN Security Council and domestic sanction list checked properly before opening of account and while making any international transaction;
- keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts will not be allowed without compliance of BFIU's instruction;
- ensure regular transaction monitoring to find out any unusual transaction (In case of an automated bank, the bank will follow a triggering system against transaction profile or other suitable threshold. In case of a traditional bank, transaction will be examined at the end of day against transaction profile or another suitable threshold. Records of all transaction monitoring will be kept in the file);
- review cash transaction to find out any structuring;
- review of CTR to find out STR/SAR;
- ensure the checking of UN sanction list before making any foreign transaction;
- ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
- compile self-assessment of the branch regularly and arrange quarterly meeting regularly;
- accumulate the training records of branch officials and take initiatives including reporting to CCC, HR and JB Staff College;
- ensure all the required information and document are submitted properly to ML & TF Prevention Department and any freeze order or stop payment order are implemented properly;
- 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 will make an STR/SAR;
- ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements
- ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU.

5.9 Internal Control and Compliance

In line with the instructions under BFIU Circular-26 dated 16 June 2020, Internal Audit or Internal Control and Compliance (ICC) of the bank have an important role for ensuring proper implementation of bank's AML & CFT Compliance Program. Bank management needs to ensure that ICC is equipped with enough manpower and autonomy to look after the prevention of ML & TF. The ICC has to oversee the implementation of the AML & CFT 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. Auditors of the bank will be well resourced and enjoy a degree of independence within the organization.

The internal audit must-

- understand ML & TF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML & CFT Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML & CFT Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
 - the importance of the board and the senior management place on ongoing education, training and compliance,
 - employee accountability for ensuring AML & CFT compliance,
 - comprehensiveness of training, in view of specific risks of individual business lines,
 - training of personnel from all applicable areas of the bank,
 - frequency of training,
 - coverage of bank policies, procedures, processes and new rules and regulations,
 - coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
 - Penalties for noncompliance and regulatory requirements.

5.10 External Auditor

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

Chapter: 6

CUSTOMER DUE DILIGENCE

6.1 Introduction

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 MLPA, 2012 including 'Predicate Offences' and the relevant offences under ATA, 2009.

Risk sensitive CDD measures are based on-

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

The adoption of effective KYC standards is an essential part of bank's risk management policies. Inadequate KYC program may create significant legal and reputational risk to the bank. Sound KYC Policies and Procedures not only contribute to the bank's overall safety and soundness, they also protect the integrity of the banking system by reducing money laundering, terrorist financing and other unlawful activities.

The banks therefore need to carry out customer due diligence for two broad reasons:

- to help the organization to be reasonably satisfied about those customers who are suspected to act 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 whether customer's transactions and activity are consistent with his business.

6.2 General Rules of CDD

6.2.1 Completeness and Accuracy

The bank required to be certain about the customer's identity and underlying purpose of establishing relationship with the bank, 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 under MLPA, 2012 for the bank to maintain complete and accurate information of their customers 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/acceptable ID card with photo, phone/ mobile number etc. 'Accurate' refers to such complete information that whose authenticity has been verified.

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

The verification procedures to confirm the identity of a prospective customer should basically be the same whatever type of account or service is required. It will be best to obtain the identification documents from the prospective customer which is the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity, so verification will generally be a cumulative process. The overriding principle is that every bank must know who their customers are, and have the necessary documentary evidences to verify this. Annexure-C provides an example of collection of documents that bank find it useful for their purpose.

The bank should not open the account, commence business relations or perform the transaction; or should terminate the business relationship if it 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; and
- unable to obtain information on the purpose and intended nature of the business relationship;

In this case the bank will consider the customer as suspicious and make a suspicious transactions report in relation to the customer.

6.2.2 Ongoing CDD measures (Review and update)

The bank will take necessary measures to review and update the KYC of the customer after a certain interval. This procedure will have to be conducted in every five years in case of low risk customers. Furthermore, this procedure will have to be conducted in every year in case of high-risk customers. Moreover, the bank will update KYC information anytime if there is any particular necessity realized. Depending on the updated information, the risks associated with these accounts will have to be assessed again without any delay.

Any subsequent change to the customer's name, address, or employment details of which the bank becomes aware should be recorded as part of the CDD process. Generally, this will be undertaken as part of good business practice and due diligence but also serves for prevention of money laundering and terrorist financing.

The bank will prepare 'Transaction Profile' of customer account in the specified form. After reviewing the nature of the customer, the source of money in the account and the nature of transaction, the bank will revise the 'Transaction Profile' by reviewing the transactions of the customer within 6 (six) months of establishing business relation and assessing the effectiveness with a logical consideration.

6.2.3 Enhanced CDD measures

The bank will conduct Enhanced CDD measures, when necessary, in addition to normal CDD measures. Bank should conduct Enhanced Due Diligence (EDD) under the following circumstances:

- Individuals or legal entities scored with high risk;
- Individuals who are identified as politically exposed persons (peps), IPs 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).

Enhanced CDD measures include:

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

6.3 Timing of CDD

The bank 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

6.4 Transaction Monitoring

The bank 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 will have to be more emphasized during monitoring. An effective system has to be developed by the bank 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.

The bank 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 bank;
- Cash transactions under CTR threshold to find out structuring;
- Transactions related with international trade;
- Transaction screening with local and UN Sanction list.

6.5 Exception When Opening a Bank Account

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).

6.6 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, the bank 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.

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

If the bank 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 bank must then retain the funds until consent has been given to return the funds to the source from which they came.

6.7 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 the bank 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 the 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.

6.8 Verification of Source of Funds

The bank will 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:

- a) present employment identity,
- b) salary certificate/copy/advice,
- c) pension book,
- d) financial statement,
- e) income tax return,
- f) business document or
- g) any other document that could satisfy the bank.

The bank will request the person to produce E-TIN (Electronic Tax Identification No) certificate which declares taxable income.

6.9 Verification of Address

The bank will 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 bank or by standard mail or courier service correspondence. The bank will collect any other document (recent utility bill mentioning the name and address of the customer) as per its 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 bank, or by a combination of both. Where business is conducted face-to-face, bank will see originals of any documents involved in the verification.

6.10 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 will not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common-sense approach and some flexibility 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 manager 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 will 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.

6.11 Walk-In/ One Off Customers

The bank should collect complete and correct information while serving Walk-in customer, i.e. a customer without having account. The bank will know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT. A detail provisions are discussed in the paragraph 6.17 of this Guidelines.

The bank will collect complete and correct information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit the bank will identify sources of funds as well.

6.12 Non-Face to Face Customers

The bank will assess money laundering and terrorist financing risks while providing service to non-face to face customers and will develop the policy and techniques to mitigate the risks, as well as will review that time to time. 'Non-face to face customer' refers to "the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the bank".

6.13 Customer Unique Identification Code

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

6.14 Correspondent Banking (As Per BFIU Circular 26 Dated 16 June 2020)

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

Bank will 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-19 dated 17 September, 2017. The bank will also obtain approval from CAMLCO 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.

Banks must 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 will have to be obtained.

If any respondent bank allows direct transactions by their customers to transact business on their behalf (i.e. payable through account), the corresponding bank must be sure about the appropriate CDD of the customer has done by the respondent bank. Moreover, it has to be ensured that collecting the information on CDD of the respective customer is possible by the respondent bank on request of the correspondent bank. Here, ‘Payable through accounts’ refers to “Corresponding accounts that are used directly by third parties to transact business on their behalf.”

6.15 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 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. According to FATF these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatizing PEPs as such being involved in criminal activity. The FATF has categorized PEPs into 3 (three) criteria which include:

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

It is important to note that only foreign PEPs automatically should be treated as high risk and therefore we 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.

6.15.1 Definition of PEPs

A politically exposed person (PEP) is defined by the FATF as an individual who is or has been entrusted with 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 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;
- 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
- Ambassadors, Charges d'affairs and high-ranking officers in the armed forces;
- Head or the senior executives or members of the administrative, management or supervisory bodies or State-owned enterprises;
- Chief, directors, deputy directors and members of the board or equivalent function of an international organizations

6.15.2 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 intended to cover middle ranking and more junior individuals as mentioned in 6.15.1 and 6.15.2.

6.15.3 Family Members of PEPs

Family members of a PEP will include:

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

However, this is not an exhaustive list. We 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 PEP to pose a higher risk as per assessment of the bank. This would not apply in relation to lower risk PEPs. In low-risk situations, we 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.

6.15.4 Close Associates of PEPs

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.

6.15.5 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 bank'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. The bank will apply measures for a longer period to address risks of money laundering or terrorist financing in relation to that person, but this will only be necessary in the cases of PEPs/IPs where it has assessed that PEP/IP is posing a higher risk.

6.15.6 Risk Related with PEPs

a) All PEPs do not pose the same risk

The risk of corruption will differ between PEPs. The bank will 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 it has considered in its risk assessment.

This guidance discusses on how we may differentiate between PEPs. In this guidance, the terms 'lower risk' and 'higher risk' are used to recognize that we should 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.

b) 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 an area where ML/TF risks is lower
- If he/she does not have executive decision-making responsibilities (e.g. an opposition Member of the Parliament)

c) Indicators that a PEP might pose a higher risk

The following indicators suggest a PEP poses a higher risk:

i. Higher risk indicator – product

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

ii. 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, we should have regard to whether, based on information available, the country has the following characteristics:

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

iii. Higher risk indicators – personal and professional

The following characteristics might suggest a PEP poses higher risk:

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

- responsible for, or able to influence, allocation of scarce government licenses such as mineral extraction concessions or permission for significant construction projects.

d) 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.

e) 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

6.15.7 Obligations Under the Regulations

In line with FATF Guidance, BFIU stated some requirements regarding Due Diligence with PEPs. According to that regulation our obligations are as follows:

- a) The bank has to keep 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 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.). In these situations, we have to understand as part of due diligence why a PEP, family member or close associate is using such an arrangement and use that as part of their assessment of risk.
- b) In determining whether these systems and procedures are appropriate, we should refer to:
 - our own risk assessment of the money laundering/terrorist financing risks;
 - An assessment of the extent to which the risk would be increased by a business relationship with a PEP, family member or close associate. According to expectation of BFIU, this is a case-by-case assessment and not an automatic assessment that a relationship creates a high risk of money laundering; and
 - We should follow any information further provide by the BFIU.
- c) If identified that a customer (or beneficial owner of a customer) does meet the definition of a PEP (or a family member or known close associate of a PEP), we must assess the level of risk associated with that customer and, as a result of that assessment, the extent to which enhanced due diligence measures need to be carried out to be clearly documented.

- d)** We should make use of information that is reasonably available to identify PEPs, family members or known close associates. This could include the following:
- Public domain information such as websites of the governments, reliable news sources and work by reputable pressure groups focused on corruption risk. We should use a variety of sources where possible.
- e)** We should not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or a family member of a PEP or known close associate of a PEP). After collecting appropriate information and completing its assessment, conclude the risks posed by a customer are higher than we can effectively mitigate; only in such cases it will be appropriate to decline or close that relationship.
- f)** The following measures should be taken where a customer meets the definition of a foreign PEP, IPs/Chief of International Organization posing higher risk or a family member or known close associate of a foreign PEP, IPs/Chief of International Organization posing higher risk:
- Obtain appropriate approval for establishing or continuing business relationships with such persons as follows:
 - a) obtain approval from CAMLCO before establishing business relationship in case of Foreign PEPs, their high-risk family members & close associates and local high-risk IP accounts;
 - b) obtain senior managements' approval before establishing business relationship with low risk family members & close associates of foreign PEPs and low risk local IP;
 - 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 bank has assessed in relation to the customer. The bank will apply more extensive measures for relationships assessed as high risk and less extensive measures for lower risk customers.

g) Measures may take in lower risk situations

In lower risk situations we 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, we should minimize the amount of information we collect and verify.
- 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.

h) Measures may take in higher risk situations

In higher risk situations we 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 from CAMLCO before establishing the relationship;
- 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.

i) Beneficial owners of legal entities who are PEPs

We 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 identified 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, we 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 we 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 us.

6.16 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.

6.16.1 Cross-Border Wire Transfers

Under general or special consideration in case of threshold cross-border wire transfers of 1000 (one thousand) or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank. Furthermore, for cross-border wire transfers, below the threshold full and meaningful originator information with account number or Unique Transaction Reference Number has to be preserved. For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information with account number or Unique Transaction Reference Number 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, the bank will include the account number of the originator.

6.16.2 Domestic Wire Transfers

In case of threshold domestic wire transfers of at least 25000/- (twenty-five thousand) BDT, full 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 bank 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.

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

Ordering Bank:

The ordering bank should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information. This 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.

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 that information through mutual communication or using any other means. During the payment to receiver/beneficiary, the bank should collect full and accurate information of receiver/beneficiary and should preserve that information for 5 (five) years.

An intermediary bank 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.

6.17 Beneficial Ownership and Control

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

6.17.1 Definition:

The definition of beneficial owner means the individual who-

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

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

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

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.

6.17.2 Importance to identify the beneficial owner

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

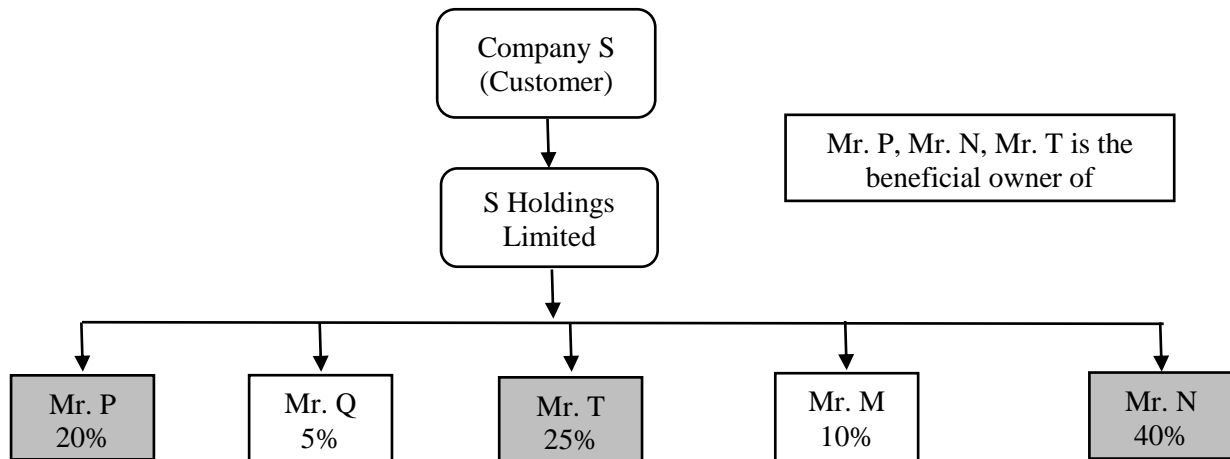
Various studies conducted by Financial Action Task Force (FATF), World Bank, United Nations Office on Drugs and Crime (UNODC) have explored the misuse of corporate entities for illicit purposes, including for ML/TF. In general, the lack of adequate, accurate and timely beneficial ownership information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

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

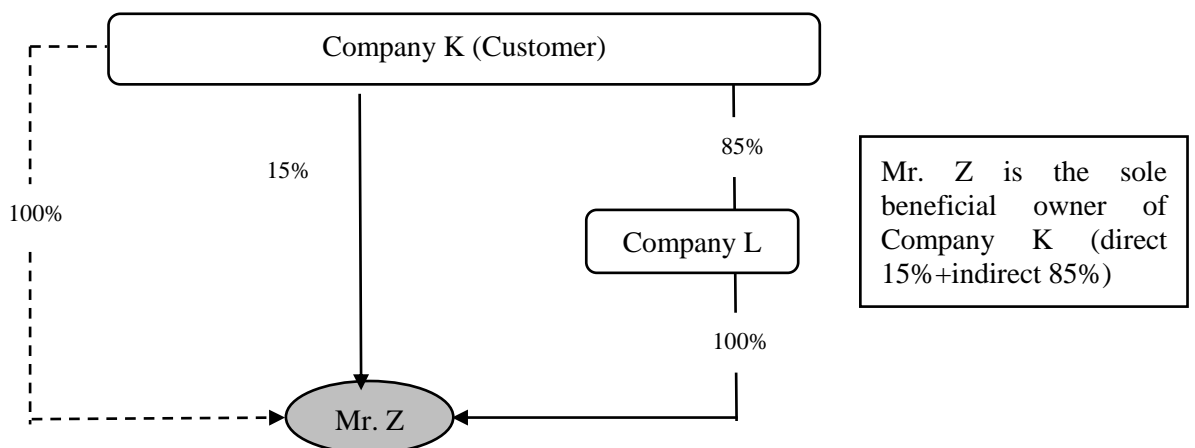
6.17.3 Ownership

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

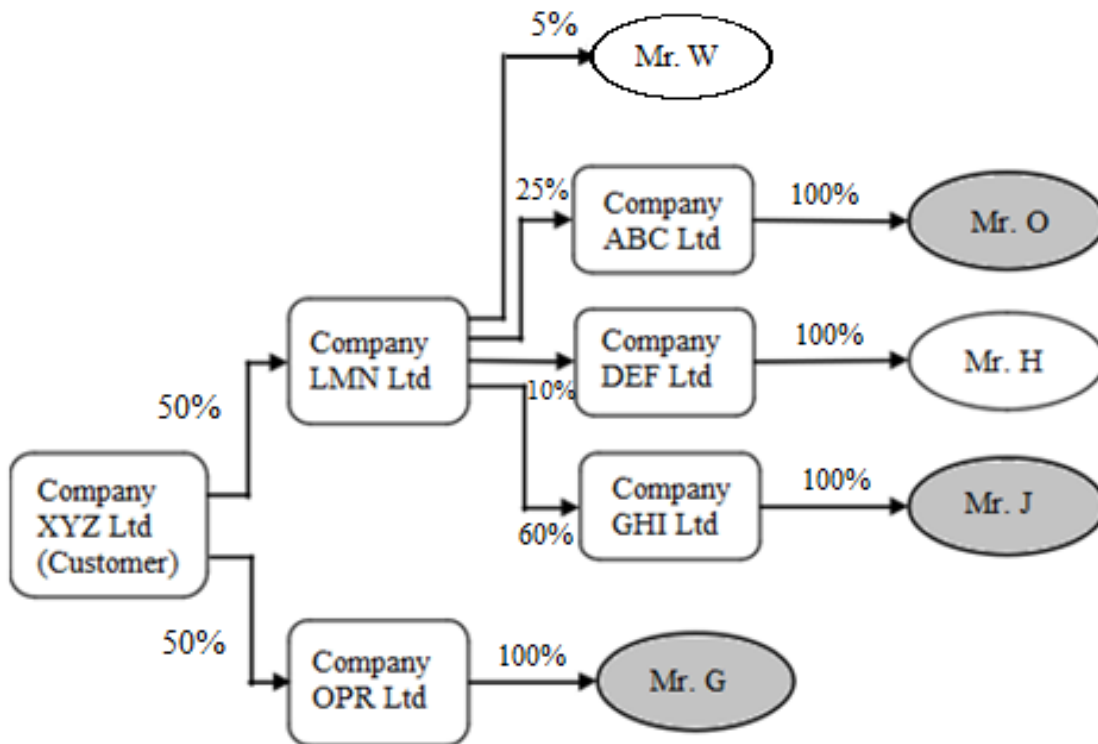
a) Simple ownership



b) Simple (Direct and Indirect) ownership



c) Complex (Multi Level indirect) ownership



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

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

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

6.17.4 Effective Control

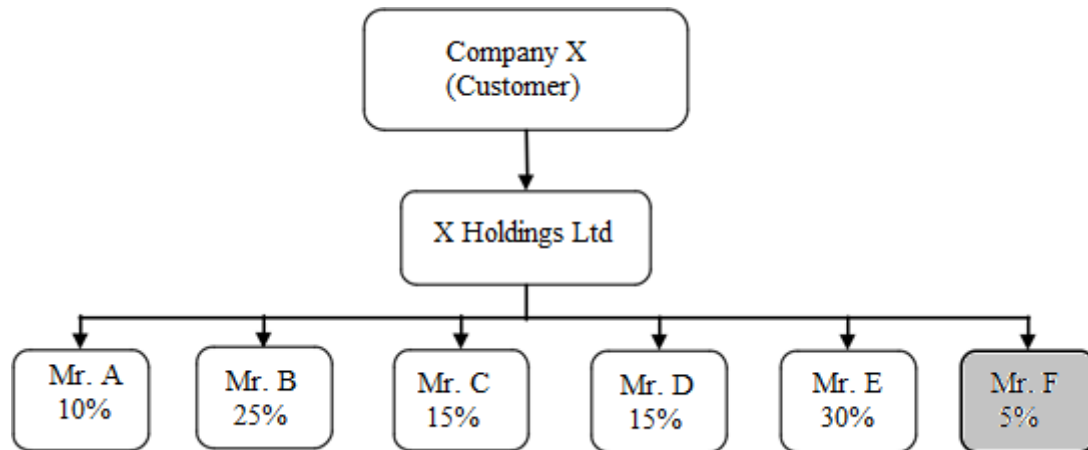
It is essential to understand the customer’s governance structure as an aid in identifying those persons that exercise effective control over the customer. In deciding the effective controller(s) in relation to a customer, reporting entities should consider:

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

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

- a) Personal connections to persons in positions such as Executive Directors/ CEOs/ Managing Director or that possess ownership;

- b) Significant authority over a legal person’s financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person;
- c) Control without ownership by participating in the financing of the enterprise, or because of close family relationships, historical or contractual associations, or if a company defaults on certain payments;
- d) Use, enjoyment or benefiting from the assets owned by the legal person even if control is never exercised



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

6.17.5 Person on whose behalf a transaction is conducted

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

An example is, if a 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.

6.17.6 Beneficial owner of legal arrangements

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

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

The bank will 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).

It is 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.

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

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

- a) Use of shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions,
- b) Use of legal persons as directors,
- c) 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,
- d) Bearer shares and bearer share warrants,
- e) Formal nominee shareholders and directors where the identity of the nominator is in disclosed,
- 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.

6.17.8 Identification of Beneficial Owner

The obligation is to determine the individual(s) who are the beneficial owner(s). A beneficial owner is an individual (a natural person). Therefore, the beneficial owner can only be an individual, not a company or organization. There may be more than one beneficial owner associated with customers. The task is to identify and verify the identity of all the beneficial owners of the customers. If the customer is an individual to treat that person as the beneficial owner unless there are reasonable grounds to make the suspect that are acting on behalf of another.

If the customer is acting on behalf of another person, anyone will need to establish that person's identity, the beneficial ownership of the customer and any other beneficial owners.

When the bank will identify a customer, it will 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.
- f) 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.
- g) 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

6.17.9 Applying a risk-based approach

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

for assessing customer risk and deciding how to identify and verify beneficial ownership should be set out into the AML/CFT program.

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

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

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.

6.17.10 Record keeping

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

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

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

In this example, it is 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 bank 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 bank determine that there is no such individual; The manner in which the bank obtained this information; and
- The measures taken to verify accuracy of information

Example 2: Record for ownership and control structure of partnership

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

In this example the bank 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 bank 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.

6.17.11 Who is required to submit data to the Bank in supporting beneficial ownership?

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

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

- Apartment association
- Building association

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

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

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

6.17.14 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

6.17.15 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.

6.17.16 General instruction while identifying beneficial ownership

- a) The bank should consider following aspects while identifying beneficial ownership:
- b) If a customer operates an account on behalf of another person, the bank will collect and preserve complete & accurate information of that person along with the customer;
- c) The bank will collect and preserve complete & accurate information of the person who apparently controls, directly or indirectly, the customer;
- d) In case of Company, the bank will collect and preserve complete & accurate information of the beneficial owner; in that case, the shareholders who have controlling ownership interest in the company will be treated as beneficial owner. A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 20%);
- e) The bank will collect and preserve complete & accurate information of the CEO if no Natural Person is identified as mentioned in clause b & c

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

6.18 Reliance on Third Party

Bank could rely on the third parties to perform the CDD measures with the prior permission of Bangladesh Bank which may include

- i) identify and verify customer identity;
- ii) identify the beneficial ownership and control structure; and
- iii) identify the purpose and nature of the business relationship under the following criteria:
 - A third party should immediately obtain necessary information related to i) -iii) as mentioned above;
 - All necessary data and documents held with the third party must be available for the bank without any delay;
 - Bank should satisfy that third party is regulated, supervised and monitored for, and has taken appropriate measures in compliance with CDD and record keeping requirements set out in this Guidelines.

6.19 Management of Legacy Accounts

Legacy accounts refer 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. ML & TF Prevention Department should preserve data of such accounts at their end.

6.20 Management of Foreign Currency Account

Bangladeshi wage earners can open and maintain foreign currency (FC) accounts with AD branches of the bank. These accounts are interest bearing whose balance can be sent abroad freely. These accounts can be either savings or term nature. FC accounts can be maintained in USD, GBP, Euro or Japanese Yen. Foreign exchange earned through business done or services rendered in Bangladesh cannot be put into these accounts.

Source of Fund of the Accounts:

- a) Remittances sent from abroad through banking channel,
- b) Fund sent by other wage earners,
- c) Fund sent from other FC accounts,
- d) Proceeds of convertible foreign exchange viz. currency notes, travelers' cheques, drafts etc.
- e) Brought into Bangladesh by the account holders while on visit to Bangladesh may be deposited to such accounts.

6.20.1 NRB Foreign Currency (FC) Account:

Such accounts are normally maintained on savings basis. The Following persons are eligible to open these accounts:

- a) Bangladesh nationals working/residing abroad,
- b) Foreign nationals residing abroad or in Bangladesh,
- c) Foreign missions and their expatriate employees,
- d) Bangladeshi nationals proceeding abroad for employment/immigration/self-employment may open such account even without initial deposit. Account may be opened after departure for abroad by sending necessary papers/documents or after return from abroad.

General Rules to Maintain the Account

- Such account may be operated by accountholders or by persons nominated by themselves. The nominated person entitled to withdraw only and cannot deposit money from Bangladesh.
- Balance of foreign currency account may be sent abroad through banking channel, can be encashed to BDT for local disbursement, can be taken in the forms of currency notes, TCs (maximum 2000 in USD notes, the remaining in other forms viz. TCs, other foreign currencies, card, etc.) while proceeding abroad.
- Such accounts may be maintained as long as the account holder desires even after permanent return to Bangladesh.

6.20.2 Non-Resident Foreign Currency Deposit (NFCD) Account

These accounts are in the nature of term deposits maturing after 1/3/6/12 months. Eligible persons to open account:

- a) Bangladeshis working/residing abroad
- b) Bangladeshis having dual nationality residing abroad
- c) Bangladesh nationals serving with missions of Bangladesh in foreign countries

- d) Officers/staff of the government/semi-government organizations /nationalized banks and employees of body corporate posted abroad or deputed with international and regional agencies can open such accounts against foreign currency remitted through banking channel or brought in cash.

General Rules to Maintain the Account

- a) Such account may be opened with initial deposit of USD 1000 or GBP 500 or equivalent.
- b) Foreign nationals, companies/firms registered and or incorporated abroad, other financial institutions including institutional investors abroad and Type-A units in EPZ may open and maintain such account with minimum deposit of USD 25,000 or equivalent.
- c) Such accounts may be maintained as long as the account holder desires even after permanent return to Bangladesh.

Balance of NFCD accounts may be sent abroad through banking channel, can be encashed to BDT for local disbursements, can be taken in the forms of currency notes, TCs (maximum 2000 in USD notes, the remaining in other forms viz. TCs, other foreign currencies, card, etc.) while proceeding abroad.

6.20.3 Resident Foreign Currency Deposit (RFCD) Account:

Persons ordinarily resident in Bangladesh may open RFCD account after return to Bangladesh. However, up to USD 5000 or equivalent can be deposited any time after return from abroad while amount exceeding USD 5000 or equivalent (with declaration to customs authority in FMJ Form) can be deposited within one month of return from abroad.

The source of deposit to this account must be Foreign exchange brought in from abroad in the forms of notes, coins, TCs, draft, etc.

Balance of RFCD accounts can be freely transferred abroad through banking channel, can be encashed to Bangladesh Taka for local disbursements, can be taken in the forms of currency notes, TCs (maximum 2000 in USD notes, the remaining in other forms viz. TCs, other foreign currencies, card, etc.) while proceeding abroad. Funds from this account may also be issued to the account holder for the purpose of his foreign travels in the usual manner.

6.20.4 KYC Documentation to opening NRBFC/NFCD/RFCD Accounts:

Eligible persons can open NRBFC/NFCD/RFCD accounts easily with any AD Branch of the Bank in Bangladesh by submitting following Documents:

- The account opening form and signature card to be filled in and duly signed and verified by authorized Officer.
- Photocopy of first 7 pages of valid passport
- Signature in the account opening form/card must be same with the signature of the passport.
- Copies of employer's certificate/work permit.

Persons residing abroad interested to open NRBFC/NFCD accounts can open account by sending necessary papers/documents from abroad duly verified by Bangladesh mission abroad or a branch/exchange house located abroad or any other reputable bank or any person known to the AD in Bangladesh.

Chapter: 7

RECORD KEEPING

7.1 Introduction

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 to detect and confiscate the criminal funds by the authorities.

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

7.2 Legal Obligations

The bank has some obligations under MLPA, 2012 (amendments at 2015), MLP Rules, 2019 and under BFIU Circular-26 dated 16/06/2020. The obligations are as follows:

1. The bank will 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;
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. Bank will preserve the information/documents related to AML/CFT training, conference, inspection/audit and special audit.
5. Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence.
6. 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.

7.3 Records to be Kept

The objective of record keeping is to provide relevant documents to the audit authorities during an investigation which includes:

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

7.4 Records to be kept by the Bank

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

- AML/CFT Circular & circular letters issued by ML & TF Prevention Department from time to time;
- Account Information file as queried by ML & TF Prevention Department with any reference;
- CEO & MD's yearly message;
- BAMLCO Nomination File;
- AML/CFT Training, Workshop/Awareness record;
- Cash Transaction Report (serially month wise hard copy verified with T-24 to JB Middleware for goAML Software and duly signed);
- Suspicious Transaction/Activity Report (STR/SAR) (List of initiated STR/SARs that have been sent to ML & TF Prevention Department);
- Quarterly meeting Notice, Agenda and Minutes on AML/CFT issues;
- Self-Assessment report (Half yearly);
- Internal and External AML/CFT Inspection Report and their Compliances;
- High Risk Account List (as per KYC);
- PEPs & IPs Account List;
- Transaction Monitoring (with Structuring identification) file;
- False positive (Sanction screening) file;
- Any other files as instructed by AMLD.

7.5 Customers' Information

In relation to the evidence of a customer's identity, the bank must keep a copy of or the references to, the evidence of the customer's identity obtained during the application of CDD measures. Where the bank has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. The bank will 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.

7.6 Transactions

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the bank'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 form from which a satisfactory audit trail may be compiled where necessary. It can 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.

7.7 Internal and External Reports

The bank will 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.

7.8 Other Measures

A 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 by the ML Reporting Officer to senior management; and
- records of consideration of those reports and of any action taken as a consequence.

7.9 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 branch has reliable procedures for keeping records in electronic form, as appropriate, and that these can be reproduced without undue delay.

Chapter: 8

REPORTING TO BFIU

8.1 Legal Obligations

Under Section 25(1)(d) of MLPA, 2012, the bank has the obligation to report any doubtful transaction or attempt of such transaction as defined under Section 2(z) of MLPA, 2012 the same act as suspicious transaction report to the BFIU immediately on its own accord

The bank is also obliged to send various reports (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.

8.2 Definition of Suspicious Transaction

Money Laundering Prevention Act, 2012 defines suspicious transaction as follows-

‘Suspicious transaction’ means such transactions –

- which deviates from usual transactions;
- of which 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;
- which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh bank from time to time.

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

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

8.3 Reporting Process

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

Generally, STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seeming to be usual manner. Such report is to be submitted by the branch to CCC and CCC will report to BFIU. Suspicion basically involves a personal and subjective assessment. The branches have to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

In case of reporting of STR/SAR, the bank should conduct the following 3 stage

8.3.1 Identification of STR/SAR

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

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

Some red flag indicators for identifying STR/SAR related to ML & TF are mentioned below:

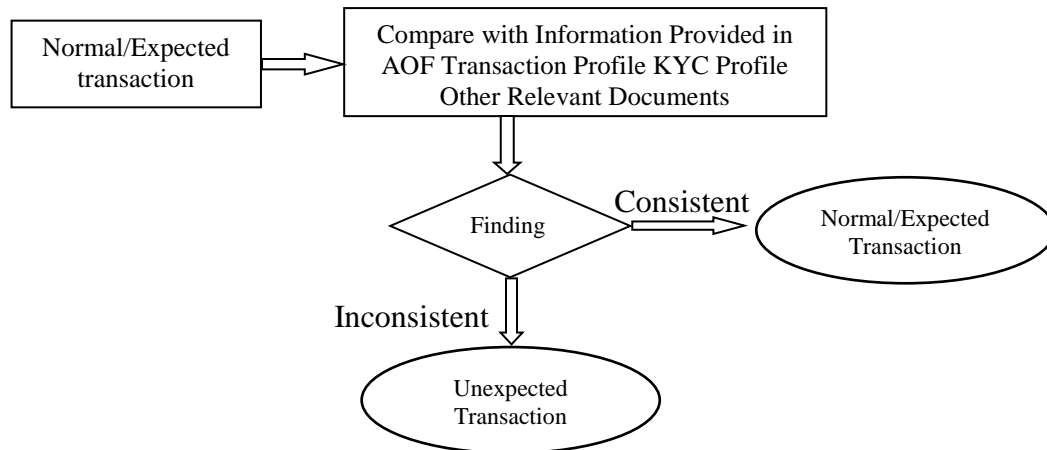
1. Significant mismatch with financial status of the customer.
2. Fake documents & false information submitted by the customer.
3. Customer is reluctant to provide documents.
4. Frequent cash transaction not aligned with the business or, profession of the customer.
5. Structuring.
6. Pay order & Demand Draft purchased or/and encased without bona fide transaction.
7. Cheque kitting and fraudulent activity related to financial instruments.
8. Large number and amount of transaction with minimum balance.
9. Sudden pay off of loan or, multiple number of unpaid installments.
10. Account opened and transacted large amount in the name of non-earning members and close aides.
11. Customer or beneficiary has link with terrorist activities or, terrorist financing or, sanctioned organization.
12. Adverse media report against the customer or, beneficiary.
13. Transaction or activities related to TBML/TF related trade financing.
14. Transaction with high risk jurisdiction.
15. Suspicious cross border inward/ outward transaction.
16. Relationship with front company or Shell Company.
17. Use of funds by the NGO/NPO/ Co-operative inconsistent with the purpose.
18. An atypical incidence of pre-payment of insurance premiums.

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 CCC 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 rises 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-



This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of branches monitoring of unusual transactions may be automated, manually or both. Monitoring mechanisms should be more rigorous in high-risk areas of the branch and supported by adequate information systems to alert management and other appropriate staffs of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should always be an ongoing activity.

8.3.2 Evaluation:

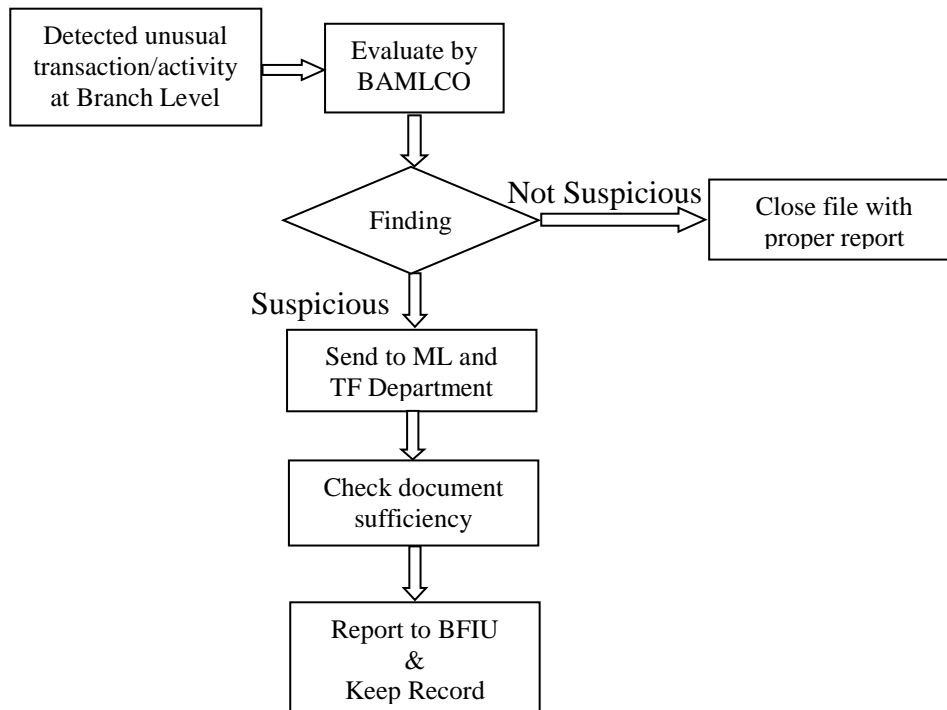
This part must be in place at branch level. After identification of STR/SAR at branch level, BAMLCO will evaluate the transaction/activity in an appropriate manner and will preserve his observations on it in a written format. If the transaction or activity seems to be suspicious, it, along with all necessary supportive documents, has to be sent to the Central Compliance Committee/ ML and TF Prevention Department without any delay. After receiving report from branch, ML and TF Prevention Department will review whether the reported suspicious transaction or activity from the branch has been reported in an appropriate manner with all necessary information, data and documents.

8.3.3 Disclosure:

This is the final stage and CCC of the bank should submit STR/SAR to BFIU if it still seems suspicious. After checking the sufficiency of the required documents, Central Compliance Committee/ML and TF Prevention Department will submit a suspicious transaction/activity report to BFIU without delay by using goAML web as per instruction mentioned in goAML Manual. Every stages of evaluation Bank should keep records with proper manner.

Central Compliance Committee/ML and TF Prevention Department will submit suspicious transaction/activity report to BFIU if it identifies any transaction or activity as suspicious even though the concerned branch did not identify as suspicious

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



8.4 Documenting Reporting Decisions

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

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

These records can be simple or sophisticated, depending on the size of the business and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. The maintenance and retention of such records is important as they justify and defend the actions taken by the BAMLCO and/or other members of staff and should be made available to the Competent Authorities and BFIU upon request.

For practical purposes and ease of reference, a reporting index could be kept and each SAR/STR could be given a unique reference number.

8.5 Some Special Scenarios for Reporting

- a) If a reporting organization fails to perform conducting Customer Due Diligence (CDD) due to the non-cooperation of customer and the collected information/data of the

customer appears unreliable, the bank should submit suspicious transaction/activity report on such customers;

- b) If the bank identifies any account or transaction in the name of listed or proscribed person or entity under any United Nations Security Council Resolution or any person or entity listed or proscribed by Bangladesh Government or any individual or entity directly or indirectly under their control or association, the bank must stop transaction of the account and report BFIU with detailed information within the next working day;
- c) If any news on Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction is published in the media and if any account of any person or entity related to that activity is maintained with the bank, detailed information must be reported to BFIU without any delay.

8.6 Tipping Off

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

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

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

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

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

8.7 Penalty

8.7.1 Penalty of not reporting

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

8.7.2 Penalty of Tipping Off

Under section 6 of MLPA, 2012, if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act will be punished

with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both

8.8 Cash Transaction Report (CTR)

Every branch will prepare the monthly cash transaction report and send it to ML & TF Prevention Department through JB Middleware for goAML Software in due time. If the branch has not any such transaction, it should report as ‘there is no reportable CTR’. Simultaneously, branches need to identify whether there is any suspicious transaction reviewing the cash transactions. If any suspicious transaction is found, the branch will submit it as ‘Suspicious Transaction Report’. If no such transaction is identified, it needs to inform as ‘no suspicious transaction has been found’ while reporting the CTR. Besides, every branch needs to preserve its CTR in their own branch.

The ML & TF Prevention Department needs to prepare the accumulated CTR received from its all branches. The Department must ensure the accuracy and timeliness while reporting to BFIU. Moreover, it has to review all the cash transaction from the branches above the threshold (BDT 10 lac and above or equivalent FC) and search for any suspicious transaction. If any suspicious transaction is found, the bank will submit it as ‘Suspicious Transaction Report’ to the BFIU. The department has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR. Moreover, the department must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

8.9 Self-Assessment Report (As per BFIU Circular 26 dated 16 June 2020)

According to the instructions of BFIU, branches 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 Instruction circular no. 965/20 dated 12 July, 2020 (BFIU Circular 26 dated 16/06/2020). Before finalizing the evaluation report, there will have to be a meeting presided over by the branch manager with all concerned officials of the branch.

In that meeting, there will 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 will 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 (Corporate/General) and the ML & TF Prevention Department of the Head Office within the 15th of the next month.

8.10 Independent Testing Procedure

The audit function must be independently done by Internal Audit Department (i.e. performed by people not involved with the bank’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 Instruction circular no. 965/20, dated 12 July, 2020.

8.11 Internal Audit Department's or ICC's Obligations Regarding Self-Assessment or Independent Testing Procedure

The Internal Audit Department will assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it will inspect the branch immediately and will inform the matter to the ML & TF Prevention Department.

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

8.12 Central Compliance Committee'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 Internal Audit Department or ICC, the ML & TF Prevention Department will 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 Internal Audit Department 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 CCC to prevent those irregularities.
- d) The general and special irregularities mentioned in the report submitted by the Internal Audit Department and the measures taken by the CCC 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: 9

TRANSACTION MONITORING

Monitoring of transaction will be an ongoing process in the normal course of the business relationship. The purpose is to be vigilant for any significant changes or inconsistencies in the pattern of transactions as against declared one.

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

Concerned officials of the branch will arrange periodic reviews of accounts by monitoring transaction/activity reports. Any account not appearing in conformity with the declared transaction will be isolated for further scrutiny and if still not convincing with any reasonable explanation from the concerned customer, the account will be documented under internal Suspicious Activity Reports (SARs) with action plans for approval by the relevant Manager at the branch and review with the BAMLCO.

BAMLCO will review the SARs and responses from the other concerned officers. If the explanation for the exception does not appear reasonable then the Branch Head will review the transaction prior to considering submitting them to the CAMLCO/DCAMLCO.

- The bank will closely monitor Cash Transaction find out the possibility of structuring
- In branch level, if the BAMLCO believes the transaction should be reported then the Branch Head will supply the relevant details to the ML & TF Prevention Department.
- The ML & TF Prevention Department will investigate any reported accounts and will send a status report about the accounts reported. No further action will be taken on the account until notification has been received.
- If, after confirming with the client, the transaction trend is to continue the related officer is responsible for documenting the reasons why the transaction profile has changed and should amend the KYC profile accordingly.

Inconsistency is measured against the stated original purpose of the accounts, possible areas to monitor are:

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

9.1 Transaction Profile (TP)

Transaction Profile (TP) is an important document for monitoring transactions and recognizing suspicious transactions. The following steps and points should be noted while preparing transaction profiles:

- Take interview with the customer and prepare the Transaction Profile Form as recommended by the authorities. The main features of the Form for both deposit and withdraw will be:
 - Various types of transactions (i.e. nature of transactions)
 - No. of transactions (monthly)
 - Maximum size (per transaction)
 - Total value (monthly)

In order to be vigilant for any significant changes or inconsistencies in the pattern of transactions, monitoring of transactions should be done

- The transactions which are complex, unusual and apparently have no financial or legitimate purpose should be monitored by giving more emphasis.
- The bank will identify Structuring and report STR to ML & TF Prevention Department for onward submission to BFIU, if applicable, as per instructions given in chapter 8 of this guideline.
- In transaction monitoring, all foreign currency transactions and technology-based transactions should also be included.
- In transaction monitoring, the UN Security Council resolution and the jurisdiction that do not meet or have significant deficiencies in complying international standards for the prevention of money laundering and terrorist financing are to be taken into consideration.

9.2 Transaction Monitoring Process

9.2.1 Review of TP violation report:

The tellers will take evidence from customers in case of violation of TP while ongoing transaction. The BAMLCO will review/analyze TP violation report after transaction hours in daily basis. If any mismatch found between Customers speech/evidence and the observation of BAMLCO it should be filed as Suspicious Transaction Report immediately and should send to Anti Money Laundering Department/DCAMLCO.

9.2.2 Review of Structuring:

Structuring is the act of parceling what would otherwise be a large financial transaction into a series of smaller transactions to avoid scrutiny by Banks and reporting to BFIU. Typically, each of the smaller transactions is executed in an amount below some statutory limit that normally does not require the bank to file a report with a controlling authority. Criminal enterprises may employ several agents to make the transaction. Structuring may be done in the context of money laundering, fraud, and other financial crimes.

BAMLCO will review this type of transactions by threshold-based transaction monitoring from the system at least monthly basis.

9.2.3 Review of Placement and Layering:

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

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

In layering process money transfer began at the source account and transfer through many other accounts before it returns back again to the initiator after conceal the illegal origin and illegitimate ownership of property and assets that are the proceeds or results of their criminal activities. It is difficult to be discovered manually, so the bank implemented system generated report for analyzing to discover layering and placement on its Core Banking Software.

The analysis should do at branch, area, division and head office level to identify relations between accounts, customers and transactions by monitoring of-

- Unusually large amount transactions
- Geographical origin/destination of transactions
- Number of transactions within a month.
- Funding speeds: deposits of money into accounts that are then rapidly withdrawn.
- Frequent transfers between accounts within different branches of the bank (one to many and many to one basis transactions).
- Frequent use of wire transfers to deposit and withdraw of accounts.
- Geographical location to or from the transaction occurs
- Funds deposit to or from high-risk countries or accounts.
- Changes in account signatories

9.2.4 Reporting of STR to ML & TF Prevention Department:

If the branch does not become satisfied with the customer's clarification then the issue will have to be reported as a Suspicious Transaction Report (STR) to the Branch AML Compliance Officer (BAMLCO). BAMLCO will review the STRs along with responses from the customer as well as designated officer and record in writing, with reasons, in details whether the transactions are to be viewed as connected with money laundering or not. If the reported issue does not appear to be connected with money laundering, then BAMLCO will close the issue at his end after putting his comments on the STR form. If the reported issue appears to be connected with money laundering, then BAMLCO will send immediately the details of the incident along with a copy of the above form to the ML & TF Prevention Department at Head Office.

9.3 Maintaining Secrecy:

The above review will be done as a part of the daily functions of the branch. It should be kept in mind that all exceptions may not be suspicious. Also, branch officials should be very much cautious in dealing with customers. They should perform the job in a manner that do not create any panic and do not disclose any information to any person.

Chapter:10

TERRORIST FINANCING & PROLIFERATION FINANCING

10.1 Introduction

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

To 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 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 the bank and thus was to carry out terrorist acts.

10.2 Legal Obligations

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

The Board of Directors, or in the absence of the Board of Directors, the CEO & Managing Director of the bank should approve and issue directions regarding the duties of its officers, and will ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, 2009; which are applicable to the bank, have been complied with or not.

10.3 Obligations Under Circular

As per BFIU Circular no, 26 dated 16/06/2020, every bank will 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, will 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 transaction are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or proscribed by Bangladesh government. Immediately after the identification of any account of any listed individual or entity concerned bank will stop that transaction and inform BFIU the detail information at the following working day

10.4 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.

10.5 Sources of Fund/Raising of Fund

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

10.6 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 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.

10.6.1 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.

10.6.2 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.

10.6.3 Cash Couriers

The physical movement of cash is a way that 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 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, for this it has become an attractive method of transferring funds by the remitters without leaving an audit trail.

10.6.4 Use of Alternative Remittance Systems (ARS)

Alternative remittance systems (ARS) are used by terrorist organizations for convenience and access. Terrorist organizations have additional attraction for ARS where record keeping is weaker and regulatory vigilance is generally less stringent. Although FATF standards call for significantly strengthened controls over such service providers, the level of anonymity and the rapidity offered by such systems, have made those (ARS) a favored mechanism for terrorists.

10.6.5 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 great problem.

10.7 Targeted Financial Sanctions

In recent years, the concept and strategy of targeted sanctions imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, have been receiving increased attention. The considerable interest in the development of targeted sanctions regimes has focused primarily on financial sanctions, travel and aviation bans, and embargoes on specific commodities such as arms or diamonds.

Targeted financial sanctions entail the use of financial instruments and institutions to apply coercive pressure on transgressing parties ‘senior officials, elites who support them, or members of non-governmental entities’ in an effort to change or restrict their behavior.

Sanctions are imposed only to a subset of the population—usually the leadership, responsible elites, or operationally responsible individuals through asset freezing, blocking of financial transactions, or financial services.

However, targeted financial sanctions represent a potential refinement of the sanctions tool that could be used in conjunction with other coercive efforts, such as travel bans; thus, the unintended effects of comprehensive sanctions could be minimized and achieve greater effectiveness.

To implement TFS in Bangladesh, the Government has issued Statutory Regulatory Order (SRO) under section 2 of the United Nations (Security Council) Act, 1948 (29 November, 2012) and amended the SRO to make it more comprehensive (June, 2013). To make the process enforceable, a separate section has been included in ATA, 2009 through amendment of ATA in 2013. Section 20(A) of ATA, 2009 covers all the requirements under UNSCR’s tool were

taken and will be taken under chapter VII of the charter of UN. Before that BFIU used to issue circular letters for reporting organizations to implement UNSCR resolutions.

For effective implementation of these provisions, detailed mechanism has been developed in Anti-terrorism Rules, 2013. Under rule 16 of AT rules, 2013, the bank as a reporting agency has to 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. In case there is any fund or economic resources held by the listed individuals and entities, the banks should immediately stop payment or transaction of funds, financial assets or economic resources and report to the BFIU within the next working day with full particulars of the listed and/or the suspected individuals or entities or related or connected individual identities.

10.8 Automated Screening Mechanism of UNSCRS

For effective implementation of TFS relating to TF & PF the bank is required to have automated screening mechanism that could prohibit any listed individuals or entities to enter into the banking channel. We should operate in such system where we could detect any listed individuals or entities prior to establish any relationship with us. In particular, the bank needs to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individual or entity could not use the formal financial channel. In a word, the bank will ensure that screening has been done before-

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

For proper implementation of UN sanction list, all official of the bank must have enough knowledge about-

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

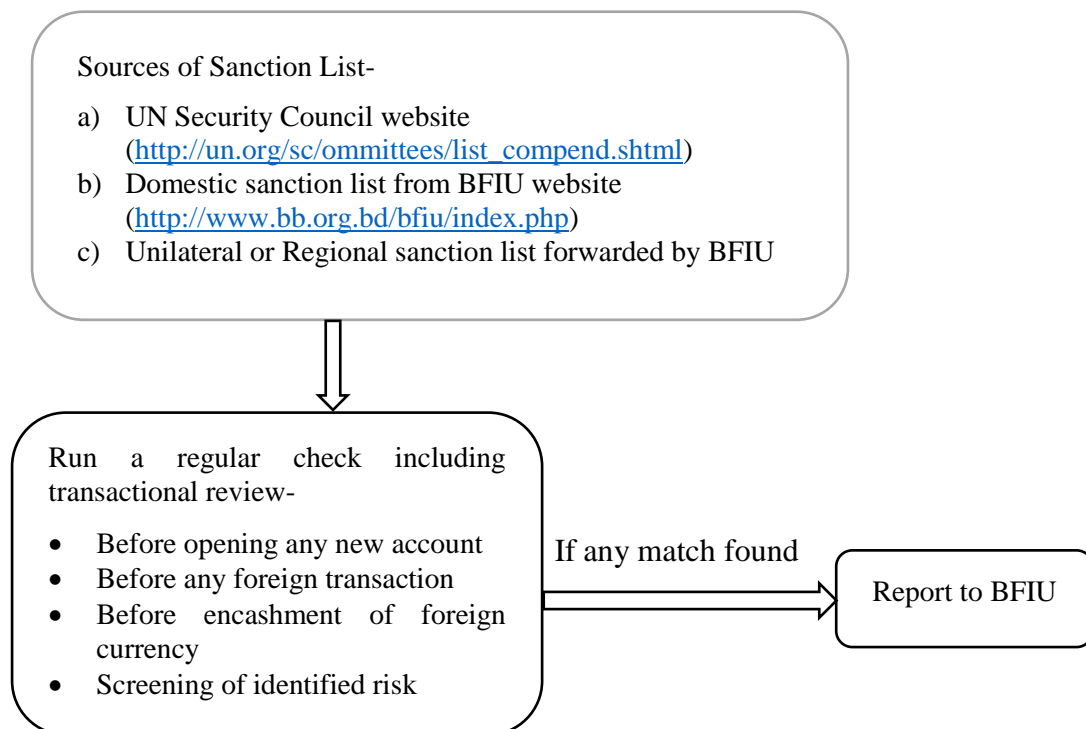
10.9 Role of The Bank in Preventing TF & PF

- The bank will establish a procedure by the approval of Board of Directors for detection and prevention of financing of terrorism and financing in proliferation of weapons of mass destruction, will 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.
- The bank should take necessary measures, with appropriate caution and responsibility to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 and if any suspicious transaction is identified, the bank will spontaneously report it to BFIU 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, the bank will send the

details of the accounts (if any is found) of any persons who are engaged in those activities to BFIU immediately.

- The bank should 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. It should 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 the bank.
- The bank should run a check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009; 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 it.

10.10 Flow-Chart for Implementation of TFs By Banks



Chapter: 11

TRADE BASED MONEY LAUNDERING

11.1 Definition of Trade Based Money Laundering

Trade Based Money Laundering (TBML) is a form of money laundering that uses trading operations with the aim of conceal the origins of funds. It is the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.

This is usually done by the fraud of trade-description such as the over- and under-invoicing of goods, over- and under-shipment of goods, multiple invoicing or falsely describing goods.

11.2 Techniques of Trade Based Money Laundering

TBML techniques involve some simple fraud, such as, misrepresentation of the price, quantity or quality of goods on an invoice, through to complex networks of trade and financial transactions. The most uses techniques are discussed below:

11.2.1 Trade description fraud

Trade description fraud is the most commonly described form of TBML and generally comprises one of the following techniques:

- a) **Over invoicing of goods and services-** By misrepresenting the price of the goods in the invoice and other documentation stating it at above the true value) the seller/exporter gains excess value as a result of the payment.
- b) **Under-invoicing of goods and services-** By misrepresenting the price of the goods in the invoice and other documentation (stating it at below the true value) the buyer/importer gains excess value when the payment is made.
- c) **Multiple invoicing of goods and services-** By issuing more than one invoice for the same goods a seller can justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than one bank to facilitate the payments/transactions.
- d) **Over shipments of goods and services-** The seller/exporter ships more than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to under invoicing.
- e) **Under shipments of goods and services-** The seller ships less than the invoiced quantity or quality of goods which misrepresenting the true value of goods in the documents. The effect is similar to over invoicing.
- f) **Falsely described goods and services (Fake Shipping)-** No goods are shipped and all documentation is completely falsified. Also known as “ghost shipping” or “phantom shipping” or Fictitious Trades.
- g) **Structured transaction-** Parties may structure a transaction in a way to avoid alerting any suspicion to Banks or to other third parties which become involved. This may

simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it.

11.2.2 Other Types of Trade Based Money Laundering

a) Related party transactions

- TBML requires agreement between traders at both ends of the import/export chain, but they do not need to be linked (in the sense of ownership).
- Related party transactions (i.e. transactions between entities that are part of the same corporate or business group) can possibly make TBML easier to conduct and more difficult to detect as it is done ‘in-house’.
- Differing tax rates and government incentives encourage international organizations to move funds and assets within the group.

b) High-risk jurisdictions

There are some high TBML risk countries due to the volume of trade, value of the trade, the type of commodity or service traded and the domestic regulatory environment.

For example-

- **Some countries** present a TBML risk on the basis of volume of trade alone.
- Some jurisdictions in the Asia–Pacific region are a high TBML risk because of the type of trade that passes through the border.
- **Transshipment** jurisdictions have a higher risk of TBML and trade fraud because transshipped consignments are not inspected always.
- **Some countries** also identifying the country as a potential TBML risk because of the presence of organized crime there and their status as a major trading power.

11.3 Role of Financial Institutions in the Settlement of Trade Transactions

- a) **Money transmission** – is the transfer of funds between parties associated with the trade transaction. (e.g. a wire transfer).
- b) **Provision of finance** – is the provision of credit to support the trade transaction. In these situations, as a standard practice, the financial institution conducts standard credit checks against the customer. In addition, the financial institution may conduct a check against the underlying transaction.
- c) **Lending the financial institution’s name to the transaction** – it occurs in two situations:
 - where the financial institution undertakes to make payment subject to certain conditions (e.g. a letter of credit), and
 - where the financial institution undertakes to make payment if the buyer defaults (e.g. a guarantee).

11.4 Trade Based Money Laundering “Red Flag” Indicators:

- The type of commodity being shipped is designated as “high risk” for money laundering activities; For example, high-value, low-volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties.

- The type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities;
- The shipment does not make economic sense; For example, the use of a forty-foot container to transport a small amount of relatively low-value goods.
- The commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities;
- The commodity is transshipped through one or more jurisdictions for no apparent economic reason;
- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice;
- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped;
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value;
- The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities;

In addition, red flag indicators that are used to detect other methods of money laundering could be useful in identifying potential trade-based money laundering cases.

11.5 Response of Janata Bank Limited to Combat Trade Based Money Laundering

- Janata Bank Limited is well-aware of trade-based money laundering. Authorized Dealer (AD) branches of the bank are instructed to closely monitor over- and under-invoicing of goods and services.
- In line with the instruction of BFIU we have been developed 'Guidelines for Prevention of Trade Based Money Laundering' for mitigation of risk associated with TBML in our bank. The guidelines has been duly approved by the Board of Directors in its 632th meeting held on 28 September 2020.
- The Bank arrange training courses on "Prevention of Trade Based Money Laundering" for the concerned officers working in the Foreign Exchange Desks every year in regular basis.
- All AD branches used to inspect by Foreign Exchange Audit Department every year.
- Foreign Trade Monitoring Department will monitor the trading activities effectively.

11.6 Trade Related CDD Requirements

The bank will consider the following minimum requirements:

- Comply the customer acceptance policy;
- Ensure collection of complete & accurate KYC information of the customers;
- Be careful enough about HS Code, unit price, credit report of supplier, importer's credibility over/under invoicing, cash incentives, timely collection of Bill of Entry, submission of EXP form etc.;
- Collection of required documents & information such as:
 - a) Business nature including major products, jurisdictions and markets
 - b) Delivery / transportation mode for goods or services

- c) Major suppliers and buyers
 - d) Products and services to be utilized from the bank
 - e) The countries with which the importer trades
 - f) Account activities
 - g) Methods and terms of payment and settlement
 - h) Internal customer risk assessment ratings
 - i) Any previous suspicious transaction reports filed with BFIU; and
 - j) Other information from the relevant staff
- Verification of the above documents & information through reliable and independent sources
 - Ascertaining and verifying the identity of the beneficial owners of the trade customer
 - Conducting Enhance Due diligence if required
 - Record Keeping
 - The bank should understand the business, the principal counterparties, the countries where the counterparties are located and the goods or services that are exchanged, as well as the expected annual transaction volumes and flows to conduct Customer Due Diligence (CDD) for trade customers;
 - CDD information should be updated in accordance with this Guideline;
 - The Bank should maintain customer-wise trade transaction profile (TTP) including items of Goods value, volume, production capacity, end-use of goods and principal counterparty names. TTP should be made available to trade processing staff so that they can easily check that a transaction is within the agreed profile of the customer;
 - The CDD processes are expected to include —feed-back loops where a trigger event in a transaction or normal review process leads to new information or questions about a relationship. This updating of the CDD profile ensures that the information in the CDD profile is current. The event reviews may also lead to the status of the relationship with the customer being escalated for decisions related to additional controls being applied or the exit of the customer;
 - The bank is required to screen/check the persons, entities, third parties, goods, country, ports, point of transshipment, carrier, master, agents and/or any other names or entities appearing in LC, sales contract and/or presented document related to trade transactions against the names in the Targeted Financial Sanctions databases of UNSC, OFAC & BFIU. If there is any name match, it is required to take reasonable and appropriate measures to verify and confirm the identity of name(s) match. Once confirmation has been obtained about the true matching, it must immediately stop the transaction and report it to AMLD so that AMLD can report it to BFIU;
 - The bank should be aware of the potential red flags related to International Trade

Chapter: 12

RECRUITMENT, TRAINING AND AWARENESS

12.1 Recruitment

To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, the bank will follow proper Screening Mechanism in case of recruitment and ensure proper training for existing and newly recruited officials.

12.2 Employee Screening

The bank may be subject to ML & TF risk from its customers as well as from its employees in absence of proper risk mitigating measures. ML & TF risks arise by or through its employees can be minimized if it follows fair recruitment procedure. This fair recruitment procedure will not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, the bank will follow the following measures (at least two from below) during recruitment/hiring:

- 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, the bank will examine the consistency and capability of the employee and be ensured that the employee will have necessary training on AML & CFT lessons for the particular job or desk.

12.3 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 employee's 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 auditors should be conversant with these and other requirements, and see that they are constantly and uniformly updated. KYE requirements should be included in the banks HR policy.

12.4 Training for Employee

Every employee of our bank will 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, we are required to impart refreshment training programs of its employees on a regular basis.

AML & CFT basic training should cover the following-

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

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

12.5 Awareness of Senior Management

Without proper concern and awareness of senior management, it is difficult to have effective implementation of AML & CFT measures in the bank. Our bank will arrange, at least once in a year, an awareness program for all the members of its board of directors and people engaged with policy making of the bank.

12.6 Customer Awareness

The bank will 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.

12.7 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 our bank in implementing the regulatory requirement. For this, BFIU, Bangladesh Bank, other regulators as well as the government sometimes arrange public awareness programs on AML & CFT issues. Representatives of our bank will participate with those initiatives and also arrange public awareness programs like advertisements through billboard, poster, festoon and mass media, distribution of handbills, leaflet and so on.

CONCLUSION

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

Money laundering and terrorist financing risk is very vital issue now a day. Bangladesh Financial Intelligence Unit (BFIU) has imposed a lot of importance on it and urged that each scheduled bank will prepare its own Risk Management Guidelines and on the basis of that relevant risks of ML/TF will be determined. In this context, the bank prepared its own 'Money Laundering and Terrorist Financing Risk Management Guidelines'. It is an ongoing process and will be updated or revised regularly in every two years and as requirement.

Annexure -A

Calculation of Risk Score

Risk Measurement:

The risk associated with an event is a combination of likelihood and impact. Here "likelihood" means the chance of the risk occurring and "impact"- the amount of loss/damage. Therefore, Risk Score can be identified by blending of likelihood and impact.

Calculation of Risk Score:

Likelihood Scale X Impact= Risk Level/Score

(I) Likelihood Scale:

Frequency	Likelihood of an ML/TF risk	Score
Almost Certain	There is a high chance to occur	6
Very likely	It may probably occur several times a year	5
Likely	Probability to happen once a year	4
Unlikely	Unlikely, but not impossible	3

(II) Impact Scale:

On the basis of consequences of damage/loss three levels of impact scale may be considered which are shown in the following table:

Impact scale

Consequence	Impact-of an ML/TF risk	Score
Major	Huge consequences-major damage or effect. Serious Terrorist act or large-scale money laundering.	4
Moderate	Moderate level of money laundering or terrorism financing impact.	3
Minor	Minor or negligible consequences or effects	2

Risk levels:

Considering total score, Risk levels will be considered as follows:

Low	Medium	High
Below 6	Above 6 to 15	Above 15 to 24

Considering the operational components the following five Risk Registers should be maintained at Branch levels:

- (i) ML & TF Risk Register for customer.
- (ii) Risk Register for Products & Services.
- (iii) Risk Register for Business Practices/delivery methods or Channels.
- (iv) Risk Register for Country/jurisdiction.
- (v) Register for Regulatory Risk.

RISK REGISTER

Annexure -B

1. ML & TF Risk Register for Customers

SI no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Banking Customer</i>					
1.0	A new customer				
1.1	Individual (Savings/Current Deposit Account)				
1.1.1	Yearly average transaction Up to Tk. 10 lac	Unlikely 3	Minor 2	Low 6	(1) Obtain Complete & accurate information; (2) Prepare KYC & TP; (3) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund- from employer/trade license etc. (iii) Address through thanks letter /utility bill. (4) Ensure reason of account opening; (5) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening.
1.1.2	Yearly average transaction Tk -above 10lac -50 lac	likely 4	Moderate 3	Medium 12	(1) Obtain Complete & accurate information; (2) Prepare KYC & TP; (3) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/ trade license etc. (iii) Address through thanks letter /utility bill (4) Ensure reason of account opening; (5) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening. (6) Apply CDD to reduce risk at preferable level.
1.1.3	Yearly Average transaction above Tk- 50.00 lac-5 crore	Very likely 5	Moderate 3	High 15	(1) Obtain Complete & accurate information; (2) Prepare KYC & TP; (3) Perform Standard verification of - (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/trade license etc. (iii) Address through thanks letter/ utility bill . (4) Ensure reason of account opening; (5) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening; (6) Apply EDD and ongoing transaction monitoring to reduce risk at acceptable level.
1.1.4	Yearly Average transaction above -5 crore	Very likely 5	Major 4	High 20	(1) Obtain Complete & accurate information; (2) Prepare KYC & TP; (3) Perform Standard verification of - (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/trade license etc. (iii) Address through thanks letter/ utility bill. (4) Ensure reason of account opening; (5) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening; (6) Apply EDD and ongoing transaction monitoring to reduce risk at acceptable level.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer					
1.2	Entity (Savings/Current/Short Notice (SN) Deposit Account)				
1.2.1		Unlikely 3	Minor 2	Low 6	(1) Obtain Complete & accurate information of the entity; (2) Obtain Complete & accurate personal information of proprietor/director/operator of the a/c (3) Prepare KYC & TP; (4) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, from trade license etc. (iii) Address through thanks letter/ utility bill / physical visit of entity. (5) Ensure reason of account opening; (6) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening; (7) Apply CDD & ongoing transaction monitoring to reduce risk at preferable level.
1.2.2	Yearly average transaction Tk -above 10 lac -50 lac	likely 4	Moderate 3	Medium 12	(1) Obtain Complete & accurate information of the entity; (2) Obtain Complete & accurate personal information of proprietor/director/operator of the a/c (3) Prepare KYC & TP; (4) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, from trade license etc. (iii) Address through thanks letter/ utility bill / physical visit of entity. (5) Ensure reason of account opening; (6) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening; (7) Apply CDD & ongoing transaction monitoring to reduce risk at preferable level.
1.2.3	Yearly Average transaction above Tk- 50.00 lac-5 crore	Very likely 5	Major 4	High 20	(1) Obtain Complete & accurate information of the entity; (2) Obtain Complete & accurate personal information of proprietor/director/operator of the a/c (3) Prepare KYC & TP; (4) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, from trade license etc (iii) Address through thanks letter/ utility bill / physical visit of entity. (5) Ensure reason of account opening; (6) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening; (7) Apply EDD & ongoing transaction monitoring to reduce risk at preferable level.
1.1.4	Yearly Average transaction above -5 crore	Very likely 4	Moderate 3	Medium 12	(1) Obtain Complete & accurate information of the entity; (2) Obtain Complete & accurate personal information of proprietor/director/operator of the a/c (3) Prepare KYC & TP; (4) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, from trade license etc (iii) Address through thanks letter/ utility bill / physical visit of entity. (5) Ensure reason of account opening; (6) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening; (7) Apply EDD & ongoing transaction monitoring to reduce risk at preferable level.

SI	Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer					
1.3	(1) Fixed Deposit Receipt				
1.3.1	FDR Account up to 5.00 Lac	Unlikely 3	Minor 2	Low 6	(1) Obtain Complete & accurate KYC, source of fund; (2) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/trade license etc. (iii) Address through thanks letter / utility bill; (3) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening.
1.3.2	FDR Account Tk> 5.00-10 Lac	likely 4	Moderate 3	Medium 12	(1) Obtain Complete & accurate KYC, source of fund; (2) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/ trade license etc. (iii) Address through thanks letter/ utility bill; (3) Check UNSCRs OFAC, EU and domestic sanction list before a/c opening.
1.3.3	FDR Account Tk> 10-50Lac	Very likely 5	Moderate 3	High 15	(1) Obtain Complete & accurate KYC, source of fund; (2) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/ trade license etc. (iii) Address through thanks letter/ utility bill; (3) Check UNSCRs OFAC, EU and domestic sanction list before a/c opening. (4) Apply EDD to reduce risk at acceptable level.
1.3.4	FDR Account Tk> 50 Lac and above	Very likely 5	Major 4	High 20	(1) Obtain Complete & accurate KYC, source of fund; (2) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/trade license etc.; (iii) Address through thanks letter/utility bill; (3) Check UNSCRs OFAC, EU and domestic sanction list before a/c opening. (4) Apply EDD to reduce risk at acceptable level.
1.4	Any deposit Schemes/Products	Unlikely 3	Minor 2	Low 6	(1) Obtain Complete & accurate KYC, (2) Verify NID from Election Commission Data Base; (3) Check UNSCRs OFAC, EU and domestic sanction list before a/c opening.
1.5	SB Account – Students /Low income women/ Safety net Program	Unlikely 3	Minor 2	Low 6	(1) Obtain Simplified KYC, (2) Verify NID from Election Commission Data Base; (3) Check UNSCRs OFAC, EU and domestic sanction list before a/c opening.
1.6	CD/SB/SND account of PEPs/IPs/Head of International organizations	Very likely 5	Major 4	High 20	(1) Obtain Complete& accurate KYC, TP; (2) Perform Standard verification of- (i) NID from Election Commission Data Base; (ii) Source of fund, occupation from employer/trade license etc. (iii) Address through thanks letter/ utility bill /physical visit in case of entity. (3) Ensure reason of account opening; (4) Check UNSCRs OFAC, EU and domestic sanction list before a/c opening. (5) Obtain Senior Management’s Approval/CAMLCO’s Approval; (6) Follow Foreign Exchange Guidelines and Rules, 1947; (7) Apply EDD & ongoing transaction monitoring to reduce risk at acceptable level.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer					
1.7	Foreign Currency Account	Very likely 5	Major 4	High 20	(1) Obtain Complete & accurate KYC, TP; (2) Perform Standard verification of- (i) NID from Election Commission Database; (ii) Obtain valid passport (Domestic/ Foreign); (iii) Obtain valid work permit and visa; (iv) Source of fund, occupation from employer/trade license etc. (v) Address through thanks letter/ utility bill /physical visit in case of entity. (3) Ensure reason of account opening; (4) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list before a/c opening; (5) Ensure Senior Management's Approval; (6) Follow Foreign Exchange Guidelines and Rules, 1947; (7) Apply EDD & ongoing transaction monitoring to reduce risk at acceptable level.
1.8	Loan/Investment Account	Very likely 5	Major 4	High 20	(1) Obtain complete & accurate information of loan customer from face to face interview & verify that; (2) Ensure purpose of loan; (3) Confirm repayment schedule; (4) Apply EDD & ongoing transaction monitoring to reduce risk at acceptable level.
2.0	Walk-in customer (beneficiary is government/ semi government/ autonomous body/ bank & NBF)	Unlikely 3	Minor 2	Low 6	(1) Confirm purpose of transaction & source of fund; (2) Obtain complete & accurate information of applicant & beneficiary i.e. KYC. (3) Obtain Phone/Cell no of Sender/ Applicant; (4) Make a call to check the authenticity of the given Cell no.
3.0	Walk-in customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBF)	Very likely 5	Major 4	High 20	Ensure threshold based CDD process as describe bellow: (1) Transaction up to-Tk =50 Thousand- (i) Obtain Name, Address and Phone/Cell no of Sender/ Applicant & Receiver/ Beneficiary. (ii) Make a call to check the authenticity of the given Cell no; (2) Transaction Tk above 50 Thousand-5 Lac- (i) Obtain Name, Address and Phone/Cell no of Sender/ Applicant & Receiver/ Beneficiary; (ii) Make a call to check the authenticity of the given Cell no; (iii) Obtain photo ID of Sender/ Applicant & Receiver/ Beneficiary; (iv) Verify NID from Election Commission Data Base; (v) Check UNSCRs, OFAC, EU and domestic sanction list. (3) Transaction Tk above 5 Lac- (i) Obtain KYC of Sender/ Applicant & Receiver/ Beneficiary (ii) Make a call to check the authenticity of the given Cell no; (iii) Obtain photo ID of Sender/ Applicant & Receiver/ Beneficiary; (iv) Verify NID from Election Commission Data Base; (v) Perform screening of the customer with UNSCRs, OFAC, EU and domestic sanction list

SI	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Banking Customer</i>					
4.0	Non-resident customer (Bangladeshi)	Very likely 5	Moderate 3	High 15	(1) Ensure reason for opening account; (2) Obtain necessary documents; (3) Perform Standard verification of KYC; (4) Check UNSCRs, OFAC, EU and domestic sanction list; (5) Follow Foreign Exchange Guidelines and Rules, 1947; (6) Do not allow transaction until identification of NRC (7) Apply EDD to reduce the risk at acceptable level
5.0	A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	Very likely 5	Major 4	High 20	(1) Ensure source of fund; (2) Confirm purpose of the transaction; (3) Verify transaction with nature of occupation/ volume of business; (4) Try to understand the KYCC; (5) Apply EDD & ongoing transaction monitoring; (6) If purpose of the transaction is not satisfactory and there is reason for suspicion, make STR to CCC.
6.0	A customer making series of transactions to the same individual or entity.	Very likely 5	Major 4	High 20	(1) Check transactions with his source of fund & TP given by the customer & supported documents; (2) Verify identification of the beneficiary; (3) Obtain explanation of such transaction & declaration of the relation with beneficiary from customer; (4) If purpose of the transaction is not satisfactory and there is reason for suspicion, make STR to CCC.
7.0	Customer involved in outsourcing business	likely 4	Moderate 3	Medium 12	(1) Perform ongoing transaction monitoring; (2) Ensure the nature of the outsourcing business. (3) Apply CDD measure.
8.0	Customer appears to do structuring to avoid reporting threshold	Very likely 5	Major 4	High 20	(1) Check TP with source of fund; (2) Monitor transaction for 2/3 months to identify structuring whether there is a matter of structuring or not; (3) Discuss with customer reason of such transaction; (4) If purpose of the transaction is not satisfactory and there is reason for suspicion, make STR to CCC.
9.0	Customer appears to have accounts with several banks in the same area	likely 4	Major 4	High 16	(1) Know the reason of opening several bank accounts from Customer; (2) Confirm source of fund; (3) If reason and source of fund are not clear & satisfactory, do not open account and submit SAR to CCC.
10.0	Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Very likely 5	Major 4	High 20	(1) Keep a close eye to Customer's activity. (2) Review KYC and confirm nature and quality of Customer's profession/business; (3) Ongoing transaction monitoring must be done; (4) Collect information from trusted source about Customer i.e. do EDD measure; (5) If there is any suspicion, make SAR to CCC.
11.0	Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Almost certain 6	Major 4	High 24	(1) Review KYC of customer; (2) Inform CCC/MANCOM about the Customer; (3) Do not allow transactions until risk is reduced.
12.0	Negative news about the customers' activities/ business in media or from other reliable sources	Almost certain 6	Major 4	High 24	(1) Review KYC & TP; (2) Check the transaction pattern, whether it is match with the profession/nature and volume of business of the Customer; (3) If there is any suspicious transaction send STR to CCC.

SI	Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer					
13.0	Customer is secretive and reluctant to meet in person.	Very likely 5	Major 4	High 20	(1) Meet customer in personally; (2) Physical visit the customer's place/business entity; (3) Keep transaction under close monitoring; (4) If transactions become suspicious make STR to CCC.
14.0	Customer is a mandate who is operating account on behalf of another person/ company	Very likely 5	Major 4	High 20	(1) Justify the reason for mandate; (2) Check the validity of mandate; (3) Obtain complete & accurate KYC of the mandate holder; (4) Obtain written confirmation from Mandatory; (5) Conduct CDD & ongoing transaction monitoring.
15.0	Large deposits in the account of customer with low income	Very likely 5	Major 4	High 20	(1) Obtain written declaration regarding large deposit amount with supporting valid document; (2) If the Customer fails to submit documents or submitted supporting documents are not sufficient and satisfactory Send STR to CCC.
16.0	Customers about whom BFIU seeks information (individual)	Very likely 5	Major 4	High 20	(1) Review and update KYC and information of the Customer; (2) Search media/ Other reliable sources if there is any negative news about the customer; (3) Conduct EDD & ongoing transaction monitoring.
17.0	A customer whose identification is difficult to check	Almost certain 6	Major 4	High 24	(1) Verify the identity of the customer from reliable sources / third party; (2) Perform physical verification by bank officials; (3) Conduct standard identification process; (4) If unable to do CDD for non-co-operation of the customer do not open account; (5) In case of existing account close the account with prior notice to the customer.
18.0	Significant and unexplained geographic distance between the bank and the location of the customer.	Very likely 5	Major 4	High 20	(1) Confirm the purpose of Opening account to the bank in a distance location of the customer; (2) If the purpose not clear and justified do not establish any business relationship.
19.0	Customer is a foreigner	likely 4	Major 4	High 16	(1) Apply Enhanced Due Diligence; (2) Ensure reason for opening account in Bangladesh; (3) Obtain complete KYC, Passport, Visa & work permit / agreement where necessary. (4) Verify source of fund. (5) Follow foreign exchange guideline and circulars of FEPD.
20.0	Customer is a minor	Unlikely 3	Moderate 3	Medium 9	(1) Perform CDD for minor and his guardians; (2) Obtain birth certificate as identity and keep record; (3) Obtain personal information of the beneficial owner (if any) (4) and perform CDD for BO; (5) Ascertain source of fund with supporting documents. (6) Do not allow transaction by guardians after 18 years of the minor.
21.0	Customer is Housewife	Unlikely 3	Minor 2	Low 6	(1) Perform CDD for both customer and beneficial owner; (2) Ensure purpose of opening account; (3) Declaration of source of fund with supporting documents.

SI	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Banking Customer</i>					
22.0	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	Very likely 5	Major 4	High 20	(1) Obtain Complete & accurate KYC, TP; (2) Perform standard identification verification process; (3) (Check UNSCRs OFAC, EU and domestic sanction list before a/c opening. (4) Obtain Senior Management's Approval/ CAMLCO's Approval; (5) Follow Foreign Exchange Guidelines and Rules, 1947; (6) Apply EDD & ongoing transaction monitoring to reduce risk at acceptable level.
23.0	Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Very likely 5	Major 4	High 20	(1) Identify beneficial owner(s) of the account; (2) Obtain their complete & accurate information.; (3) Verify source of fund and obtain supporting documents; (4) Perform ongoing transaction monitoring.
24.0	Customers doing significant volume of transactions with higher-risk geographic locations.	Almost certain 6	Major 4	High 24	(1) Obtain written explanation regarding such transaction from customer; (2) Verify KYC and confirm the business type, volume and nature; (3) TP whether it is consistent with the customer's business line and source of income; (4) Ensure purpose of transaction and justify with the nature of business; (5) Perform sanction screening of the customer with UNSCRs, OFAC, UN and domestic list (6) Monitor source of fund and transaction (7) If not satisfy terminate business relation with customer and submit STR to BFIU.
25.0	A customer who brings in large amounts of used notes and/or small denominations.	likely 4	Minor 3	Medium 12	Obtain written explanation from the customer regarding the condition and small denominations of notes which justify with the nature of business.
26.0	Customer dealing in high value or precious goods (e.g. jewel, gem and antique dealers and auction houses, estate agents and real estate brokers)	Very likely 5	Major 4	High 20	(1) Perform EDD. (2) Ensure ongoing transaction monitoring; (3) Identify source of fund & verify with given documents; (4) Obtain information of the customer from 3 rd party and reliable source (such as media, internet) ; (5) Obtain membership certificate from relevant trade authority. (6) Submit report to CCC if any suspicious.
27.0	Customer is a money changer/ courier service agent / travel agent	likely 4	Major 4	High 16	(1) Collect information about the customer from neutral & authentic e.g. media, peer group.; (2) Verify license from issuing authority; (3) Ensure source of fund with supporting documents; (4) Keep on-going transaction monitoring; (5) Follow foreign exchange guideline and circulars of FEPD (if necessary)
28.0	Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Very likely 5	Major 4	High 20	(1) Ensure EDD; (2) Collect information about the customer from authentic source; (3) Obtain license issued by proper authority; (4) Perform standard verification process; (5) Identify the source of fund with supporting documents; (6) Perform sanction screening of the customer with UNSCRs, OFAC, UN and domestic list; (7) Keep transaction under monitoring with TP.

SI no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Banking Customer</i>					
29.0	Customer is involved in Manpower Export Business	Very likely 5	Major 4	High 20	(1) Collect information about the customer from independent & authentic source; (2) Prepare KYC from submitted information; (3) Obtain license issued by Ministry of Expatriates, Welfare and Overseas Employment; (4) Obtain membership certificate of BAIRA; (5) Ensure purpose of transaction and source of fund; (6) Perform sanction screening of the customer with UNSCRs, OFAC, UN and domestic list; (7) Keep transaction under monitoring with TP.
30.0	Customer has been refused to provide banking facilities by another bank	likely 4	Major 4	High 16	(1) Perform enhance due diligence; (2) Ascertain the cause and Justification of refusal; (3) Obtain complete & correct KYC; (4) Obtain and verify ID such as NID/Passport/ birth certificate along with recent photo ID and valid driving license or other identification documents for the satisfaction of bank; (5) Confirm address by physical verification in case of entity/ utility bill; (6) Ensure source of fund from trade license, E-TIN or any other document.
31.0	Accounts opened before 30 April, 2002	likely 4	Moderate 3	Medium 12	(1) Update KYC & transaction profile ; (2) Mark as Dormant manually and in T24 Software using code 17 if not updated; (3) Allow deposit but must prohibit withdrawal until update the KYC & TP ; (4) Communicate with customer for updating
32.0	Customers with complex accounting and huge transaction	Very likely 5	Major 4	High 20	(1) Collect papers in support of income and accounting (i.e. balance sheet, sales register etc); (2) Monitor transaction and compare with source of fund.
33.0	Receipt of donor fund from foreign source by micro finance institute (MFI)	Very likely 5	Major 4	High 20	(1) Obtain Documents of donor fund and verify; (2) Collect information about the donor/donor agency; (3) Perform screening of the customer and donor/donor agency with UNSCRs OFAC, EU and domestic sanction list; (4) Obtain NGO Bureau/MFI permission; (5) Obtain certificate from regulatory authority, genuineness of source to be ensured; (6) Transaction to be monitored frequently; (7) Update registration to be obtained; (8) Must verify Beneficiary's KYC; (9) EDD must be applied.
34.0	Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source.	Very likely 5	Major 4	High 20	(1) Obtain complete and accurate KYC; (2) Obtain written statement whether the customer follow MLP Act 2012 and respective guideline as a reporting organization; (3) Do not open account if case of noncompliance.
35.0	Entity customer having operations in multiple location	likely 4	Moderate 3	Medium 12	(1) Obtain written explanation regarding the operation in various location; (2) Analyze the annual report/balance sheet of entity; (3) Keep the transaction under monitoring with TP.
36.0	Customer about whom BFIU seeks information (large corporate)	Very likely 5	Major 4	High 20	(1) Check whether there is any negative information about the customer in media/other reliable sources; (2) Keep their transaction under close monitoring with TP. (3) Update KYC and TP.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Banking Customer</i>					
37.0	Owner of the entity that are Influential Persons (IPs) and their family members and close associates	Very likely 5	Major 4	High 20	(1) Perform Enhanced Due Diligence. (2) Obtain approval from higher authority/ CAMLCO; (3) Keep transaction under close monitoring with TP; (4) Check whether the source of fund commensurate with the designation/profession.
38.0	A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	likely 4	Major 4	High 16	(1) Obtain information about the customer from public media or other reliable sources or peer group; (2) Visit the client's business premises. prepare call report and visit web-site; (3) Ensure CDD by obtaining necessary documents in support of identity apart from Trade License, Partnership Deed, Memorandum of Association, Article of Association, Certificate of Incorporation, Board Resolution, Form XII, by laws and source(s) of fund; (4) Identify the beneficial owner and obtain complete (5) & accurate information of beneficial owner; (6) Check whether TP of customer commensurate with the nature of business and transaction pattern; (7) Check cash flow statement (audited/unaudited), sales register and previous Bank statement.
<i>Wholesale Banking Customer</i>					
39.0	A Customer or group of customer making lots of transaction to the same individual or group (wholesale)	likely 4	Major 4	High 16	(1) Generate statement / report from system review transaction including on-line transaction. (2) Make sure that Transaction Profile (TP) provided by the customer is consistent with the nature of business and sources of funds supported by necessary documents; (3) Monitor the on line transaction exceeding the limits declared in the TP; (4) Obtain justification from the customer; (5) Obtain the purpose of transaction.
40.0	Owner of the entity that are Politically Exposed Persons (PEPs) or chief/senior officials of International Organizations and their family members and close associates.	Very likely 5	Major 4	High 20	(1) Conduct Enhance Due Diligence Obtain approval from CAMLCO before establishing relationship; (2) Keep transaction under monitoring with TP; (3) Follow foreign exchange guideline and circulars; (4) Check whether the source of fund commensurate with the designation.
41.0	Charity or NPOs (especially operating in less privileged areas).	Very likely 5	Major 4	High 20	(1) Perform EDD; (2) Identify beneficial owner of the account and obtain KYC of the beneficial owner; (3) Transaction shall be monitored & checked; (4) Source of fund must be confirmed; (5) Perform screening of the customer and donor/ donor agency with UNSCRs OFAC, EU and domestic sanction list; (6) Report to ML & TFPD if there is any suspicion.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Credit Card Customer</i>					
42.0	Customer who changes static data frequently	Very likely 5	Major 4	High 20	(1) Verify address & contact person verification (CPV) through third party; (2) Obtain documents in support of change information; Customer acknowledgement obtains by sending letter to old and new addresses; (3) Keep transactions under monitoring with TP.
43.0	Credit Card customer	likely 4	Major 4	High 16	(1) Collect required documents as per product program guideline (PPG) and bank policy; (2) Obtain Complete and accurate KYC; (3) Perform address & contact person verification through third party. (4) Check CIB report; (5) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list; (6) Check whether customer is already availing credit card.
44.0	Customer doing frequent transaction through Card (Prepaid & Credit card) and making quick adjustments	likely 4	Major 4	High 16	(1) Confirm source of fund & reason of adjustment; (2) Keep transactions under Monitoring If found suspicious, submit STR to ML & TFPD, HO.
45.0	Prepaid Customer	likely 4	Major 4	High 16	(1) Collect required documents as per product program guideline (PPG) and bank policy; (2) Obtain Complete and accurate KYC; (3) Perform address & contact person verification through third party. (4) Check CIB report; (5) Check whether customer is already availing credit card.
<i>International Trade Customer</i>					
46.0	A new Customer (Outward remittance through SWIFT)	likely 4	Moderate 3	Medium 12	(1) Ensure CDD, collect correct and complete information of the customer and required documents; (2) Verify NID, address and source of fund; (3) Perform screening of the customer with UNSCRs OFAC, EU and domestic sanction list; (4) Ensure the purpose of the remittance with supporting documents; (5) The remitting amount must be within the limit or approval of Bangladesh bank; (6) Obtain TM Form filled up by the remitter; (7) Follow foreign exchange guideline and FEPD circulars.
47.0	A new customer (Import/Export)	Very likely 5	Major 4	High 20	(1) Obtain all necessary document and ensure EDD; (2) Verify NID; (3) Perform screening of the customer and with UNSCRs OFAC, EU and domestic sanction list; (4) In case of old customer of other bank, Obtain certificate from previous Bank on -"no overdue or no outstanding bill of entry & NOC"; (5) Ensure the IRC/ERC issued mentioning the bank; (6) Verify IRC & ERC from respective issuing authority; (7) Follow Foreign Exchange guideline and FEPD circulars.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>International Trade Customer</i>					
48.0	A new customer (Inward remittance through SWIFT)	likely 4	Moderate 3	Medium 12	(1) Obtain complete and accurate KYC conduct CDD of beneficiary; (2) Verify NID; (3) Perform screening of the customer and sender with UNSCRs, OFAC, EU and domestic sanction list; (4) Obtain Form C for remittance equivalent to \$ 2000 and above; (5) Ensure the purpose of the remittance and relationship with the sender with supporting documents; (6) Remittance received against export should be certified and reported on EXP form; (7) Follow Foreign Exchange guidelines and FEPD circulars.
49.0	A new customer who wants to carry out a large transaction (Import/ Export)	Very likely 5	Major 4	High 20	(1) Conduct EDD; (2) Obtain no objection certificate from previous bank as —no overdue or no outstanding bill of entry; (3) Perform screening of the customer and seller/buyer of home and abroad sender with UNSCRs OFAC, EU and domestic sanction list; (4) New customer confirms that respective IRC & ERC issued mentioned Janata Bank Ltd; (5) Follow foreign exchange guideline and FEPD circulars.
50.0	A new customer who wants to carry out a large transaction (Inward/Out ward remittance)	likely 4	Moderate 3	Medium 12	(1) Ensure CDD & source of fund; (2) Check whether the transaction pattern matches with volume and nature of business; (3) Follow Foreign Exchange guideline and FEPD circulars.
51.0	A new customer who wants to conduct business beyond its line of business (Import/ Export)	Very likely 5	Major 4	High 20	(1) Ensure EDD. (2) Obtain permission from regulatory body(s); (3) Obtain justification from the customer regarding diversification of business; (4) If not satisfied do not conduct business with the customer and submit report to CCC.
52.0	Owner/director/shareholder of the customer is influential person(s) or their family members or close associates.	Very likely 5	Major 4	High 20	(1) Conduct Enhance Due Diligence; (2) Obtain approval from CCC before establishing relationship.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>International Trade Customer</i>					
53.0	Correspondent Banks	Very likely 5	Major 4	High 20	(1) Follow BFIU circulars no.-26 dated 16.06.2020 while establishing relationship; (2) Obtain sufficient information to understand fully the nature of business of the correspondent/ respondent bank; (3) Collect publicly available information such as from Bankers Almanac; (4) Review KYC periodically; (5) Obtain Financial position of the respective correspondent Bank; (6) Confirm whether the proposed Bank is not a any shell as because Correspondent Relationship with any shell Banks strongly prohibited by International Standard setter as well as BFIU; (7) Check the proposed correspondent bank's name with the UNSCR, EU, OFAC Sanction list and any other list by the competent authorities; (8) Other Safety & Security Measures must be taken.
54.0	Money service businesses (remittance Houses ,exchange houses)	Very likely 5	Major 4	High 20	(1) Must be perform EDD; (2) The remitting amount must be within the limit of individual; (3) Number of transaction in a month should be monitored; (4) Perform Sanction screening both the remitter & beneficiary with UNSCRs, EU, OFAC and domestic list; (5) Ensure that no Export/Import proceed remitted through MSBs as per Guidelines for Foreign Exchange Transaction Volume-1, APP 6/2 sec-3(xviii) and Report to CCC if there is any suspicion; (6) Other AML/CFT rules & Regulation Related to this business must be ensured.

2. Risk Register for Products & Services

(All the products and services of the bank has been included here)

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Banking Product</i>					
1	Accounts for students where large amount of transactions are made (student file)	likely 4	Moderate 3	Medium 12	(1) Perform CDD for student, guardian (if minor) and beneficial owner (BO); (2) Birth certificate shall be obtained as identity proof (for minor); (3) Obtain documents in support of source of fund that is commensurate with TP.
2	Gift Cheque				Not Applicable
3	Locker Service	Very likely 5	Major 4	High 20	(1) Ensure customer's maintaining an account with the bank; (2) Perform CDD of the link account; (3) Update KYC annually; (4) Monitor customer's activity.
4	Foreign currency endorsement in Passport	Un Likely 3	Minor 2	Low 6	(1) Obtain TM form duly filled up by the customer; (2) Obtain copy of P.P, visa, confirm air ticket; (3) In case of walk-in customer complete KYC; (4) Endorse as per foreign exchange guideline and FEPPD circulars.

Sl n	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Banking Product</i>					
5	Large transaction in the under privileged people	Very likely 5	Major 4	High 20	(1) Perform CDD; (2) Ensure source of fund & object/reason of transaction; Justify the purpose of transaction; (3) If not satisfied raise STR.
6	FDR (less than 2 million)	likely 4	Moderate 3	Medium 12	Ensure source of fund with supporting documents.
7	FDR (2 million and above)	Very likely 5	Major 4	High 20	(1) Check whether the customer is maintaining multiple FDRs with the Bank. (2) Check the source of fund; (3) If suspicious submit STR.
8	Special scheme deposit accounts opened with big installment and small tenure	Un Likely 3	Minor 2	Low 6	Obtain document in support of source of fund.
9	Multiple deposit scheme accounts opened by same customer in a branch	Un Likely 3	Minor 2	Low 6	Obtain document in support of source of fund.
10	Multiple deposit scheme accounts opened by same customer from different location	Very likely 5	Major 4	High 20	(1) Confirm KYC and perform CDD; (2) Scrutiny ,monitoring source of fund; (3) If suspicious raise STR. (4) Obtain written statement from customer about the reason in multiple location.
11	Open DPS in the name of family member Or Installments paid from the account other than the customer's account	Likely 4	Moderate 3	Medium 12	(1) Identify beneficial owner and obtain complete & accurate information; (2) Justify the purpose of opening deposit scheme in the (3) name of family member; (4) Check other relationship of the customer with the bank and keep the transaction under monitoring.
12	Early encashment of FDR, special scheme etc.	Likely 4	Moderate 3	Medium 12	Obtain declaration of specific reason of early encashment.
13	Non face to face business relationship/transaction	Very likely 5	Major 4	High 20	(1) Collect data/information/documents/of the clients from a reliable & independent source& ensure EDD; (2) Verify authentication of the above data/information; (3) Conduct ongoing transaction monitoring of the account; (4) Submit STR to ML & TFPD if any transaction found suspicious.
14	Payment received from unrelated/un-associated third parties	Very Likely 5	Major 4	High 20	(1) Collect evidence of actual relationship or reason for such receipt; (2) If found any unusual matter submit SAR to ML & TFPD ; (3) Don't allow transaction until risk is reduced; (4) Do proper KYC and collect standard ID and additional ID and perform EDD.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Retail Privilege Facilities</i>					
15	Pre- Approved Credit Card with BDT 300K limit	Likely 4	Moderate 3	Medium 12	(1) Perform CDD; (2) Obtain document in support of source of fund.
16	Enhanced ATM cash withdrawal Limit BDT 100K	Very Likely 5	Major 4	High 20	(1) Obtain document in support of source of fund; (2) Complete KYC; (3) Obtain Written justification from the customer regarding the purpose of requesting high withdrawal limit from ATM.
<i>SME Banking Product</i>					
17	Want to open FDR where source of fund is not clear	Very Likely 5	Major 4	High 20	(1) Obtain document in support of source of fund. (2) If not satisfied, do not open FDR submit; (3) Perform EDD.
18	Early encashment of FDR	Likely 4	Mode rate 3	Medium 12	Obtain declaration of specific reason of early encashment.
19	Repayment of loan EMI from source that is not clear	Likely 4	Mode rate 3	Medium 12	Monitor transaction and check whether it matches with source of fund.
20	Repayment of full loan amount before maturity Risk	Likely 4	Mode rate 3	Medium 12	(1) Obtain the reason behind early adjustment of loan; (2) Ensure source of fund of repayment before early adjustment in writing.
21	Loan amount utilized in sector other than the sector specified during availing the loan.	Very likely 5	Major 4	High 20	Monitor the utilization of loan, if suspicious, raise STR.
22	In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	Very likely 5	Major 4	High 20	(1) Obtain document in support of source of fund; (2) If suspicious, raise STR;
23	Source of fund used as security not clear at the time of availing loan.	Very likely 5	Major 4	High 20	Ensure source of fund of FDR keeping as security before sanctioning loan.
<i>Wholesale Banking Product</i>					
24	Development of new product & service of bank	Very likely 5	Major 4	High 20	(1) Identify ML & TF risk of the product, assess the risk and devise action plan to treat the risk; (2) Obtain (by the concerned department) vetting from CCC.
25	Payment received from unrelated third parties	Likely 4	Major 4	High 16	(1) Receive payment only from the distributors agents and suppliers of the customer; (2) Complete short KYC of depositor/withdrawer; (3) Obtain the relationship of the parties; (4) Monitor transaction report regularly if any suspicion report submitted to MI & TFPD.
26	High Value FDR	Likely 4	Modera te 3	Mediu m 12	(1) Perform CDD; (2) Obtain supporting document of source of fund.
27	Term loan, SOD (FO), SOD (RE), SOD (G-work order), SOD (Garment), SOD (PO), Loan General, Lease finance, Packing Credit, BTB L/C	Likely 4	Major 4	High 16	(1) Obtain CIB report & perform CDD; (2) Prepare comprehensive credit memo; (3) Analyze customer's credit worthiness; (4) Visit customer's office, factory and mortgaged properties; (5) Monitor use of fund.

SI no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
Wholesale Banking Product					
28	BG (bid bond), BG(PG), BG(APG)	Very Likely 5	Major 4	High 20	(1) Obtain CIB report & perform EDD; (2) Verify the work-order from concerned authority; (3) Ensure assignment of bill from concerned authority; Obtain margin & sufficient collateral.
29	L/C subsequent term loan, DP L/C	Likely 4	Moderate 3	Medium 12	(1) Ensure proper verification of price of the imported items from market; (2) Obtain certificate from the respective country's chamber of commerce; (3) Obtain undertaking from the customer regarding the fair price. (4) Verify all the relevant documents submitted by the customer.
30	C.C(H), SOD(G-Business), STL	Likely 4	Moderate 3	Medium 12	(1) Keep transactions under monitoring; (2) Ensure physical verification of sales register and stock report; (3) Verify the credit worthiness of the customer.
31	OBU (Offshore Banking Unit)	Very likely 5	Major 4	High 20	(1) Perform EDD; (2) Preserve the permission obtained by customer from competent authority; (3) Obtain information about the customer from market, media, web etc; (4) Obtain credit report of the customer; (5) Ensure that advance is allowed considering the category.
32	Syndication Financing	Very likely 5	Major 4	High 20	(1) Perform EDD. (2) Verify the value of plant & capital machinery and imported items; (3) Obtain certificate from the respective chamber of commerce. (4) Take undertaking from the customer regarding the price; (5) Lead Bank/ Participating Banks documentation to be obtained.
33	Supplementary Credit Card Issue	Very likely 5	Major 4	High 20p	(1) Collect required documents as Per Product Program Guideline(PPG) and bank's policy; (2) Ensure the relationship of supplementary cardholder with customer with supporting document; (3) Perform complete and accurate KYC; (4) Collect & check CIB report; (5) Verify address & contact number; (6) UNSCR sanction list check; (7) Check whether customer is already availing bank credit card; (8) Keep transaction under monitoring.
Credit Card					
34	Frequent use of Card Cheque	Very likely 5	Major 4	High 20	(1) Obtain the purpose of transaction; (2) Obtain relationship with the account holder the account where the fund is transferred; (3) Keep transaction under monitoring; (4) Update KYC annually.
35	BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)	Very likely 5	Major 4	High 20	(1) Allow the facility only to renowned and selected Merchants; (2) Conduct EDD.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<i>Credit Card</i>					
36	Credit card issuance against ERQ and RFCD accounts	Very likely 5	Major 4	High 20	(1) Collect required documents as Per Product Program guideline (PPG) and bank's policy; (2) Obtain complete and accurate KYC; (3) Collect & check CIB report; (4) Verify address & contact number ; (5) Check the name of customer with the UNSCR, EU, OFAC Sanction list and any other list by the competent authorities; (6) Check whether customer is already availing bank credit card; (7) Ensure that transactions are conducted as per Foreign Exchange guideline & FEFD circulars.
<i>International Trade</i>					
38	Line of business mismatch (import/export/remittance)	Very likely 5	Major 4	High 20	(1) Check the business diversification; (2) Obtain complete and correct KYC; (3) Perform EDD and verification of standard & additional ID; (4) Perform ongoing monitoring & reviewing of transaction; (5) want to know the explanation of the customer regarding export/import of the item that is not in line with his business; (6) If the explanation of the customer is not satisfactory/ rational reject the transaction & submit SAR; (7) Comply regulations of AML/CFT Act & rules;
39	Under/Over invoicing (import/export/remittance)	Very likely 5	Major 4	High 20	(1) Perform EDD; (2) Collect information of the exporter /importer; (3) Check the unit price of the product intended for import and export with the present market price & quantity with standard rate of commodities. (4) Follow Bangladesh Bank's guidelines/circulars; (5) If found suspicious, reject/suspend transaction & submit SAR to ML & TFPD.
40	Retirement of import bills in cash (Import/export/remittance)	Likely 4	Moderate 3	Medium 12	(1) Check the size of the transaction with customer's cash flow; (2) Perform EDD.
41	Wire transfer	Very likely 5	Major 4	High 20	(1) Ensure complete and accurate KYC or meaningful information of Applicant & Beneficiary; (2) Preserve purpose /reasons of transfer as per BFIU Cir-26 dt 16.06.2020.
42	Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)	Very likely 5	Major 4	High 20	(1) Confirm the purpose of remittance by valid supporting documents; (2) Obtain information of applicant and beneficiary; (3) Ensure the relationship of applicant and beneficiary with supporting document; (4) In case of insufficient originator information collect that information from ordering bank/exchange house through mutual communication; (5) If the information is insufficient and the relationship between the remitter and beneficiary and purpose of remittance is not clear/ satisfactory/ rational or found suspicious, reject /suspend transaction & submit SAR to ML & TFPD. as per BFIU Cir-26, dt-16.06.2020. (6) Follow Bangladesh Bank's guidelines/circulars;

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

Sl no	Risk	Likelihood	Impact	Risk core	Treatment/Action
1	Online (multiple small transaction through different branch)	Likely 4	Moderate 3	Medium 12	(1) Obtain accurate KYC of Applicant & Beneficiary; must be ensured CDD and standard verification; (2) Generate report of on-line transaction and monitor; (3) Confirmation of transaction must be ensured; (4) If there is any suspicious, report to ML & TFPD.
2	BEFTN	Likely 4	Moderate 3	Medium 12	(1) Obtain relationship with customer & beneficiary and purpose of fund transfer; (2) CDD must be ensured and ensure that customer executes transaction as per agreement; (3) Safety & Security measure like monitoring transaction pattern; (4) Update TP and track of deposit volume must be taken.
3	BACH	Likely 4	Moderate 3	Medium 12	(1) CDD & EDD must be ensured (2) Transaction Profile must be monitored. (3) If found mismatch submit STR to ML & TFPD. (4) Safety & Security measure must be taken.
4	IDBP	Very likely 5	Major 4	High 20	Must be performed CDD and check the genuineness of the LC and acceptance from BB dashboard.
5	Mobile Banking	Very likely 5	Major 4	High 20	Not Applicable
6	Third party agent or broker	Very likely 5	Major 4	High 20	Not Applicable
Credit Card					
7	New Merchant sign up	Unlikely	Minor		Not Applicable
8	High volume transaction through POS	Very likely 5	Major 4	High 20	Not Applicable
Alternate Delivery Channel					
9	Large amount withdrawn from ATMs	Very likely 5	Major 4	High 20	(1) Generate Report on high value ATM transactions from the system and monitor the transaction whether not exceed sanction limit. (2) If occurs report to /ML & TFPD as suspicious. (STR) and inform issuer bank and the cards payment Association until risk reduced. (3) Other Safety & Security Measures must be taken as per transaction restriction policy.
10	Larger amount transaction from different location and different time(mid night) through ATM	Very likely 5	Major 4	High 20	(1) Not allow transaction above sanction limit or reduce the risk to acceptable level. (2) Generate report on high value (3) ATM transactions along with time from the system and monitor the transaction. (4) To monitor transactions, Sensitive CDD and other safety, security measures must be taken. (5) If found suspicious raise STR.

Sl no	Risk	Likelihood	Impact	Risk Score	Treatment/Action
Alternate Delivery Channel					
1.09	Large amount of cash deposit in CDM	Very likely 5	Major 4	High 20	Not yet Applicable
1.10	Huge fund transfer through internet	Very likely 5	Major 4	High 20	Not yet Applicable
1.11	Transaction Profile updated through Internet Banking	Very likely 5	Major 4	High 20	Not yet Applicable
1.12	Customer to business transaction-Online Payment Gateway -Internet Banking International Trade	Very likely 5	Major 4	High 20	Not yet Applicable
1.13	Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Very likely 5	Major 4	High 20	(1) Obtain purpose of the remittance from the customer and check whether the transaction meets the central bank guideline/circular; (2) Should conduct adequate CDD measures to reduce the risk.
1.14	Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103) .	Very likely 5	Major 4	High 20	1) Obtain C form before release of remittance. 2) Conduct adequate CDD measures to reduce the risk.

4. Risk Register for Country/jurisdiction

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
1	Import and export from/to sanction country	Almost Certain 6	Major 4	High 24	1) Perform sanction screening to reduce the risk to acceptable level. 2) Do not allow transaction until delisting from Sanction and inform CCC immediately.
2	Transshipments, container, flag vessel etc. under global sanction	Almost Certain 6	Major 4	High 24	1) Perform sanction screening reduce the risk to acceptable level and inform CCU immediately. 2) If any sanction imposed, do not allow transaction or shipment until confirmation & delisting from global sanction.
3	Establishing correspondent relationship with sanction bank and/or country	Almost Certain 6	Major 4	High 24	1) Perform sanction screening and inform CCC immediately. 2) Do not establish correspondent relationship until delisting from sanction.

SI	Risk	Likelihood	Impact	Risk score	Treatment/Action
4	Establishing correspondent relationship with poor AML & CFT practice country	Very likely 5	Major 4	High 20	(1) Ensure the specific purpose for establishing correspondent relationship; (2) Obtain KYC from the correspondent bank.; (3) Apply appropriate EDD measures; (4) Perform detailed assessment reports of effective AML/ CFT systems.
5	Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas	Almost Certain 6	Major 4	High 24	(1) EDD must be ensured. (2) Do not established any relationship or any transaction until reduce the risk to acceptable level.
6	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.	Almost Certain 6	Major 4	High 24	(1) Do not allow any transaction and freeze the account. (2) STR must be reported to BFIU as early as possible to mitigate the risk.
7	Customer belongs to High Risk ranking countries of the Basel AML index.	Almost Certain 6	Major 4	High 24	(1) Do not allow any transaction (2) STR must be reported to BFIU as early as possible to mitigate the risk as acceptable level. (3) Perform EDD also.
8	Customer belongs to the countries identified by the bank as higher-risk because of its prior experiences or other factors.	Almost Certain 6	Major 4	High 24	(1) Perform EDD; (2) Ensure purpose of transaction ; (3) Do not allow any transaction & reduce the risk to acceptable level by conducting regular monitoring & scrutiny.
9	Any country identified by FAT For FSRBs-(FATF style Regional Body) as not having adequate AML&CFT systems	Almost Certain 6	Major 4	High 24	Do not accept as customer until adequate AML/CFT system is complied.
8	Any bank that provide service to 'Shell Bank'	Almost Certain 6	Major 4	High 24	Do not establish any relationship & do not allow any transaction /service to shell bank.
9	Any bank that allow payable through account	Very likely 5	Major 4	High 20	(1) CDD must be ensured; (2) Do not allow Corresponding accounts to made any transaction by third parties on their behalf.
10	Any country identified as destination of illicit financial flow	Almost Certain 6	Major 4	High 24	(1) Strong CDD & EDD measures should be maintained; (2) Ensure the origin of fund flow either illicit or not; (3) Do not allow transaction to occur until the risk to acceptable level.
11	Branches in a Border Area	Very likely 5	Major 4	High 20	(1) Must review & update KYC of accounts in shorter interval than other areas. (2) Monitor high risk accounts transactions specially cash deposit and online transactions. (3) Perform EDD and do proper KYC and check standard ID.
12	Area identified as high risk in the National Regulatory Authority (NRA) .	Very likely 5	Major 4	High 20	Monitor the effectiveness of and compliance with its internal AML/CFT systems and procedures as per BFIU instructions.

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
13	Countries subject to UN embargo /sanctions	Almost Certain 6	Major 4	High 24	(1) If there is any existing customer immediately stop transaction and inform BFIU; (2) Do not establish new business /customer; (3) In case of existing Customer stop transaction immediately and inform ML & TFPD to submit STR to BFIU.
14	Countries subject to BD embargo /sanctions (Israel, Taiwan)	Almost Certain 6	Major 4	High 24	(1) If there is any existing customer immediately stop transaction and inform BFIU; (2) Do not establish new business /customer; (3) In case of existing Customer stop transaction immediately and inform ML & TFPD to submit STR to BFIU.

5. Register for Regulatory Risk

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
1	Not having AML/CFT guideline	Very likely 5	Major 4	High 20	Develop bank's own AML/CFT guideline and update the guideline from time to time.
2	Not forming a Central Compliance Committee (CCC)	Very likely 5	Major 4	High 20	Incorporate formation and TOR of CCC in guideline and constitute CCC as per the requirement of BFIU.
3	Not having an AML&CFT Compliance Officer	Very likely 5	Major 4	High 20	Must nominate AML/CFT Compliance Officer as per the requirement of BFIU.
4	Not having Branch Anti Money Laundering Compliance Officer	Very likely 5	Major 4	High 20	(1) CCC will nominate Branch Anti Money Laundering Compliance Officer (BAMLCO) as per instruction of BFIU; (2) Must mention TOR and duties and responsibility of the BAMLCO in the nomination order.
5	Not having an AML & CFT program	Very likely 5	Major 4	High 20	Develop and review AML/CFT program from time to time.
6	No senior management commitment to comply with MLP and AT Act	Very likely 5	Major 4	High 20	(1) In AML & CFT Policy guideline provision of commitment of senior management to be included. (2) Communicate the senior management commitment with all bank officials every year at 1 st week of the year.
7	Failure to follow the AMLD /BFIU circular, circular letter, instructions etc.	Very likely 5	Major 4	High 20	AMLD/BFIU Circular/circular letter, instructions have to followed from time to time.
8	Unique account opening form not followed while opening account	Very likely 5	Major 4	High 20	Develop/revise account opening form for the bank Similar to unique account opening form prescribed by BFIU.

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
9	Non screening of new and existing customers against UNSCR Sanction and OFAC lists	Very likely 5	Major 4	High 20	(1) Ensure that all branches perform screening all new customers against UNSCR, OFAC and EU Sanction lists. (2) Perform quarterly basis screening of all existing customers against UNSCR, OFAC and EU Sanction lists by ML & TFPD, HO.
10	Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Very likely 5	Major 4	High 20	Bank follows the Foreign Exchange Regulation Act, 1947 while dealing with NRB account sit ensured.
11	Complete and accurate information of customer not obtained	Very likely 5	Major 4	High 20	Develop control mechanism to check that all branches (1) Obtain complete and accurate information of customer as per BFIU Circular-26, (2) If fails do not open or close existing account with prior notice to customer.
12	Failure to verify the identity proof document and address of the customer	Very likely 5	Major 4	High 20	Develop control mechanism to check whether branches (1) Verify the identity proof document with the support of database from concerned authority; (2) Verify address by sending thanks letter ; (3) Conduct CPV or physical verification by bank official; (4) Receive, record supporting document with AOF.
13	Beneficial owner identification and verification not done properly	Very likely 5	Major 4	High 20	Develop control mechanism to check whether branches are identify beneficial owner and obtain complete and accurate information of them as per BFIU Circular-26.
14	Customer Due Diligence (CDD) not practiced properly	Very likely 5	Major 4	High 20	Improve control mechanism to check whether branches as per BFIU Circular-26.
15	Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPs and influential person and senior official of international organization.)	Very likely 5	Major 4	High 20	Check whether Branches are (1) Obtaining Senior management's approval before opening high risk customers (such as IP) account; (2) Obtaining CAMLCO's approval before opening PEPs, family members and close associates of PEPs account; (3) Conducting both CDD & EDD for high risk customers as per BFIU Circular-26.
16	Failure to complete KYC of customer including walk in customer	Very likely 5	Major 4	High 20	Develop control mechanism to check that all Branches: (1) Prepare complete KYC of customer including walk-in-customer as per BFIU Circular -26; (2) Prepare complete KYC of walk-in-customer in case of occasional transaction i.e. transaction amount higher than 5 lac.

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
17	Failure to update TP and KYC of customer	Very likely 5	Major 4	High 20	Develop control mechanism to check that all branches must: (1) Review and update TP & for high risk account yearly and low risk account every five years; (2) Update KYC & TP any time for any change of address, profession, business, income etc. noticed by the customer with proper documents;
18	Keep the legacy accounts operative without completing KYC	Very likely 5	Major 4	High 20	Perform monitoring from CCC and ensure that (1)The braches updating KYC of legacy account; (2)Keeping as dormant the account of 19 which KYC not updated.
19	Failure to assess the ML & TF risk of a product or service before launching	Very likely 5	Major 4	High 20	Check whether (1)the ML & TF risk of a product or service has been assessed; (2)action plan devised to manage the same before launching the product or service (3)all the PPGS approved by CCC before launching.
20	Failure to complete the KYC of Correspondent Bank	Very likely 5	Major 4	High 20	(1)Complete the KYC of Correspondent Bank (2)Reciprocally update from time to time.
21	Senior Management approval not obtained before entering into a Correspondent Banking relationship	Very likely 5	Major 4	High 20	Obtain Senior Management and CAMLCOs approval before entering into a correspondent Banking relationship.
22	Failure to comply with the instruction of BFIU by bank Foreign subsidiary	Very likely 5	Major 4	High 20	Monitor the AML & CFT activity of foreign subsidiary and obtain confirmation from the subsidiary on compliance.
23	Failure to keep record properly	Very likely 5	Major 4	High 20	According to instruction of MLPA-2012 (amendments at 2015) & BFIU Cir-26 dated 16/06/2020 (1)The branches will preserve previous records of all transactions, both domestic and international of any close account for at least 5(five) years from the date of such closure; (2)the branches will preserve all information /documents of transaction made by Walk-in Customer up to 5 years; (3)the branches will preserve all information/documents of meeting, Audit & Inspection & Training.

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
24	Failure to report complete and accurate CTR on time	Very likely 5	Major 4	High 20	1) Branch level- <ul style="list-style-type: none"> • generate CTR statement from T-24 report portal; • ensure complete, exact no and proper posting of cash transaction as per BFIU instruction of the month within 7th of next month in jb Middleware for goAML web portal, • if there is no reportable cash transaction submit nil report • review the cash transaction to identify whether there is a suspicious transaction ,if not found submit nil report while reporting the CTR ; • if any suspicious transaction is found submit as suspicious transaction to ML & TFPD, HO. • preserve the hard copy of CTR for the review of any audit. 2) ML & TFPD, HO level- <ul style="list-style-type: none"> • ensure accuracy and conformity of the data after receiving CTR from the branches; • if found any error in the CTR mark that and ask for correction to related Area Offices of the branches; • prepare XML file of the CTR received from all branches; • upload complete and accurate CTR of the month within 21st of next month to goAML web portal of BFIU; • review all cash transaction received from branches to search whether there is a suspicious transaction, if found any suspicious transaction submit as STR to BFIU. • preserve the information related to cash transaction report up to 5 years from the month of submission to BFIU.
25	Failure to review CTR	Very likely 5	Major 4	High 20	1) Monitor and review the transactions reported as CTR both branch & ML & TFPD on monthly basis; 2) if any suspicious transaction is found submit as suspicious transaction BFIU.
26	Failure to identify and monitor structuring	Very likely 5	Major 4	High 20	(1) Generate structuring report from T24 report portal monthly basis; (2) Analyze and Identify structuring if any; (3) Perform transaction monitoring of the suspected; (4) If it is done repeatedly and not rational with the profession/business volume, submit STR to ML & TFPD.
27	Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Very likely 5	Major 4	High 20	(1) Generate high value transaction report from T24 report portal; (2) Check TP Violation report daily; (3) Generate structuring report from T24 report portal monthly basis; (4) manually verify the transactions with TP, business volume or activities of customers; (5) If any transaction found as suspicious report to ML & TFPD as STR.
28	Failure to conduct quarterly meeting properly	Unlikely 3	Minor 2	Low 6	Conduct quarterly meeting at branch in line with the agenda and instruction of BFIU Circular-26 and send the minutes to ML & TFPD properly.

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
29	Failure to report suspicious Transactions (STR)	Very likely 5	Major 4	High 20	(1) As per definition of STR in MLPA-2012, AT Rules 2013, & BFIU Cir-26 dated 16/06/2020, the branches will perform ongoing monitoring of transaction and activity of the customer on risk based approach; (2) Analyze system generated structuring report; (3) Analyze CTR both branch & ML & TFPD on monthly basis; (4) If there is any suspicious findings report to ML & TFPD.
30	Failure to conduct self assessment properly	Unlikely 3	Minor 2	Low 6	(1) All the branch must prepare self-assessment report to evaluate themselves on half yearly basis using Check list (Annexed-GA) of BFIU Cir-26 dated 16/06/2020; (2) Conduct a meeting presided over by the branch manager with all concerned officials of the branch to identify problems if any before preparing of self-assessment report; (3) Take reasonable measure to solve the identified problems and finalize the report with recommendations and submit to concern Area Office; (4) In the subsequent quarterly meetings on AML/CFT, the branch should have discussed the progress of the related matters; (5) The Area Office after getting self-assessment report from the branches under their control will submit all the report in a bundle to ML & TFPD, HO; (6) ML & TFPD, Ho will cross examine the self-assessment report of the branches with ITP& inspection report received from Audit & Inspection Dept. HO prepare a consolidated report with recommendation, and submit the report to BFIU after getting approval of CEO& MD of the bank; (7) Compliance report must be completed to reduce risk.
31	Failure to submit statement/ report to BFIU on time	Unlikely 3	Major 4	Medium 12	(1) As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020, submit the reports/statements to BFIU timely; (2) Check the reporting records at the time of inspection; (3) Comply the instructions of BFIU for submission of returns to reduce risk.
32	Submit erroneous statement/ report to BFIU	Very likely 5	Major 4	High 20	(1) As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020, check seriously the statement/ report before send to BFIU; (2) Follow and implement the instructions of BFIU to reduce risk.
33	Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Almost certain 6	Major 4	High 24	(1) Possible this could happen and/or have serious consequence. As per MLPA-2012, ATA 2009, Rules-2013, BFIU Circular-26 dated 16/06/2020, must comply the order for freezing or suspension of transaction issued by BFIU or BB instantly; (2) CCU must check the compliance of above order either branch implemented or not .

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
34	Not submitting accurate information or statement sought by BFIU or BB.	Very likely 5	Major 4	High 20	As per MLPA-2012, ATA 2009, Rules-2013, BFIU Circular-26 dated 16/06/2020, provide accurate information & returns sought by BFIU/BB timely to reduce risk.
35	Not submitting required report to senior management regularly	Unlikely 2	Moderate 3	Low 6	It has moderate consequence. As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020, submit all the report to Senior management on time & complied instructions Of BFIU to reduce risk.
36	Failure to rectify the objections raised by BFIU or bank inspection teams on time	Very likely 5	Major 4	High 20	(1) As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020,CCU must monitor /follow up to rectify or regularize the objections/irregularities raised by BFIU or BANK inspection team. (2) Compliance report must submit timely to reduce risk.
37	Failure to obtaining formation during wire transfer	Likely 4	Major 5	High 20	(1) Possible this could happen and /or have major consequence. As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020, must obtain information during wire transfer based on the threshold . (2) Inspection team must check compliance status during audit. (3) Follow the rules in case of wire transfer to reduce risk.
38	Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely 4	Major 5	High 20	As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020, must comply the instructions of the responsibilities of ordering, intermediary and beneficiary bank to reduce risk.
39	Failure to scrutinize staff Properly	Unlikely 3	Major 4	Medium 12	(1) As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020, Human Resource Division of the bank must follow the KYE procedures and to screen the staff's information before recruitment; (2) Must check the Code of Conduct rules as per service rules to reduce risk.
40	Failure to circulate BFIU Guidelines and circulars to branches	Unlikely 3	Major 4	Medium 12	(1) Possible this could happen and /or have moderate consequence. As per MLPA-2012 & Rules-2013, BFIU Circular-26 dated 16/06/2020, CCU must inform or issue guidelines, Circulars/ Circular letters to all branches to update themselves; (2) All instructions of BFIU must be complied & implemented to reduce risk.

Sl no	Risk	Likelihood	Impact	Risk score	Treatment/Action
41	Inadequate training/ Workshop arranged on AML & CFT	Unlikely 3	Major 4	Medium 12	(1) As per MLPA-2012 & Rules-2013 , BFIU BFIU Circular-26 dated 16/06/2020, Arrange workshop/training program on AML/CFT for all employees to build up awareness, conduct and compliance , procedures with evaluation test; (2) Check whether all staffs/employees aware of AML/CFT policy, procedures, legal requirements, own statutory obligation sand handling of suspicious transactions or not; (3) Bank will also maintain training records properly on yearly basis to reduce risk.
42	No independent audit function to test the AML program	Unlikely 3	Major 4	Medium 12	As per BFIU Circular-26 dated 16/06/2020, All Head office/ Divisional /Zonal office inspection team including CCC examine the AML/CFT program and conduct AML system Checking inspection including independent testing procedures (ITP) to branches independently for reduce risk.
43	Failure to detection of Trade Based ML and reporting of suspicious activity to BFIU	Almost certain 6	Major 4	High 24	(1) As per MLPA-2012 &ATA(2009), AML & AT - Rules-2013 , BFIU Circular-26 dated 16/06/2020, and Foreign Exchange Act-1947 to follow the instructions & verify the market price, quality of goods & HS codes. (2) Genuine L/C and foreign exchange policy & rules of Trade Based ML must be complied to reduce the risk. (3) Follow Guidelines for Prevention of Trade Based Money Laundering issued by BFIU Circular no-24 dt.10/12/2019 & Janata Bank.

Annexure- C
KYC Documentation

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
<p>Individuals & Joint Account (including illiterate person, pardanashin ladies, minor & guardian)</p> <p>Key issue: Name Source of Fund Address Telephone</p>	<ol style="list-style-type: none"> 1. Passport 2. National Id Card 3. Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) 4. Valid driving license (if any) 5. TIN (if any) 6. Any other documents that satisfy to the bank. <p>NB: It is mandatory to provide at least one document mentioned in serial no. 1 to 3. But in case of submitting the birth registration certificate, any other photo id (issued by a Government department or agency) of the 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. That certificate must include a photo which is duly attested by the signing renowned person. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.</p>	<ul style="list-style-type: none"> • Salary Certificate • (for salaried person). • Employed ID (For ascertaining level of employment). • Self-declaration acceptable to the bank. (commensurate with declared occupation) • 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 • TIN (if any) • Documents of property sale. (if any) • Other Bank statement (if any) • Document of FDR encashment (if any) • Document of foreign remittance (if any fund comes 	<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). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency

	<p>**Here renown person refers to member of parliament, Mayor, Deputy Mayor and Councilors of the City Corporation, Gazetted Officials of 9th grade and above as per National Pay Scale, Teachers of Public University, Chairman and Vice-Chairman of Upazilla Parishad, Chairman of Union Parishad, Mayor and Councilors of Municipality, Professor of Private University, Principal of Private College, Head Master of Private High School, Editor of National Daily Newspaper Notary Public, Officials of 7th grade and above as per National Pay Scale of Semi-Autonomous/Autonomous/Government Entities and Officials of 9th grade and above as per National Pay Scale of Bangladesh Bank</p>	<p>from outside the country)</p> <ul style="list-style-type: none"> • Document of retirement benefit. • Bank Loan 	
--	--	---	--

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
<p>Sole Proprietorships or Individuals doing business</p> <p><u>Key issue:</u></p> <ul style="list-style-type: none"> • Shop name • Shop Address • Name of proprietor and 	<ul style="list-style-type: none"> • Passport of owner • National Id Card of owner • Birth Registration Certificate of owner (Printed copy, with seal & signature from the Registrar) • Valid driving license of owner (if any) • Credit Card of owner (if any) 	<ul style="list-style-type: none"> • Trade License • TIN • Self-declaration acceptable to the bank. (commensurate with nature and volume of business) • Documents of property sale. (if 	<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.

<p>residence address</p> <ul style="list-style-type: none"> • Telephone number • Source of Fund 	<ul style="list-style-type: none"> • 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. 	<p>injected any fund by selling personal property)</p> <ul style="list-style-type: none"> • Other Bank statement (if any) • Document of FDR encashment (if any fund injected by en-cashing personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan (if any) • Personal borrowing (if any) 	<ul style="list-style-type: none"> • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency.
---	---	--	--

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
<p>Partnerships Farms</p> <p><u>Key issue:</u></p> <ul style="list-style-type: none"> • Legal name • Address • Names of all Partners and their addresses • Telephone numbers of the firm and partners. 	<ul style="list-style-type: none"> • Partnership deed/ partnership letter • Registered partnership deed (if registered) • Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. • Passport of Partners • National ID Card of partners • Birth Registration Certificate of partners (Printed copy, with seal 	<ul style="list-style-type: none"> • Trade License • 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 en-cashing Personal FDR) 	<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

<ul style="list-style-type: none"> • Source of Fund 	<p>& signature from the Registrar)</p> <ul style="list-style-type: none"> • 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 comers, 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"> • 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"> • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency
--	--	--	--

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
<p>Private Limited Companies</p> <p><u>Key issue:</u></p> <ul style="list-style-type: none"> • Name of the company & Address • Principal place of business • Mailing address of 	<ul style="list-style-type: none"> • Passport of all the directors • National Id Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • List of directors • 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 	<ul style="list-style-type: none"> • A copy of last available financial statements duly authenticated by competent authority • Other Bank statement • Trade License • TIN • VAT registration • Bank loan 	

<p>the company</p> <ul style="list-style-type: none"> • Telephone /Fax number 	<p>Employees to transact business on its behalf.</p> <ul style="list-style-type: none"> • 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. 		
--	---	--	--

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
<p>Public Limited Companies</p> <p><u>Key issue:</u></p> <ul style="list-style-type: none"> • Name of the company & Address • Principal place of business • Mailing address of the company • Telephone /Fax number 	<ul style="list-style-type: none"> • Passport of all the directors • National Id Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form -XII • Resolution of the board 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 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by a professional accountant • Other Bank statement (if any) • Trade License • TIN • Cash flow statement • VAT registration • Bank loan • Any other genuine source 	

	<ul style="list-style-type: none"> • 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. 		
--	---	--	--

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Government-Owned entities	<ul style="list-style-type: none"> • 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) 	N/A	N/A

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
NGO	<ul style="list-style-type: none"> • National Id Card of the operator (s) • Passport of the operator (s) • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Documents of nature of the NGO • Certificate of registration issued by competent authority • 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 accountant. • Other Bank statement • TIN • Certificate of Grand / Aid 	

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Charities or Religious Organizations	<ul style="list-style-type: none"> • National Id Card of the operator (s) • Passport of the operator (s) • Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the Organizations • Certificate of registration issued by competent authority (if any) • Bye-laws (certified) • List of Management Committee/ Directors 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by a professional accountant • Other Bank statement • Certificate of Grant / Aid/ donation • Any other legal source 	N/A

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Embassies	<ul style="list-style-type: none"> • Valid Passport with visa of the authorized official • Clearance of the foreign ministry • Other relevant documents in support of opening account 	N/A	

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Clubs or Societies	<ul style="list-style-type: none"> • National Id Card of the operator (s) • Passport of the operator (s) • Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by a professional (if registered) • Other Bank statement 	

	<ul style="list-style-type: none"> • 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"> • Certificate of Grant / Aid • Subscription • If unregistered declaration of authorized person/ body. 	
--	---	---	--

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
<p>Trusts, Foundations or similar entities</p> <p><u>Key issue:</u></p> <ul style="list-style-type: none"> • Names of trustees, settlors, beneficiaries and signatories • Names and addresses of the founder, the managers /directors and beneficiaries • Telephone/fax numbers. 	<ul style="list-style-type: none"> • National Id Card of the trustee (s) • Passport of the trustee (s) • Resolution of the Managing body of the Foundation/Association to open an account and identification of those who have authority to operate the account. • 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 	

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
FC Account	<ul style="list-style-type: none"> • Photocopy of first 7 pages of valid passport with valid visa. • Signature in the account opening form/card must be same with the signature of the passport. • Copies of employer's certificate/work permit. 		

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Financial Institutions (NBFI)	<ul style="list-style-type: none"> • Passport of all the directors • National Id Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form -XII • Resolution of the board 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 	<ul style="list-style-type: none"> • A copy of last available financial statements duly certified by a professional accountant. • Other Bank statement • Trade License • TIN • VAT registration • Cash flow statement 	



Annexure- D

SUSPICIOUS TRANSACTION REPORT (STR)

(For Banks and Non Bank Financial Institutions)

A. Reporting Institution:

1. Name of the Bank

2. Name of the Branch

B. Details of Report:

1. Date of sending report

2. Is this the addition of an earlier report? Yes No

3. If yes, mention the date of previous report

C. Suspect Account Details:

1. Account Number

2. Name of the Account

3. Nature of the Account
(Current/savings/loans/others, pls specify)

4. Nature of Ownership:
(Individual/proprietorship/partnership/company/other, pls. specify)

5. Date of Opening:

6. Address:

D. Account holder details:

1. 1. Name of the account holder

2. Address

3. Profession

4. Nationality

5. Other account(s) number (if any)

6. Other business

7. Father's Name

8. Mother's Name

9. Date of birth

10. TIN

11. NID/Passport/ other doc. no.

12. Mobile Number

2. 1. Name of the account holder

2. Relation with the account holder mention in sl. No. D1

3. Address

4. Profession

5. Nationality

6. Other account(s) number (if any)

7. Other business

8. Father's Name	<input type="text"/>
9. Mother's Name	<input type="text"/>
10. Date of birth	<input type="text"/>
11. TIN	<input type="text"/>

E. Introducer Details:

1. Name of introducer	<input type="text"/>
2. Account number	<input type="text"/>
3. Relation with account holder	<input type="text"/>
4. Address	<input type="text"/>
5. Date of opening	<input type="text"/>
6. Whether introducer is maintaining good relation with bank	<input type="text"/>

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

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

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

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

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

H. Transaction Details:

Sl. No.	Date	Amount	Type*

*Cash/Transfer /Clearing /TT/etc.

Add paper if necessary



I. Counter Part's Details:

Sl. No.	Date	Bank	Branch	Account No.	Amount

J. Has the suspicious transaction/activity had a material impact on or otherwise affected the financial soundness of the bank?

Yes

No

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

L. Documents to be enclosed:

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

Signature:
(CAMLCO or authorized officer of CCC)
Name:
Designation:
Phone:
Date:

Annexure- E

COMMON INDICATORS OF SUSPICIOUS TRANSACTIONS

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

1. General Indicators

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

2. Intervene to Reporting or Record Keeping Requirements

- Client attempts to convince employee not to complete any documentation required for the transaction.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client seems very conversant with money laundering or terrorist activity financing issues.
- Client appears to be structuring amounts to avoid record keeping, client identification or reporting thresholds.
- Client appears to be collaborating with others to avoid record keeping, client identification or reporting thresholds.

3. Identity Documents

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

4. Cash Transactions

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Client uses notes in denominations that are unusual for the client, when the norm in that business is different.
- Client presents notes that are packed or wrapped in a way that is uncommon for the client.
- Client makes cash transactions of consistently rounded-off large amounts (e.g., BDT 100,000.00 BDT 500,000.00 etc.).
- Client consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Client presents uncounted fund for a transaction. Upon counting, the client reduces the transaction to an amount just below that which could trigger reporting requirements.
- Client conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Large transactions using a variety of denominations.

- Client asks the bank to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

5. Economic Purpose

- Transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities.
- Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the client.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- No business explanation for size of transactions or cash volumes.
- Transactions of financial connections between businesses that are not usually connected (for example, a food importer dealing with an automobile parts exporter).
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

6. Transactions Involving Accounts

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

- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.
- Frequent deposits in amounts just below BDT 10,00,000.00 which may be considered as structuring/smurfing.
- Regular return of cheques for insufficient funds.

7. Personal Transactions

- Client appears to have accounts with several financial institutions in one geographical area.
- Client has no employment history but makes frequent large transactions or maintains a large account balance.
- The flow of income through the account does not match what was expected based on stated occupation of the account holder or intended use of the account.
- Client makes frequent or large payments through online services.
- Client runs large positive credit card balances.
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Client frequently makes deposits to the account of another individual who is not an employer or family member.
- Client deposits large endorsed cheques in the name of a third-party.
- Client's access to the safety deposit facilities increases substantially or is unusual in light of their past usage.
- Many unrelated individuals make payments to one account without rational explanation.
- Third parties make cash payments or deposit cheques to a client's credit card.
- Client gives power of attorney to a non-relative to conduct large transactions.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Client acquires significant assets and liquidates them quickly with no explanation.
- Client requests movement of funds that are uneconomical.
- High volume of wire transfers is made or received through the account.

8. Corporate and Business Transactions

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

- Accounts are used to receive or disburse large sums but show virtually no normal business-related activities.
- Accounts have a large volume of deposits in drafts and electronic funds transfers, which is inconsistent with the client's business.
- Business does not want to provide complete information regarding its activities.

- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity.
- Financial statements of the business differ noticeably from those of similar businesses.
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them.
- Deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations.
- Client maintains a number of trustee or client accounts that are not consistent with that type of business or not in keeping with normal industry practices.
- Client pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments.
- Client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.
- Client makes a large volume of cash deposits from a business that is not normally cash-intensive.
- Client makes large cash withdrawals from a business account not normally associated with cash transactions.
- Client consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad.
- Unexplained transactions are repeated between personal and commercial accounts.
- Activity is inconsistent with stated business.

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

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

Annexure- F**KYC for Walk-in/One-off Customers**

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

Thank you for your co-operation

A. Personal Detail:

1. Name:
2. Occupation:
3. Nationality:
4. Father/Husband's name:
5. Date of birth:
6. Mother's name:
7. Phone/Mobile:
8. Ref No. (If Any):
9. Address:

B. Identification Detail:

1. NID Card number:
2. Passport details:

Photocopy Attached

Photocopy Verified

C. Transaction Detail:

1. Value of Transaction:
2. Source of Fund:
3. Purpose of Transaction:

D. Beneficiary/Remitter Detail:

1. Name:
2. Relation:
3. Address:
4. Phone/Mobile:
5. Account No. (if Any):

Date:

Signature

Janata Bank Limited
_____ Branch

Annexure- G

BAMLCO Nomination Form

1. Name of Officer/Executive: _____
2. Designation of Officer/ Executive: _____
3. Date of Joining in the Bank: _____ as _____
4. Date of Joining at the present Branch: _____
5. Number of training obtained regarding AML & CFT related issues: _____
6. Last date & place of training obtained: _____
7. Nominated officer/executive has experience in-
 - Ac opening & KYC maintenance
 - CTR analyzing
 - Local Remittance
 - Foreign Remittance (Inward, Outward)
 - Clearing, Batch Operation, Cheque Payments, Real Time Gross Settlement (RTGS)
 - Over all General Banking
 - Credit Operation
 - Foreign Exchange & International Trade
8. The nominated officer has sufficient knowledge on the following:
 - Money Laundering Prevention Act-2012 (with Amendment 2015)
 - Anti-Terrorism Act-2009 (with Amendment 2013)
 - AML Policy of Janata Bank Limited
 - Circulars issued by ML & TF Prevention Department
 - ML&TF Risk Management Guidelines of Janata Bank Limited
9. Whether the nominated officer/Executive is aware of Sanction Screening Criteria and capable to operate Sanction Screening System using existing software. YES NO
10. Whether the nominated officer/executive has knowledge regarding computer literature and capable of email communication. YES NO

11. Reformed BAMLCC Member Information:

Sl.	Name	Designation	Role/Responsibility
1.			BAMLCO
2.			GB In-Charge
3.			Credit In-Charge
4.			Foreign Exchange In-Charge
5.			A/C Opening Officer
6.			Others (Please Specify)

Manager/ Branch In charge

Annexure- H**Glossary****1. Anti-Money Laundering Program**

The system designed to assist the bank to fight against money laundering and terrorist financing. At a minimum, the anti-money laundering program should include:

- Written internal policies, procedures and controls;
- Designated AML compliance officer;
- On-going employee training; and
- Independent review to test the program.

2. Asia/Pacific Group on Money Laundering (APG)

The Financial Action Task Force (FATF)-style regional body consisting of jurisdictions in the Asia/Pacific Region.

3. Bangladesh Financial Intelligence Unit (BFIU)

Central national agency of Bangladesh responsible for coordinating the AML/CFT program of the country. It is situated inside Bangladesh Bank.

4. Beneficial Owner

The term beneficial owner has two different definitions depending on the context:

- The natural person who ultimately owns or controls an account through which a transaction is being conducted.
- The natural persons who have 20% and above ownership, as well as those who exercise ultimate effective control over a legal person or arrangement.

5. Beneficiary

The person (natural or legal) who benefits from a transaction, such as the party receiving the proceeds of a wire, a payout on an insurance policy.

6. Correspondent Banking

The provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Large international banks typically act as correspondents for hundreds of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers of funds, check clearing services, payable-through accounts and foreign exchange services.

7. Cross Border

Used in the context of activities that involve at least two countries, such as wiring money from one country to another or taking currency across a border.

8. Cash Transaction Report (CTR)

A report that documents a physical cash transaction that exceeds a certain monetary threshold. A CTR can also be filed on multiple currency transactions that occur in one day exceed the required reporting amount. According to BFIU instruction at present the threshold amount for CTR in Bangladesh is equal to BDT 10.00 lac or above or equivalent foreign currencies. CTRs is filed with BFIU in Bangladesh.

9. Customer Due Diligence (CDD)

CDD is the process of identifying the customers where relevant information about the customer is collected and evaluated for any potential risk for the organization or money laundering/terrorist financing activities. CDD includes not only establishing the identity of customers, but also establishing a baseline of account activity to identify those transactions that do not conform to normal or expected transactions.

10. Egmont Group of Financial Intelligence Units

The Egmont Group consists of a numerous national of financial intelligence units (FIUs) that meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the area of information exchange, training and the sharing of expertise. The goal of the group is to provide a forum for FIUs to improve cooperation in the fight against money laundering and the financing of terrorism, and to foster the implementation of domestic programs in this field.

11. Enhanced Due Diligence (EDD)

In conjunction with Customer Due Diligence (CDD), EDD calls for additional measures aimed at identifying and mitigating the risk posed by high risk customers. It requires to develop more information about the nature of the customer, the customer's business and understanding of the transactions in the account than a standard or lower risk customer.

12. Financial Action Task Force (FATF)

FATF was chartered in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy-making body that sets anti-money laundering standards and counter-terrorist financing measures worldwide. Thirty-seven countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. FATF develops annual typology reports showing current money laundering and terrorist financing trends and methods.

13. Know Your Customer (KYC)

Determination of the true identity of a customer and the type of activity that is "normal and expected," and to detect activity that is "unusual" for a particular customer.

14. Know Your Employee (KYE)

To acquiring a better knowledge and understanding of the employees of the bank for the purpose of detecting conflicts of interests, money laundering, past criminal activity and suspicious activity.

15. Money Laundering

The process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly- derived property or funds to make them appear legitimate. It usually involves a three-part system: **placement** of funds into a financial system, **layering** of transactions to disguise the source, ownership and location of the funds, and **integration** of the funds into society in the form of holdings that appear legitimate. The definition of money laundering varies in each country where it is recognized as a crime.

16. Monitoring

An element of anti-money laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed "normal and expected" for the customer.

17. Offshore

Literally, away from one's own home country, if one lives in Europe, Bangladesh is "offshore." In the money laundering context, the term refers to jurisdictions deemed favorable to foreign investments because of low or no taxation or strict bank secrecy regulations.

18. Payable Through Account

Transaction account opened at a depository institution by a foreign financial institution through which the foreign institution's customers engage, either directly or through subaccounts, in banking activities and transactions in such a manner that the financial institution's customers have direct control over the funds in the account. These accounts pose risks to the depository institutions that hold them because it can be difficult to conduct due diligence on foreign institution customers who are ultimately using the PTA accounts.

19. Politically Exposed Person (PEP)

According to FATF's revised 40 Recommendations of 2012, a PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates. The term PEP does not extend to middle-ranking individuals in the specified categories. Various country regulations will define the term PEP, which may include domestic as well as foreign persons.

20. Red Flag

A warning signal that should bring attention to a potentially suspicious situation, transaction or activity.

21. Risk-Based Approach

The assessment of the risks associated with different types of businesses, clients, accounts and transactions in order to maximize the effectiveness of an anti-money laundering program.

22. Shell Bank

Bank that exists on paper only and that has no physical presence in the country where it is incorporated or licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

23. Smurfing

A commonly used money laundering method, smurfing involves the use of multiple individuals and/or multiple transactions for making cash deposits, buying monetary instruments or bank drafts in amounts under the reporting threshold.

24. Structuring

Illegal act of splitting cash deposits or withdrawals into smaller amounts, or purchasing monetary instruments, to stay under cash reporting threshold.

25. Suspicious Activity

Irregular or questionable customer behavior or activity that may be related to a money laundering or other criminal offense, or to the financing of a terrorist activity. May also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities, or the normal level of activity for that kind of business or account.

26. Terrorist Financing

The process by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue-generating activities, some illicit, including smuggling and credit card fraud.

27. Tipping Off

Improper or illegal act of notifying a suspect that he or she is the subject of a Suspicious Transaction Report or is otherwise being investigated or pursued by the authorities.

28. Unusual Transaction

Transaction that appears designed to circumvent reporting requirements, is inconsistent with the account's transaction patterns or deviates from the activity expected for that type of account.



Janata Bank Limited

ML & TF Prevention Department

Head Office: 110, Motijheel C/A, Dhaka-1000, Phone: +88-02-9558386, Fax: +88-02-9564644

SWIFT: JANBDDDH, E-mail: aml@janatabank-bd.com, Website: www.jb.com.bd

PABX: 9560000, 9560039, 9566020, 9556245-49, 9560027-30, Ext: 549,205