



বাংলাদেশ কৃষি ব্যাংক  
ঝুঁকি ব্যবস্থাপনা বিভাগ  
প্রধান কার্যালয়, কৃষি ব্যাংক ভবন  
৮৩-৮৫, মতিঝিল বাণিজ্যিক এলাকা, ঢাকা

মানিলভারিং প্রতিরোধ সেল  
dcamlco@krishibank.org.bd  
Phone: ০২২২৩৩৮৪৪৮৬

প্রকা/(আরএমডি/অপারেশন-২)/বোর্ড/২০২৩-২৪/১২৬৮

তারিখ ০১-১০-২০২৩ খ্রীষ্টাব্দ

**বিষয় : BKB Money Laundering & Terrorist Financing Risk Management Guidelines-2023 জারীকরণ প্রসঙ্গে।**

সূষ্ঠ আর্থিক ব্যবস্থাপনা টেকসই অর্থনৈতিক সমৃদ্ধির অন্যতম প্রধান শর্ত। আর্থিক ব্যবস্থার সুস্থিত নিশ্চিত করতে সকল ধরনের আর্থিক লেনদেনকে শৃঙ্খতার পরীক্ষায় উত্তীর্ণ হতে হয়। এক্ষেত্রে মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে (AML/ CFT) পরিপালনীয় ব্যবস্থাদির কার্যকরী প্রয়োগ অতীব জরুরী।

০২। উক্ত মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রমে আন্তর্জাতিক মানদণ্ড, দেশে বিদ্যমান আইন এবং প্রযোজ্য বিধি ও নীতিমালা দক্ষতা ও স্বচ্ছতার সাথে অনুসরণ ও বাস্তবায়ন করতে হয়। আবার সময়ের প্রয়োজনে এ সম্পর্কিত আইন, বিধি ও নীতিমালা যুগোপযোগী করে হালনাগাদ কার্যক্রম জারী রাখাও একটি চলমান প্রক্রিয়া।

০৩। এ সম্পর্কিত বিএফআইইউ সার্কুলার নং-২৬ এর ১.১ এর নির্দেশনা নিম্নরূপ :


“মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে আন্তর্জাতিক মানদণ্ড, দেশে বিদ্যমান আইন, বিধিমালা ও বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশন ইউনিট (বিএফআইইউ) কর্তৃক জারীকৃত নির্দেশনাবলীর সমন্বয়ে প্রতিটি ব্যাংকের নিজস্ব নীতিমালা থাকবে; যা ব্যাংকের পরিচালক পর্ষদ বা প্রযোজ্য ক্ষেত্রে সর্বোচ্চ ব্যবস্থাপনা কমিটি অনুমোদন করবে। ব্যাংক উক্ত নীতিমালা সংশ্লিষ্ট সকলের অবগতিতে আনবে ও বাস্তবায়নের জন্য প্রয়োজনীয় পদক্ষেপ গ্রহণ করবে। এছাড়া ব্যাংক নিজস্ব ঝুঁকি ব্যবস্থাপনার অংশ হিসেবে সময় সময় নীতিমালাটি পর্যালোচনা করবে ও প্রযোজ্য ক্ষেত্রে, সংশোধন বা পরিমার্জন করবে।”

০৪। “BKB Money Laundering & Terrorist Financing Risk Management Guidelines-2023” উল্লিখিত পরিপালনীয় বাধ্যবাধকতার একটি বাস্তব প্রতিফলন। উল্লেখ্য, বিগত ১৫-০৩-২০২৩ তারিখে অনুষ্ঠিত বিকেবি পরিচালনা পর্ষদের ৮২৮তম সভায় গাইডলাইনটি অনুমোদিত হয়।

০৫। এ গাইডলাইন কেবলমাত্র অত্র ব্যাংকের কর্মকর্তা/কর্মচারীগণের দাপ্তরিক কাজে ব্যবহৃত হবে এবং এর বিষয়বস্তু প্রত্যক্ষ বা পরোক্ষভাবে জনসাধারণের মধ্যে প্রকাশ করা যাবে না। তবে সম্ভাব্য বা প্রয়োজনীয় ক্ষেত্রে এর অংশ বিশেষ প্রকাশ করা যেতে পারে।

০৬। এমতাবস্থায় “BKB Money Laundering & Terrorist Financing Risk Management Guidelines-2023” ব্যাংকের প্রধান কার্যালয়সহ মাঠপর্যায়ের সকল বিভাগ, কার্যালয় এবং শাখা কর্তৃক যথাযথভাবে অনুসরণ ও পরিপালনের জন্য জারী করা হলো।


অনুমোদনক্রমে,

  
০১.১০.২০২৩  
(আবু সাঈদ মো. রশাদুল হক)  
মহাব্যবস্থাপক (আন্তর্জাতিক ও হিসাব)  
এবং  
প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা (CAMLCO)

**সংযুক্তি : BKB Money Laundering & Terrorist Financing Risk Management Guidelines-2023**

**সদয় অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য অনুলিপি :**

- ০১। চীফ স্টাফ অফিসার, ব্যবস্থাপনা পরিচালক মহোদয়ের সচিবালয়, বিকেবি, প্রধান কার্যালয়, ঢাকা।
- ০২। স্টাফ অফিসার, উপব্যবস্থাপনা পরিচালক মহোদয়গণের সচিবালয়, বিকেবি, প্রধান কার্যালয়, ঢাকা।
- ০৩। স্টাফ অফিসার, সকল মহাব্যবস্থাপক মহোদয়ের দপ্তর, বাংলাদেশ কৃষি ব্যাংক।
- ০৪। অধ্যক্ষ (মহাব্যবস্থাপক), বিকেবি স্টাফ কলেজ, মিরপুর, ঢাকা।
- ০৫। সকল উপমহাব্যবস্থাপক/সচিব, বাংলাদেশ কৃষি ব্যাংক।
- ০৬। সকল বিভাগীয় নিরীক্ষা কর্মকর্তা, বাংলাদেশ কৃষি ব্যাংক।
- ০৭। সকল মুখ্য আঞ্চলিক/আঞ্চলিক ব্যবস্থাপক, বাংলাদেশ কৃষি ব্যাংক।
- ০৮। সকল আঞ্চলিক নিরীক্ষা কর্মকর্তা, বাংলাদেশ কৃষি ব্যাংক।
- ০৯। সকল শাখা ব্যবস্থাপক (মুখ্য আঞ্চলিক/আঞ্চলিক ব্যবস্থাপকের মাধ্যমে), বাংলাদেশ কৃষি ব্যাংক।
- ১০। নথি/মহানথি।

  
০১/১০/২০২৩  
(এফ এম এ রহিম)  
উপমহাব্যবস্থাপক  
এবং  
উপপ্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা (DCAMLCO)

# **MANAGING CORE RISK IN BANKING**

## **BKB MONEY LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT GUIDELINES-2023**



**Published by:  
Anti-Money Laundering (AML) Cell  
Bangladesh Krishi Bank  
Head Office  
83-85 Motijheel C/A  
Dhaka-1000, Bangladesh**

# FOCUS GROUP

---

**Advisor**

**Md. Shawkat Ali Khan**  
Managing Director

**Supervised & Guided By**

**Chanu Gopal Ghosh**  
Deputy Managing Director  
&  
CAMLCO

**Composed & Compiled By**

**F M A Rahim**  
Deputy General Manager  
Risk Management Department  
& DCAMLCO

**Muhammad Obaidul Akbar**  
Assistant General Manager  
Anti-Money Laundering Cell  
Risk Management Department

**Zannatara Ferdaush**  
Senior Principal Officer  
Anti-Money Laundering Cell  
Risk Management Department

**In Association with**

**Md. Mamunur Rashid**  
Deputy General Manager  
ICT System, Card & Mobile Banking Department

**Mohammad Moinul Islam**  
Deputy General Manager  
Credit Department

**Md. Akter Hossain**  
Deputy General Manager  
Loan Classification Department

**Md. Khorshed Anwar**  
Deputy General Manager  
Human Resource Management Department-1

**Md. Mostafizur Rahman**  
Deputy General Manager  
International Trade Department

**Khan Tamzid Ahmed**  
Deputy General Manager  
Central Accounts Department

**K M Habib-Un-Nabi**  
Deputy General Manager  
Branch Control & Business Development Department

**Md. Farid Hasan**  
Deputy General Manager  
ICT Operation Department

## Preface

Money Laundering and Terrorist Financing is a giant loophole at global & national level in terms of unscrupulous financial transactions causing huge losses in gross domestic product (GDP). It erodes financial system, degrades moral values, corrupt society which stamp bad impact on the country & the world. As a part of financial system, Bangladesh Krishi Bank (BKB) is pledged-bound & courageous enough to overthrow the threats in this regard for maintaining a sound, stable & vibrant moving-on of economy. The introduction of "BKB Money Laundering and Terrorist Financing Risk Management Guidelines-2023" is a part of this endeavor.

Now-a-days, every deed is considered to be a successful one provided it is sustainable. The sustainability depends on how much compliance it has maintained while completing the assigned job. Prevention of money laundering & terrorist financing is the key compliance to all financial transactions without which the economy gradually moves forward to self-annihilation. Human resources and methodologies relating to Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) must be well equipped with technological know-how to cope up with the challenges. And those efforts are required to be evaluated at a certain interval with time-befitting effective measures.

I hope "BKB Money Laundering and Terrorist Financing Risk Management Guidelines-2023" would be a major step to fight for AML/CFT. Along with this, we are to be upgraded with related laws, regulations, circulars responding to the call of time. My heartfelt thanks to all concerned associated with the effort for introducing this guideline. It would be an effective venture when the guideline is to be followed prudently for the benefit of BKB.

I would like to seek cordial cooperation from all to play an active role for promoting a transparent financial system with outmost sincerity, honesty & courage.



Md. Shawkat Ali Khan  
Managing Director



**Md. Nasiruzzaman**  
Chairman  
Board of Directors  
Bangladesh Krishi Bank

## Message

Money Laundering & Combating the Financing of Terrorism (AML & CFT) is a much discussed and widely practiced issue in the global financial system. This is a compliance concern in terms of maintaining transparency in the financial market with a sound & accountable atmosphere. To attain a sustainable financial prospect, transparency & accountability are the call of time. “BKB Money Laundering & Terrorist Financing Risk Management Guidelines-2023” is a part of addressing the said obligations.

Financial market is expanding gradually responding to the requirement of the era. The market is getting inclusive day by day. Alongside it keeps carrying new dimensions of challenges in the form of different risk factors. These factors stand as impediments of diversified phenomenon to all the avenues of financial way-forward. The loopholes require to be mended to make the journey a success.

To handle the deviations in the financial market, time befitting technological know-how with smarter approach is a must. It would make the venture easier. Side by side, the rules, regulations, policies in this regard must be upgraded as required to face the challenges. I hope the guideline would help the concerned officials to be enlightened with the on-going compliance issues of AML & CFT by which they could wipe out the spikes spreading over the widely spread network of financial market.

I am happy to have associated with this enterprise and this initiative by BKB would contribute to affirm a healthy and credible financial platform.

  
**Md. Nasiruzzaman**

# Contents

<b>Chapter 1</b>	<b>An Overview of Money Laundering and Terrorist Financing</b>	<b>1-5</b>
1.1	Introduction	1
1.2	Purpose of the guidelines	1
1.3	Money Laundering	2
1.4	Causes of Money Laundering	2
1.5	Stage of Money Laundering	3
1.6	Action of Money Laundering	3
1.7	Terrorist Financing	3
1.8	The Link Between Money Laundering and Terrorist Financing	4
1.9	Why we must Combat ML & TF	4
<b>Chapter 2</b>	<b>International Initiatives on ML and TF</b>	<b>6-12</b>
2.1	Introduction	6
2.2.	The United Nations	6
2.3	The Vienna Convention	6
2.4	The Palermo Convention	6
2.5	International Convention for the Suppression of the Financing of Terrorism	7
2.6	Security Council Resolution 1267 and Successors	7
2.7	Security Council Resolution 1373	7
2.8	Security Council Resolution 1540	8
2.9	The Counter Terrorism Committee	8
2.10	Counter Terrorism Implementation Task-Force(CTITF)	8
2.11	Global Program Against Money Laundering	8
2.12	The Financial Action Task-Force	9
2.13	FATF 40+9 Recommendations	9
2.14	FATF New Standards	9
2.15	Monitoring Members Progress	10
2.16	The NCCT List	10
2.17	International Cooperation and Review Group (ICRG)	10
2.18	Asia Pacific Group on Money Laundering (APG)	10
2.19	The Egmont Group of Financial Intelligence Units	11
2.20	The Basel Committee on Banking Supervision	11
2.21	Statement of Principles on Money Laundering	12
2.22	Basel Core Principles for Banking	12
2.23	Customer Due Diligence	12
<b>Chapter 3</b>	<b>Major national AML &amp; CFT Initiatives</b>	<b>13-17</b>
3.1	Introduction	13
3.2	Legal Framework	13
3.3	Founding Member of APG	13
3.4	Bangladesh Financial Intelligence Unit (BFIU)	13
3.5	Central and Regional Taskforce	14
3.6	Anti-Money Laundering Department	14
3.7	National Coordination Committee and Working Committee	14

3.8	Egmont Group Membership	15
3.9	Chief Anti-Money Laundering Compliance Officers (CAMLCO) Conference	16
3.10	National Coordination Committee and Working Committee	16
3.11	Coordinated Effort on the Implementation of the UNSCR	17
<b>Chapter 4</b>	<b>Compliance Requirements Under the Laws</b>	<b>18-25</b>
4.1	MLP Act, 2012 (Amendment in 2015)	18
4.1.1	Predicate Offence and Related Investigating Authority/ Organization	18
4.1.2	Offences of ML and Punishment (As per Section 4 of MLPA,2012)	20
4.1.3	Establishment of BFIU (As per Section 24 of MLPA,2012)	20
4.1.4	Responsibilities of Reporting Organizations in Preventing the Offence of Money laundering (As per Section 25 of MLPA, 2012)	21
4.2	Anti-Terrorism Act 2009(Amendment in 2012 &2013)	23
4.3	Duties of Reporting Organizations(As per Section 16 of ATA, 2009)	24
4.4	Circular and Circular Letters of BFIU	25
<b>Chapter 5</b>	<b>AML &amp; CFT Compliance Program of BKB</b>	<b>26-30</b>
5.0	Compliance Requirements Under Circulars	26
5.1	Establishment of Central Compliance Committee	26
5.2	Appointment Compliance Officer	26
5.3	Responsibilities of CAMLCO	26
5.4	Nomination of Branch Anti-Money Laundering Compliance Officer	27
5.5	Responsibilities of a DCAMLCO	27
5.6	Responsibilities of a BAMLCO	27
5.7	Responsibilities of Employees	27
5.8	Manual for Prevention Money Laundering & Terrorist Financing	28
5.9	Control Mechanism	29
5.10	Senior Management Role	30
<b>Chapter 6</b>	<b>Compliance Structure of BKB</b>	<b>31-42</b>
6.0	Central Compliance Committee (CCC)	31
6.1	Formation of CCC	31
6.2	Holding of Meeting by CCC	32
6.3	Authorities and Responsibilities of the CCC	32
6.4	Separation of CCC from Internal Control and Compliance (ICC)	32
6.5	Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)	33
6.6	AML & CFT Function of Divisional Office	33
6.7	Regional Office Compliance Unit	33
6.8	Branch Anti Money Laundering Compliance Officer (BAMLCO)	34
6.8.1	Authorities and Responsibilities of BAMLCO	34
6.9	AML / CFT Compliance Officer	35
6.10	Internal Control and Compliance (ICC)	35

6.11	External Auditor	36
6.12	Fixing Up the Responsibilities	37
<b>Chapter 7</b>	<b>Customer Due Diligence (CDD)</b>	<b>39-50</b>
7.1	Know Your Customer Program	39
7.2	Know Your Customer (KYC) Procedure	39
7.2.1	Nature of Customer's Business	39
7.2.2	Identifying Real Person	39
7.2.3	Document is not Enough	39
7.2.4	Components of KYC Program	40
7.3	Simplified Customer Due Diligence (SCDD)	40
7.4	In case where conducting the CDD measure is not possible	41
7.5	Enhanced Due Diligence (EDD)	41
7.6	Customer Unique Identification Code	42
7.7	Correspondent Banking	42
7.8	PEPs, IPs and Chief Executives or Top-Level Officials of any IO	43
7.9.1	CDD Measures for Influential Persons	44
7.10	Definition of Chief Executives or Top-Level Officials of any IO	45
7.10.1	CDD Measures for Chief Executives or Top-Level Officials of any IO	45
7.11	Close Family Members and Close Associates of PEPs, Influential Person's & Chief Executives or Top-Level Officials of any IO	46
7.12	Wire Transfer	46
7.13	Cross Border Wire Transfer	47
7.14	Domestic Wire Transfer	47
7.14.1	Duties of Ordering, Intermediary and Beneficiary Bank in Case of Wire Transfer	47
7.15	CDD for Beneficial Owners	48
7.16	Person's Without Standard Identification Documentation	49
7.17	Management of Legacy Account	49
<b>Chapter 8</b>	<b>Customer Acceptance Policy</b>	<b>50-84</b>
8.1	Definition of Customer	50
8.2	Customer Acceptance Policy (CAP)	50
8.3	Customer Identification	52
8.4	What Constitutes a Customer's Identity	53
8.5	Account of Individual Customer	54
8.6	Joint Accounts	55
8.7	Accounts of Sole Proprietorships or Individuals Doing Business	56
8.8	Accounts of Partnership Firms	57
8.9	Account of Limited Company	59
8.10	Account of Private Limited Companies	60
8.11	Account of Public Limited Companies	61
8.12	Account of Government Owned Entities	62
8.13	Accounts Of Societies, Associations, NGOs, Clubs, Trust And Other Organizations	62
8.14	Non-Banking Financial Institutions (NBFI)	63
8.15	Embassies	64
8.16	Appropriateness of Documents	64

8.17	Change in address or other details	64
8.18	Introducer	64
8.19	Power of Attorney/ Mandates to Operate Accounts	64
8.20	Timing and Duration of Verification	64
8.21	Verification of source of funds	65
8.22	Verification of Address	65
8.23	Joint Accounts	65
8.24	No Face to Face Contact	65
8.25	Record Keeping	65
8.26	Persons Without Standard Identification Documentation	65
8.27	Minor	66
8.28	Cards/Electronic Banking/Mobile Banking	66
8.29	Know Your Customer's Customer	66
8.30	Know Your Employee (KYE)	67
8.31	Walk-in /One of/Online Customers	67
8.32	Customer Acceptance Policy of BKB	68
<b>Chapter 9</b>	<b>Risk Register</b>	80-101
9.1	Risk Measurement	80
9.2	Risk Score Calculation	80
9.3	ML & TF Risk Register for customer	81
		102-
<b>Chapter 10</b>	<b>Screening</b>	
10.1	Sanctions Screening	103
10.2	Concerned Bodies for Screening	103
10.3	The Lists to be Screened with	103
		103-
<b>Chapter 11</b>	<b>Transaction Monitoring</b>	
11.1	Transaction Monitoring Method	103
11.2	Transaction Monitoring Process	103
		106
<b>Chapter 12</b>	<b>Reporting of STR &amp; CTR</b>	
12.1	Suspicious Transaction Reporting According to Laws	106
12.2	Identification of STR/SAR	106
12.3	Documenting Reporting Decisions	108
12.4	Reporting Guidance	108
12.5	Some Special Scenarios for Reporting	108
12.6	Tipping Off	109
12.7	Penalty	109
12.8	Penalty of Tipping Off	109
12.9	Safe Harbor Provision	110
12.10	Red Flags	110
12.11	The Following Red Flags can be used as indicators of STR/SAR	110
12.12	Necessary Papers/Documents for STR	111
12.13	Submission of CTR	111

<b>Chapter 13</b>	<b>Self-Assessment &amp; Independent Testing Procedure (ITP)</b>	112-120
13.1	Self-Assessment Report	112
13.2	Independent Testing Procedure	112
13.3	Responsibility of Audit & Inspection Division	113
13.4	Why the Audit Function is Necessary	113
13.5	Responsibility of CCC regarding Self-Assessment & ITP	113
<b>Chapter 14</b>	<b>Terrorist Financing &amp; Proliferation Financing (TF &amp; PF)</b>	114-119
14.1	Defining Terrorist Financing	114
14.2	The Link Between Money Laundering and Terrorist Financing	115
14.3	Legal Obligations	115
14.4	Obligations Under Circular	115
14.5	Flow-chart for Implementation of TFS by Bank	116
14.6	Necessity of Funds by Terrorist	116
14.6	Sources of Fund/Raising of Fund	116
14.7	Movement of Terrorist Fund	116
14.8.1	Formal Financial Sector	116
14.8.2	Trade Sector	117
14.8.3	Cash Couriers	117
14.8.4	Flow-chart for Implementation of TFS by Bank	117
14.8.5	Use of Charities and Non-Profit Organizations	117
14.8.6	Targeted Financial Sanctions (TFS)	117
14.9	Implementation of FATF Recommendation 6 & 7, FATF Recommendation-6, TFS related Terrorist & Terrorist Financing	118
14.10	Automated Screening Mechanism of UNSCR's	118
14.11	Role of BKB in Preventing TF& PF	119
<b>Chapter 15</b>	<b>Trade-Based Money Laundering (TBML)</b>	120-159
15.1	What is Trade	120
15.2	Trade Products	120
15.3	Three Methods of TBML	121
15.4	Methods & Scope of TBML in Bangladesh	121
15.5	The Regulatory Framework Governing Foreign Trade	122
15.6	Trade Based Money Laundering-Examples Cont'd	127
15.7	Some Conventional Avenues for TBML through OBU, EPZs, EZs & PEZs	127
15.8	Key Challenges and Difficulties in Preventing TBML	128
15.9	Challenges Ahead	128
15.10	Trade Operational Structure of BKB	130
15.10.1	Products & Services Offered by Bangladesh Krishi Bank Related to Foreign Trade	130
15.10.2	Scope/Definition of Customer	131
15.10.3	Parties Involved and their Role in Trade	131
15.10.4	Major Parties and their Role in Import	131
15.10.5	The Process Flow in a Documentary Credit	131
15.10.6	Major parties and their Role in Export	132
15.10.7	The Process Flow in a Documentary Collection	132

15.11	National Law	134
15.11.1	Responsibilities of the Reporting Organizations Under the MLP Act, 2012	135
15.11.2	According to Section 16 of Ant Terrorism (Amendment) Act, 2009, Bank's responsibilities to combat Financing of Terrorism	136
15.11.3	Penalties for Non-Compliance with the Responsibilities of Reporting Organization	136
15.11.4	Penalties for Non-Compliance with the Directives of Bangladesh Bank	136
15.12	International Initiatives	138
15.12.1	The Financial Actions Task Force (FATF); in response to Mounting	138
15.12.2	FATF Guidelines on Trade Based Money Laundering-2006	138
15.12.3	FATF Best practices paper on Trade Based Money Laundering-2008	138
15.12.4	FATF Document on Money Laundering Vulnerabilities in Free Trade Zone-2010	139
15.12.5	Wolfsburg	139
15.12.6	APG Typology Report on Trade Based Money Laundering-2012	139
15.12.7	Guidance paper on Combating Trade Based Money Laundering-2016, The Hong Kong Association of Banks	139
15.13	TBML Risk Assessment & Mitigation Mechanism	140
15.14	Infrastructure Level Risk Assessment	141
15.15	Customer Level TBML Risk Assessment and Mitigation Mechanism	142
15.16	Customer Level Risk Assessment	143
15.17	Trade Related CDD Requirements	147
15.18	Integrated TBML Controls with existing AML/CTF Program	149
15.19	KYC Profile and TBML	149
15.20	Typically the following elements are, but not limited to, checked via automated/manual procedure	151
15.21	Red Flags For TBML	156
<b>Chapter 16</b>	<b>Recruitment, Training and Awareness</b>	<b>160-162</b>
16.1	Appointment and Training	160
16.2	Training for the Officials	160
16.2.1	New Employee	160
16.2.2	Educations and Training for customers	160
16.2.3	AML/CFT Compliance Officers	160
16.2.4	Training Procedures	161
16.2.5	Refresher Training	161
16.3	Obligation Under Circular	161
16.4	Employee Screening	162
16.5	Know Your Employee(KYE)	162

<b>Chapter 17</b>	<b>Record Keeping</b>	163-169
17.1	Record Keeping	163
17.1.1	Legal Obligations	163
17.1.2	Reporting to BFIU	163
17.1.3	Suspicious Transaction Reporting	164
17.2	Records kept by Bangladesh Krishi Bank	164
17.2.1	Walk-in/One Off/Online Customers	165
17.2.2	Wire Transfer	165
17.2.3	Cross-Border Wire Transfers	165
17.2.4	Domestic Wire Transfer	165
17.3	Customer Information	166
17.3.1	Appropriateness of Documents	166
17.4	Transactions	166
17.5	Internal And External Reports	167
17.6	Other Measures	167
17.7	Documents Verifying Evidence of identity And Transaction Records	167
17.8	Wire Transfer Transaction	167
17.9	Investigations	168
17.10	Training Records	168
17.11	Branch Level Record Keeping	169
<b>Chapter 18</b>	<b>BKB &amp; Miscellaneous</b>	170-174
18.1	Whistle Blowing	170
18.2	Corporate Vehicles	172
18.3	Virtual Currency (VC)	172
18.4	Fin Tech & Reg Tech	172
18.5	E-KYC	173
18.5.1	Security Measures	173
18.5.2	Objectives of Promoting e-KYC	173
<b>Annexure-1</b>	Suspicious Transaction Reporting (STR) Format.	175
<b>Annexure-2</b>	Common Indicators for Suspicious Transactions	178
<b>Annexure-3</b>	Short KYC Format for Walk- in-Customer/ Non face to face customer.	179
<b>Annexure-4</b>	BAMLCO Nomination Form	180
<b>Annexure-5</b>	Account Opening Officer Nomination Form	181
<b>Annexure-6</b>	Glossary	182-184

## **ABBREVIATIONS & ACRONYMS**

AML= Anti-Money Laundering

ATA= Anti-Terrorism Act

APG= Asia Pacific Group on Money Laundering

BAMLCO= Branch Anti-Money Laundering Compliance Officer

BFIU= Bangladesh Financial Intelligence Unit

BOD= Board of Directors

CCC= Central Compliance Committee

CFT= Combating Financing of Terrorism

CTC= Counter Terrorism Committee

CTR= Cash Transaction Report

CEO= Chief Executive Officer

CTITF= Counter Terrorism Implementation Task Force

CDD= Customer Due Diligence

CAMLCO= Chief Anti-Money Laundering Compliance Officer

EDD= Enhanced Due Diligence

FATF= Financial Action Task Force

IP= Influential Person

ICC= Internal Control and Compliance

KYC= Know Your Customer

MD= Managing Director

MLPA= Money Laundering Prevention Act

ML= Money Laundering

PEP= Politically Exposed Person

PF= Proliferation Financing

RBA= Risk Based Approach

STR= Suspicious Transaction Report

SAR= Suspicious Activity Report

TF= Terrorist Financing

TFS= Target Financial Sanctions

WMD= Weapons of Mass Destruction

## **The Predicate Offences of AML/CFT**

- Corruption and bribing
- Counterfeiting Notes and coins (PC 489 A- E)
- Counterfeiting Documents (PC 471- 476)
- Extortion (Collecting illegal tolls)
- Cheating (PC 415-424)
- Forgery (PC 463- 469)
- Illegal Arms Trade
- Illegal Trade of Narcotics and Psychotropic Substances (Drugs)
- Illegal trade of stolen and other properties (PC 410- 414)
- Abduction, Illegal Confinement and Abduction for Ransom (359-361)
- Murder, causing grievous injury/ hurt (PC 299- 338)
- Illegal trafficking of women and children
- Smuggling
- Illegal cross border transfer of local and foreign currency
- Theft, Robbery, Dacoity, Piracy and Air Piracy (PC 378-382, 390- 402)
- Illegal human trafficking
- Dowry
- Smuggling and Offence relating to Custom duties evasion
- Offence relating to Tax
- Infringement of Intellectual Property Right
- Terrorism and Terrorist Financing
- Production of goods by adulteration or violating the patent right
- Environment Polluting
- Sexual exploitation
- Insider trading and Market Manipulation regarding Stock business.
- Organized Crime or participation in organized criminal group
- Racketeering (Collecting money through intimidation, terrorization or threatening)
- Any other offence as declared in gazette from time to time

# Chapter 1

## Introduction

### 1.1. INTRODUCTION

Money Laundering is defined as the process of converting money/property, which is derived from illegal activities to give it a legitimate appearance. Its main objectives is to hide the true source of illegal proceeds and make them legal useable, by converting them into legitimate money through a series of financial transactions. It happens in almost every country in the world.

Money Laundering has devastating role in economic, security and social consequences up on any nation around the world. The social and political cost of laundering money are also serious as laundered money may be used to corrupt national institution as well as others private financial institution, bribing officials, undermined the moral fabric in society by weakening collective ethical standard. When money laundering goes unchecked, it encourages the underlying criminal activity, from which such money is generated. As a responsible financial reporting institution, we at Bangladesh Krishi Bank consider it our moral, social and economic responsibility to prevent the misuse of the financial system for laundering proceeds of criminal activities and to co-ordinate national war against Money Laundering.

In Bangladesh, this issue has been initially dealt with the prevention of Money Laundering Act-2002 (Act No-vii of 2008). During Caretaker Government, to prevent the illegal uses of money, Bangladesh has introduced the Money Laundering Prevention Ordinance-2009 repealing the AML Act-2002 and newly introduced Anti-Terrorism Act -2009. Recently in line with the international initiatives and standards, Bangladesh has also enacted the Money Laundering Prevention Act -2012 (repealing the Money Laundering Prevention Act, 2009) and Anti-Terrorism (Amendment) Act-2012. Bangladesh Bank is performing the main role in combating ML & TF through issuing Guidance and directives for reporting agencies including financial institutions.

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.

### 1.2. PURPOSE OF THE GUIDELINES

The purpose of this guideline is to ensure that Bangladesh Krishi Bank is aware of risks for -

- ❖ Mitigating the banks to be a medium for criminal activities both intentionally and unintentionally.
- ❖ Aiming towards inclusion of AML (Anti-Money Laundering) and CFT (Countering Financing of Terrorism) within overall risk management.
- ❖ Ensuring that all directors, senior management and employees understand and comply with the implemented system. The document interprets the requirements of the relevant laws and regulations and how they may be implemented in practice.

### 1.3. MONEY LAUNDERING

Money laundering can be defined in a number of ways. But the fundamental concept of money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins.

Money Laundering is defined in Section 2 (v) of the Money Laundering Prevention Act 2012 as follows:

**“money laundering” means –**

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

### 1.4. CAUSES OF MONEY LAUNDERING

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

### 1.5. STAGES OF MONEY LAUNDERING

There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewelry) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). Despite the variety of methods employed, the laundering process is accomplished in three basic stages which are as follows:

- Placement:** The physical disposal of the initial proceeds derived from illegal activity.
- Layering:** Separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
- Integration:** The provision of apparent legitimacy to derive wealth criminally. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or more commonly, may overlap. These steps may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organizations.

### 1.6. ACTION OF MONEY LAUNDERING

Different actions of money laundering may be-

- Money laundering distinguishes Tax return.
- Financial Institution lost its sufficient treasury.
- Malpractices of power hindrances society.

### 1.7. TERRORIST FINANCING

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

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

According to the article 7 of the Anti-Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means:

Offences relating to financing terrorist activities–

- (1) If any person or entity knowingly provides or expresses the intention to provide money, services, material support or any other property to another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person, entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.
- (2) If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.
- (3) If any person or entity knowingly makes arrangement for money, services, material support or any other property for another person or entity where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any.

### **1.8. 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 to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

### **1.9. WHY WE MUST COMBAT ML & TF**

Money laundering and Terrorist financing have potentially devastating economic, security, and social consequences. These provide vital fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupted public officials and others to operate and expand their criminal enterprises. It overall leads to increase of cost of government leading to misallocation of resources (example- government needing to spend money on rehabilitation of addicts, who are victims of drug dealing). The issues that arises would be –

- ❖ These decrease the government tax revenue. The loss of revenue would increase the living cost of people and public expenditure would face inflation due to corruption. It shifts the economic power of the market to criminals as they get the most benefits monetarily.
- ❖ These could be a potential cause to destabilization of assets and resources which can furthermore lead to the loss of credibility and investors' confidence, particularly in smaller economies.

## Chapter 1: Introduction

- ❖ Severe microeconomic effects of money laundering can be 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, who have access to substantial illicit funds which enables them to support front company products and services at levels well below market rates. This enables a rift where it becomes troublesome for legitimate business to be forced out by criminal organizations.
- ❖ Laundered money can be used to bribe corrupted official and national institutions, leading to deterioration of moral fabric of the society. It can give people incentive to turn to crime to generate unethical income.
- ❖ A nation cannot afford to have its reputation and financial institutions tarnished by involvement with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions (FIs) and the underlying criminal activities like fraud, counterfeiting, narcotics trafficking and corruption weaken the reputation and standing of any financial institution. Actions taken by FIs to prevent money laundering are not only a regulatory requirement, but also an act of self-interest.
- ❖ The negative effects of ML & TF can also disrupt in a macro scale. If a money launderer uses a financial institution for making his/her money legitimate, the business of that financial institution may hamper. It would face liquidity crisis if the malefactor withdraws their deposited money while attaining legitimate front in the economy. The institute would also face legal risks from the country's laws if they were found to be used for ML & TF activities later on, due to failure to identify such schemes and report to the proper authority.

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

# **Chapter 2**

## **International Initiatives on 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 this Guideline discusses the various international organizations and their initiatives relating to anti-money laundering (AML) and combating the financing of terrorism (CFT). It further describes the documents and instruments that have been developed for AML & CFT purposes.

### **2.2. THE UNITED NATIONS**

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

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

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

Third, and perhaps most important that the UN has the ability to adopt international treaties or conventions that obligate the ratifying countries to reflect those treaties or conventions in their local laws. In certain cases, the UN Security Council has the authority to bind all member countries through a Security Council Resolution, regardless of other actions on the part of an individual country.

### **2.3. 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.

### **2.4. THE PALERMO CONVENTION**

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

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

## **Chapter 2: International Initiatives on ML and TF**

- ❖ Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
- ❖ Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyze and disseminate information; and
- ❖ Promote international cooperation.

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

### **2.5. INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM**

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

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

### **2.6. SECURITY COUNCIL RESOLUTION 1267 AND SUCCESSORS**

The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the Sanctions Committee (now called the 1267 Committee). The initial Resolution 1267 of October 15, 1999 dealt with the Taliban and was followed by 1333 of December 19, 2000 on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002), provided some exclusion (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.

### **2.7. SECURITY COUNCIL RESOLUTION 1373**

Unlike an international convention, which requires signing, ratification, and recognition in local law by the UN member country to have the effect of law within that country, a Security Council Resolution 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;

## **Chapter 2: International Initiatives on ML and TF**

- ❖ prohibit active or passive assistance to terrorists; and
- ❖ co-operate with other countries in criminal investigations and share information about planned terrorist acts.

### **2.8. SECURITY COUNCIL RESOLUTION 1540**

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

### **2.9. THE COUNTER-TERRORISM COMMITTEE**

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

### **2.10. COUNTER-TERRORISM IMPLEMENTATION TASK FORCE (CTITF)**

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

### **2.11. GLOBAL PROGRAM AGAINST MONEY LAUNDERING**

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

**2.12. THE FINANCIAL ACTION TASK FORCE**

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 39 countries and territories and two regional organizations.

**2.13. 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.

**2.14. FATF NEW STANDARDS**

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

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

## **Chapter 2: International Initiatives on ML and TF**

### **2.15. 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 ME is going on.

### **2.16. THE NCCT LIST**

FATF adopted a process of identifying those jurisdictions that serve as obstacles to international cooperation in implementing its recommendations. The process used 25 criteria, which were consistent with 40+9 recommendations, to identify such non-cooperative countries and territories (NCCT's) and place them on a publicly available list. Considering its massive impact on respective country, the FATF introduced new implementation mechanism known as International Cooperation and Review Group (ICRG).

### **2.17. INTERNATIONAL COOPERATION 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.

### **2.18. ASIA PACIFIC GROUP ON MONEY LAUNDERING (APG)**

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

## Chapter 2: International Initiatives on ML and TF

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.

### 2.19. THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

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

### 2.20. THE BASEL COMMITTEE ON BANKING SUPERVISION

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of 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.

### **2.21. 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.

### **2.22. 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.'

### **2.23. 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 the international efforts, Bangladesh has also taken many initiatives to prevent money laundering and terrorist financing, considering their severe effects on the country. Some important initiatives are shown below:

### **3.2. LEGAL FRAMEWORK**

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. Subsequently, Bangladesh, as the first South Asian country, promulgated Money Laundering Prevention Act (MLPA), 2002 which came into force on 30 April, 2002. For exercising the power and shouldering the responsibilities, as stated in the MLPA, a separate department named Anti-Money Laundering Department (AMLDD) was established at Bangladesh Bank.

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.

To combat terrorism and terrorist financing Bangladesh also enacted Anti-Terrorism Act (ATA), 2009. To address the gap identified in the Mutual Evaluation Report, some provisions of ATA 2009 have been amended through enactment of Anti-Terrorism (Amendment) Act 2012.

### **3.3. FOUNDING MEMBER OF APG**

Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40 recommendations. Bangladesh has formally endorsed by the APG Membership out-of-session in September 2014 as the Co-Chair for 2018-2020. Bangladesh hosted the 13th APG Typologies Workshop in 2010 and also hosted the APG Annual Meeting of 2016.

### **3.4. BANGLADESH FINANCIAL INTELLIGENCE UNIT (BFIU)**

On May 16, 2007 financial intelligence unit (FIU) was established in BB for receiving, analyzing and disseminating Suspicious Transaction Reports (STRs) related to ML/TF and Cash Transaction Reports (CTRs). As per the provision of MLPA, 2012 AMLDD is now working as separate unit in BB as Bangladesh Financial Intelligence Unit (BFIU).

Bangladesh Bank (BB) has already issued Guidance Notes under 'core risk' management titled 'Guidance Notes on Prevention of Money Laundering' for banks. BB has also issued guidance notes for insurance companies and money changers.

Bangladesh has enacted Mutual Assistance in Criminal Matters Act, 2012 to enhance international cooperation on ML/TF and other related offences.

## Chapter 3: Major National AML & CFT Initiatives

To facilitate exchange of information and intelligence among FIUs, Bangladesh FIU has already signed 13 (thirteen) MoUs with other FIUs. BFIU in cooperation with Anti-Corruption Commission has assessed ML/TF risk and vulnerabilities in Bangladesh and drafted the National ML/TF Risk and Vulnerability Assessment Report. 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 finalized the procurement process of goAML software for online reporting and software based analysis of CTRs and STRs.

BFIU has established MIS to preserve and update all the information and to generate necessary reports using the MIS. BFIU 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. The Bank and Financial Institutions Division, Ministry of Finance has issued a circular instructing all the related agencies to provide relevant information to Bangladesh Bank.

### **3.5. CENTRAL AND REGIONAL TASKFORCE**

The Government of Bangladesh has formed a central and 7 regional taskforces (Chattogram, Rajshahi, Bogura, Sylhet, Rangpur, Khulna and Barishal) 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 forces 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 implemented through banks, financial institutions and Government agencies concerned.

### **3.6. ANTI MONEY LAUNDERING DEPARTMENT**

Anti-Money Laundering Department (AMLDD) was established in Bangladesh Bank in June 2002 which worked as the FIU of Bangladesh. It was the authority for receiving, analyzing and disseminating Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs). Bangladesh Krishi Bank has also established a separate AML Cell at Head Office. From then it is still running as per instruction of BFIU. The Cell is headed by DGM, Deputy CAMLCO.

### **3.7. NATIONAL COORDINATION COMMITTEE AND WORKING COMMITTEE**

To provide guidance for effective implementation of 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 Finance Ministry were formed consisting representatives from all regulatory authorities.

Bangladesh Government has developed the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2011-2013. The strategy consists of following 12 (twelve) strategies against 12 (twelve) strategic objectives:

1. Strengthening the legal framework.
2. Enhancing effectiveness of the FIU.
3. Enforcing compliance of all reporting agencies.
4. Structural improvement and capacity building in tracing out methods, techniques and channels of money laundering and terrorist financing.

## Chapter 3: Major National AML & CFT Initiatives

5. Improving transparency in financial reporting on AML/CFT issues.
6. Ensuring transparency in the ownership of legal entities.
7. Enhancing financial inclusion.
8. Maintaining a comprehensive AML/CFT database.
9. Boosting national coordination both at policy and operational levels.
10. Developing and maintaining international and regional cooperation on AML/CFT.
11. Heightening public awareness.
12. Stemming the illicit outflows and inflows of fund.

Issued a comprehensive circular for banks and non-bank financial institutions addressing the following issues:

- ❖ Definition of Customer for KYC purpose
- ❖ Process and timing of Customer Due Diligence(CDD)
- ❖ Defining and identifying Beneficial Owner
- ❖ Politically Exposed Persons related issues
- ❖ Correspondent Banking
- ❖ Employee screening mechanism
- ❖ Awareness program for the customer

Self-assessment and independent testing procedure system were introduced for banks on March 24, 2008 to assess their own compliance. Side by side, Bangladesh Bank has also been monitoring the same through a process called system check inspection.

A rigorous Customer Due Diligence (CDD) procedure has been introduced to protect identity theft by customer through issuance of Uniform Account Opening Form for all banks. It includes standardized Know Your Customer (KYC), Transaction Profile (TP) and Risk Grading of Customer.

### **3.8. EGMONT GROUP MEMBERSHIP**

Bangladesh has continued its pursuance to get membership of the Egmont Group, the global forum for cooperation. In this regard, the off-site evaluation has already been conducted by Malaysia and Thailand as sponsor and co-sponsor respectively.

## Chapter 3: Major National AML & CFT Initiatives

### 3.9. CHIEF ANTI-MONEY LAUNDERING COMPLIANCE OFFICERS (CAMLCO) CONFERENCE

Separate annual conferences for the Chief Anti-Money Laundering Compliance Officer (CAMLCO) of Banks, Insurance Companies and Financial Institutions were organized. Separate annual conferences for the Chief Anti-Money Laundering Compliance Officers (CAMLCO) of Banks, Financial Institutions, Insurance Companies and Capital Market Intermediaries are arranged by BFIU. It also 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 regularly. Last CAMLCO Conference was held on 14-16 February, 2020 and CAMLCO Conference for Mobile Financial Service held on March, 2020.

### 3.10. 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. National Strategy for Preventing Money Laundering and Combating Financing of Terrorism, 2019-21 was adopted by the NCC. The strategies are given below-

- ❖ To curb illicit financial flows from the country- Stemming Illicit flow of funds (IFF) by preventing the generation of proceeds of crime, restricting channel of illicit transfer and strengthening stolen asset recovery mechanism.
- ❖ To reduce the magnitude of trade based money laundering- Providing tools and techniques and cementing stake holders cooperation to minimize trade based money laundering.
- ❖ To improve the quality of financial investigation- Prioritizing the investigation of ML & TF and other related offences including tracing, restraint and confiscation of proceeds of crime by law and enforcement agencies.
- ❖ To ensure proportionate and dissuasive sanctions expediting the prosecution- Developing effecting judicial system by providing required resources and training to the judges and prosecutors.
- ❖ To deter profitable use of proceeds of corruption (both public and private sector)- Determining all sorts of corruption induced money laundering considering corruption as a high risk.
- ❖ To reduce the vulnerabilities of reporting organizations to ML & TF- Maintaining strict AML & CFT compliance by the reporting organizations as well as increasing the capacity of the regulators.
- ❖ To prevent smuggling of goods and trafficking of drugs and humans- Modernizing border control mechanism and depriving perpetrators from use of proceeds of crime to prevent smuggling of drugs, gold, arms and human trafficking and other transnational organized crimes considering the risk thereon.
- ❖ To deprive the offenders from the consumption of proceeds of crime - Ensuring systematic freezing and confiscation of proceeds of crime and managing them effectively.
- ❖ To mitigate the risk of abuse of the legal persons and arrangement for ML & TF purposes- Promoting transparency in the ownership of legal persons and legal arrangements through strengthening legal and institutional arrangements.
- ❖ To preclude the use of corporate vehicles from generating illegal proceeds- Ensuring sound corporate governance in the ROs (reporting organization) and other corporate vehicles so that they can't be abused for generating proceeds of crime.

### **3.11. Coordinated effort on the implementation of the UNSCR**

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

# Chapter 4

## Compliance Requirements under the Laws

In Bangladesh, compliance requirements for FIs, as reporting organization, are based on-

- Money Laundering Prevention Act (MLPA), 2012 (Amendment in 2015)
- Money Laundering Prevention Rules (2019)
- Anti-terrorism Act 2009 (Amendment in 2012 & 2013) and
- Circulars or instructions issued by BFIU

### 4.1. MONEY LAUNDERING PREVENTION ACT, 2012 (AMENDMENT IN 2015)

Some important fundamentals of Money Laundering Prevention Act, 2012 are given below-

#### 4.1.1. PREDICATE OFFENCES AND RELATED INVESTIGATING AUTHORITY /ORGANIZATION

As per Section 2 of MLPA, 2012 and MLPR, 2019 predicate offence means the offences mentioned below, by committing which within or outside the country, the money or property derived from is laundered or attempt to be laundered, namely following and its related investigating Authorities are also mentioned below:

S.N.	Predicate Offence	Investigating Authority/ Organization
01.	Corruption and bribery	Anti-Corruption Commission
02.	Counterfeiting currency	Crime Investigation Division of Bangladesh Police
03.	Counterfeiting deeds and documents	Crime Investigation Division of Bangladesh Police
04.	Extortion	Crime Investigation Division of Bangladesh Police
05.	Fraud	Crime Investigation Division of Bangladesh Police
06.	Forgery	Crime Investigation Division of Bangladesh Police
07.	Illegal trade of firearms	Crime Investigation Division of Bangladesh Police
08.	Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication	Department of Narcotics Control and Crime Investigation Division of Bangladesh Police
09.	Illegal trade of stolen and other goods	Bangladesh Customs and Crime Investigation Division of Bangladesh Police
10.	Kidnapping, illegal restrain and hostage taking	Crime Investigation Division of Bangladesh Police
11.	Murder, grievous physical injury	Crime Investigation Division of Bangladesh Police
12.	Trafficking of women and children	Crime Investigation Division of Bangladesh Police
13.	Black marketing	National Board of Revenue (NBR) and Crime Investigation Division of Bangladesh Police

#### Chapter 4: Compliance Requirements under the Laws

S.N.	Predicate Offence	Investigating Authority/ Organization
14.	Smuggling of domestic and foreign currency	National Board of Revenue (NBR) and Crime Investigation Division of Bangladesh Police
15.	Theft or robbery or dacoit or piracy or hijacking of aircraft	Crime Investigation Division of Bangladesh Police
16.	Human trafficking	Crime Investigation Division of Bangladesh Police
17.	Dowry	Crime Investigation Division of Bangladesh Police
18.	Smuggling and offences related to customs and excise duties	National Board of Revenue (NBR) and Crime Investigation Division of Bangladesh Police
19.	Tax related offences	National Board of Revenue (NBR)
20.	Infringement of intellectual property rights	Crime Investigation Division of Bangladesh Police
21.	Terrorism or financing in terrorist activities	Crime Investigation Division of Bangladesh Police
22.	Adulteration or the manufacture of goods through infringement of title	Crime Investigation Division of Bangladesh Police
23.	Offences relating to the environment	Department of Environment and Crime Investigation Division of Bangladesh Police
24.	Sexual exploitation	Crime Investigation Division of Bangladesh Police
25.	Offenses regarding capital market (insider trading and market manipulation)	Bangladesh Securities & Exchange Commission
26.	Organized crime and participation in organized criminal groups	Crime Investigation Division of Bangladesh Police
27.	Racketeering	Crime Investigation Division of Bangladesh Police
28.	Any other offence declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official Gazette, for the purpose of MLP Act, 2012	The body that will be appointed for investigation, would be declared in the official Gazette

## Chapter 4: Compliance Requirements under the Laws

### 4.1.2. OFFENCE OF MONEY LAUNDERING AND PUNISHMENT (AS PER SECTION 4 OF MLPA, 2012)

- ❖ For the purposes of this Act, money laundering shall be an offence.
- ❖ Any person who commits the offence of money laundering, abets or conspires in the commission of the offence of money laundering, shall be punished with imprisonment for a minimum period of 4 (four) years and not more than 12 (twelve) years and in addition to this a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lacs, whichever is greater may be imposed.
- ❖ In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved or related with money laundering or any of the predicate offences.
- ❖ Any entity which commits an offense under this section shall be punished with a fine of not less than twice the value of the property or taka 20 (twenty) lacs whichever is greater and in addition to this the registration of the said entity will be liable to be cancelled.
- ❖ It shall not be a prerequisite to be convicted or sentenced for any predicate offence to pass an order of conviction or sentence for a money laundering crime.

### 4.1.3. ESTABLISHMENT OF THE BANGLADESH FINANCIAL INTELLIGENCE UNIT (BFIU) (AS PER SECTION 24 OF MLPA, 2012)

The main objective of the BFIU is to establish an effective system for prevention of money laundering, combating financing of terrorism and proliferation of weapons of mass destruction. BFIU was established in June **2002**, in Bangladesh Bank (Central bank of Bangladesh) named as 'Anti Money Laundering Department'.

BFIU Receive Suspicious Transaction/Activity Reports (STRs/SARs) from the reporting organizations and Cash Transaction Reports (CTRs) from banks, complaints from different sources, analyze the same and disseminate ML/TF related cases to respective investigating authority for further action.

Bangladesh Financial Intelligence Unit (BFIU) is the central agency of Bangladesh responsible for analyzing Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs) & information related to money laundering (ML) /financing of terrorism (TF) received from reporting agencies & other sources.

In order to exercise the power and perform the duties vested in Bangladesh Bank under section 23 of this Act, there shall be a separate unit to be called the Bangladesh Financial Intelligence Unit (BFIU) within Bangladesh Bank.

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

## Chapter 4: Compliance Requirements under the Laws

### 4.1.4. RESPONSIBILITIES OF REPORTING ORGANIZATIONS IN PREVENTING THE OFFENCE OF MONEY LAUNDERING (AS PER SECTION 25 OF MLPA, 2012)

#### Compliance Requirements under the Laws-

Compliance requirements for BKB, as reporting organization, are based on Money Laundering Prevention Act (MLPA), 2012, Anti-terrorism (Amendment) Act, 2012 and circulars or instructions issued by BFIU. According to section 25 of MLPA, 2012 responsibilities to prevent money laundering are –

- a) to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
- b) to preserve previous records of transactions of any customer's account for at least 5(five) years from the date of closure;
- c) to provide with the information maintained under clauses (a) and (b) to Bangladesh Bank from time to time, on its demand;
- d) if any suspicious transaction or attempt of such transaction as defined under clause (z)<sup>3</sup> of section 2 is observed, to report the matter as suspicious transaction report' to the Bangladesh Bank immediately on its own accord.

#### Penalties under MLPA:

According to section 25 (2) of MLPA, 2012, if any reporting organization violates the directions mentioned in sub-section

- (1) of section 25 of MLPA, 2012, Bangladesh Bank may-
  - (a) impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty five) lacs on the reporting organization; and
  - (b) in addition to the fine mentioned in clause (a), 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 case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

In addition to the above mentioned provisions there are some new provisions of penalties in the section 23 of MLPA, 2012. These are:

- (1) If any reporting organization fails to provide with the requested information timely under this section, Bangladesh Bank may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lakhs at the rate of Taka 10 (ten) thousand per day and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

#### **Chapter 4: Compliance Requirements under the Laws**

- (2) If any reporting organization provides with false information or statement requested under this section, Bangladesh Bank may impose a fine on such organization not less than Taka 20 (twenty) thousand but not exceeding Taka 5 (five) lakhs and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.
- (3) If any reporting organization fails to comply with any instruction given by Bangladesh Bank under this Act, Bangladesh Bank may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lakhs at the rate of Taka 10 (ten) thousand per day for each of such non-compliance and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.
- (4) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Bank under clause (c) of sub-section 23(1) of MLPA, 2012, Bangladesh Bank may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.
- (5) If any person or entity or reporting organization fails to pay any fine imposed by Bangladesh Bank under sections 23 and 25 of this Act, Bangladesh Bank may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank, and in this regard if any amount of the fine remains unrealized, Bangladesh Bank may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.
- (6) If any reporting organization is imposed fine under sub-sections 23 (3), (4), (5) and (6), Bangladesh Bank may also impose a fine not less than Taka 10 (ten) thousand but not exceeding taka 5 (five) lakhs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

### 4.2. ANTI-TERRORISM ACT 2009 (AMENDMENT IN 2012 & 2013)

Some important elements of this act are given below-

#### Offences relating to financing for terrorist activities (as per section 7 of ATA 2012)

- If any person or entity knowingly supplies or expresses the intention to supply money, service, material support or any other property to another person or entity and where there are reasonable grounds to believe that the full or partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity shall be treated committing the offence of financing for terrorist activities.
- If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that full or partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization, then he or she or the said entity shall be treated committing the offence of financing for terrorist activities.
- If any person or entity knowingly makes arrangements for collecting money, services, material support or any other property for another person or entity and where there are reasonable grounds to believe that the full or the partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity will be treated committing the offence of financing for terrorist activities.
- If any person or entity knowingly instigate in such a manner, another person or entity to supply, receive, or arrange money, services, material support or any other property and where there are reasonable grounds to believe that the full or the partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity will be treated committing the offence of financing for terrorist activities.
- If any person is found guilty of any of the offences set out in sub-sections (1) to (4) of ATA 2009, that person will be sentenced to imprisonment for a term between a maximum of twenty and a minimum of four years, and in addition to this a fine may be imposed not less than the greater of twice the value of the property involved with the offence or taka 10(ten) lac.
  - (1) If any entity is found guilty of any of the offences set out in sub-sections (1) to (4) of ATA 2009, steps may be taken under section 18 and in addition to this a fine may be imposed not less than the greater of thrice the value of the property involved with the offence or taka 50(fifty) lac and
  - (2) The head of such entity, Chairman, Managing Director, Chief Executive Officer whatever may be called by shall be punished with an imprisonment of a term up to maximum of 20 and a minimum of 4 years and in addition to this a fine may be imposed the greater of twice the value of the property involved with the offence or taka 20(twenty) lac unless he is able to prove that the said offence was committed without his knowledge or he had tried utmost to prevent the commission of the said offence.

## **Chapter 4: Compliance Requirements under the Laws**

### **PENALTIES UNDER ATA:**

The provision laid down in section 16 (3) of Anti-Terrorism (Amendment) Act, 2012, if any reporting agency fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding Taka 10 (ten) lacs and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency. According to section 16 (4) if any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank according to sub-section 16 (3) of ATA, Bangladesh Bank may recover the amount from the reporting agency by debiting its accounts maintained in any bank or financial institution or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

### **4.3. DUTIES OF REPORTING ORGANIZATIONS (AS PER SECTION 16 OF ATA, 2009)**

- Each reporting organization shall take necessary measures, exercising appropriate caution and responsibility, to prevent and identify financial transactions through them connected to any offence committed under this act and if any suspicious transaction is identified, shall spontaneously report it to the Bangladesh Bank without any delay.
- The Board of Directors, or in the absence of the Board of Directors the Chief Executive Officer or whatever may be called by, of each reporting organization shall approve and issue directions regarding the duties of its officers, and will ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting organizations, have been complied with.
- If any reporting organization fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provide any wrong information or false information or statement, the said reporting organization shall be liable to pay a fine determined and directed by Bangladesh Bank, not exceeding Taka 10 (ten) lakhs and Bangladesh Bank may suspend the registration or license with a purpose to close the operation of the said agency/organization or any branch, service center, booth or agent of that organization within Bangladesh or where applicable, shall inform the registration/licensing authority about the subject matter to take appropriate action against the organization.
- If any Reporting Organization fails to pay any fine imposed by Bangladesh Bank under sub sections 3 of this Act, Bangladesh Bank may recover the amount from the reporting organizations by debiting their accounts maintained in any bank or financial institution or Bangladesh Bank. In this regard if any amount of the fine remains unrealized Bangladesh Bank may make an application before the relevant court for recovery.

## Chapter 4: Compliance Requirements under the Laws

### 4.4. CIRCULAR AND CIRCULAR LETTERS OF BFIU

BFIU published its circular 26 on 16.06.2020 as Instructions to be followed by the scheduled bank for prevention of money laundering, terrorist financing and proliferation financing. And others circular and circular letter which should be followed by bank are as follows:

<b>Circular/Circular Letter no</b>	<b>Date of Impose</b>	<b>Subject</b>
AML Circular No-22	21/04/2009	Anti-Terrorism Act, 2009
BFIU Circular No-02	15/03/2012	Regarding "Money Laundering Prevention Act, 2012"
BFIU Circular Letter No-01	30/01/2012	Naming of BFIU
BFIU Circular No-07	14/07/2013	Anti-Terrorism (Amendment) Act, 2013
BFIU Circular Letter No-01	08/04/2015	Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector
BFIU Circular Letter No-03	09/04/2015	Circulation of Money Laundering Prevention Rules, 2013 and Anti-Terrorism Rules, 2013
BFIU Circular Letter No-06	08/12/2015	Circulation of Money Laundering Prevention (Amendment) Act, 2015
BFIU Circular Letter No-01	11/02/2016	Instructions to be followed for the compliance of Freezing Accounts of listed Individuals or Institutions and Other Issues under the Sanction List of Different Resolutions of United Nations Security Council
BFIU Circular Letter No-01	22/04/2018	Instructions to be followed by the schedule banks for preserving secrecy of information.
BFIU Circular No-22	31/01/2019	Instructions regarding Exchange of Information among the reporting organizations
BFIU Circular No-23	31/01/2019	Instructions regarding Internal Control and Foreign Branches and Subsidiaries of "Financial Institution Group"
BFIU Circular Letter No-01	24/02/2019	Regarding Guidelines for Prevention of Trade Based Money Laundering
BFIU Circular No-24	10/12/2019	Regarding Guidelines for Prevention of Trade Based Money Laundering
BFIU Circular No-25	08/01/2020	Issuance of Guidelines on Electronic Know Your Customer (e-KYC)
BFIU Circular No-26	16/06/2020	Prevention of Money Laundering, Terrorist Financing and Proliferation Financing

# **Chapter 5**

## **AML & CFT Compliance Program of BKB**

### **5. COMPLIANCE REQUIREMENTS UNDER CIRCULARS:**

#### **5.1. ESTABLISHMENT OF CENTRAL COMPLIANCE COMMITTEE**

To ensure compliance of the Money Laundering Prevention Act, 2012 and ATA 2009 (as amended in 2012) BKB established a Central Compliance Committee (CCC) under the leadership of a high official at the Head Office for internal monitoring and control. To determine institutional strategy and program and in order to accomplish proper jurisdiction and function, CCC will issue the instructions to be followed by the branches; these instructions will be prepared on the basis of combination of issues in monitoring of transactions, internal control, policies and procedures from the point of view of preventing money laundering & terrorist financing. The responsibilities of a CCC shall include:

- a) preparing an overall assessment report after evaluating the self-assessment reports received from the branches and submitting it with comments and recommendations to the chief executive of the bank;
- b) preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Audit Department on that particular quarter;
- c) Submitting a half-yearly report to BFIU within 60 days after end of a quarter.

#### **5.2. APPOINTMENT COMPLIANCE OFFICER**

To implement instructions related to AML policy guidelines and compliance of Bangladesh Bank's instructions Bangladesh Krishi Bank has appointed/nominated a high level officer i.e. Deputy General Manager as a Chief Anti-Money Laundering Compliance Officer (CAMLCO) and the DEPUTY General Manager of AML cell appointed as Deputy Chief Anti-Money Laundering Compliance Officer (DCAMLCO). The CAMLCO will responsible to coordinate and monitor day to day compliance with applicable AML/CFT related laws, rules and regulations as well as with its internal policies, practices, procedures and controls. The CAMLCO will directly report to the Chief Executive Officer/Managing Director for his/her responsibility.

#### **5.3. RESPONSIBILITIES OF CAMLCO:**

The major responsibilities of a CAMLCO are as follows:

1. To monitor, review and coordinate application and enforcement of the financial institution's compliance policies including AML/CFT Compliance Policy. This will include an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity, and a written AML/CFT training plan.
2. To monitor changes of laws/regulations and directives of Bangladesh Bank and revise its internal policies accordingly;
3. To respond to compliance questions and concerns of the staff and advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk;
4. To ensure that the financial institution's AML/CFT policy is complete and up-to-date, to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered by the financial institution;
5. To develop the compliance knowledge of all staff, especially the compliance personnel and conduct training courses in the institution in this regard;

## Chapter 5: AML & CFT Compliance Program of BKB

6. To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;
7. To assist in review of control procedures in the financial institution to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
8. To monitor the business through self-testing for AML/CFT compliance and take any required corrective action;
9. To manage the STR/SAR process:
  - reviewing transactions referred by divisional, regional, branch or unit compliance officers as suspicious;
  - reviewing the transaction monitoring reports (directly or together with account management personnel);
  - ensuring that internal Suspicious Activity Reports (SARs):
    - are prepared when appropriate;
    - reflect the uniform standard for "suspicious activity involving possible money laundering or terrorist financing" established in its policy;
    - are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy;
    - are advised to other branches of the institution who are known to have a relationship with the customer;
    - are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk .
  - ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;
  - maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner;
  - managing the process for reporting suspicious activity to BFIU after appropriate internal consultation;

## Chapter 5: AML & CFT Compliance Program of BKB

### 5.4. NOMINATION OF BRANCH ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

The Branch Managers will nominate Branch Anti-Money Laundering Compliance officer (BAMLCO) according to the instruction of BFIU Circular No-26, Date- 26.06.2020 and send the nominations to CCC (Central Compliance Committee). After verification CCC will approve the nominations and issue a by name appointment letter to the BAMLCOs. If any nominated BAMLCO gets transfer order, then the respective branch manager must have to inform it to CCC and take a new nomination.

### 5.5. Responsibilities of Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)

- Monitor and take necessary steps that the required reports and systems are in place to maintain an effective program.
- To monitor changes of laws/regulations and directives of Bangladesh Bank and revise its internal policies accordingly;
- To respond to compliance questions and concerns of the staff and advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk;
- To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;

### 5.6. Responsibilities of a BAMLCO:

1. Manage the transaction monitoring process
2. Report any suspicious activity to Branch Manager, and if necessary to the CAMLCO
3. Provide training to Branch staff
4. Communicate to all staff in case of any changes in national or its own policy
5. Submit branch returns to CAMLCO timely.

### 5.7. RESPONSIBILITIES OF EMPLOYEES-

The table below details the individual responsibilities of the employees:-

<b>Function</b>	<b>Role / Responsibilities</b>
Staff Responsible for account opening	<ul style="list-style-type: none"><li>: Perform due diligence on prospective clients prior opening an account.</li><li>: Be diligent regarding the identification (s) of account holder and the transactions relating to the account.</li><li>: Ensure all required documentation is completed satisfactorily.</li><li>: Complete the KYC Profile for the new customer.</li><li>: Ongoing monitoring of customers KYC profile and transaction activity.</li><li>: Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO.</li></ul>
Customer Service Officer	<ul style="list-style-type: none"><li>: Support the Account Officer in any of the above roles.</li><li>: Perform the Account Officer roles in their absence.</li></ul>
Operations Staff	<ul style="list-style-type: none"><li>: Ensure that all control points are completed prior to transaction monitoring.</li><li>: Be diligence on transaction trends for clients.</li><li>: Update customer transaction profiles in the ledger/system.</li></ul>

## Chapter 5: AML & CFT Compliance Program of BKB

Branch Manager (Unit Head)	: Ensure that the program is effective within the branch/unit. : First point of contact for any issues.
Risk Management /Credit Officer/ Internal Control Officer	: Perform Risk Assessment for the Business. : Perform periodic Quality Assurance on the program in the unit. : Communicate updates in laws and Internal policies.
Chief Regional Manager (RAMLCO)	: Overall responsibility to ensure that the branches have a program in place and that it is working effectively.
Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)	: Monitor and take necessary steps that the required reports and systems are in place to maintain an effective program.
Chief Anti Money Laundering Compliance Officer (CAMLCO)	: Ensures that the required reports and systems are in place to maintain an effective program.
Managing Director (MD)	: Overall responsibility to ensure that the Business has an AML program in place and it is working effectively.

### 5.8. MANUAL FOR PREVENTION MONEY LAUNDERING & TERRORIST FINANCING

In pursuance of instruction of BFIU circular number 04 dated 16th September, 2012 Bangladesh Krishi Bank prepared a Money Laundering Prevention manual approved by Board that delivered to all concern offices and Branches. This policy manual framed in conformity with national standard and laws and regulations in force in Bangladesh shall review from time to time and confirm the meticulous compliance of the circulars issued by Bangladesh Bank (Central Bank of Bangladesh).

### 5.9. CONTROL MECHANISM

The compliance program also relies on the variety of internal controls, including management report, built-in safeguards and exception report that keep the program working. FATF recommendation 18 requires that financial institutions have an internal control program. The following elements should be included in the operational controls of any policy:

- Statement of responsibility for compliance with policy;
- Customer due diligence;
- Customer identification/verification
- Additional know your customer information
- High risk customers
- Non face to face business (if applicable)
- Handling of politically exposed persons
- Monitoring for suspicious transaction/activity;
- Cooperation with the authorities;
- Record keeping;
- Screening of transactions and customers;
- Training and awareness;
- Adoption of risk management practices and use of a risk-based approach.

## Chapter 5: AML & CFT Compliance Program of BKB

### 5.10. SENIOR MANAGEMENT ROLE

For the purposes of preventing ML, TF & PF, senior management in our case includes members of the board of directors and the Managing Director (MD).

Obligation under Law (ATA, 2009)	The Board of Directors, or in the absence of the Board of Directors, the Chief Executive of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, which are applicable to the reporting agency, have been complied with or not.
Obligation under BFIU Circular-10; Dated: December 28, 2014) Section-1(1.1 & 1.2)	All banks must have their own policy manual that must confirm 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 their Board of Directors or by the highest management committee, where applicable. This policy manual shall be communicated to all concerned persons. Banks shall conduct review of the policy manual from time to time and shall amend/change where necessary. The chief executive of the bank shall announce effective and specific commitment, give the necessary instructions to fulfill the commitments in preventing ML & TF to all the employees of all branches, agent offices, Zonal offices and the head office and shall ensure the implementation of the commitments. This statement of commitment shall be issued in every year.

## Chapter 6

# Compliance Structure of BKB

### **CENTRAL COMPLIANCE COMMITTEE (CCC)**

The Central Compliance Committee (CCC) of Bangladesh Krishi Bank shall be headed by a high official, who will be known as the Chief Anti Money Laundering Compliance Officer (CAMLCO). In this case, high official would be considered as an official up to 2 (two) steps below of the Managing Director/ Chief Executive Officer. Bangladesh Krishi Bank shall inform of any change regarding CAMLCO to BFIU without delay. It will also ensure the involvement of CAMLCO regarding AML & CTF activities in case of assigning him to other duties of the bank. Bangladesh Krishi Bank will also nominate two Deputy Anti-Money Laundering Compliance Officers (DCAMLCO) whose rank will not be below Deputy General Manager. The CAMLCO and DCAMLCO have to possess detailed knowledge about the existing acts, rules and regulations, directions issued by BFIU from time to time and international standards on Anti Money Laundering & Combating Terrorist Financing. Under the guidance of the Central Compliance Committee (CCC), Anti Money Laundering and Combating Terrorist Finance Division shall issue instructions for the branches obtaining KYC, transaction monitoring system, internal control system, policies and procedures to prevent Money Laundering and Terrorist Financing.

#### **6.1. FORMATION OF CCC**

CCC shall be formed consisting of at least 7 (Seven) members wherein Heads / Senior officials from different Divisions/ Departments of Head Office along with CAMLCO & DCAMLCO will be included. The members of the CCC need to have enough knowledge on AML & CTF measures of Bangladesh including MLPA, ATA and the related rules and instructions issued by BFIU or Bangladesh Bank. Duties and Responsibilities of CCC shall be specified.

The Central Compliance Committee (CCC) of Bangladesh Krishi Bank is headed by the CAMLCO (Chief Anti Money Laundering Officer). The members of the committee are-

<b>S. N.</b>	<b>Position</b>	<b>Division</b>	<b>Position in CCC</b>
1	DMD-1	--	Head of CCC & CAMLCO
	DMD-2	--	Member
	General Manager (Admin)	Admin Division	Member
2	Deputy General Manager	Risk Management Department (Anti Money Laundering Cell), HO	Member Secretary & DCAMLCO
3	Deputy General Manager	Central Accounts Department, HO	Member
4	Deputy General Manager	International Trade Department, HO	Member
5	Deputy General Manager	Credit Department, HO	Member
6	Deputy General Manager	Foreign Remittance Department, HO	Member
7	Deputy General Manager	Human Resource Management Department-1, HO	Member
8	Deputy General Manager	ICT Operation Department, HO	Member
9	Deputy General Manager	ICT Systems, Card & Mobile Banking Department, HO	Member
10	Deputy General Manager	Branch Control & Business Development Department, HO	Member
11	Assistant General Manager/ Senior Principal Officer	Anti-Money Laundering Cell, HO	Member

### 6.2. HOLDING OF MEETING BY CCC

CCC will hold at least 4(Four) meetings on quarterly basis in a year. But if required, CAMLCO may call CCC meeting at any time.

### 6.3. AUTHORITIES AND RESPONSIBILITIES OF THE CCC

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

- 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 or 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 employee of the bank;
- Take required measures to submit information, report or documents in time.

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

- Appointment of BAMLCO and assign their specific job responsibilities
- Requisition of human resources and logistic supports for CCC
- Make suggestion or administrative sanction for non-compliance by the employees.
- Take required measures to submit information, report or documents in time.

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

- Appointment of BAMLCO and assign their specific job responsibilities
- Requisition of human resources and logistic supports for CCC
- Make suggestion or administrative sanction for non-compliance by the employees.
- Take required measures to submit information, report or documents in time.

### 6.4. SEPARATION OF CCC FROM INTERNAL CONTROL & COMPLIANCE (ICC)

For ensuring the independent audit function in the bank, CCC shall be completely separated from Internal Control & Compliance. Either the Division may perform same job but in different and independent way. In this regard, ICC shall also examine the performance of CCC and the bank's AML & CFT compliance program. To ensure this independency, there shall not be any member from Audit and Inspection to CCC vice-a-vice; but there shall be enough co-ordination and co-operation in performing their responsibility and information exchange. There shall not be any obstruction to transfer employee from ICC to CCC and vice-a-vice but no one shall be posted in these 2 (two) Divisions/Committee at the same time. A Separate and Independent Division with the name and title “Anti Money Laundering & Combating Terrorist Financing Division” headed by the DCAMLCO shall be placed under the Central Compliance Committee (CCC) to provide all sorts of secretarial assistance to the CCC with sufficient manpower & logistic supports for ensuring effective AML & CFT compliance of the Bank.

### **6.5. DEPUTY CHIEF ANTI MONEY LAUNDERING COMPLIANCE OFFICER (DCAMLCO)**

According to BFIU Circular 26 dated-16/06/2020 Anti Money Laundering and Combating Terrorist Financing Division will play the secretarial role of CCC and ensure implementing and enforcing the Bank's AML & CFT policies in 580 branches of Bangladesh Krishi Bank. Deputy Chief Anti Money Laundering Compliance Officer is also responsible for all type of reporting to BFIU like STR/SAR, CTR, Self Assessments and others.

### **6.6. AML & CFT FUNCTION OF DIVISIONAL OFFICE**

Divisional Offices will supervise the AML & CFT functions of Regional office under their control as per Bangladesh Bank guideline and Head Office instructions. They will also supervise the AML & CFT functions of inspection cells under their jurisdiction and will issue necessary instructions to them.

### **6.7. REGIONAL OFFICE COMPLIANCE UNIT**

All Regional office of Bangladesh Krishi Bank will constitute a Money Laundering Prevention Committee under the Chairmanship of the Regional head, made up of 3/4 members. The committee will supervise the Anti-Money Laundering and Combating the Financing of Terrorism activities of the branches under their jurisdiction through on-site and off-site supervision. The committee will evaluate their performances at least monthly and minutes of meeting must be recorded and sent to the AML & CFT Division regularly with a copy through respective Divisional office.

### **6.8. BRANCH ANTI MONEY LAUNDERING COMPLIANCE OFFICER (BAMLCO)**

The Manager, the second Officer of the branch or a high official experienced in general banking /investment/foreign exchange shall be nominated as the BAMLCO by the CAMLCO. 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. The job description and the responsibilities of BAMLCO shall be mentioned in his/her appointment letter. BAMLCO shall arrange AML & CFT meeting with other concerned important officials of the branch on quarterly basis and shall 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
- Record keeping
- Implementation of Local Sanction List along with resolutions of UN Security Council
- Activities regarding Self-Assessment Reporting
- Sending Minutes of BCU Meeting Money Laundering and Combating Terrorist Financing Division on quarterly basis.

### 6.8.1. Authorities and Responsibilities of BAMLCO

For preventing ML, TF & PF in the branch, the BAMLCO will perform the following responsibilities along with the circular regarding their responsibilities given by AML & CTF Division –

- Ensure that the KYC of all customers have been done properly as well as making the KYC of the new customers are properly done too.
- Ensure that the UN Security Council and domestic sanction list is being checked properly.
- Before establishing business relationship with a customer or before providing any banking facilities to the existing customers both local and international transactions are to be checked.
- Keep information of dormant accounts and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction.
- Ensure regular transaction monitoring including those of staffs/ PEPs/ IPs/ high risk one to find out any suspicious/ unusual transaction.
- Shall follow a triggering system against transaction profile or other suitable threshold through an automated manner.
- Review cash transaction to find out any structuring.
- Review CTR to find out STR/SAR.
- Ensure the checking of UN sanction list before making any foreign transaction.
- Ensure arresting of any potential Trade Based Money Laundering (TBML) in branch level.
- Ensure that all the employees of the branch are well aware and capable of identifying any unusual transaction or any attempt of unusual transaction.
- Compile self-assessment of the branch regularly and arrange quarterly meeting regularly and submit the minutes of the same to Anti Money Laundering and Combating Terrorist Financing Division.
- Accumulate the training records of branch officials and take initiatives including reporting to Anti Money Laundering and Combating Terrorist Financing Division, Central Compliance Committee (CCC), Bangladesh Krishi Bank Training Institute.
- Ensure all the required information and document are submitted properly to CCC
- Ensuring any freeze order or stop payment order is being implemented properly and timely.
- 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 whether the involved persons have any affiliation to with the branch; if so the BAMLCO shall take necessary steps.
- Ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements.
- Ensure that corrective actions have been taken by the branch to address the deficiency identified by the BFIU, or BKB's internal/ external audit/ visit.

### 6.9. AML/ CFT COMPLIANCE OFFICER

The AML/CFT Compliance Officer should receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, Bangladesh Bank directives and internal policies. In addition, the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

### 6.10. INTERNAL CONTROL AND COMPLIANCE (ICC)

Internal Audit of BKB means Internal Audit & Inspection Division, and Internal Control and Compliance (ICC) of BKB are divided into Monitoring Division, Compliance Division and Risk Management Division. All Divisions shall have an important role for ensuring proper implementation of bank's AML & CFT Compliance Program. BKB 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.

To ensure the effectiveness of the AML & CFT compliance program, Bangladesh Krishi Bank shall assess the program regularly and look for new risk factors' internal auditors shall be well resourced and will enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable. The internal audit of shall-

- 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 shall include a sample test check of teller's 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 unit/person.
- Examine that corrective actions have been taken on deficiency identified by the BFIU or Bank's internal/external auditors.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

Followings shall be determined while assessing the training program and materials-

- The importance of the board and the senior management place on going 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.

Besides, Audit & Inspection Division shall perform the following duties in connection with AML & CFT compliance-

- Audit & Inspection Division shall assess the Self-assessment received from the branches and if there is a risk proximity in any branch, it shall inspect the branch immediately and shall inform the matter to the Anti-Money Laundering & Combating Terrorist Financing Division.
- While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the Audit & Inspection Division shall examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure; and after determining the rating of the branch, it shall produce the report on that concerned branch. Furthermore, under a separate inspection program of at least 10% more branch beside regular yearly inspection/audit schedule, the Audit & Inspection Division shall examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure; and after determining the rating of the branch, it shall produce the report on that concerned branch.
- The Audit & Inspection Division shall send a copy of the report with the rating of the branches inspected/audited by the Audit & Inspection Division to the Money Laundering and Combating Terrorist Financing Division of the bank.

### **6.11. EXTERNAL AUDITOR**

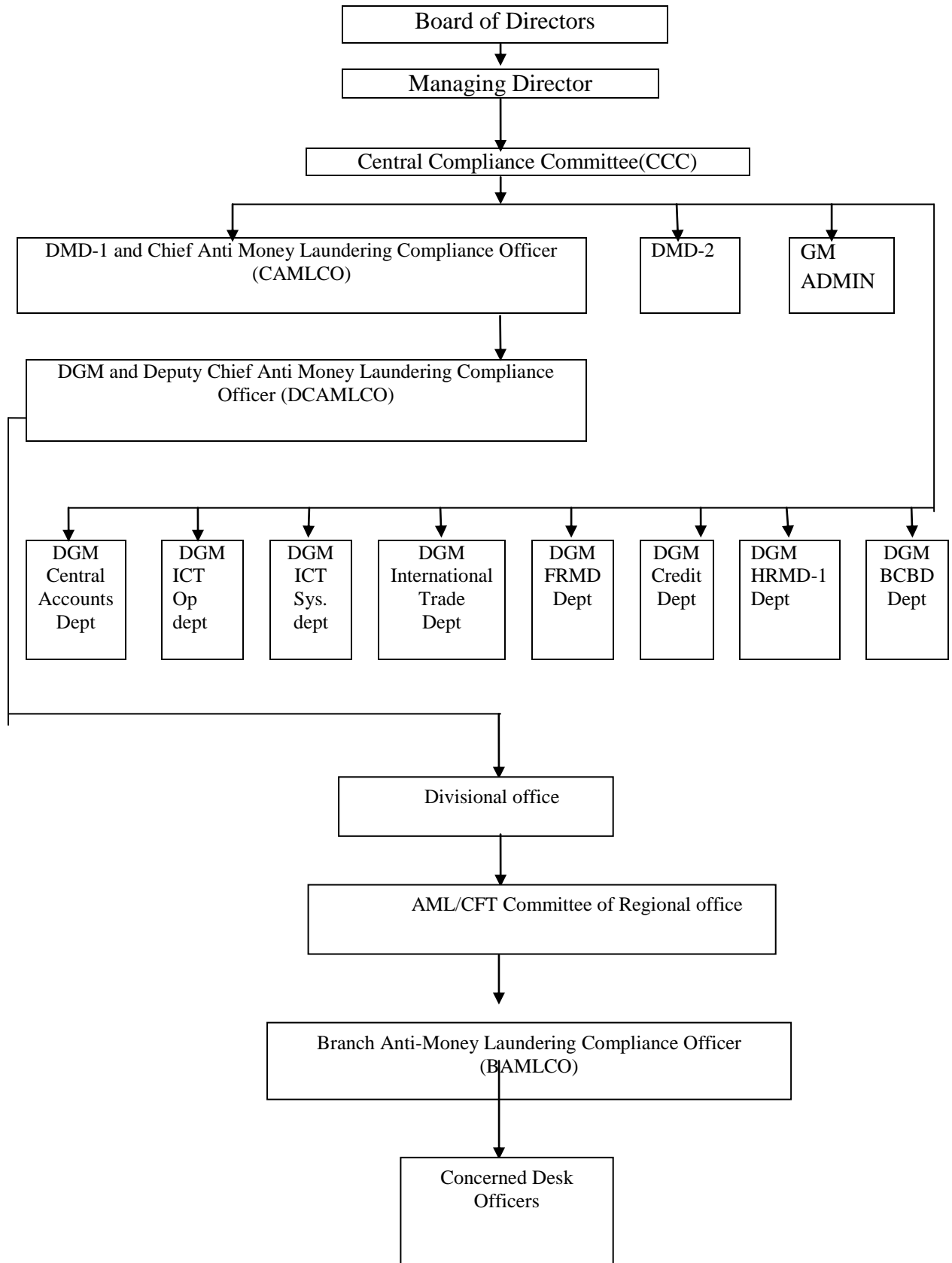
External auditor will also play an important role in reviewing the adequacy of AML & CFT controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External auditor would be risk-focus while developing their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors shall report incidences of suspected criminal activity uncovered during audits in its audit report. But due to confidentiality, they must not ask about any SAR/ STR already reported to BFIU, as per BFIU Circular No.26 dated 16.06.2020.

### 6.12. FIXING UP THE RESPONSIBILITIES

The table below details the individual responsibilities of the above functions but not limited to-

<b>Position for performing Function</b>	<b>Role/Responsibilities</b>
Accounts Officer	<ul style="list-style-type: none"> <li>• Perform due diligence on prospective clients prior to opening an account using the bank's standard account opening form.</li> <li>• Be diligent regarding the identification (s) of account holder and the transactions relating to the account.</li> <li>• Ensure all required documentation is completed satisfactorily.</li> <li>• Complete the KYC Profile for the new customer.</li> <li>• Ongoing monitoring of customer's KYC profile and transaction activity.</li> <li>• Escalate any suspicion to the Supervisor/BAMLCO.</li> </ul>
Customer Service Officer	<ul style="list-style-type: none"> <li>• Support the Accounts Officer in any of the above roles.</li> <li>• Perform the Accounts Officer roles in his/their absence.</li> <li>• Perform AML risk assessment for the branch.</li> </ul>
Operations Officer	<ul style="list-style-type: none"> <li>• Ensure that all control points are completed prior to transaction monitoring.</li> <li>• Be diligent on transaction trends for clients.</li> <li>• Update customer transaction profiles in the ledger/system.</li> <li>• Obtain documentary evidence of large cash deposits.</li> </ul>
BAMLCO/ Branch Manager	<ul style="list-style-type: none"> <li>• As per BFIU Circular No. 26 dated 16.06.2020 and stated above also</li> </ul>
Regional office Compliance Unit	<ul style="list-style-type: none"> <li>• To ensure that branches under their control comply with AML &amp; CFT rules and regulations and Bank's internal strategies properly</li> <li>• Must monitor whereas the instructions of circular given by Managing Director &amp; CEO as well as CAMLCO are followed or not by the Branches</li> <li>• To ensure timely submission of branches AML &amp; CFT returns (CTR, STR, self-assessment and others) to AML &amp; CTF Division</li> <li>• To monitor AML &amp; CFT activities of the branches under their control on regular basis.</li> </ul>
CAMLCO	<ul style="list-style-type: none"> <li>• To ensure the implementation of above stated responsibilities regarding AML &amp; CFT program of the Bank efficiently</li> </ul>
Deputy CAMLCO	<ul style="list-style-type: none"> <li>• To assist CAMLCO in implementing and enforcing the Bank's AML &amp; CFT policies.</li> </ul>
Managing Director & CEO	<ul style="list-style-type: none"> <li>• Overall responsibility to ensure that the Bank has a compliance culture with efficient AML &amp; CFT program.</li> </ul>

# Compliance Structure of BKB



# Chapter 7

## Customer Due Diligence

### 7.1. KNOW YOUR CUSTOMER PROGRAM

The adoption of effective Know Your Customer (KYC) program is an essential part of financial institutions' risk management policies. Having sufficiently verified/corrected information about customers, knowing Your Customer (KYC) and making use of that information underpins all AML/CFT efforts, and is the most effective defence against being used to launder the proceeds of crime. Financial institutions with inadequate KYC program may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the financial institution's overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences.

### 7.2. KNOW YOUR CUSTOMER (KYC) PROCEDURE

Money Laundering Prevention Act, 2012 requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. FATF recommendation 10 states that where the financial institution is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, and to identify the beneficial owner, and to take reasonable measures to verify the identity of the beneficial owner and unable to obtain information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

#### 7.2.1. Nature of Customer's Business

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. In order to judge whether a transaction is or is not suspicious, branches need to have a clear understanding of the business carried out by their customers.

#### 7.2.2. Identifying Real Person

Branch authority must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally. This will safeguard against opening of fictitious account.

#### 7.2.3 Document is not Enough

The best identification documents possible should be obtained from the prospective customer i.e. those that are 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 branch must know who their customers are, and have the necessary documentary evidence to verify this. Collection of document is not enough for KYC, identification is very important.

### 7.2.4. Components of KYC Program

A. To designing the KYC program for BKB have included the following elements which should start from the financial institutions' risk management and control procedures and should include –

- (1) Customer acceptance policy,
- (2) Customer identification,
- (3) On-going monitoring of high risk accounts and
- (4) Identification of suspicious transactions.

Bank should not only establish the identity of their customers, but should also monitor account activities to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of financial institutions' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programs beyond these essential elements should be tailored to the degree of risk.

B. To identify 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-

- (1) Who owns 20 or more percent of a company or legal arrangements?
- (2) Who has effective control of the customer?
- (3) The person on whose behalf a transaction is conducted

C. 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.

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

Bank, upon its own satisfaction ensure CDD of beneficial ownership by collecting information and documents from independent and reliable sources that includes publicly available information, information from customer or information from other reliable sources. In this regard, the prescribed KYC form for Beneficial Owner shall be used.

### 7.3. SIMPLIFIED CUSTOMER DUE DILIGENCE (SCDD)

Bangladesh Krishi Bank must apply Simplified Customer Due Diligence (SCDD) in the following cases-

- In case of carrying out occasional transactions below Tk.50,000/- (fifty thousand) by the Walk-in customers, name and address of the Sender/ Applicant and Receiver/ Beneficiary are required.
- If the transaction amount is above Tk.50,000/- (fifty thousand) but less than Tk.5,00,000/ (five lakh), Photo paste ID of the Sender/ Applicant/ Depositor/ Withdrawer is required along with information as mentioned at clause 'a' above.
- In case of financial inclusive accounts (School Student A/C, Farmer A/C and other No-Frill Accounts).

### 7.4. IN CASE WHERE CONDUCTING THE CDD MEASURE IS NOT POSSIBLE

If conducting the CDD measure becomes impossible because of the non-cooperative behavior of the customer or if the collected information turned out to be unreliable, that is, Bangladesh Krishi Bank could not collect satisfactory information on customer identification and could not verify that, BKB shall take the following measures-

- Not carry out a transaction with or for the customer through a bank account.
- Not establish a business relationship or carry out an occasional transaction with the customer.
- Terminate any existing business relationship with the customer.
- The branch shall preserve the information and documents of such A/C and send the same to Anti Money Laundering & Combating Terrorist Financing Division and they shall circulate the same to the branches for their information and necessary cautionary measures.
- Consider whether it ought to be making a report to the BFIU through an STR.
- Bangladesh Krishi Bank shall always consider whether an inability to apply CDD measures is caused by the customer. In this case, the Bangladesh Krishi Bank shall consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the bank shall consider whether there are any circumstances which give grounds for making a report to BFIU.
- If Bangladesh Krishi 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.
- If Bangladesh Krishi Bank concludes that there are no grounds for making a report, it will need to make a decision on the appropriate course of action. This may be retaining the funds while it seeks other ways of being reasonably satisfied as to the customer's identity or returning the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

### 7.5. ENHANCED DUE DILIGENCE (EDD)

In case of High Risk rated customers BKB shall conduct Enhanced Due Diligence which combines the following measures-

- Additional KYC information will be collected from independent and reliable sources.
- Enhanced measures will be observed to know the purpose of the respective A/C.
- Obtaining permission from CAMLCO if required.
- Conducting on-going transaction monitoring of the respective A/C.

## **Chapter 7: Customer Due Diligence**

Bangladesh Krishi Bank will 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), influential persons and chief executives or top level officials of any international organization.
- Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes.
- While establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering and terrorism financing (such as the countries and territories enlisted as High – Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force’s Public Statement).
- STR submitted Accounts.
- In-house investigated suspicious Accounts.

### **7.6. CUSTOMER UNIQUE IDENTIFICATION CODE**

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

### **7.7. CORRESPONDING BANKING**

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

Bank should establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank through collection of information as per BFIU circular. The bank should also obtain approval from its Senior Management before establishing and continuing any correspondent relationship. The bank must be sure about the effective supervision of that foreign bank by the relevant regulatory authority. Bank should not establish or maintain any correspondent relationship with any shell bank and not to establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank.

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

If any respondent bank allow 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.

### **7.8. POLITICALLY EXPOSED PERSONS (PEPs), INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION**

All Clients must be subject to an assessment to determine whether they are PEPs or Influential Persons or chief executives or top level officials of any international organization and their linked entities. These customers pose a higher risk of money laundering, bribery, corruption and reputational risk to the bank due to their current or former position of political power or influence, which makes them more vulnerable to corruption. Relationships with these customers may increase the risk to the bank due to the possibility of that individuals holding such positions may misuse their power and influence for personal gain or advantage or for the personal gain or advantage of their Close Family Members and Close Associates. The person's status (PEPs, Influential Persons and Chief Executives or top level officials of any international organization) itself does not incriminate individuals or entities. It does, however, put a prospective or existing Client into a higher risk category.

#### **7.8.1. Definition of Peps**

Politically Exposed Persons (PEPs) refer to "Individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials." The following individuals of other foreign countries must always be classed as PEPs:

- Heads and deputy heads of state or government;
- Senior members of ruling party;
- Ministers, deputy ministers and assistant ministers
- Members of parliament and/or national legislature
- Members of the governing bodies of major political parties;
- Members of supreme courts, constitutional courts or other high level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
- Heads of state-owned enterprises.
- Ambassadors, charge d'affaires.

### 7.8.2. CDD Measures for PEP

Bank need to identify whether any of its customers is a PEP. Once identified bank need to apply enhanced CDD measures. Moreover, they need to perform the following-

- a) Bank has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a PEP;
- b) obtain senior managements' approval before establishing such business relationship;
- c) take reasonable measures to establish the source of fund of a PEP's account;
- d) monitor their transactions in a regular basis; and
- e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly .

### 7.9. DEFINITION OF INFLUENTIAL PERSONS

'Influential persons' refers to, "Individuals who are or have been entrusted with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials."

The following individuals must always be classed as Influential persons:

- a) Heads and deputy heads of state or government;
- b) Senior members of ruling party;
- c) Ministers, state ministers and deputy ministers;
- d) Members of parliament and/or national legislatures;
- e) Members of the governing bodies of major political parties;
- f) Senior Secretary, Secretary, Additional Secretary, Joint secretary in the ministries;
- g) Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- h) Governors, deputy governors, executive directors and general managers of central bank;
- i) Heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
- j) Heads of state-owned enterprises;
- k) Members of the governing bodies of local political parties;
- l) Ambassadors, charge d'affaires or other senior diplomats;
- m) City mayors or heads of municipalities who exercise genuine political or economic power;
- n) Board members of state-owned enterprises of national political or economic importance.

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

### 7.9.1. CDD Measures for Influential Persons:

Bank need to identify whether any of their customers is an IP. Once identified bank need to apply enhanced CDD measures. Moreover, they need to perform the following-

- a) Banks have to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is an IP);
- b) Obtain senior managements' approval before establishing such business relationship;
- c) Take reasonable measures to establish the source of fund of a IP's account;
- d) Monitor their transactions in a regular basis; and
- e) All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

### 7.10. DEFINITION OF CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

'Chief executive of any international organization or any top level official' refers to, "Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the boards or equivalent functions." The heads of international organizations and agencies that exercise genuine political or economic influence (e.g. the United Nations, the International Monetary Fund, the World Bank, the World Trade Organization, the International Labor Organization) must always be classed as this category.

#### 7.10.1. CDD Measures for Chief Executives or Top Level Officials of Any International Organization

Bank need to identify whether any of its customers is a CEO or top level officials of any international organization. Once identified bank need to apply enhanced CDD measures.

Moreover, they need to perform the following-

- a) Banks have to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a CEO or top level officials of any international organization;
- b) obtain senior managements' approval before establishing such business relationship;
- c) take reasonable measures to establish the source of fund of the account of a CEO or top level officials of any international organization;
- d) monitor their transactions in a regular basis; and
- e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly .

**7.11. CLOSE FAMILY MEMBERS AND CLOSE ASSOCIATES OF PEPs, INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION**

In addition, close family members and close associates of these categories will also be classified as the same category. Close Family Members include:

- a) the PEP's/influential persons/chief executive of any international organization or any top level official's spouse (or any person considered as equivalent to the spouse);
- b) the PEP's/influential persons/chief executive of any international organization or any top level official's children and their spouses (or persons considered as equivalent to the spouses); and
- c) the PEP's/influential persons/chief executive of any international organization or any top level official's parents;

There may be exceptional circumstances where the individual should not be classified as a 'Close Family Member' of the PEPs, such as estrangement, divorce etc. In such cases, the circumstances must be thoroughly investigated, examined and caution exercised. In addition, where other family members such as the siblings, cousins, relatives by marriage of the PEP are deemed, by virtue of the nature of the relationship, to have a close relationship with the PEPs, they should also be classified as PEPs.

A Close Associate of a PEPs/Influential Person/Chief executive of any international organization or any top level official include-

- a) an individual who is known to have joint beneficial ownership or control of legal entities or legal arrangements, or any other close business relations with the PEPs; and
- b) an individual who has sole beneficial ownership or control of a legal entity or legal arrangement which is known to have been set up for the benefit of the PEPs.

In addition, it should include any person publicly or widely known to be a close business colleague of the PEP, including personal advisors, consultants, lawyers, accountants, colleagues or the PEP's fellow shareholders and any person(s) that could potentially benefit significantly from close business associations with the PEPs.

**7.12. 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.

### 7.13. 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 has to be preserved. For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved.

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

### 7.14. DOMESTIC WIRE TRANSFERS

In case of threshold domestic wire transfers of at least BDT 50,000/- (fifty thousand), 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. For providing Mobile financial services the concerned 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.

### **Duties of Ordering, Intermediary and Beneficiary Bank in case of Wire Transfer-**

#### **Ordering Bank:**

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

#### **Intermediary Bank:**

For cross-border and domestic wire transfers, BKB 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.

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

As a beneficiary bank BKB 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 those information for 5 (five) years.

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

### 7.15. CDD FOR BENEFICIAL OWNERS

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

- Any natural person operating accounts on behalf of customer;
- Any person (whether acting alone or together) who has controlling interest or ownership interest on a customer who might be legal entity or legal arrangements. Where there is any doubt identifying controlling interest, the banks should consider other means to determine controlling interest or ownership of a legal entity or arrangements. In addition to that bank should also consider.
- reasonable measures to verify the identity of the relevant natural person who hold senior management position;
- Any person or entity who has controlling or 20% or above shareholding within any or legal entity.
- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercises control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) should consider for other types of legal arrangements.

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

### **7.16. PERSONS WITHOUT STANDARD IDENTIFICATION DOCUMENTATION**

It is generally believed that financial inclusion is helpful in preventing money laundering and terrorist financing. Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous AML procedures is recommended. Internal procedures must allow for this, and must provide every specific advice to staff on how identity can be confirmed in these exceptional circumstances. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph. BKB should not allow 'high value' transactions to this kind of customers. Simplified Due Diligence should be done for low risk accounts like Student Accounts, Farmer's Accounts and other No Frill accounts.

### **7.17. 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. Central Compliance Unit should preserve data of such accounts.

# Chapter 8

## Customer Acceptance Policy

### 8.1. DEFINITION OF CUSTOMER

For the purpose of KYC Procedure a "Customer" is defined in BFIU Circular No.26 dated 16/06/2020, as:

Any person or institution is maintaining any type of account with a Bank or financial institution;

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

#### **And in general customer is defined as**

- A person or entity that maintains an account or has a business relationship with the Bank/FI-
- One on whose behalf the account is maintained (i.e. the beneficial owner); Beneficial owner means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is conducted and exercise ultimate effective control over a juridical person.
- Beneficiaries of transactions conducted by professional intermediaries, such as stock brokers, Chartered accountants, Solicitors etc. as permitted under the law, and
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

### 8.2. CUSTOMER ACCEPTANCE POLICY (CAP):

Customers are vitally important for banking business. Increasing competition is forcing banks to pay much more attention to satisfy customers. Our motto is to extend best services to our customers. We are also aware that sometimes customers pose the risk of money laundering and financing of terrorism to the financial institutions particularly the banks. So the inadequacy or absence of KYC standards can result in serious customer and counterpart risks, especially reputation, operational, legal and compliance risks. Collecting sufficient information about our customers is the most effective defense against being used as the medium to launder the proceeds of crimes and to finance the terrorism through bank accounts. As per Sec. 25 of Money Laundering Prevention Act- 2012 each bank requires to keep satisfactory evidence of the identity of those it deals with and also requires making necessary arrangement to prevent any transaction related to crimes as described in Anti-Terrorism (Amendment) Act- 2012. It is also the responsibility of each bank to identify suspicious transactions of their customers with due care and diligence.

## Chapter 8: Customer Acceptance Policy

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

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

In anonymous or fictitious name or any numbered account should not be open.

"Shell Company"- a company that is incorporated but has no significant assets or operations. These companies are often used by fraudulent operators as fronts in many money laundering schemes.

"Shell Banks"- Shell Bank means a bank that has no physical presence in the country which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence. As defined in the USA Patriot Act, banks are prohibited from opening or maintaining accounts for shell banks.

- Internet gaming companies, firearms dealers and other entities that may pose potential reputational risk to the bank.
- Persons/entities about which information is available through reliable sources indicating involvement in criminal conduct (e.g., those allegedly having links to drug trafficking, terrorism, corruption or organized crime).
- Persons/entities with businesses where we have doubts about the legitimacy of their activities or the source of funds.
- Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grades.
- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.
- Not to open an account or close an account where the financial institution is unable to apply appropriate customer due diligence measures i.e. financial institution is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the financial institution. Decision by a financial institution to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a 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 financial service 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.
- Uniform A/C Opening Forms, KYC Profile Form and Transaction Profile Form developed in line with the guidelines of Bangladesh Bank should be properly filled and duly signed in;

## Chapter 8: Customer Acceptance Policy

- In case of opening a Politically Exposed Person (PEP) / Influential Person (IP) / Chief Executives or Top Level Officials of any International Organization account, the branch shall comply the instructions contained in BFIU Circular No. 26 dated 16.06.2020 issued by Bangladesh Bank and amendments issued from time to time. Such types of account will be classified as high risk and will be required very high level monitoring;
- Source of funds, income or wealth and complete information on the actual or beneficial owners.
- Accounts holding 20% or more share of the account must be obtained at the time of opening of any account
- In case of establishing correspondent banking relationship, the branch /concerned division /department shall follow the guidelines as contained in BFIU Circular No. 26 dated 16.06.2020 issued by Bangladesh Bank and amendments issued from time to time meticulously.
- In case of opening an account of Non Residents Bangladeshi (NRB) the rules of Foreign Exchange Regulation Act, 1947 and the instructions under this rules promulgated by Bangladesh Bank have to be followed.
- The branches, where locker service facilities exist, will also follow the identification procedure for their locker customers.

It is important to bear in mind by all employees of the bank that the customer identification process does not end at the point of application. Once account relationship has been established, reasonable steps should be taken by the branch from time to time to ensure that descriptive information is kept updated. Decisions to enter into business relationships with higher risk customers, such as public figures or politically exposed persons (PEPS) should be taken exclusively at senior management level.

The customer Acceptance Policy has to ensure that explicit guidelines are in place on the following aspects of customer relationship in the financial institution-

- Customer's background
- Country of origin
- Public or high profile
- Linked accounts
- Volume of business activities
- Risks associated in the business of customers
- Other risk indicators
- Basic requirements for Account Opening
- All information is available for judging the creditworthiness of borrowers.
- All information on walk-in customers as required in AML circular.

### 8.3. CUSTOMER IDENTIFICATION

Customer identification is an essential element of KYC standards & CDD measures. 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 financial institution to undertake regular reviews of existing records time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a financial institution becomes aware at 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 of BDT 5,000 or more 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 to undertake subsequent transactions. However, information should be updated or reviewed as appropriate and records must be maintained.

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 at 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.

### **8.4. WHAT CONSTITUTES A CUSTOMER'S IDENTITY**

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

- The physical identity (e.g. Birth Certificate, TIN/ VAT Registration Certificate, Passport/ National ID/ Smart ID, Driving License etc.);
- The activity undertaken.

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

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

Once account relationship has been established, reasonable steps should be taken by the institution to ensure that descriptive information is kept up-to-date as opportunities arise. It is important to emphasize that the customer identification process does not end at the point of application. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector. It will also depend on the nature of the product or service being offered, and whether personal contact is maintained enabling file notes of discussion to be made or whether all contact with the customer is remote.

## Chapter 8: Customer Acceptance Policy

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

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

### 8.5. ACCOUNT OF INDIVIDUAL CUSTOMER:

Following information must be obtained by the Branches while opening account or establishing other relationships with individual customers:

- Full and accurate name;
- Parents names in full;
- Spouse Name;
- Date of birth;
- Current and permanent address;
- Details of occupation/employment and source of fund;
- Contact information, such as mobile/ telephone number/ e-mail;
- Nominee information;
- Photograph of both Account Holder and Nominee duly signed by the introducer and a/c holder respectively.

The original, certified copy of the following Photo ID also play vital role to identify the customer;

- Valid passport; or
- Valid driving license; or
- National ID Card; or
- Employer provided ID Card, bearing the photograph and signature of the applicant;

The following documents may be considered for identity also. Any photocopies of documents showing photographs and signatures should be clearly understandable:

- Birth Registration Certificate (Printed copy, with seal & signature from the Register)
- Credit Card (if any)
- Any other documents that satisfy to the bank

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 person has to be submitted according to the bank's requirement. The certificate must include a photo which is duly attested by the signing renowned person.

The following documents should be considered for verification of source of funds:

- Salary Certificate (For salaried person)
- Employee's 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)
- Document of FDR encashment (if any)
- Document of foreign remittance (if any fund comes from outside the country)
- Document of retirement benefit (if any)
- Other Bank statement (if any)
- Bank Loan

## Chapter 8: Customer Acceptance Policy

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

- Provision of a recent utility bill (not beyond 3 months old), tax assessment or Bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- Acknowledgement receipt of Thanks Letter through postal department/courier
- Proof of delivery of thanks letter through courier
- Third party verification report
- Physical verification report of bank official
- Residential address appearing on an official document prepared by a
- Government Agency
- Checking the telephone directory;
- Checking the National ID Card;
- Sending thanks letter to introducer.

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

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

### 8.6. JOINT ACCOUNTS:

Following information must be obtained by the Branches while opening account or establishing other relationships with Joint Account customers:

- Valid passport; or
- Valid driving license; or
- National ID Card; or
- Employer provided ID Card, bearing the photograph and signature of the applicant; or
- Birth Registration Certificate (Printed copy, with seal & signature from the Register)
- Credit Card (if any)
- Any other documents (photo) that satisfy the bank

The following documents should be considered for verification of source of funds:

- 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 housewife, students etc.)
- Trade License if the customer declared to be a business person
- TIN (if any)
- Documents of property sale (if any)
- Document of FDR encashment (if any)
- Document of foreign remittance (if any fund comes from outside the country)
- Document of retirement benefit (if any)
- Other Bank statement (if any)
- Bank Loan

## Chapter 8: Customer Acceptance Policy

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

- Provision of a recent utility bill (not beyond 3 months old), tax assessment or Bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- 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.
- Residential address appearing on an official document prepared by a Government Agency.
- Checking the telephone directory.
- Checking the National ID Card.
- Sending thanks letter to introducer.

### 8.7. ACCOUNT OF SOLE PROPRIETORSHIPS OR INDIVIDUALS DOING BUSINESS

Following information must be obtained by the Branch/Bank while opening account or establishing other relationships with Sole Proprietorships or Individuals doing business:

- Proof of the name, address and activity of the concern.
- Valid and updated Trade License /Certificate issued by the Municipal authorities.
- TIN certificate.
- 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.)
- Photos of the A/C holder duly signed by the introducer.
- Photo of the nominee duly signed by the A/C holder.
- Personal information of the Proprietor.
- Passport / National ID Card / Valid driving license/ Birth Registration Certificate (Printed copy, with seal & signature from the Registrar).
- Credit Card (if any).
- Any other documents that satisfy to the Bank.

The following documents should be considered for verification of source of funds:

Self-declaration acceptable to the Bank (commensurate with nature and volume of business)

- Trade License
- TIN (if any)
- Documents of property sale (if injected any fund by selling personal property)
- 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)
- Other Bank statement (if any)
- Bank Loan (if any)
- Personal borrowing (if any)

## Chapter 8: Customer Acceptance Policy

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

- Provision of a recent utility bill (not beyond 3 months old), tax assessment or Bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined).
- 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.
- Residential address appearing on an official document prepared by a Government Agency.
- Checking the telephone directory.
- Checking the National ID Card.
- Sending thanks letter to introducer.

### 8.8. ACCOUNT OF PARTNERSHIP FIRMS

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

Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable) should retain with Account Opening Form.

An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

Following information must be obtained by the Branch/Bank while opening account or establishing other relationships with Partnership Firms:

- Partnership deed / partnership letter (Notarized).
- Registered partnership deed (if registered).
- Resolution of the partners, specifying operational guidelines/ instruction of the partnership account.
- National ID Card of all partners or Passport of partners or Birth Registration Certificate of partners (Printed copy, with seal & signature from the Registrar)
- Valid driving license of partners (if any)
- Credit Card of partners (if any)
- Rent receipt of the shop (if the shop is rental)
- Ownership documents of the shop (i.e purchase 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 association etc.) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf.
- Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses.

## Chapter 8: Customer Acceptance Policy

- TIN certificate of the firm and TIN of the partners.
- Personal information and Photos of all the partners.
- Any other documents that satisfy to the bank.

The following documents should be considered for verification of source of funds:

- Trade License.
- Documents of property sale (if injected any fund by selling personal property of a partner).
- Document of FDR encashment (if any partner injected capital by encashing personal FDR).
- Document of foreign remittance (if any fund comes from outside the country)
- Other Bank statement (if any).
- Bank Loan (if any).
- Personal Borrowing (if any).

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

- Provision of a recent utility bill (not beyond 3 months old), tax assessment or Bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- 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;
- Residential address appearing on an official document prepared by a Government Agency, Checking the telephone directory;
- Checking the National ID Card;
- Sending thanks letter to introducer .

### 8.9. ACCOUNT OF LIMITED COMPANY

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

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

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

The following documents should normally be obtained from companies:

- Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the Board Resolution to open the account relationship with the respective Branch /Bank and the empowering authority for those who will operate the account;
- Explanation of the nature of the applicant's business, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.
- TIN certificate of the company/firm and all of the Directors.
- Personal Information or profile of all the Directors.

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

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

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

### **8.10. ACCOUNT OF PRIVATE LIMITED COMPANIES:**

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

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

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

The following documents should normally be obtained from companies:

- Passport of all the directors.
- National ID Card of all the directors.
- Personal information or profile of all the Directors.
- TIN certificate of the company/firm and all of the Directors.
- Certified copy of Certificate of incorporation or equivalent, details of the registered office, and place of business.
- Certified copy of the Memorandum and Articles of Association.
- Update List of Directors (Form XII).
- Copy of the Board Resolution to open the account relationship with the respective Branch/Bank and identification of those who have authority to operate the account.
- Explanation of the nature of the applicant's business, the source of funds, and a copy of the last available financial statements where appropriate.
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company. Subsequent changes to signatories must be verified.
- Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf.
- Nature of the company's business.

## Chapter 8: Customer Acceptance Policy

- Expected monthly turnover.
- Identity of beneficial owners, holding 20% share 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.

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

- All of the directors who will be responsible for the operation of the account/ transaction.
- All the authorized signatories for the account/ transaction.
- All holders of powers of attorney to operate the account/ transaction.
- The beneficial owner(s) of the company.
- The majority (20% or more) shareholders of a private limited company.

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

The following documents should be considered for verification of source of funds:

- A copy of last available financial statements duly authenticated by competent authority
- Trade License
- TIN
- VAT registration
- Other Bank statement
- Bank Loan

### 8.11. ACCOUNT OF PUBLIC LIMITED COMPANIES

The following documents should normally be obtained from companies:

- Passport of all the directors
- National ID Card of all the directors
- TIN certificate of the company/firm and all of the Directors.
- Personal information or profile of all the Directors.
- Certificate of incorporation
- Memorandum and Articles of Association
- Certificate of commencement of business
- List of directors in form -XII
- Copy of the Board Resolution to open the account relationship with the respective Branch/Bank 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% share 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.

The following documents should be considered for verification of source of funds:

- A copy of last available financial statements duly certified by a professional accountant.
- Trade License
- TIN
- Cash Flow Statement
- VAT registration
- Other Bank statement
- Bank Loan
- Any other genuine source

### **8.12. ACCOUNT OF GOVERNMENT OWNED ENTITIES:**

Following information must be obtained by the Branch/Bank while opening account:

- Statue of formation of the entity;
- Copy of the Board Resolution to open the account relationship with the respective Branch/Bank and identification of those who have authority to operate the account;
- Passport of the operator (s)
- National ID Card of the operator

### **8.13. ACCOUNTS OF SOCIETIES, ASSOCIATIONS, NGOs, CLUBS, TRUST, FOUNDATIONS, CHARITIES / RELIGIOUS ORGANIZATIONS AND OTHER ORGANIZATIONS:**

Following information /document(s) must be obtained by the Branch/Bank while opening account or establishing other relationships with Societies, Associations NGOs, Clubs, Trust, Foundations, Charities or Religious Organizations and other organizations:

- National ID Card of the operator (s) / the Trustee(s)
- Passport of the operator (s) / the Trustee(s)
- By-laws (certified)
- Certified true copy of the Trust Deed
- Documents of nature of the Organizations / NGO
- Certificate of Registration issued by competent authority (if registered)
- Telephone/Utility Bill in the name of the organization
- List of Managing Committee Members / Directors and their bio-data
- Resolution of the Managing body / Board of Directors/ the Executive Committee of the NGO/ Organization/trust for opening of the account and identification of those who have authority to operate the account
- Power of attorney allowing transaction in the account (for Trusts, Foundations or similar entities accounts)
- Photos of authorized Managing committee Members duly signed by the introducer.

The following documents should be considered for verification of source of funds:

- A copy of last available financial statements duly certified by a professional accountant.
- TIN
- Other Bank statement
- Certificate of Grant / Aid/ Donation
- Any other legal source
- Subscription (If any)
- Donation (If any)
- If unregistered declaration of authorized person / body

### **8.14. NON BANKING FINANCIAL INSTITUTIONS (NBFI) :**

Following information must be obtained by the Branches while opening account or establishing other relationships with NBFI Account customers:

- Passport of all the directors
- National ID Card of all the directors
- TIN certificate of the company/firm and all of the Directors.
- Personal information or profile of all the Directors.
- Certificate of incorporation
- Memorandum and Articles of Association
- Certificate of commencement of business
- List of directors in Form XII
- Copy of the Board Resolution to open the account relationship with the respective Branch/Bank 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% share 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.

The following documents should be considered for verification of source of funds:

- A copy of last available financial statements duly certified by a professional accountant.
- Trade License
- TIN
- Cash Flow Statement
- VAT registration
- Other Bank statement
- Bank Loan

### 8.15. EMBASSIES

Following information must be obtained by the Branches while opening account or establishing other relationships with Embassy Account customers:

- Valid Passport with visa of the authorized officials
- Clearance of the Ministry of Foreign Affairs
- Other relevant documents in support of opening account

### 8.16. APPROPRIATENESS OF DOCUMENTS:

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

### 8.17. CHANGE IN ADDRESS OR OTHER DETAILS:

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

### 8.18. INTRODUCER:

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

### 8.19. POWERS OF ATTORNEY/ MANDATES TO OPERATE ACCOUNTS:

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept. On the other hand, valid reasons to execute mandate under the law for operating the accounts should exist.

### 8.20. TIMING AND DURATION OF VERIFICATION:

The best time to undertake verification is prior to entry into the account relationship. Verification of identity should be completed before any transaction is completed in account,

However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority. This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing.

Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is itself suspicious.

### **8.21. VERIFICATION OF SOURCE OF FUNDS**

BKB should collect and verify the document supporting source of fund of the person at the time of establishing any business relationship or while conducting CDD. The document could include present employment identity, salary certificate/copy/advice, pension book, financial statement, income tax return, business document or any other document that could satisfy the bank. The bank should request the person to produce E-TIN (Electronic Tax Identification No) certificate which declares taxable income.

### **8.22. VERIFICATION OF ADDRESS**

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

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

### **8.23. JOINT ACCOUNTS**

In respect of joint accounts the full name and accurate name and address of the account holders should be in accordance with valid documents.

### **8.24. NO FACE-TO-FACE CONTACT**

Where there is no face-to-face contact, Bank should not allow in establishing relationship with the clients.

### **8.25. RECORD KEEPING**

All documents collected or gathered for establishing relationship must be filed in with supporting evidence. Where this is not possible, the relevant details should be recorded on the applicant's file. Bank which regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records.

### **8.26. PERSONS WITHOUT STANDARD IDENTIFICATION DOCUMENTATION**

It is generally believed that financial inclusion is helpful in preventing money laundering and terrorist financing. Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous AML 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. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph. Bank shall not allow “high value” transactions to this kind of customers.

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number.

### 8.27. MINOR

- For minor, Bank shall obtain following information while opening accounts relationship:
- Full and accurate name ;
- Parent's names in full;
- date of birth;
- current and permanent address;
- Birth Certificate
- Contact information, such as mobile/telephone number
- Full information of the Guardian like Photos, Passport/ NID and Personal Information.

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

### 8.28. CARDS/ ELECTRONIC BANKING/ MOBILE BANKING:

The KYC procedures is invariably be applied to new technologies including Debit Card /Electronic Banking/Mobile Banking facility or such other product which may be introduced by the Bank in future that might favour anonymity, and take measures, if needed to prevent their use in money laundering schemes.

Branches should ensure that appropriate KYC/e-KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that if at any point of time Bank appoints/engages agents for marketing of these cards / products are also subjected to KYC/e-KYC measures.

### 8.29. KNOW YOUR CUSTOMER'S CUSTOMER:

Enhance due diligence is required to be in practice to Know Your Customer's Customer ensuring the highest level of compliance in AML & CFT issues. KYC'C has become the most important tool for identification/verification of the customer's business. It is essential to find out the customer's customer to whom they are dealing with. On the other hand, Customers close association or family members or beneficiary of the account should be known in to.

A Financial Institution should -

1. Take a list with the true identification like name, address, type of business, etc. of customer's customer;
2. Review the given list and check the background of the customer's customer at least half yearly basis if necessary;
3. Monitor the transaction occurred by the customer's customer;
4. Monitor the customer's customer business indirectly.

### 8.30. KNOW YOUR EMPLOYEE (KYE)

1. Institutions and business learn at great expense that an insider can pose the same ML/TF threat as a customer. It has become clear in the field having co-equal programs to know your customer and to know your employee is essential /vital. In an effort to identify and anticipate trouble before its costs time, money and reputational damage/risk. Financial Institutions should develop program to look closely at the people inside their own organizations.
2. A Know your Employee (KYE) program means that the institution has in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job description, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, dual control, and other deterrents /restrictions should be firmly in place.
3. Background screening of prospective and current employees, especially for criminal history, is essential to keep out unwanted employees and identifying those to be removed. It can be an effective risk management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. It can be used effectively, the pre-employment background checks/examines may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. An institution should verify that contractors are subject to screening procedures similar to its own.
4. The sensitive of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications. The extent of the screening depends on the circumstances, with reasonableness the standard as well as source of income.

### 8.31. WALK-IN/ ONE OFF/ONLINE CUSTOMER

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

The Branch 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 banks should identify sources of funds as well.

### 8.32. CUSTOMER ACCEPTANCE POLICY OF BKB

Considering the above described features, BKB introduced Customer Acceptance Policy (CAP) given bellow-

**1.0. Particular-** Common procedures/ documents to be required for all types of Account.

**Policy-** CDD & EDD will be ensured including identification of the persons/ Entity & verification of Address/ Sources of Fund and uses of fund with proper documentation.

**Procedures-** CDD/ EDD shall be ensured by the following process:

- AOF in force to be filled in accurately and completely and signed by each applicant/Authorized person (in case of Entity accounts).
- Sanction Screening of all the persons/ Entity/ Partners/Directors/legal persons.
- Ensuring of every customer's present address by physical verification, sending thanks letter by registered mail or any other reliable means etc.
- Sources of income shall be verified by Trade License, Professional ID Card/ Salary Sheet, financial statements or any other reliable means.
- Screening of Adverse Media Report/ Local Black List before on boarding.
- Transaction Profile shall be prepared in commensurate with customer's total income and approved as per norms of the Bank.
- Constant Transaction Monitoring of all customers
- Risk Grading of all Customers and CDD/EDD shall be ensured accordingly and KYC profile of BFIU Circular No. 26, dated 16.06.2020
- Introduction of the proposed customer shall be ensured
- Customer having National Identification Number (NID) needs not an introducer to introduce him/her to bank as per BRPD Circular 02, dated 23.02.2020.
- In the case of having no NID, Introduction of the proposed customer shall be ensured by introducer. The prospective customer must be mentally sound and capable to make a contract

**1.1. Particular- Accounts Introduction Policy**

**Policy-** Introduction shall be ensured for the Customers

**Procedures-** Customer having National Identification Number (NID) needs not an introducer to introduce him/her to bank as per BRPD Circular 02, dated 23.02.2020.

In the case of having no NID, Introduction of the proposed customer shall be ensured under the following ways:

- Current Account (CA) shall be introduced by the CA Account Holders. Besides, Manager/ Executive of BKB shall be allowed to introduce CA Account.
- Savings Account (SA) shall be introduced by the SA/ CA Account Holders.
- Staff, below the rank of officer, shall not be allowed to introduce any account.
- Account holder who is maintaining a regular account for at least 06 (six) months satisfactorily with BKB shall be eligible for introduction of accounts.
- However, suitable introduction shall be obtained from the respectable person known to the Bank or any account holder acceptable to the Bank.

### 1.2. **Particulars-** Photo ID

#### **Procedures-** Photo ID means-

- Copy of the National ID Card/ Valid Passport/ valid Driving License or any other Photo ID Card acceptable to the Bank (i.e. ID card of Armed forces, Bangladesh Police, etc.)
- In case of opening of account with only Birth Registration Certificate, the customer must submit an additional certificate (with photo attested) from the competent authority

### 1.3 **Particulars-** Nomination

#### **Procedures-** Nomination must be ensured in case of Individual and Joint Account.

- Nominee's details and photo paste ID along with 1 (one) copy of recent passport size photograph for each nominee duly attested by the applicant shall be obtained.
- In case of Minor Nominee, particulars of the legal guardian along with his/ her Photo ID & recent Passport size Photograph shall be obtained in addition to the Birth certificate, recent passport size photograph & particulars of the Minor Nominee.

### 2.1. **Particular-** Individual Account including Joint Account.

**Policy-** Any individual competent to make a contract may open an account in his own name with the bank by submitting the account opening form duly completed including selection of nominee(s).

#### **Procedures-** CDD/EDD is to be ensured taking the following documents-

- Copy of National ID Card/Valid Passport/ Driving License or any other photo ID Card.
- Two copies of passport size recent photograph in case of having NID for each Account holder.
- In case of other than NID, 2 (two) copies of passport size recent photograph attested by the introducer for each Account holder.
- In case of opening of account with only Birth Registration Certificate, the customer must submit an additional certificate (with photo attested) from the competent authority
- Introduction by any Savings or Current Account holder of BKB (who has been maintaining regular account for at least 6 months).
- Nominee's details and photo ID of the Nominee along with 1 (one) copy of recent passport size photograph for each nominee to be attested by the applicant.
- In case of Minor Account, photocopy of the birth certificate and recent passport size photograph duly attested by the guardian.
- Ensuring of every customer's present address by physical verification, sending thanks letter by registered mail or any other reliable means etc.
- Photocopy of up-to-date TIN Certificate (if any).

Additional documents required for non-residential customers:

- Copy of valid passport along with valid VISA/ Work permit to be enclosed (in case of foreign passport, the page sealed with no visa is required for Bangladesh to be attached).
- Proof of employment/income (employment certificate/pay slip/ employment contract mentioning annual income/ Bank statement mentioning monthly salary or latest tax return).

## Chapter 8: Customer Acceptance Policy

### 2.2 **Particular-** Non Individual Accounts (Sole Proprietorship/ Partnership /Private Limited Company/ Public Limited Company/ Others Entity

**Policy-** Following usual practices Bank can open this type of account

**Procedures-** Common Documents to be required to ensure CDD-

- In case of having NID, 2 (two) copies of passport size recent photograph for Proprietor/ each partners or directors or legal persons.
- In case of photo ID other than NID, 2 (two) copies of passport size recent photograph for Proprietor/ each partners or directors or legal persons and to be attested by the Introducer.
- Copy of National ID Card/ Valid Passport/ valid driving License or any other photo ID Card for proprietor/ each partner/ director/ legal operator.
- In case of opening of account with only Birth Registration Certificate, the customer must submit an additional certificate (with photo attested) from the competent authority.
- Required introduction shall be obtained:
- Trade License no. & Authority/Registration no. & Authority
- Photocopy of up-to-date TIN/BIN Certificate (where applicable).

### 3.1 **Particular-** Sole Proprietorship Firm

**Policy-** Following usual practices Bank can open this type of account.

**Procedures-** CDD/EDD shall be ensured taking the following special documents as a Proprietorship concern-

- All necessary papers must be submitted in the letterhead pad of the firm with Seal & signature by the proprietor.
- Up to date Rental Agreement (in case of rented establishment), purchase deed, Inheritance certificate (In case of inherited establishment) of the business establishment.
- Financial statement.
- All other necessary procedures and documents as mentioned in Sl. No. 1, 2 & 3 are applicable for on-boarding of this type of customers.

### 3.2 **Particular-** Partnership Firm

**Policy-** Following usual practices Bank can open this type of account

**Procedures-**CDD/EDD shall be ensured taking the following special papers/ documents as partnership firm:

- Partnership Deed.
- Resolution for opening and operating of accounts.
- Financial Statement.
- All necessary papers must be submitted in the letterhead pad of the firm with Seal & signature by the Managing Partner.
- Up to date Rental Agreement (in case of rented establishment), purchase deed, Inheritance certificate (In case of inherited establishment) of the business establishment.
- All other necessary procedures and documents as mentioned in Sl. No. 1, 2 & 3 are applicable for on-boarding of this type of customers.

### 3.3 **Particular-** Private Limited Company -

**Policy-** Following usual practices Bank can open this type of account.

**Procedures-** CDD/EDD shall be ensured taking the following special papers/ documents as partnership firm-

- Attested photocopy of Memorandum & Articles of Association.
- Photocopy of Certificate of Incorporation.
- Photocopy of Resolution of the Board of Directors authorizing operators to open and operate the account.
- Photocopy of Agreement with Agent with regard to open & operate the account by the Agent (if applicable).
- Up to date Rental Agreement (in case of rented establishment), purchase deed, Inheritance certificate (In case of inherited establishment) of the business establishment.
- Audited Financial Statement.
- All necessary papers and documents shall be obtained through a forwarding letter duly affixed seal and signature of the Authorized person.
- All other necessary procedures and documents as mentioned in Sl. No. 1 & 3 are applicable for on-boarding of this type of customer.

### 3.4. **Particular-** Public Limited Company

**Policy-** Following usual practices Bank can open this type of account

**Procedures-**

- Attested photocopy of Memorandum & Articles of Association.
- Photocopy of Certificate of Incorporation.
- Photocopy of Certificate of Commencement of Business
- Photocopy of Resolution of the Board of Directors authorizing operator(s) to open and operate the account.
- Photocopy of Agreement with Agent with regard to open & operate the account by the Agent (if applicable).
- Up to date Rental Agreement (in case of rented establishment), purchase deed, Inheritance certificate (In case of inherited establishment) of the business establishment.
- Audited Financial Statement
- No Cheque Book shall be issued without Certificate of commencement of business.
- All necessary papers and documents shall be obtained through a forwarding letter duly affixed seal and signature of the Authorized person.
- All other necessary procedures and documents as mentioned in Sl. No. 1 & 3 are applicable for on-boarding of this type of customers

### 4. **Particular-** Co-operative Society/ Samity.

**Policy-** Following usual practices Bank can open this type of account

**Procedure** CDD/EDD shall be ensured taking the following special papers/ documents as co-operative society/ samity-

- Up to date list of the members of Governing body supported by the resolution of the Governing body meeting.
- List of the previous Governing body and Charge handover take over Note (if applicable).
- Constitution/ by-laws certified by competent Authority.
- Copy of the approval letter from the Concerned Authority to run the business.
- List of office bearers (with address) along with their Bio data.

## Chapter 8: Customer Acceptance Policy

- Photocopy of Resolution of proper authority authorizing operator to open and operate the account. All necessary papers and documents shall be obtained through a forwarding letter duly affixed seal and signature of the Authorized person.
- All other necessary procedures and documents as mentioned in Sl. No. 1 & 3 are applicable for on-boarding of this type of customers.

### 5. **Particular-** Trust

**Policy-** Following usual practices Bank can open this type of account

**Procedures-** CDD/EDD shall be ensured taking the following special papers/ documents

- Certified copy of Trust Deed. In case of Trust Registered in the Foreign Countries, the Trust Deed shall be duly verified by the authorized officer of Bangladesh Embassy in that country.
- Up to date list of member of the Governing body supported by the resolution of the Governing body meeting.
- List of members of the previous Governing body and Charge handover take over Note.
- Up to date list of Board of Trustees authenticated by the concerned authority.
- List of office bearers (with address) along with their Bio data. Photocopy of Resolution of proper authority authorizing operator(s) to open and operate the account. Signature of all authorized trustees is to be obtained in the AOF. All necessary papers and documents shall be obtained through a forwarding letter duly affixed seal and signature of the Authorized person. All other necessary documents as mentioned in Sl. No. 1, 3 shall also be applicable for this type of accounts.

### 6. **Particular-** Minor

**Policy-** Legal Guardian on behalf of minor can open the account

**Procedures-**

- (Two) copies of recent passport size photograph attested by the introducer of both Minor and operator (guardian) in case of not having NID of operator (guardian). In case of having NID of operator (guardian), photograph of minor will be attested by operator (guardian).
- Operator's details shall be obtained in the AOF along with all necessary papers/ documents as a customer.
- Nominee's details and photo ID of the Nominee along with 1 (one) copy of recent passport size photograph to be attested by the operator (guardian).
- Application to be signed by its operator (guardian).
- Source of income and their relationship to be confirmed.
- Physical presence of Guardian is required for withdrawal of money, risk grading and apply EDD for high risk clients.
- All other necessary documents as mentioned in Sl. No. 1, 2 shall also be applicable for this type of accounts

### 7. **Particular-** Illiterate Person

**Policy-** Illiterate Person can open account with the bank following the norms in practice.

**Procedures-**

- All others necessary documents as mentioned in Sl. No. 1, 2 shall also be applicable for this type of accounts.
- Apply EDD for high risk clients.
- Physical presence is required for withdrawal of money.

### 8.1 **Particular-** PEPs (Politically Exposed Persons):

**Policy-** PEPs can open account complying Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations introduced by BFIU and prior approval to be taken from competent authority (CAMLCO)

#### **Procedures-**

- All other appropriate documents required to open an individual/ joint accounts & Foreign Residence as mentioned in Sl. No. 1 & 2.
- KYC to be obtained considering high risk component, extra due diligence to be given. In case of operation F. Ex. Regulation Act-1947 & Guidelines for Foreign Exchange Transaction-2018 to be followed along with ensuring FATCA Compliance.
- CAMLCO's approval is required to open a PEPs Account

### 8.2. **Particular-** IPs (Influential Persons)

**Policy-** PEPs can open account complying Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations introduced by BFIU and prior approval to be taken from competent authority (CAMLCO).

#### **Procedures-**

- All other appropriate documents required to open an individual/ joint accounts & Foreign Residence as mentioned in Sl. No. 1 & 2.
- KYC to be obtained considering high risk component, extra due diligence shall be ensured.
- CAMLCO's approval is required to open an IPs Account.

### 9. **Particular-** Non Residential Bangladeshi and Foreign National.

**Policy-** Non Resident Bangladeshi and Foreign Citizen can open account as per usual norms & practice

#### **Procedures-**

- All other appropriate documents required to open an individual/ joint accounts & Foreign Residence as mentioned in Sl. No. 1 & 2.
- Proof of employment/ income (employment certificate/pay slip/ employment contract mentioning annual income/ Bank statement mentioning monthly salary or latest tax return).
- Foreign Exchange Regulation Act-1947 & Guideline for Foreign Exchange Transaction-2018 to be followed meticulously. Ensure FATCA compliance.

### 10. **Particular-** Pardanishin Women

**Policy-** Pardanishin Women can open account as per usual norms & practice

**Procedures-** Women who are not interested to unveil their face-

- All other appropriate documents required opening an individual/ joint accounts & Foreign Residence as mentioned in Sl. No. 1 & 2.
- The Woman, if educated (or, illiterate) and having NID, has to submit face exposed photograph and keep her face open at the time of each transaction
- The Woman, if educated (or, illiterate) and having no NID, has to be introduced by the client known to the Bank. She has to submit face exposed photograph and keep her face open at the time of each transaction
- Physical presence of such women is required at the time of opening of account. Her photograph is to be attested by responsible officer and confirm her genuineness of identification. Ensure sanction screening
- conduct risk grading and apply EDD for high risk clients

### 11. **Particular-** Blind Man

**Policy-** Blind man can open account as per usual norms & practice.

**Procedures-**

- All other appropriate documents required to open an individual/ joint accounts & Foreign Residence as mentioned in Sl. No. 1 & 2.
- Physical presence is required at the time of money withdrawal. Apply all other AML, CFT & PF prevention regulations.
- No ATM card shall be issued against this account. Withdrawal shall be executed through cheque in the physical presence of customer and the satisfaction of Manager

### 12. **Particular-** NGO/NPO/ Club or Association

**Policy-** Bank can open such account as per usual terms & practices.

**Procedures-**

- Appropriate documents as mentioned in Sl. No. 1, 3, 4 & 5 shall be applicable for this account
- Extra due diligence for organizational deal to be taken as regards of source of fund and their use-
  - Sources & Uses of fund should be ensured with proper documents.
  - Necessary Permission from National NGO Bureau Affairs.
  - Up to date list of the members of Governing Body with bio data.
  - Opening & operational instruction of Governing Body.
  - In case of small loan business, necessary permission to be obtained.
  - In case of relief/ sanction, proper documents to be obtained.
- Regular monitoring of their transaction to be done.
- Compliance with all regulations regarding AML, CFT and prevention of PF.

### 13. **Particular-** Travel Agency/ Hajj Agency

**Policy-** Concerned Documents to be obtained

**Procedures-**

- Appropriate documents mentioned in Sl. No. 1, 3 shall be obtained.
- Besides following documents must be obtained to ensure CDD/ EDD:
  - Hajj License.
  - Civil Aviation License.
  - International Air Transportation Association (IATA) Certificate.
  - Association of Travel Agency of Bangladesh (ATAB).
- Compliance with all regulations regarding AML, CFT and prevention of PF.

### 14. **Particular-** Manufacturing Industry

**Policy-** Accounts of Manufacturing Industry shall be opened following necessary procedures of the Bank

**Procedures-**

- Appropriate documents mentioned in Sl. No. 1, 3 shall be obtained.
- Besides following documents must be obtained to ensure CDD/ EDD:
  - ETP (Effluent Treatment plant).
  - WTP (Water Treatment Plant).
  - Environmental Certificate (where applicable)
- Compliance with all regulations regarding AML, CFT and prevention of PF.

## Chapter 8: Customer Acceptance Policy

### 15. **Particular-** Export/ Import related Business

**Policy-** Accounts of Export/ Import related Business shall be opened following necessary procedures of the Bank.

**Procedures-**

- Appropriate documents mentioned in Sl. No. 1 & 3 shall be obtained.
- IRC (Import Registration Certificate) & ERC (Export Registration Certificate) from office of CCI & E (Chief Controller of Import & Export).

### 16. **Particular-** NPO/ Educational/ Religious Institutions

**Policy-** Branch will open such accounts except UN/ OFAC sanction listed institutions or prohibited by Bangladesh Government.

**Procedures-**

- Appropriate documents as mentioned in clause Sl. No. 1, 3, 4 & 5 shall be obtained.
- Branch must ensure getting full identification of the members of Governing Body or Managing Committee, Resolution for account opening, source of fund and destination/ using of fund etc.
- Compliance with all regulations regarding AML, CFT and prevention of PF.

### 17. **Particular-** Companies Registered Abroad

**Policy-** Accounts opened in the name of companies registered abroad may be opened with all formalities including verification of supporting documents

**Procedures-**

- All other necessary documents as mentioned in Sl. No. 1 & 3 shall be applicable for this account.
- Photocopy of Agreement with Agent with regard to open & operate the account by the Agent.
- Documents showing evidence of registration of the companies with the concerned regulatory bodies abroad depending on their nature.
- Documents verified/ attested by Bangladeshi High Commission/ Embassy to that country where the entity is registered.
- Documents verified by the High Commission/ Embassy of the License giving country working in Bangladesh.
- Any other 3rd party verification (if required).
- Compliance with all regulations regarding AML, CFT and prevention of PF

### 18. **Particular-** Foreign National

**Policy-** Accounts in the name of foreign nationals may be opened with all formalities including verification of supporting documents

**Procedures-** Following Documents to be obtained to ensure CDD/ EDD-

- Appropriate documents as mentioned in Sl. No. 1 & 2 shall be obtained.
- Certificate from Bangladesh Investment Development Authority (BIDA).

**19. Particular-** Diagnostic Center/ Hospital or others Medical Service Providers including Medical College

**Policy-** Accounts in the name of Diagnostic Center/ Hospital or others Medical Service Providers including Medical College may be opened with all formalities including verification of supporting documents

**Procedures-** Following Documents shall be obtained to ensure CDD/ EDD-

- Appropriate documents as mentioned in Sl. No. 1 & 3 shall be obtained.
- Certificate from Ministry of Health & Family Welfare/ Directorate General of Health Services to run the Business.
- Certificate from Ministry of Education (In case of Medical College).
- Membership from Bangladesh Medical and Dental Council (BM&DC) (In case of Medical College).
- Compliance with all regulations regarding AML, CFT and prevention of PF

**20. Particular-** Publication (Print & Electronic Media including online newspapers)

**Policy-** Accounts in the name of Publication (Print & Electronic Media including online newspapers) may be opened with all formalities including verification of supporting documents

**Procedures-** Following Documents shall be obtained to ensure CDD/ EDD:

- Appropriate documents as mentioned in Sl. No. 1 & 3 shall be obtained.
- Self-declaration in the stipulated Form certified by Competent Authority.

**21. Particular-** Executor/ Administrator/ Liquidator.

**Policy-** Following usual practices Bank can open this type of account.

**Procedures-**

- Confirm Power & functions of signatories, obtain KYC/ TP for concerned person/ firm.
- Confirm source of fund and risk grading and identify the beneficial owner of the account.
- Compliance with all regulations regarding AML, CFT and prevention of PF

**22. Particular-** Correspondent Banking

**Policy-** Correspondent Banking to be established after obtaining information about respondent bank's commitment to prevent money laundering and combat terrorist financing

**Procedures-** Through AML & CFT questionnaires, it will be ensured that their general policies are satisfactory, risk level is acceptable and all AML & CFT related programs i. e. KYC, TP, Enhanced Due Diligence(EDD), transaction monitoring, AML training, etc. are established. Compliance with all regulations regarding AML, CFT and prevention of PF.

**23. Particular-** Shell Banking.

**Policy-** Bank will not open any account with Shell Bank (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group)

**Procedures-**

Bank will follow the rules of prohibiting accounts/ relationships with shell banks

**24. Particular-** Mobile Financial Services (MFS)

**Policy-** The Mobile Banking account will be opened & operated through every branch and Bank's panel agents.

**Procedures-** Specific terms and conditions are applicable for the CDD/EDD with KYC, TP in agent's a/c.

- KYC, TP, Photograph & Identifying documents shall be collected for each and every account holder.

**25. Particular-** Walk-in Customer / Walk-in Customer for Remittance

**Policy-** The customers who do not maintain any account with the bank is entitled to get some specific services by following KYC profile.

**Procedures-** Branches shall confirm to obtain satisfactory evidence of identification of applicants/ depositors/ withdrawal holders through Short KYC including name, address, mobile number, occupation, source of fund, reasons for remittance, relationship with the beneficiary, etc.

Including these, branches will obtain Full KYC and perform CDD/EDD for occasional transactions as well as transactions more than Tk. 5,00,000.

**26. Particular-** On-line Customer

**Policy-** On-line customer is one who wishes to conduct electronic banking via the internet or similar technology, the verification problem is made more difficult. In accepting business from on-line customers, bank shall apply equally effective customer identification procedure.

**Procedures-** Branches shall confirm to obtain satisfactory evidence of identification of applicants/ depositors/ withdrawal holders through Short KYC including name, address, mobile number, occupation, and relationship with beneficiary, source of fund etc. Monitor the transactions regularly.

**27. Particular-** Account of Non face-to-face Customer

**Policy-** Following usual practices Bank can open this type of account

**Procedures-** As the Non-face-to-face customer for opening an account is not physically present at bank, customer identification is performed by an employee or a representative of branches.

- All other appropriate documents required to open an individual/ joint accounts as mentioned in Sl. No. 1 & 2.
- Compliance with all regulations regarding AML, CFT and prevention of PF

**28. Particular-** Account of undischarged insolvent/ insane person

**Policy-** No account shall be opened in the name of an Undercharged Insolvent or a person of Unsound Mind

**Procedures-** When a Branch receives definite evidence of bankruptcy or lunacy of an existing customer, all operations on his account shall forthwith be suspended till the receipt of order from the Court or definite proof of the customer's solvency/ sanity.

- Compliance with all regulations regarding AML, CFT and prevention of PF

## Chapter 8: Customer Acceptance Policy

### 29. **Particular-** Accounts of Banks and Military Funds.

**Policy-** Following usual practices Bank can open this type of account.

**Procedures-** Branches shall not open accounts for Banks which are not established at their own stations nor shall they enter into any agency arrangements with other banks without prior approval of the Head Office.

Regimental and Non-public funds may be deposited subject to certain conditions and prior consent of the respective Controllers of Accounts. Compliance with all regulations regarding AML, CFT and prevention of PF power. If satisfied, he may open account in the name of the officer concerned and not in the personal name of the official concerned and obtain signature. Full particulars of the account must be taken. In case of any change of the official, the outgoing official must attest the specimen signature of the incoming signature together with an intimation regarding change incumbency. Compliance with all regulations regarding AML, CFT and prevention of PF

### 30. **Particular-** Account of Semi Government/ Autonomous bodies/Corporations/Nationalized organization, etc

**Policy-** Before opening the account of any semi Government/ Autonomous bodies/ Corporations/ Nationalized Organization, a certified copy of the Statute or any other law by which the body is formed and governed should be obtained.

**Procedures-** Copy of the ACT/Order by which the same comes into existence together with the copy of resolution of the Board to open the account should be obtained. The copy of the resolution should be under the signature of the Chairman and Secretary of the Board. Account opening form must be signed by the chairman secretary of the Board and the person(s) authorized to operate the account. Manager must see the powers embodied in the relative act/order are not exceeded or suppressed by the resolution. Manager must also see whether the account operate jointly or singly. In case of any change of the authority fresh resolution must be obtained together with specimen signature of new authority duly attested by the outgoing official or by Chairman and Secretary of the board.

Accounts of Semi-Government/ Autonomous bodies/Corporations /Nationalized Organization shall be opened in Savings A/C, Current A/C, Special Notice Deposits Account, FDR Account and related AOF shall be used for opening accounts. KYC will be obtained of every individual of authorized operator of those accounts.

Compliance with all regulations regarding AML, CFT and prevention of PF.

### 31. **Particular-** Accounts of Local Authorities

**Policy-** Before opening the account of any local body, certified copy of the Statute or any other law by which the body is formed and governed should be obtained

**Procedures-** The accounts of Local Authorities, Municipal corporations, District Council, etc. shall be opened in Savings A/C, Current A/C, Special Notice Deposits Account, FDR Account and related AOF shall be used for opening accounts. KYC will be obtained of every individual of operator of those accounts.

- Compliance with all regulations regarding AML, CFT and prevention of PF.

## Chapter 8: Customer Acceptance Policy

**32. Particular-** Locker services

**Policy-** Such services can be provided by opening a mother account.

**Procedures-** KYC & DD process shall have to be completed at the time of opening the mother account.

- At the time of providing such services, all the transactions and documents to be checked further for accomplishment of the DD Process.

**33. Particular-** Induction of Investment Clients.

**Policy-** No investment facilities shall be allowed to any customer without having satisfactory deposit account conduct.

**Procedures-** KYC & DD process shall have to be completed at the time of opening the mother account.

- At the time of providing such services, all the transactions and documents to be checked further for accomplishment of the DD Process.

**34. Particular-** MSBs, CBS, C&F Agents etc.

**Policy-** Due process to be followed.

**Procedures-** KYC, EDD & Screening process to be executed for on-boarding and renewal.

**35. Particular-** SB Account for financial inclusion/no-frill Account–Student/ Pathophul/ Farmers /Low income women/ other SB Accounts.

**Policy-** Following usual practices Bank can open this type of account with minimum initial deposit free of charges of yearly/half-yearly account maintenance.

**Procedures-** Bank must initially screen the name with the UNSCR sanction list. Simplified Customer

- Due Diligence (SCDD) must be applied. Verify NID/other photo ID/Birth Certificate and address of customer as per BFIU Circular no 26.

# Chapter 9: Risk Register

## Risk Score Calculation

### 9.1. 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.

### 9.2. Risk Score Calculation

The following method can be applied for Calculation of Risk Score:

$$\text{Likelihood Scale} \times \text{Impact} = \text{Risk Score}$$

#### (I) Likelihood Scale:

BKB considers three levels of risks which are shown below:

#### Likelihood Scale

Frequency	Likelihood of an ML/TF risk	Score
Very likely	It may probably occur several times a year	4
Likely	Probability to happen once a year	3
Unlikely	Unlikely, but not impossible	2

#### (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.	3
Moderate	Moderate level of money laundering or terrorism financing impact.	2
Minor	Minor or negligible consequences or effects	1

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 levels:

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

Low	Medium	High
≥ 5	6 to 9	10 to 12

1. ML & TF Risk Register for customer

Risk	Likelihood	Impact	Risk Score	Treatment/Action
<b>Retail Banking customer</b>				
A new customer	4	3	12	<ul style="list-style-type: none"> <li>a) UNSCR sanction list to be checked</li> <li>b) Know the reason for opening the account</li> <li>c) KYC to be maintained properly</li> <li>d) CDD shall be applied properly.</li> <li>e) EDD shall also be applied for highly risky</li> <li>f) Clients &amp; accounts opened without physical presence of the clients.</li> </ul>
Walk-in-customer (beneficiary is Government / semi Government / autonomous body/bank & NBF)	2	1	2	Obtaining proper KYC of the Remitter
Walk-in-customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBF)	4	3	12	<ul style="list-style-type: none"> <li>a) Proper KYC to be obtained.</li> <li>b) Ask the purpose of transaction and source of fund.</li> <li>c) Reporting STR/ SAR if suspicious anything found</li> </ul>
Non-resident customer (Bangladeshi)	4	3	12	<ul style="list-style-type: none"> <li>a) Obtain complete KYC</li> <li>b) Verification of necessary papers/ documents including work permit, passport &amp; visa.</li> <li>c) Follow the foreign exchange guideline</li> <li>d) Follow EDD</li> </ul>
Large transaction (transaction above CTR threshold or below the threshold)	4	3	12	<ul style="list-style-type: none"> <li>a) Source of fund should be ascertained.</li> <li>b) Obtain the information of beneficial owner</li> <li>c) STR shall be submitted to ML &amp; TFPD if any transaction found suspicious</li> <li>d) Collect complete KYC</li> <li>e) Apply CDD</li> </ul>
A customer making series of transactions to the same individual or entity	4	2	8	<ul style="list-style-type: none"> <li>a) Reasons of such transaction to be clarified by the customer and to be satisfied by the branch.</li> <li>b) STR shall be submitted to ML &amp; TFPD if any transaction found suspicious</li> <li>c) Perform EDD</li> </ul>
Customer involved in outsourcing business	3	2	6	<ul style="list-style-type: none"> <li>a) Obtain documents of the source of fund</li> <li>b) CDD shall be applied properly</li> <li>c) EDD to be applied</li> </ul>
Customer appears to do structuring to avoid reporting threshold	4	3	12	<ul style="list-style-type: none"> <li>a) Obtain justification of transaction</li> <li>b) Source of fund to be known.</li> <li>c) EDD shall be applied properly for the clients &amp; also outsource partners</li> <li>d) If found suspicious, then report as SAR</li> </ul>
Customer appears to have accounts with several banks in the same area	3	2	6	<ul style="list-style-type: none"> <li>a) Explanation regarding opening of several accounts to be obtained.</li> <li>b) Confirm the source of fund.</li> <li>c) If the branch is not satisfied account should not be opened.</li> <li>d) STR shall be submitted to ML&amp;TFPD if any transaction found suspicious.</li> <li>e) May go ahead but preferably reduce risk.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	4	3	12	<ul style="list-style-type: none"> <li>a) Activities &amp; Transaction of the client will be monitored</li> <li>b) Perform EDD properly</li> <li>c) CDD shall be applied properly.</li> </ul>
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	4	3	12	<ul style="list-style-type: none"> <li>a) Business relationship shall not be established.</li> <li>b) For existing client, information shall be provided the regulatory Authority through STR/ SAR</li> <li>c) Keep CCU/Senior Management informed about the customer and the transaction of the account.</li> </ul>
Negative news about the customers' activities/ business in media or from other reliable sources	4	3	12	<ul style="list-style-type: none"> <li>a) Review KYC</li> <li>b) No such customer to be on boarded until risk is reduced. <b>For existing customers-</b> CDD/ EDD shall be applied properly.</li> <li>c) Keep CCU/Senior Management informed about the customer and the transaction of the account.</li> <li>d) Court order/ instruction shall be followed.</li> <li>e) STR/ SAR shall be filed if any transaction found suspicious</li> </ul>
Customer is secretive and reluctant to meet in person	4	2	8	<ul style="list-style-type: none"> <li>a) Visit customer's address.</li> <li>b) Keep the transaction under close monitoring with TP.</li> <li>c) Perform CDD.</li> <li>d) Do not allow transaction until risk reduced.</li> </ul>
Customer is a mandate who is operating account on behalf of another Person/ company.	3	2	6	<ul style="list-style-type: none"> <li>a) Obtain complete KYC of the mandate.</li> <li>b) Keep transaction under monitoring with TP.</li> <li>c) Conduct CDD of mandate.</li> <li>d) CDD/ EDD shall be applied properly. Transaction &amp; activities of the client shall be monitored.</li> <li>e) STR/ SAR shall be filed if any transaction found suspicious.</li> </ul>
Large deposits in the account of customer with low income	4	3	12	<ul style="list-style-type: none"> <li>a) Source of fund to be verified with documentary evidence. If the customer failed to provide the supporting documents, raise STR</li> <li>b) Perform EDD</li> <li>c) If necessary, TP shall be updated (if the case is genuine/ pertinent)</li> <li>d) Constant Transaction monitoring shall be undertaken</li> </ul>
Customer about whom BFIU seeks information (individual)	4	2	8	<ul style="list-style-type: none"> <li>a) Update KYC</li> <li>b) Check whether there is any negative information about the customer. c) Perform EDD</li> <li>c) Transaction &amp; activities of the client shall be monitored</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
A customer whose identification is difficult to check	4	3	12	<ul style="list-style-type: none"> <li>a) Do not allow transaction until risk reduced.</li> <li>b) Verify the customer's identity through the third party</li> <li>c) For new customer, if the checking of identification is not possible then do not open any account</li> <li>d) For existing client, information shall be provided to the regulatory Authority through STR/ SAR</li> </ul>
Significant and unexplained geographic distance between the bank and the location of the customer	3	2	6	<ul style="list-style-type: none"> <li>a) CDD shall be done properly.</li> <li>b) Justification to be obtained regarding business relationship with distance branch and reason to be acceptable by branch management</li> <li>c) If not satisfactory, no relationship will be allowed.</li> <li>d) STR shall be submitted to ML &amp; TFPD if any transaction found suspicious</li> </ul>
Customer is a foreigner	4	2	8	<ul style="list-style-type: none"> <li>a) Obtain reason for opening account in Bangladesh.</li> <li>b) Obtain complete KYC, Passport, Visa &amp; work permit agreement where necessary.</li> <li>c) Obtain the purpose of transaction and source of fund.</li> <li>d) Perform Enhanced Due Diligence.</li> <li>e) Follow foreign Exchange Guideline and Circulars.</li> <li>f) Permission shall be obtained from competent Authority of the Bank.</li> <li>g) STR/ SAR shall be submitted to ML&amp;TF PD if any transaction found suspicious</li> </ul>
Customer is a minor	3	2	6	<ul style="list-style-type: none"> <li>a) Proper CDD shall be applied.</li> <li>b) Obtain complete KYC.</li> <li>c) Ensure CDD for minor, guardian and beneficial owners of the accounts.</li> <li>d) Obtain birth certificate as identity proof.</li> <li>e) Obtain the purpose of transaction and source of fund with supporting documents.</li> </ul>
Customer is housewife	3	1	3	<ul style="list-style-type: none"> <li>a) Ensure CDD for both customer and beneficial owners of the accounts.</li> <li>b) CDD shall also be applied for Beneficial Owner.</li> <li>c) Obtain the purpose of transaction and source of fund with supporting documents.</li> <li>d) Transaction shall be monitored.</li> </ul>
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	4	3	12	<ul style="list-style-type: none"> <li>a) The official approval letter to open the account shall be obtained in case of Foreign PEPs.</li> <li>b) Obtain complete KYC. Perform Enhance Due Diligence.</li> <li>c) Obtain approval from CCU before establishing relationship.</li> <li>d) Keep transaction under monitoring with TP.</li> <li>e) Check whether the source of fund Permission shall be obtained from Competent Authority of the Bank.</li> <li>f) Commensurate with the designation.</li> <li>g) Follow foreign exchange guideline and circulars.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer opens account in the name of his/ her family member who intends to credit large amount of deposits	4	3	12	<ul style="list-style-type: none"> <li>a) Identify beneficial owners of the account and obtain their complete &amp; accurate information.               <ul style="list-style-type: none"> <li>i) Obtain documents in support of source of fund.</li> <li>ii) Verifying the genuineness of the data including sources of fund applying EDD</li> <li>iii) Transaction shall be done with constant monitoring of the account.</li> <li>iv) STR shall be submitted to ML &amp; TFPD if any transaction found suspicious.</li> </ul> </li> <li>b) May go ahead but preferably reduce risk.</li> <li>c) Perform Enhanced Due Diligence.</li> </ul>
Customer doing significant volume of transactions with higher risk geographical locations.	4	3	12	<ul style="list-style-type: none"> <li>a) KYC Procedures including physical verification of the client's information shall be done properly.</li> <li>b) Transaction (especially sources &amp; uses of fund) shall be monitored. If the transaction is not justified with nature of business/profession, STR/SAR to be reported.</li> </ul>
A customer who bring in large amounts of used notes and/ or small denominations	3	2	6	<ul style="list-style-type: none"> <li>a) Check whether the nature of business justifies the condition and small denominations of notes.</li> <li>b) STR shall be done if anything found suspicious</li> <li>c) Obtain written justification supported by documents (if any) from the customer regarding the transaction.</li> <li>d) Update KYC of the customer (if necessary).</li> <li>e) Perform Enhance Due Diligence.</li> </ul>
Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)	4	3	12	<ul style="list-style-type: none"> <li>a) Identify the source of fund with supporting document.</li> <li>b) EDD shall be applied, Verifying the genuineness of the data/ information of the client</li> <li>c) Obtain information about the customer's business.</li> <li>d) Obtain the membership certificate issued from relevant trade body.</li> <li>e) Perform Enhance due Diligence.</li> </ul>
Customer is a money changer/ courier service agent/ travel agent	4	2	12	<ul style="list-style-type: none"> <li>a) For new customers, account shall not be opened until all obligatory data/ information are obtained through physical verification</li> <li>b) For the existing customers EDD shall be done</li> <li>c) Identify the source of fund with supporting documents.</li> <li>d) Obtain information about the customer from available sources e.g. media, peer group.</li> <li>e) Obtain license issued from competent authority.</li> <li>f) Keep transactions under monitoring with TP.</li> <li>g) Follow foreign exchange guideline and circulars (if applicable).</li> </ul>
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above.	4	3	12	<ul style="list-style-type: none"> <li>a) Ensure CDD.</li> <li>b) Identify the source of fund with supporting documents.</li> <li>c) STR shall be submitted to ML&amp;TFPD if any transaction found suspicious</li> <li>d) Keep transaction under monitoring with TP.</li> <li>e) Check certification with concern authority.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer is involved in Manpower Export Business	4	3	12	<ul style="list-style-type: none"> <li>a) Obtain KYC.</li> <li>b) Obtain the purpose of transaction and source of fund.</li> <li>c) Obtain manpower export license.</li> <li>d) Perform Enhanced Due Diligence.</li> <li>e) STR shall be submitted to ML &amp; TFPD if any transaction found suspicious.</li> </ul>
Customer has been refused to provide banking facilities by another bank	4	2	8	<ul style="list-style-type: none"> <li>a) Sufficient information of the client shall be collected through proper verification EDD shall be applied.</li> <li>b) Proper justification of such refusal by the client shall be obtained.</li> <li>c) Justification of refusal.</li> <li>d) Cause of refusal asked for.</li> <li>e) Obtain Complete KYC.</li> <li>f) Perform EDD.</li> </ul>
Accounts opened before 30 April,2002	4	3	12	<ul style="list-style-type: none"> <li>a) Deposit facility shall be provided but no withdrawal facility shall be allowed.</li> <li>b) EDD shall be applied while allowing transaction.</li> <li>c) SAR may be filed if anything suspicious found.</li> <li>d) May go ahead but preferably reduce risk.</li> <li>e) Update KYC, if not possible treat the account as dormant &amp; keep it in a separate list.</li> <li>f) Deposit may be taken but withdrawal should not be allowed till KYC, TP etc. updated.</li> </ul>
Customer with complex accounting and huge transaction	4	3	12	<ul style="list-style-type: none"> <li>a) Obtain the purpose of transaction and source</li> <li>b) EDD shall be applied.</li> <li>c) Constant Monitoring of transactions.</li> <li>d) Evaluating the Risk Grading.</li> <li>e) STR/ SAR shall be filed if suspicious anything found. Obtain complete KYC.</li> <li>f) Perform Enhanced Due Diligence.</li> </ul>
Receipt of donor fund, fund from foreign source by micro finance institute (MFI)	4	3	12	<ul style="list-style-type: none"> <li>a) Documents of donor fund to be ensured &amp; verified.</li> <li>b) Sources of Fund &amp; uses of fund shall be monitored/ verified.</li> <li>c) If the submitted documents are found ok, transaction shall be allowed with constant monitoring of the account.</li> <li>d) Obtain NGO/MFI permission.</li> <li>e) Obtain certificate from regulatory authority, genuineness of source to be ensured.</li> <li>f) Transaction to be monitored frequently.</li> <li>g) Update registration to be obtained.</li> </ul>
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source.	4	3	12	<ul style="list-style-type: none"> <li>a) Obtain the purpose transaction and source of fund.</li> <li>b) Obtain complete KYC.</li> <li>c) EDD shall be applied</li> </ul>

## Chapter 9: Risk Register

<b>Wholesale Banking Customer</b>				
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/Action</b>
Entity customer having operations in multiple location	3	2	6	<ul style="list-style-type: none"> <li>a) Obtain justification from customer regarding operations in various locations.</li> <li>b) Analyze the annual report/ balance sheet. Keep transactions (especially on-line transaction) under monitoring with TP.</li> <li>c) CDD shall be applied.</li> <li>d) STR shall be filed if suspicious anything is found.</li> </ul>
Customer about whom BFIU seeks information (large corporate)	4	3	12	<ul style="list-style-type: none"> <li>a) Check whether there is any negative information about the customer in media/other reliable sources.</li> <li>b) EDD shall be applied.</li> <li>c) Transaction &amp; activities of the client shall be monitored</li> <li>d) Keep their transaction under close monitoring with TP.</li> </ul>
Owner of the entity that are Influential Persons (IPs) and their family members and close associates	4	3	12	<ul style="list-style-type: none"> <li>a) Perform Enhanced Due Diligence.</li> <li>b) Client's source of fund shall be verified</li> <li>c) Obtain approval from CCU before establishing Relationship.</li> <li>d) STR shall be submitted to ML&amp;TFPD if any transaction found suspicious.</li> <li>e) Keep transaction under close monitoring with TP.</li> <li>f) Check whether the source of fun commensurate with the.</li> <li>g) Designation/profession.</li> </ul>
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	4	3	12	<ul style="list-style-type: none"> <li>a) 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.</li> <li>b) Identify the beneficial owner and obtain complete &amp; accurate information of beneficial owner.</li> <li>c) Cheek whether TP of customer commensurate with the nature of business and transaction pattern.</li> <li>d) STR shall be submitted to ML &amp; TFPD if any transaction found suspicious, go ahead but preferably reduce risk.</li> </ul>
A Customer or group of customer making lots of transaction to the same individual or group (wholesale)	3	2	6	<ul style="list-style-type: none"> <li>a) Generate statement / report from system review transaction. Making sure that Transaction Profile (TP) provided by the customer is proportionate with the nature of business and sources of funds supported by necessary documents.</li> <li>b) CDD shall be applied properly.</li> <li>c) Monitor the on line transaction exceeding the limits declared in the TP.</li> <li>d) Obtain justification from the customer.</li> <li>e) Obtain the purpose of transaction.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer whose identification is difficult to check	4	3	12	<ul style="list-style-type: none"> <li>a) Verify the identity of the customer through third party or physical verification by bank officials. If not satisfied, do not open account.</li> <li>b) For existing client, information shall be provided the regulatory Authority through STR/ SAR.</li> <li>c) In case of existing account, close account with prior notice to customer.</li> <li>d) Obtain information about the customer from public media or other reliable sources or peer group.</li> </ul>
Owner of the entity that are Politically Exposed Persons (PEPs) or chief/senior officials of International Organizations and their family members and close associates.	4	3	12	<ul style="list-style-type: none"> <li>a) Conduct Enhance Due Diligence Obtain approval from CCU before establishing relationship.</li> <li>b) Approval from Head Office shall be obtained to set up such business relationship.</li> <li>c) Client's documents/ identity, source of fund shall be verified.</li> <li>d) Transaction shall be monitored</li> <li>e) Keep transaction under monitoring with TP</li> <li>f) Follow foreign exchange guideline and circulars</li> </ul>
Charity or NPOs (especially operating in less privileged areas).	3	2	6	<ul style="list-style-type: none"> <li>a) Obtain Complete KYC. Perform EDD</li> <li>b) Sources of Fund &amp; uses of fund shall be monitored/ verified. If the submitted documents are found ok, transaction shall be allowed with constant monitoring of the account.</li> <li>c) Monitor Transaction.</li> </ul>

<b>Credit Card Customer (yet to be introduced)</b>				
Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer who changes static data frequently	4	3	12	<ul style="list-style-type: none"> <li>a) Sources &amp; uses of fund shall be verified.</li> <li>b) Address &amp; contact person verification (CPV) through third party.</li> <li>c) Obtain documents in support of change information.</li> <li>d) Customer acknowledgement obtains by sending letter to old and new addresses.</li> <li>e) Keep transactions under monitoring with TP.</li> </ul>
Credit Card customer	3	2	6	<ul style="list-style-type: none"> <li>a) Collect required documents as per product program guideline (PPG) and bank Complete KYC.</li> <li>b) Address &amp; contact person verification (CPV) through third party.</li> <li>c) Proper KYC through CDD/ EDD shall be done at the time of opening of the related deposit accounts against which card/ service is issued/ provided</li> </ul>
Customer doing frequent transaction through card(Prepaid & Credit card) and making quick adjustments	3	2	6	<ul style="list-style-type: none"> <li>a) Collect required documents as per product program guideline (PPG).</li> <li>b) Complete KYC. Address &amp; contact.</li> <li>c) Person verification (CPV) through third party.</li> <li>d) Keep transactions under Monitoring. If found suspicious, raise STR.</li> </ul>

## Chapter 9: Risk Register

<b>International Trade Customer</b>				
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/Action</b>
A new Customer (Outward remittance through SWIFT)	3	2	6	<ul style="list-style-type: none"> <li>a) Ensure CDD/EDD</li> <li>b) Perform UNSCR sanction screening must be followed</li> <li>c) Ensure the purpose of the remittance with supporting documents.</li> <li>d) STR shall be filed if suspicious anything is found.</li> <li>e) Follow foreign exchange guideline and circulars.</li> </ul>
A new customer (Import/Export)	4	3	12	<ul style="list-style-type: none"> <li>a) Physical visit/verification of the client's personal/business</li> <li>b) Information/ establishment to check over/under invoicing. Ensure CDD. In case of old customer of the Bank obtain certificate from previous Bank on -"no overdue or no outstanding bill of entry &amp; NOC".</li> <li>c) Confirmation shall be obtained from the competent Authority to detect the fake invoices.</li> <li>d) In case of new customer confirm that respective IRC &amp; ERC issued is genuine. Follow Foreign Exchange guideline and circulars.</li> </ul>
A new customer (Inward remittance through SWIFT)	4	3	12	<ul style="list-style-type: none"> <li>a) Conduct CDD of beneficiary.</li> <li>b) STR shall be filed if suspicious anything is found. May go ahead but preferably reduce risk</li> <li>c) Perform UNSCR sanction screening.</li> <li>d) Ensure the purpose of the remittance with supporting documents.</li> <li>e) Follow Foreign Exchange guidelines and circulars.</li> </ul>
A new customer who wants to carry out a large transaction (Import/Export)	4	3	12	<ul style="list-style-type: none"> <li>a) Approval shall be obtained from the competent Authority for sanctioning limit.</li> <li>b) Conduct CDD.</li> <li>c) Obtain certificate from previous bank on no overdue or no outstanding bill of entry.</li> <li>d) Physical visit/ verification of the client's personal/business information/ establishment to check over/ under invoicing.</li> <li>e) Perform UNSCR sanction screening.</li> <li>f) New customer confirms that respective IRC &amp; ERC issued mentioned by BKB.</li> <li>g) Follow foreign exchange guideline and circulars.</li> </ul>
A new customer who wants to carry out a large transaction (Inward/Outward remittance)	4	3	12	<ul style="list-style-type: none"> <li>a) Ensure CDD &amp; source of fund.</li> <li>b) STR shall be filed if suspicious anything is found.</li> <li>c) Check whether the transaction pattern. Follow Foreign. Exchange guideline and circulars.</li> </ul>
A new customer who wants to conduct business beyond its line of business (Import/ Export)	4	3	12	<ul style="list-style-type: none"> <li>a) For existing customer: such transaction shall not be allowed.</li> <li>b) Obtain permission from regulatory body(s).</li> <li>c) Obtain justification from the customer regarding diversification of business.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Owner/director/shareholder of the customer is influential person(s) or their family members or close associates.	4	3	12	<ul style="list-style-type: none"> <li>a) Approval from Head Office shall be obtained to set up such business relationship.</li> <li>b) Conduct Enhance Due Diligence. Obtain approval from CCU before establishing relationship.</li> <li>c) Client's documents/ identity, source of fund shall be verified.</li> </ul>
Correspondent Banks	3	2	6	<ul style="list-style-type: none"> <li>a) Permission from competent Authority shall be obtained</li> <li>b) Follow BFIU circulars no.26 of 2020 while establishing relationship.</li> <li>c) Obtain sufficient information to understand fully the nature of business of the correspondent/respondent bank.</li> <li>d) Necessary formalities as per Correspondence banking &amp; F.Ex regulation Act 1947 shall be followed.</li> <li>e) Ascertain publicly available information.</li> <li>f) Review KYC periodically.</li> </ul>
Money service businesses (Remittance houses, exchange houses)	3	2	6	<ul style="list-style-type: none"> <li>a) For new customers, account shall not be opened until all obligatory data/ information are obtained through physical verification.</li> <li>b) Follow BFIU circulars no.10 of 2014 while establishing relationship.</li> <li>c) For the existing customers EDD shall be done.</li> <li>d) Obtain sufficient information to understand fully the nature of business of the correspondent/respondent bank.</li> </ul>

2. Risk Register for Products & Services

Retail Banking Product				
Risk	Likelihood	Impact	Risk Score	Treatment/Action
Accounts for students where large amount of transactions are made (student file)	3	2	6	a) CDD shall be maintained. b) Necessity of such transaction to be ensured documentary from the student/authority. c) STR shall be filed if suspicious anything is found.
Gift Cheque	3	2	6	a) CDD shall be maintained. b) Obtain purpose of transaction and sources of fund. c) Obtain complete and accurate information of both d) Applicants and beneficiary (as per BFIU circular no.26 dated -June 16, 2020 related to walk in customer).
Locker Service	4	3	12	a) Perform CDD of the link account b) Activity shall be monitored. c) Update KYC annually d) SAR shall be filed if suspicious anything is found. e) Monitor customer's activity.
Foreign Currency endorsement in Passport				a) CDD shall be maintained. b) Activity shall be monitored. c) Obtain copy of P.P, visa and confirm air ticket. d) In case of walk-in customer complete KYC.
Large transaction in the account of under privileged people				a) Source of fund to be verified with document. b) Constant Transaction monitoring shall be undertaken. c) If not satisfied raise STR.
FDR (Less than 2 million)				a) CDD shall be maintained. b) Sources of fund shall be verified. c) Source of fund to be verified with document.
FDR (2million and above)				a) Source of fund to be verified with documents & declaration. b) Sources of fund shall be verified c) CDD is to be conducted. d) In case of unauthenticated source of fund account shall be regretted
Special scheme deposit accounts opened with big installment and small tenure	4	3	12	a) Proper KYC shall be done with obtaining all required papers/ documents of the clients including source of income. b) Physical verification of the information shall be ensured c) Source of fund to be verified with document.
Multiple deposit scheme accounts opened by same customer in a branch	3	2	6	a) Customer's source of fund to be verified. b) Sources of fund & uses of fund shall be verified c) Perform EDD. d) STR shall be filed if suspicious anything is found.
Multiple deposit scheme accounts opened by same customer from different location	4	3	12	a) Customer's source of fund to be verified. b) Perform EDD. c) Sources of fund & uses of fund shall be verified.

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Open DPS in the name of family member or installments paid from the account other than the customer's account	3	2	6	a) Customer's source of fund to be verified. b) Perform EDD. c) Ensure update KYC of beneficial owner. d) Sources of fund & uses of fund shall be verified.
Early encashment of FDR, special scheme etc.	3	2	6	a) Identify the reason if drawn in cash. b) Proper CDD shall be maintained.
Non face to face business relationship/transaction	3	2	6	a) Complete KYC of Beneficial owners. b) Perform EDD. c) Monitor transaction with TP. d) Sources & uses of fund shall be verified.
Payment received from unrelated/ unassociated third parties.	4	3	12	a) Proper identification of the transaction maker/ 3 <sup>rd</sup> party b) Receive payment only from the distributors, agents and suppliers of the customer. c) Obtain the relationship of the parties. d) Complete short KYC of depositor/withdrawer. e) Monitor transaction report regularly.

<b>SME Banking Product</b>				
Risk	Likelihood	Impact	Risk Score	Treatment/Action
Want to open FDR where source of fund is not clear	4	3	12	a) No relationship to be established. b) CDD shall be maintained. c) STR shall be done if anything found suspicious.
Early encashment of FDR	3	2	6	a) Reason to be known. b) Proper CDD shall be maintained.
Repayment of loan EMI from source that is not clear.	3	1	6	a) Sources of fund shall be ascertained. b) STR/ SAR shall be filed if suspicious anything is found.
Repayment of full loan amount before maturity.	3	2	6	a) Ensure source of fund of repayment before early adjustment of loan. b) Obtain the reason behind early adjustment in writing c) STR/ SAR shall be filed if suspicious anything is found.
Loan amount utilized in sector other than the sector specified during availing the loan.	4	3	12	a) Monitor the utilization of loan. b) Immediate recovery steps to be taken c) Activities of the client shall be monitored.
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount.	3	2	6	a) Physical verification of clients establishment on regular interval/ sudden, if required. b) Ensure source of fund of repayment. If found suspicious, raise STR.
Source of fund used as security not clear at the time of availing loan	3	2	6	a) Sources of fund shall be ascertained. Activities of the client shall be monitored. b) Conduct Enhance Due Diligence. Ensure source of fund of FDR keeping as security before sanctioning loan.

## Chapter 9: Risk Register

Wholesale Banking Product				
Risk	Likelihood	Impact	Risk Score	Treatment/Action
Development of new product & service of bank	3	2	6	<ul style="list-style-type: none"> <li>a) Product vulnerability shall be ascertained.</li> <li>b) Considering the risk, guidelines should be followed.</li> <li>c) Perform CDD.</li> <li>d) Examination of software, logistics related to the product.</li> </ul>
Payment received from unrelated third parties	4	2	12	<ul style="list-style-type: none"> <li>a) Receive payment only from the distributors, agents and suppliers of the customer</li> <li>b) Obtain the relationship of the parties.</li> <li>c) Proper identification of the transaction maker/3<sup>rd</sup> party.</li> <li>d) STR shall be filed if suspicious anything is found.</li> </ul>
High value FDR	3	2	6	<ul style="list-style-type: none"> <li>a) EDD shall be applied.</li> <li>b) Sources of fund shall be verified.</li> <li>c) Proper identification of the transaction maker/ 3<sup>rd</sup> party</li> <li>d) Transaction shall be monitored</li> <li>e) STR shall be filed if suspicious anything is found.</li> </ul>
Term loan, SOD (FO), SOD (G-work order), SOD (Garment), SOD (PO), Loan General, Lease finance, Packing Credit, BTB L/C	3	2	6	<ul style="list-style-type: none"> <li>a) Over all information shall be obtained from the parent authority for sanctioning</li> <li>b) KYC shall be done at the time</li> </ul>
BG (bid bond), BG (PG), BG (APG)	3	2	6	<ul style="list-style-type: none"> <li>a) Verification of beneficiary's information.</li> <li>b) Proper documentation shall be done. CDD shall be maintained.</li> </ul>
L/C subsequent term loan, DP L/C	3	2	6	<ul style="list-style-type: none"> <li>a) Verify the creditworthiness of the customer as per guideline for foreign exchange transaction. Verify other sources of income.</li> <li>b) Ensure physical verification of sales register and stock report.</li> <li>c) Keep transaction under monitoring.</li> <li>d) Undertaking from the customer regarding the fair price to be obtained.</li> </ul>
C.C. (H), SOD (G-Business), STL	3	2	6	<ul style="list-style-type: none"> <li>a) Obtain CIB report.</li> <li>b) EDD to be applied.</li> </ul>
OBU	4	3	12	<ul style="list-style-type: none"> <li>a) Screening of on boarding process</li> <li>b) EDD to be applied.</li> <li>c) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account.</li> </ul>
Syndication Financing	3	2	6	<ul style="list-style-type: none"> <li>a) Physical visit/ verification of the client's personal/ business information/ establishment to assess his net worth.</li> <li>b) Perform EDD.</li> <li>c) Verify the value of plant &amp; machinery and imported items.</li> <li>d) Constant monitoring and follow up to recover the fund. Obtain certificate from the respective country's chamber of commerce</li> <li>e) Obtain undertaking from the customer regarding the price.</li> <li>f) Lead Bank/ Participating Banks documentation to be obtained.</li> </ul>

## Chapter 9: Risk Register

<b>Credit Card (yet to be introduced)</b>				
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/Action</b>
Supplementary Credit Card Issue	3	2	6	<ul style="list-style-type: none"> <li>a) Confidentiality of Security option of the card including PIN Code shall be strictly maintained.</li> <li>b) Collect all credit cards do as per PPG.</li> <li>c) Mention relationship with supplementary cardholder.</li> <li>d) Complete KYC.</li> <li>e) Collect &amp; Check CIB report.</li> <li>f) Perform CDD.</li> <li>g) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder).</li> </ul>
Frequent use of card cheque	4	3	12	<ul style="list-style-type: none"> <li>a) Perform CDD.</li> <li>b) Obtain the purpose of transaction.</li> <li>c) Obtain relationship with the account holder, the account where the fund is transferred.</li> </ul>
BEFTN cheque or pay order as mode of payment instead of account opening at bank(Merchant)	4	3	12	<ul style="list-style-type: none"> <li>a) Perform CDD.</li> <li>b) EDD to be applied where necessary.</li> </ul>
Credit card issuance against ERQ and RFCD accounts	3	2	6	<ul style="list-style-type: none"> <li>a) EDD to be applied where necessary.</li> <li>b) Bangladesh Bank's guidelines/circulars to be followed.</li> <li>c) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account.</li> </ul>

## Chapter 9: Risk Register

<b>International Trade</b>				
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/Action</b>
Line of business mismatch (import/export/remittance)	4	3	12	<ul style="list-style-type: none"> <li>a) Physical visit/ verification of the client's personal/ business information/ establishment to check over/ under invoicing.</li> <li>b) Confirmation shall be obtained from the competent Authority to detect the fake invoices.</li> <li>c) UN Sanction list shall be screened.</li> <li>d) Check the business diversification Perform EDD.</li> </ul>
Under/Over invoicing (import/export/remittance)	4	3	12	<ul style="list-style-type: none"> <li>a) Approval shall be obtained from the competent Authority for sanctioning limit.</li> <li>b) Physical visit/ verification of the client's personal/ business information/ establishment to check over/ under invoicing.</li> <li>c) Confirmation shall be obtained from the competent. Authority to detect the fake invoices.</li> <li>d) UN Sanction list shall be screened.</li> <li>e) Check the unit price of the product intended for import and export with the present market price as per import policy.</li> <li>f) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account.</li> <li>g) Bangladesh Bank's guidelines/circulars to be followed.</li> </ul>
Retirement of import bills in cash (import)	4	2	8	<ul style="list-style-type: none"> <li>a) Obtain KYC.</li> <li>b) UN Sanction list shall be screened.</li> <li>c) Check the size of the transaction with customer's cash flow.</li> <li>d) Perform EDD.</li> </ul>
Wire transfer	4	3	12	<ul style="list-style-type: none"> <li>a) Bangladesh Bank's guidelines/circulars to be followed.</li> <li>b) Proper identification of the transaction maker/ 3<sup>rd</sup> party.</li> <li>c) Obtain information of applicant and beneficiary as per BFIU circular No-26 Dated 16.06.2020.</li> <li>d) Obtain documents that verify identification &amp; support sources of fund.</li> <li>e) Conduct Enhanced Due Diligence.</li> </ul>
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward)				<ul style="list-style-type: none"> <li>a) Confirm the purpose of remittance with supporting documents.</li> <li>b) Obtain information of applicant and beneficiary as per BFIU Circular no. 26.</li> <li>c) UNSCR sanction list screening for all the customers involved in the transaction.</li> <li>d) Perform EDD.</li> <li>e) Bangladesh Bank's guidelines/circulars to be followed.</li> </ul>

3. Risk Register for Business Practices/ delivery methods or Channels.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Online(multiple small transaction through different Branch)	3	2	6	<ul style="list-style-type: none"> <li>a) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder).</li> <li>b) Obtain KYC of bearer as per BFIU Circular No.26. Dated June 16, 2020.</li> <li>c) Generate report on online transaction and monitor.</li> <li>d) Obtain justification from customer regarding the transaction pattern, if not satisfied, raise STR.</li> <li>e) Confidentiality of Security option of the card including PIN Code shall be strictly maintained.</li> </ul>
BEFTN	3	2	6	<ul style="list-style-type: none"> <li>a) STR shall be submitted if anything found suspicious.</li> <li>b) Obtain relationship with customer &amp; beneficiary and purpose of fund transfer.</li> <li>c) Ensure that customer executes transaction as per agreement.</li> <li>d) Monitor transaction pattern, update TP and keep track of deposit volume.</li> </ul>
BACH	3	2	6	<ul style="list-style-type: none"> <li>a) Obtain documents that verify identification &amp; supports sources of fund Ensure CDD.</li> <li>b) STR shall be submitted if anything found suspicious.</li> </ul>
IDBP	3	2	6	<ul style="list-style-type: none"> <li>a) STR shall be submitted if anything found suspicious.</li> <li>b) Check the genuineness of the LC and acceptance from BB dashboard.</li> <li>c) Perform CDD.</li> <li>d) Bangladesh Bank's instruction/circular to be followed.</li> </ul>
Mobile Banking	4	3	12	<ul style="list-style-type: none"> <li>a) Confidentiality of Security option of the card including PIN Code shall be strictly maintained.</li> <li>b) Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions</li> <li>c) Apply transaction restriction policy.</li> <li>d) Check customer transaction profile on monthly basis.</li> <li>e) Generate report on high value transaction from the system and monitor the transactions.</li> <li>f) Ensure that TP update request is received only from registered address.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
<b>Credit Card (yet to be introduced)</b>				
New Merchant sign up	4	3	12	<ul style="list-style-type: none"> <li>a) Verify the genuineness of the merchant.</li> <li>b) Cash will not be allowed against purchase in any case.</li> <li>c) Perform CDD.</li> </ul>
High volume transaction through POS	4	3	12	<ul style="list-style-type: none"> <li>a) Check, Q-cash, VISA, AMEX and NPSB transaction Obtain justification of any unusual transaction.</li> <li>b) Perform EDD.</li> </ul>
<b>Alternate Delivery Channel</b>				
Large amount withdrawn from ATMs	4	3	12	<ul style="list-style-type: none"> <li>a) Generate report on high value ATM transaction from the system and monitor the transactions.</li> <li>b) Apply transaction restriction policy (transaction limit).</li> <li>c) Inform issuer bank if possible.</li> <li>d) Follow Central Bank instruction and International Payment Association ML rules.</li> <li>e) Inform the cards payment Association.</li> </ul>
Large amount transaction from different location and different time (mid night) through ATM	4	3	12	<ul style="list-style-type: none"> <li>a) Besides, CDD shall be obtained from depositor/withdrawer (if transaction is made other than account holder).</li> <li>b) Generate report on high value ATM transaction along with time from the system and monitor the transactions, if any irregularities found, inform relevant branch or department.</li> <li>c) Apply transaction restriction policy (transaction limit).</li> <li>d) Obtain justification from the customer regarding the timing of transaction.</li> <li>e) Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions.</li> </ul>
Large amount of cash deposit in CDM	4	3	12	<ul style="list-style-type: none"> <li>a) Customer's identity &amp; source of fund shall be verified with proper documentation.</li> <li>b) Monitoring shall be done whether the deposit is under or over threshold.</li> <li>c) EDD to be applied.</li> </ul>
Huge fund transfer through internet	4	3	12	<ul style="list-style-type: none"> <li>a) Besides, CDD shall be obtained from depositor/withdrawer (if transaction is made other than account holder).</li> <li>b) EDD to be applied.</li> <li>c) Confidentiality of Security option of the card including PIN Code shall be strictly maintained. Multi factors authentication shall be introduced/applied.</li> <li>d) STR shall be submitted if anything found suspicious. May go ahead but preferably reduce risk.</li> </ul>
Transaction profile updated through Internet Banking	4	3	12	<ul style="list-style-type: none"> <li>a) Transaction to be justified with source of fund.</li> <li>b) Transaction to be monitored with TP.</li> <li>c) STR shall be submitted if anything found suspicious. May go ahead but preferably reduce risk.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer to business transaction-Online payment Gateway-Internet Banking	4	3	12	<ul style="list-style-type: none"> <li>a) Transaction to be justified with source of fund.</li> <li>b) Transaction to be monitored with TP.</li> <li>c) Perform CDD.</li> <li>d) STR shall be submitted if anything found suspicious. May go ahead but preferably reduce risk.</li> </ul>
<b>International Trade</b>				
Customer sending remittance through SWIFT under single customer credit transfer	3	2	6	<ul style="list-style-type: none"> <li>a) Check whether the transaction meets the central Bank Guideline/circular.</li> <li>b) Screening of the Transaction STR shall be filed if suspicious anything is found.</li> <li>c) Obtain purpose of the remittance from the customer (documents if required).</li> <li>d) Proper identification of the Beneficiary should be taken (such as name, a/c number, full address, country name, etc).</li> <li>e) EDD shall be applied.</li> <li>f) Applicant proper identification should be taken (such as name, a/c number, full address, country name, etc).</li> <li>g) Applicant, Beneficiary, Beneficiary's Bank and Beneficiary's Correspondent should be checked whether they are under any sanction list or not.</li> </ul>
Existing customer/other bank customer receiving remittance through SWIFT under single customer credit transfer	3	2	6	<ul style="list-style-type: none"> <li>a) Take form C (if necessary) before remittance. Obtain any other document as and when required.</li> <li>b) Screening of the Transaction.</li> <li>c) STR shall be filed if suspicious anything is found. Conduct Enhanced Due Diligence.</li> </ul>

### 4. Risk Register for Country/jurisdiction

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Import and export from/to Sanction Country.	4	3	12	<ul style="list-style-type: none"> <li>a) Perform sanction screening Inform CCU Immediately.</li> <li>b) Proper documentation shall be maintained.</li> <li>c) Follow procedure in place to treat such situation.</li> </ul>
Trans-shipment, container, flag vessel etc. under global sanction.	4	3	12	<ul style="list-style-type: none"> <li>a) Perform sanction screening Inform CCU Immediately.</li> <li>b) Screening shall be done.</li> <li>c) Follow procedure in place to treat such situation</li> </ul>
Establishing correspondent relationship with Sanction bank and/or Country.	4	3	12	<ul style="list-style-type: none"> <li>a) Perform sanction Screening.</li> <li>b) Inform CCU Immediately.</li> <li>c) Follow procedure in place to treat such situation.</li> <li>d) Perform EDD.</li> </ul>
Establishing correspondent relationship with poor AML & CFT practice country.	4	3	12	<ul style="list-style-type: none"> <li>a) Screening shall be done.</li> <li>b) Obtain KYC from the correspondent Bank.</li> <li>c) Inform CCU immediately.</li> <li>d) Ensure the specific purpose for establishing correspondent relationship.</li> <li>e) Perform EDD.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer belongs to higher risk geographic locations such as high Intensity Financial Crime Areas	4	3	12	<ul style="list-style-type: none"> <li>a) Proper documentation shall be maintained</li> <li>b) Sanction Screening.</li> <li>c) Ensure the specific purpose for establishing correspondent relationship.</li> <li>d) Perform EDD.</li> </ul>
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.	4	3	12	<ul style="list-style-type: none"> <li>a) Proper documentation shall be maintained.</li> <li>b) Sanction Screening.</li> <li>c) Ensure the specific purpose for establishing correspondent relationship.</li> <li>d) Perform EDD.</li> </ul>
Customer belongs to high risk ranking countries of the Basel AML index.	4	3	12	<ul style="list-style-type: none"> <li>a) Sanction Screening.</li> <li>b) Ensure the specific purpose for establishing correspondent relationship.</li> <li>c) Perform EDD.</li> <li>d) Proper documentation shall be maintained.</li> </ul>
Customer belongs to the countries identified by the bank as higher risk because of its prior experiences or other factors.	4	2	8	<ul style="list-style-type: none"> <li>a) Sanction Screening.</li> <li>b) Ensure specific purpose for establishing relationship.</li> <li>c) Perform EDD.</li> <li>d) Proper documentation shall be maintained.</li> </ul>
Any country identified by FATF or FSRBs- (FATF style Regional Body) as not having adequate AML & CFT systems	4	3	12	<ul style="list-style-type: none"> <li>a) Proper documentation shall be maintained.</li> <li>b) EDD to be applied for any</li> <li>c) If necessary STR shall be filed. <b>Do not allow transaction until risk reduced.</b></li> <li>d) Commercial/business relationship.</li> </ul>
Any bank that provide service to 'Shell Bank'	4	3	12	No relationship to be established.
Any Bank that allow payable through account	4	3	12	<ul style="list-style-type: none"> <li>a) If necessary STR shall be filed. <b>Do not allow transaction until risk reduced.</b></li> <li>b) EDD to be applied.</li> <li>c) Monitor transaction with TP.</li> </ul>
Any country identified as destination of illicit financial flow	4	3	12	<ul style="list-style-type: none"> <li>a) It is better not to establish relationship.</li> <li>b) EDD to be applied in import/export/ outward remittance through SWIFT.</li> <li>c) Transaction to be monitored cautiously.</li> </ul>
Branches in a border Area	4	3	12	<ul style="list-style-type: none"> <li>a) KYC Procedures including physical verification of the client's information as well as business premises shall be done properly.</li> <li>b) EDD to be applied.</li> </ul>
Area identified as high risk in the NRA	4	3	12	<ul style="list-style-type: none"> <li>a) It is better not to establish relationship.</li> <li>b) EDD to be applied.</li> <li>c) Address should be cross checked.</li> </ul>
Countries subject to UN embargo/sanctions	4	3	12	No relationship will be established.
Countries subject to BD embargo/sanctions (UN, TIWAN).	4	3	12	No relationship will be established.

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML/CFT guideline approved by the board.	4	3	12	<ul style="list-style-type: none"> <li>a) AML/ CFT guideline shall be chalked out/ updated regularly.</li> <li>b) AML, CFT &amp; Customer Acceptance Policy &amp; Guideline to be developed.</li> <li>c) Reviewed/updated time to time and have it approved by Board.</li> </ul>
Not forming a Central Compliance Unit (CCU).	4	3	12	<ul style="list-style-type: none"> <li>a) Central Compliance Committee must be formed as per instructions of BFIU and will be communicated any changes if any occurred in the same.</li> <li>b) AML Division/Department is to be established as per the requirement of BFIU.</li> </ul>
Not having an AML & CFT compliance Officer.	4	4	12	<ul style="list-style-type: none"> <li>a) AML &amp; CFT Compliance.</li> <li>b) Officer must be formed as per instructions of BFIU and will be communicated any changes if any occurred in the same.</li> <li>c) If so AML &amp; CFT Compliance Officer is to be nominated as per the requirement of BFIU.</li> </ul>
Not having Branch Anti-Money Laundering Compliance Officer.	4	3	12	<ul style="list-style-type: none"> <li>a) Branch Anti Money Laundering Compliance Officer must be deployed.</li> <li>b) Nomination of Branch Anti-money.</li> <li>c) Laundering Compliance Officer (BAMLCO) as per the requirement of BFIU.</li> </ul>
Not having an AML & CFT program.	4	3	12	AML & CFT program to be developed and reviewed from time to time.
No senior Management Commitment to comply with MLP and AT Act	4	3	12	<ul style="list-style-type: none"> <li>a) Senior Management must be committed for implementation of MLPA &amp; ATA.</li> <li>b) Senior management is committed to comply with MLP and ATA Act. Share the commitment with Bank officials (at least once in a year).</li> </ul>
Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	4	3	12	Meticulously follow the AMLD/BFIU circular, circular letter, instructions issued from time to time.
Unique Account opening form not followed while opening account.	4	3	12	Unique account opening form prescribed by Bangladesh Bank is to be used meticulously.
Non screening of new and existing customers against UNSCR sanction and OFAC list.	4	3	12	Screening process must be conducted for new & existing customers. Screen all new and existing customers against UNSCR and Local Sanction lists through Automated Sanction Screening software.
Violation of Foreign Regulation Act, 1947 while dealing with NRB Accounts.	4	3	12	Foreign Exchange Regulation Act, 1947 must be complied Follow the Foreign Exchange Regulation Act, 1947/its assessment while dealing with NRB accounts.
Complete and accurate information of customer not obtained.				<ul style="list-style-type: none"> <li>a) Complete and accurate information of customer must be obtained.as per BFIU Circular no 26 Dated JUNE 16, 2020 guideline.</li> <li>b) Develop control mechanism to check/collecting of complete and accurate information of customer and to be reviewed &amp; updated the same from time to time.</li> <li>c) Complete and accurate information of customer must be obtained as per BFIU Circular no 26; Dated JUNE 16, 2020 guidelines.</li> <li>d) Develop control mechanism to check/collecting of complete and accurate information of customer and to be reviewed &amp; updated the same from time to time.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Failure to verify the identity proof document and address of the customer.	4	3	12	Customer's information must be verified/ supported by documents.
Beneficial owner identification and verification not done properly.	4	3	12	Beneficial owner's KYC must be obtained Identify beneficial owner of the account and obtain complete and accurate information of beneficial owner as per BFIU Circular No. 26 Dated, JUNE 16, 2020.
Customer Due Diligence (CDD) is not practiced properly.	4	3	12	<ul style="list-style-type: none"> <li>a) CDD must be maintained.</li> <li>b) CDD is to be maintained as per BFIU circular no. 26 Dated, June 16, 2020.</li> <li>c) Develop control mechanism to check whether business units are performing Customer conduct.</li> </ul>
Failure to perform Enhance 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).	4	3	12	<ul style="list-style-type: none"> <li>a) EDD must be applied for high risk customers (i.e, PEPs, family members and close associates of PEPs and influential person and senior official of international organization.</li> <li>b) Senior Management approval to be obtained before opening such account. Conduct both CDD &amp; EDD of high risk customers as per BFIU instruction.</li> </ul>
Failure to complete KYC of customer including walk in customer.	4	3	12	Complete KYC of customer including walk- in customer as per BFIU Circular No. 26 ,Dated JUNE 16, 2020 to be obtained
Failure to update TP and KYC of customer.	4	3	12	<ul style="list-style-type: none"> <li>a) TP &amp; KYC of customer must be obtained.</li> <li>b) Update TP &amp; KYC as per BFIU Circular No. 26. Dated June 16, 2020.</li> <li>c) Develop control mechanism to check whether business units are updating TP &amp; KYC as per the instruction of BFIU.</li> </ul>
Failure to assess the ML & TF risk of a Product or service before launching.	4	3	12	<ul style="list-style-type: none"> <li>a) Assessment shall be done on the ML &amp; TF risk of a product or service before launching</li> <li>b) Assess the ML &amp; TF risk of a product or service, devise action plan to manage the same before launching the products or service at Head Office level.</li> <li>c) Check whether all the PPGs approved by CCU before launching.</li> </ul>
Failure to complete the KYC of correspondent Bank.	4	3	12	KYC procedures must be completed before making relationship obtain updated KYC of correspondent bank from time to time mandatorily.
Senior Management approval not obtained before entering into a Correspondent Banking relationship.	4	3	12	Senior Management approval to be obtained before entering into a Correspondent Banking relationship.
Failure to comply with the instruction of BFIU by foreign subsidiary	4	3	12	<ul style="list-style-type: none"> <li>a) Monitor the AML &amp; CFT activity of foreign subsidiary.</li> <li>b) Obtain confirmation from the subsidiary on compliance.</li> </ul>
Failure to keep record properly.	4	3	12	<ul style="list-style-type: none"> <li>a) Senior Management approval must be obtained before making relationship.</li> <li>b) Keep records as per BFIU instruction.</li> <li>c) Check compliance status during audit/inspection.</li> </ul>

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Failure to report complete and accurate CTR on time.	4	3	12	<ul style="list-style-type: none"> <li>a) Complete and accurate CTR will be submitted in time.</li> <li>b) Ensure uniformity of CTR submitted through goAML web.</li> <li>c) Submit complete and accurate CTR on time.</li> </ul>
Failure to review CTR.	4	3	12	<ul style="list-style-type: none"> <li>a) CTR to be generated from system.</li> <li>b) Transaction reported in CTR to be monitored by both branch &amp; CCC on monthly basis.</li> <li>c) Identify whether there is any suspicious transaction &amp; report.</li> </ul>
Failure to identify and monitor structuring.	4	3	12	<ul style="list-style-type: none"> <li>a) CTR must be reviewed.</li> <li>b) Structuring report to be generated from system.</li> <li>c) Identify and monitor structuring on monthly basis.</li> </ul>
Failure to provide sufficient control and monitoring system for the timely detection and reporting of suspicious activity.	4	3	12	<ul style="list-style-type: none"> <li>a) Structuring must be identified. SAR shall be filled if necessary</li> <li>b) System to be devised by Head Office to generate report that facilities identifying STR.</li> <li>c) Analyze and detect STR.</li> </ul>
Failure to conduct quarterly meeting properly.	4	3	12	<ul style="list-style-type: none"> <li>a) Meeting shall be conducted regularly.</li> <li>b) Conduct quarterly meeting at branch in line with the agenda and instruction of BFIU Circular No. 26, Dated June 16, 2020.</li> <li>c) Send the meeting minutes to CCC.</li> </ul>
Failure to report suspicious transaction (STR).	4	3	12	<ul style="list-style-type: none"> <li>a) Suspicious transaction must be detected and reported in time.</li> <li>b) Monitor Account transaction and customer activity and report when found suspicious.</li> <li>c) Monitor the transaction reported in CTR by both branch &amp; CCC on monthly basis and identify whether there is any suspicious transaction.</li> </ul>
Failure to conduct self-assessment properly.	4	3	12	<ul style="list-style-type: none"> <li>a) SAR shall be conducted properly.</li> <li>b) Conduct Self-Assessment properly. Identify the actual strength, weakness and position of the branch in self-assessment.</li> <li>c) AMLD to cross check (CCC) the self-assessment report with independent testing report and inspection report.</li> </ul>
Failure to submit statement/report to BFIU on time	4	3	12	<ul style="list-style-type: none"> <li>a) Statement/ report shall be reported to BFIU.</li> <li>b) Submission statement/report to BFIU timely.</li> <li>c) Check submission status during audit/inspection.</li> </ul>
Submit erroneous statement/report to BFIU.	4	3	12	<ul style="list-style-type: none"> <li>a) Check minutely the statements before submitting the same to BFIU.</li> <li>b) Accurate report shall be submitted to BFIU.</li> </ul>
Not complying with any order for freezing or suspicious of transaction issued by BFIU or BB.	4	3	12	<ul style="list-style-type: none"> <li>a) BFIU's order/ instruction must be complied on time</li> <li>b) Comply with the order for freezing or suspension of transaction issued by BFIU or BB instantly. Check the compliance of freezing order by CCC.</li> </ul>
Not submitting accurate information or statement sought by BFIU or BB	4	3	12	Provide accurate information to BFIU on time.
Not submitting required report to senior management regularly.	4	3	12	Submit all the report to senior management timely. Accurate information shall be reported to BFIU.

## Chapter 9: Risk Register

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Failure to rectify the objections raised by BFIU or bank inspection teams on time.	4	3	12	<ul style="list-style-type: none"> <li>a) Required reported must be submitted to senior Management.</li> <li>b) Objections raised by BFIU or inspection teams of BKB to be regularized on time and submit compliance report. CCC to follow up to rectify or regularize the irregularities.</li> </ul>
Failure to obtain information during wire transfer.	5	2	8	<ul style="list-style-type: none"> <li>a) Information during wire transfer based on the threshold as per BFIU Circular No. 26, Dated June 16, 2020 to be obtained.</li> <li>b) Inspection team to check compliance status during audit/inspection.</li> </ul>
Failure to comply with the responsibilities of ordering, intermediary and beneficiary Bank.	4	3	12	Responsibilities of ordering, intermediary and beneficiary Bank as per BFIU instruction & Foreign exchange guideline to be complied.
Failure to scrutinize staff properly.	4	3	12	<ul style="list-style-type: none"> <li>a) Staff will be scrutinized properly. May go ahead but preferably reduce risk. HR to screen the applicant's details before recruitment.</li> <li>b) Reference check, Background check</li> <li>c) Screening through or clearance from Law Enforcement Agency</li> <li>d) Personal interview, Personal Guarantee Capacity of employee and training on AML &amp; CFT.</li> <li>e) Staff will be scrutinized properly. May go ahead but preferably reduce risk. HR to screen the applicant's details before recruitment.</li> <li>f) Reference check, Background check.</li> <li>g) Screening through or clearance from Law Enforcement Agency.</li> <li>h) Personal interview, Personal Guarantee.</li> <li>i) Capacity of employee and training on AML &amp; CFT.</li> </ul>
Failure to circulate BFIU guidelines and circular to branches.	4	3	12	<ul style="list-style-type: none"> <li>a) BFIU's instruction must be circulated to the branches on time. May go ahead but preferably reduce risk.</li> <li>b) Update the branches on circular/circular letters instructions received from BFIU. Issue instruction circular and letter as and when required.</li> </ul>
Inadequately training/workshop arranged on AML & CFT.				<ul style="list-style-type: none"> <li>a) Proper training must be ensured. May go ahead but preferably reduce risk.</li> <li>b) Workshop on MLP &amp; CFT for employees to build up awareness and conduct evaluation test to be arranged.</li> </ul>

# Chapter 10

## Screening

### 10.1. SANCTIONS SCREENING

United Nations Security Council Resolution 1267 and 1373 have been adopted under Article VII of UNSCR charter, which means these resolutions are obligatory for every jurisdiction. BFIU has instructed all banks and FIs to take necessary action on UNSCR 1267 and 1373 (targeted financial sanctions). To comply with this direction all branches of BKB should consult the UN sanction list regularly and if find any account with it, they should inform the Central Compliance Unit (CCC) immediately.

### 10.2. CONCERNED BODIES FOR SCREENING

- Every deposit client
- Every investment client
- Every remitter & remittance beneficiary
- International Trade business entities or individuals
- MSBs with subsidiary, mother companies, Senior Management & Key persons
- Correspondent Banks with subsidiary, mother companies, senior management & key persons
- Vendors/suppliers
- CSR beneficiaries
- C&F agents
- Insurance companies
- Panel lawyers
- Surveyor companies
- Beneficial owners
- Employees
- Walk-in customers
- And any other potential customers

### 10.3. THE LISTS TO BE SCREENED WITH

Bangladesh Krishi Bank shall have up to date databases to screen all of its customers with the following lists but not limited to-

- UN sanction list
- OFAC List
- High risk customer/PEPs/IP list
- Govt. black listed clients/companies
- Adverse media
- Internal negative list/defaulters clients
- Rejected clients' List
- Trustee/ charitable/religious/club/societies organizations
- Non Profit organizations
- Fraud database of Bangladesh Bank
- REHAB member's list
- BoI registration list
- List of the companies registered with different associations (BGMA/BKMA/BJMA etc.).
- List of RJSC & Firms
- FI data base including management/directors list

# Chapter 11

## Transaction Monitoring

The compliance program also relies on the variety of internal controls, including management report, built-in safeguards and exception report that keep the program working. FATF recommendation 18 requires that financial institutions have an internal control program.

### 11.1. TRANSACTION MONITORING METHOD

The following elements should be included in the operational controls of any policy:

- Statement of responsibility for compliance with policy;
- Customer due diligence;
- Customer identification/verification
- Additional know your customer information
- High risk customers
- Non face to face business (if applicable)
- Handling of politically exposed persons
- Monitoring for suspicious transaction/activity;
- Cooperation with the authorities;
- Record keeping;
- Screening of transactions and customers;
- Training and awareness;
- Adoption of risk management practices and use of a risk-based approach.

It is mandatory to collect and verify the correct and complete identification of customers to prevent money laundering and terrorist financing and to keep the institution free from risks. As per AML circular, a customer is defined as:

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

### 11.2. TRANSACTION MONITORING PROCESS

To protect institution from risks of money laundering or/and terrorist financing by customers willful or unwilling activities, in the Money Laundering Prevention Policy Manual prepared by BKB clearly state how to conduct Customer Due Diligence at different stages such as:

- while establishing relationship with the customer;
- while conducting financial transaction with the existing customer;

## Chapter 11: Transaction Monitoring

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

**11.2.2.** If a person operates an account on behalf of the customer, the concerned branch must satisfy itself that the person has due authorization to operate. Correct and complete information of the person, operating the account, is to be collected.

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

**11.2.4.** While establishing and maintaining business relationship and conducting financial transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering (such as the countries and territories listed as high risk country in FATF's public statements) enhanced due diligence shall have to be ensured

**11.2.5.** The identity of the beneficial owner of the account shall have to be confirmed on the basis of the information obtained from reliable sources up to the satisfaction of the institution. Moreover, branches have to do the followings:

- Complete and correct information of identity of the persons besides the customer, shall have to be collected and preserved if a customer operate an account on behalf of another person in his/her own name.
- The controller or the owner of the customer shall have to be identified.
- Complete and correct information of identity of the beneficial owners shall have to be collected and preserved. For the purpose of this subsection, a person will be treated as a beneficial owner if:
  - a) he has controlling share of a company or/and
  - b) hold 20% or more shares of a company

# Chapter 12

## CTR and STR Reporting

### 12.1. SUSPICIOUS TRANSACTION REPORTING ACCORDING TO LAWS

According to the provision of section 25 (1) (d) of MLPA, 2012, the bank have to report BB proactively and immediately, facts on suspicious, unusual or doubtful transactions likely to be related to money laundering

Money Laundering Prevention Act, 2012 (Amendment-2015) 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
- This 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.

Anti-Terrorism Act, 2009 defines suspicious transaction as follows-

- Which is different from usual transactions
- Which invokes presumption that,
- It is the proceed 3s 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 transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.

### 12.2. IDENTIFICATION OF STR/SAR

The following chart shows the graphical presentation of 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 indicate

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 unpredictable 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. Some red flag indicators for identifying STR/SAR related to ML&TF are available in these Guidelines. All suspicions reported to the Anti-Money Laundering & Combating Terrorist Financing Division shall be documented, or recorded electronically. The report shall include full details of the customer who is the subject of concern and as full statement as possible of the information giving rise to the suspicion. All internal enquiries made in relation to the report shall 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/SARAs discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, bank shall conduct the following 3 stages:

**a) Identification**

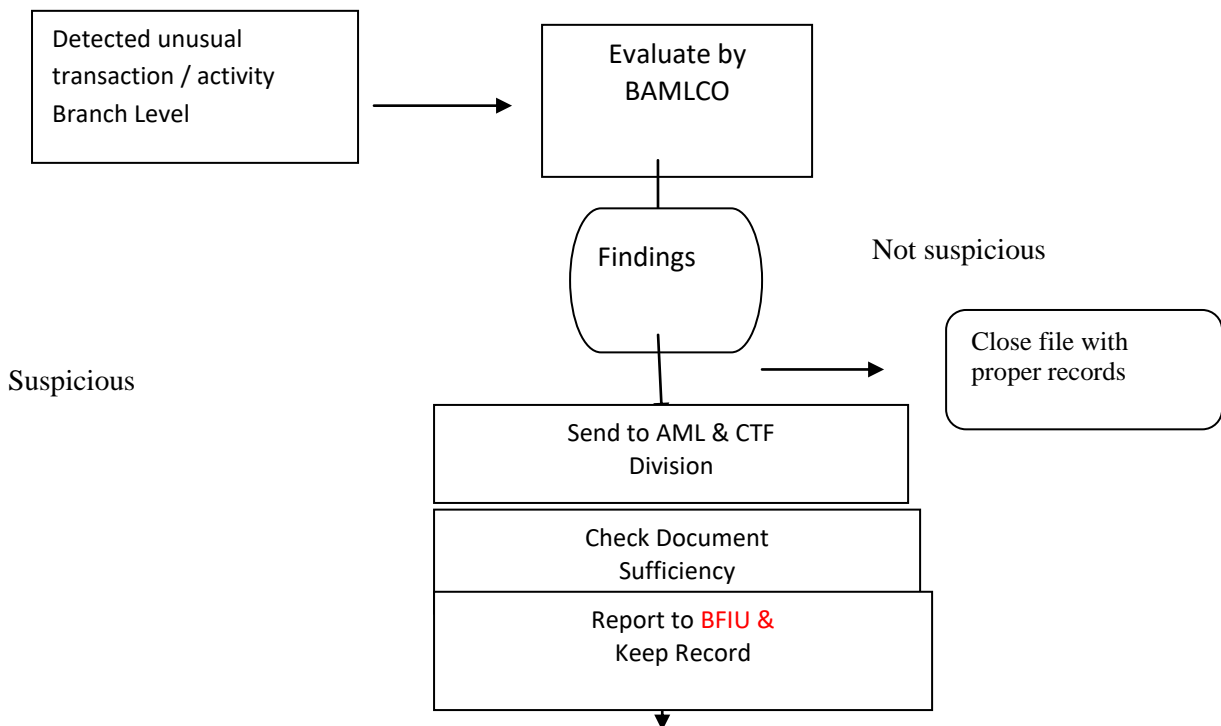
Depending on size, need and complexity of financial institutions monitoring of unusual transactions may be automated, manually or both. Some financial institutions use specialized software to detect unusual transactions or activities, however, the use of such software can only be complemented managerial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

**b) Evaluation**

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

**c) Disclosure**

This is the final stage and Bangladesh Krishi Bank should submit STR/SAR to Bangladesh Bank if it is still suspicious. For simplification the flow chart given below shows STR/SAR identification and reporting procedures:



### 12.3. DOCUMENTING REPORTING DECISIONS

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

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

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

### 12.4. REPORTING GUIDANCE

BFIU implemented a secured online reporting system namely the goAML, which requires the ROs to submit SARs and STRs through this channel. The goAML Web application provides a secure web based interface between the BFIU and its reporting organizations for the electronic upload of reports such as XML files, filling out the online report forms or sending XML files as attachments by secure e-mail, information sharing among stakeholders and other information. Bangladesh Krishi Bank shall submit STR/SAR by using goAML web as per instruction mentioned in goAML Manual (<https://www.bb.org.bd/eservices.php>). Krishi Bank can also submit STR/SAR manually by using the format prescribed by BFIU ([https://www.bb.org.bd/bfiu/reporting\\_forms.php](https://www.bb.org.bd/bfiu/reporting_forms.php)). Reporting Organizations (ROs) shall preserve all information on a reported STR until any further instruction by BFIU.

### 12.5. SOME SPECIAL SCENARIOS FOR REPORTING

- 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, reporting organization should submit suspicious transaction/activity report on such customers.
- If Reporting Organization identifies any account or transaction in the name of listed or prescribed 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, Reporting Organization must stop transaction of the account and report BFIU with detailed information within the next working day.
- If any news on Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction is published in the media and if any account of any person or entity related to that activity is maintained with the reporting organization, detailed information must be reported to BFIU without any delay.

### 12.6. 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.

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

Bangladesh Krishi Bank shall consider the confidentiality of the reporting of STR/SAR. They should not make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious. Krishi Bank shall report suspicious transaction/activity without performing Customer Due Diligence (CDD) if there is reasonable ground that Tipping Off may take place in the event of performing CDD for any transaction suspected to be related to ML & TF.

### 12.7. PENALTY

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

### 12.8. PENALTY OF TIPPING OFF

Under section 6 of MLPA, 2012, if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding Taka 50 (fifty) thousand or with both.

### 12.9. SAFE HARBOR PROVISION

In section (28) of MLPA, 2012 provides the safe harbor for persons submitting suspicious reports. As per Section 28 of MLPA, no suit or prosecution or administrative measures or any other legal proceedings shall lie against any reporting organization or its Board of Directors or any of its officers or staffs for anything which is done in good faith under this Act or Rules made there under for which any person is or likely to be affected. Disclosure of information in good faith by a reporting organization or by an employee or director of such a reporting organization shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

### 12.10. RED FLAGS

Suspicion can be defined as –

- A state of mind more definite than speculation but falling short of evidence-based knowledge.
- A positive feeling of actual apprehension or mistrust.
- A slight opinion, without sufficient evidence.

### 12.11. THE FOLLOWING RED FLAGS CAN BE USED AS INDICATORS OF SUSPICIOUS TRANSACTION OR SUSPICIOUS ACTIVITIES

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

### 12.12. NECESSARY PAPERS/DOCUMENTS FOR STR

- Separate forwarding letter to be issued for every STR.
- Copy of the related Account Opening Form to be submitted with STR.
- Copy of the related KYC, TP & other papers shall be submitted with STR.
- Related Account statement for minimum 01 (one) year to be enclosed.
- Related Investigation Report to be submitted with STR.
- STR shall be submitted in prescribed format as per BFIU Circular No.26 dated 20.06.2020.
- The copy of supporting vouchers mentioned in STR form must be submitted.

### 12.13. SUBMISSION OF CASH TRANSACTION REPORT (CTR)

Branch Anti Money Laundering Compliance Officer (BAMLCO) would observe the daily transactions of Tk.10.00 lac and above amounts of an Account transacted in cash deposit or cash withdrawal which is automatically generated and reported to BFIU through goAML. If the summation is shown excess of the aforesaid amount of one & above cash deposit or cash withdrawal of a particular account in a day then the report for deposit and withdrawal to be submitted separately. If remit in an account in a day the equal of the aforesaid amount by born one or above cash remittance or Online deposit then the same also be reported. The Central Compliance Committee (CCC) will submit CTR to the BFIU through goAML Software along with a soft-copy on monthly basis after collecting the same from the Branches or from the system by the date 21 of next month. The BAMLCO will examine the CTR items before reporting in a view whether any suspicious transaction occurred, if so he will report STR mentioning causes of suspicious to CCC. Only cash withdrawal will be considered for CTR in case of Public Accounts and the accounts of Govt. owned institutions. A precautionary procedure would have to be introduced for preventing Structuring by the Client when he transacting under the CTR limit repeatedly. BKB has been submitting CTR generated by the cash transaction limit of Tk. 10 lac & above through goAML software since January 01, 2014 on compulsory basis.

# **Chapter13**

## **Self-Assessment and Independent Testing Procedure (ITP)**

### **13.1. SELF-ASSESSMENT REPORT**

Banking system in Bangladesh is mainly based on branch banking. The branches of the banks are in every corner of the country and they have an active role in stimulating the economic growth of the country. It is very difficult for the CCU or ICC to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFIU has established a Self-Assessment Reporting system for the branches. According to the instructions of BFIU Circular-26 dated-16/06/2020, branches of Bangladesh Krishi Bank need to conduct the Self-Assessment to evaluate them on a half yearly basis through a checklist. Before finalizing the evaluation report, there shall have to be a meeting presided over by the branch manager with all concerned officials of the branch. In that meeting, there shall be a discussion on the branch evaluation report whether the identified problems according to that report are feasible to be solved at the branch level, and then necessary actions shall be taken without any delay to finalize it. In the final report, recommendations shall have to be jotted down. In the subsequent quarterly meetings on preventing money laundering and terrorist financing, the progress of the related matters shall 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 shall be submitted to the Audit & Inspection Division of the Head Office and the Central Compliance Committee within the 15th of the next month.

### **13.2. INDEPENDENT TESTING PROCEDURE (ITP)**

To ensure the effectiveness of the AML/CFT program, financial institution should assess the program regularly and look for new risk factors. FATF recommendation 15 suggests that institutions covered by laws should establish and maintain policies, procedures and controls which should include an appropriate compliance function and an audit function. Audit is a kind of assessment of checking of a planned activity. Only those will check or examine the institutions that do not have any stake in it. To ensure objective assessment it is important to engage an independent body to do audit.

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

- Address the adequacy of AML/CFT risk assessment.
- Examine/attest the overall integrity and effectiveness of the management systems and the control environment of Branches.
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements.
- Determine personnel adherence to the institution's AML/CFT policies, procedures and processes.
- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations).
- Assess the adequacy of the processes for identifying and reporting suspicious activity.
- Communicate the findings to the board and/or senior management in a timely manner.
- Recommend corrective action for deficiencies.
- Track previously identified deficiencies and ensure that management corrects them.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Determine when assessing the training program and materials:

## **Chapter 13: Self-Assessment and Independent Testing Procedure**

### **13.3. RESPONSIBILITY OF AUDIT & INSPECTION DIVISION**

Audit function shall be done by the internal audit. At the same time external auditors appointed by the Bank to conduct annual audit shall also review the adequacy of AML/CFT program during their audit. During conducting Audit function at the Branches under regular/periodic audit program Internal Audit i.e. Regional Audit office will examine all activities regarding compliance of AML & CFT issues of the branches through Independent Testing Procedures and report to Central Compliance Committee (CCC) within twenty days from the date of retirement of Audit.

### **13.4. WHY THE AUDIT FUNCTION IS NECESSARY**

To ensure the effectiveness of the AML/CFT program, financial institution should assess the program regularly and look for new risk factors. FATF recommendation 15 suggests that institutions covered by laws should establish and maintain policies, procedures and controls which should include an appropriate compliance function and an audit function. Audit is a kind of assessment of checking of a planned activity. Only those will check or examine the institution that does not have any stake in it. To ensure objective assessment it is important to engage an independent body to do audit.

### **13.5. RESPONSIBILITY OF CENTRAL COMPLIANCE COMMITTEE (CCC)**

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

- Total number of branch and number of self-assessment report received from the branches.
- The number of branches inspected/audited by the A&ID at the time of reporting and the status of the branches (branchwise achieved number).
- 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.
- The general and special irregularities mentioned in the report submitted by the A&ID and the measures taken by the CCC to prevent those irregularities.
- Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as unsatisfactory and marginal in the received report. Mentioned report shall be included with the matter mentioned in section 1.3 (3) of BFIU Circular No.26 dated 16.06.2020: The branch evaluation reports received from the branches shall have to be assessed and if there are any risk assessed in any branch, there shall be an arrangement of immediate inspection by the Audit and Inspection Division, in the branch while the matter shall be informed to the respective authority.

In case of banks that are involved in mobile financial services and agent banking activities, after reviewing the reports from the Audit and Inspection Division, in the month of January of every year, the CCC shall submit a summary of all irregularities found in previous year's audits including its observations and recommendations to the Managing Director & CEO of the bank. With the comments of the Managing Director & CEO, the report shall have to be presented at the meeting of the board of directors or management committee of the bank. By February, an annual report with the comments of the board of directors or the management committee and the accommodated measures shall have to be submitted to BFIU.

# **Chapter 14**

## **Terrorist Financing & Proliferation Financing (TF & PF)**

### **14.1. TERRORIST FINANCING**

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

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

According to the article 7 of the Anti-Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means:

Offences relating to financing terrorist activities–

- (1) If any person or entity knowingly provides or expresses the intention to provide money, services, material support or any other property to another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person, entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.
- (2) If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.
- (3) If any person or entity knowingly makes arrangement for money, services, material support or any other property for another person or entity where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any.

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

## 14.3. LEGAL OBLIGATIONS

Obligations under ATA, 2009

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

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

## 14.4. OBLIGATIONS UNDER CIRCULAR

Obligations under BFIU Circular-26; dated 26/06/2020

Every bank shall establish a procedure by approval of Board of Directors for detection and prevention of financing of terrorism and financing of proliferation of weapons of mass destruction, shall issue instructions about the duties of Bank officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.

Before any international business transaction, every bank will review the transaction to identify whether the concerned parties of those transactions are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or proscribed by Bangladesh government. 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.

### 14.5. FLOW-CHART FOR IMPLEMENTATION OF TFS BY BANK

Sources of Sanction List

- a. UN Security Council website <http://www.un.org/sc/committees/list-complied.shtml>
- b. BFIU website (<http://www.bb.org.bd/bfiu/index.php>)
- c. Domestic Sanction list from BFIU website
- d. Unilateral or Regional Sanction list forwarded by BFIU

Run a regular check including transactional review-

- a. before any foreign transaction
- b. before encashment of foreign currency
- c. before opening of any Account

If any match  
found

Report to  
BFIU

### 14.6. 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.

### 14.7. 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.

### 14.8. 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),
- The international trade system.

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

#### 14.8.1. Formal Financial Sector

Financial institutions and other regulated financial service providers' services and product 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.

### **14.8.2. 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.

### **14.8.3. Cash Couriers**

The physical movement of cash is one way terrorists can move funds without encountering the AML/CFT safeguards established in financial institutions. It has been suggested that some groups have converted cash into high-value and hard-to trace commodities such as gold or precious stones in order to move assets outside of the financial system. The movement of cash across the borders is prevalent in cash based economies and where the electronic banking system remains embryonic or barely used by the populace. Moving money using cash couriers may be expensive relative to wire transfers. As legitimate financial institutions tighten their due diligence practices, it has become an attractive method of transferring funds without leaving an audit trail. When cross border remittance of cash is interdicted, the origin and the end use of cash can be unclear. Cash raised and moved for terrorist purposes can be at very low levels – making detection and interdiction difficult.

### **14.8.4. Use of Alternative Remittance System (ARS)**

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

### **14.8.5. Use of Charities and Non-Profit Organizations**

Charities are attractive to terrorist networks as a means to move funds. Many thousands of legitimate charitable organizations exist all over the world that serve the interests of all societies, and often transmit funds to and from highly distressed parts of the globe. Terrorist abuses of the charitable sector have included using legitimate transactions to disguise terrorist cash travelling to the same destination; and broad exploitation of the charitable sector by charities affiliated with terrorist organizations. The sheer volume of funds and other assets held by the charitable sector means that the diversion of even a very small percentage of these funds to support terrorism constitutes a grave problem.

### **14.8.6. Targeted Financial Sanctions (TFS)**

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.

The term Targeted Financial Sanctions (TFS) means both 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 the UNSC. 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. 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 targeted in the sense that they apply only to a subset of the population usually the leadership, responsible elites, or operationally responsible individuals; they are financial in that they involve the use of financial instruments, such as asset freezing, blocking of financial transactions, or financial services; and they are sanctions in that they are coercive measures applied to effect change or constrain action. 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, to minimize the unintended effects of comprehensive sanctions and achieve greater effectiveness.

### **14.9. IMPLEMENTATION OF FATF RECOMMENDATION 6 & 7 FATF RECOMMENDATION-6, TFS RELATED TO TERRORIST & TERRORIST FINANCING**

FATF recommendation 6 explains Countries shall implement targeted financial sanctions regimes to comply with United Nations Security Council Resolutions (UNSCRs) 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 UNSC, including in accordance with resolution 1267(1999) and 1373(2001) or as described in section 2-(g) of Anti-Terrorist Rules-2013 and any successor resolutions to be adopted by the Security Council of the United Nations in the future, under Chapter VII of the Charter of the United Nations.

#### **FATF Recommendation 7, TFS related to Proliferation**

FATF recommendation 7 requires Countries shall implement targeted financial sanctions to comply with United Nations Security Council Resolutions (UNSCRs) 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 or 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 UNSCR.

### **14.10. AUTOMATED SCREENING MECHANISM OF UNSCR'S**

For effective implementation of TFS, BKB must maintain and update the list of individuals and entities in electronic form and regularly run a check at UNSC website for updated list. BKB shall introduce an automated screening mechanism to detect any listed individuals or entities to enter into the banking channel at the time of account opening or establishing any relationship including international relationship and prior to execute any kind of foreign exchange transaction. The bank will operate in such system whether they could detect any listed individuals or entities prior to establish any relationship with them. For proper implementation of UN sanction list, every official 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

**14.11. ROLE OF BANGLADESH KRISHI BANK IN PREVENTING TF& PF**

- Bangladesh Krishi Bank has established a procedure by the approval of Board of Directors for detection and prevention of financing of terrorism and financing in proliferation of weapons of mass destruction, shall issue instructions about the duties of BKB officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.
- Bank is taken necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 and if any suspicious transaction is identified, the agency shall spontaneously report it to Bangladesh Bank without any delay.
- If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, bank shall send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to BFIU immediately.
- The bank 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. They 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 them.
- The bank will run a check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009.
- Entities acting on behalf of, or at the direction of the individuals or entities listed or scheduled under the Act will also be inspected thoroughly to check whether have any form of relationship with the marked individuals- like holding any funds, financial assets or economic resources or related services.

# Chapter 15

## Trade Based Money Laundering (TBML)

### 15.1. WHAT IS TRADE

Trade-based money laundering (TBML) involves the exploitation of the international trade system for the purpose of transferring value and obscuring the true origins of illicit wealth. TBML schemes vary in complexity but typically involve misrepresentation of the price, quantity, or quality of imports or exports. Financial institutions may wittingly or unwittingly be implicated in TBML schemes when such institutions are used to settle, facilitate, or finance international trade transactions (e.g., through the processing of wire transfers, provision of trade finance, and issuance of letters of credit and guarantees). TBML activity is considered to be growing in both volume and global reach. Although TBML is widely recognized as one of the most common manifestations of international money laundering, TBML appears to be less understood among academics and policymakers than traditional forms of money laundering through the international banking system and bulk cash smuggling.

- Engine of growth
- Ensures optimal use of resources
- Countries need to have a ‘free and fair’ trade regime.

Dilemma faced by policy makers:

“The requirement to balance the needs of a free, fair and predictable trade regime with the needs for regulation of trade so as to prevent its abuse.”

### 15.2. TRADE PRODUCTS

While there is no exhaustive list of trade-related products and services, some indicative examples of products or services that typically fall within the scope of “trade finance” services offered by banks, include:

- Bank guarantees
- Documentary collections
- Financing under open account transaction
- Forfeiting and risk participation
- Letters of credit (L/C)
- Financing for transactions under L/Cs
- Packing credits
- Pre-shipment credits
- Structured trade financing
- Trust receipts
- Warehouse financing
- Import/export loans
- Import/export invoice
- Discounting, forfeiting (If Applicable)

### Trade and Money Laundering-

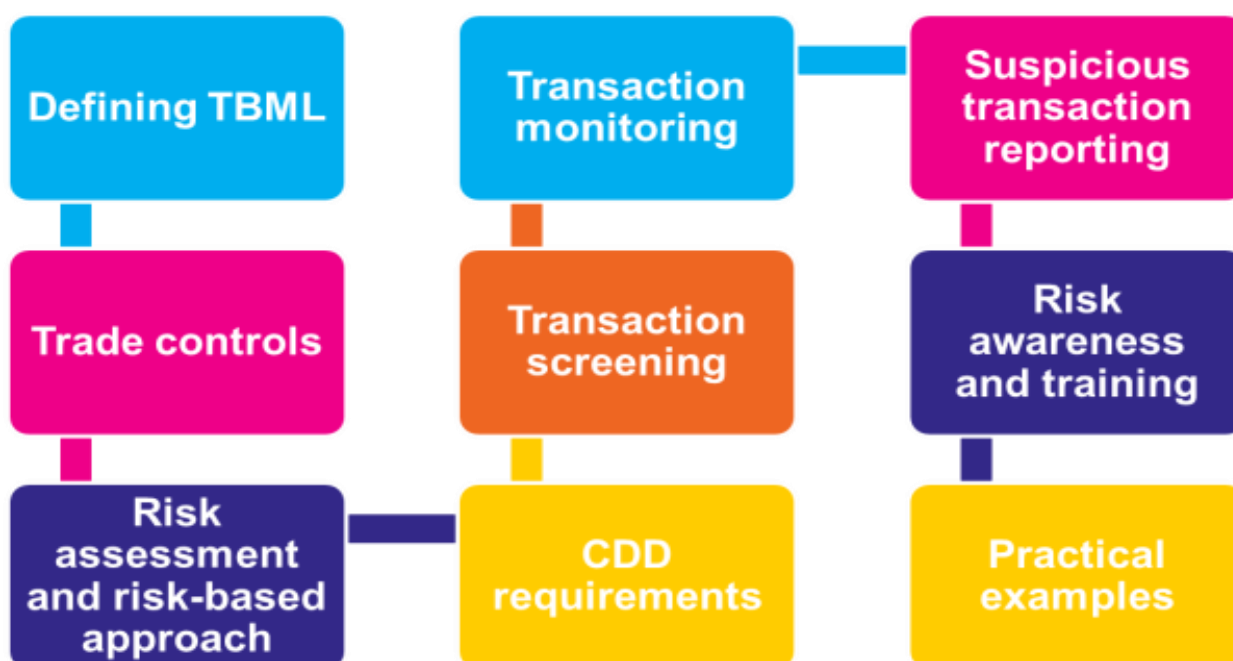
Trade is the weakest link in the fight against dirty money.

### Trade Based Money Laundering -Conceptual Framework

- 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.
- The crime involves a number of schemes in order to complicate the documentation of legitimate trade transactions.
- Trade includes Domestic as well as International Trade.
- “The use of trade to move value with the intent of obscuring the true origins of funds”.

### TBML – a lucid product to launder money

#### Trade Based Money Laundering Summary



### 15.3. THREE METHODS OF TBML

The methods of TBML are evolving day by day, country to country, business to business. But, the most common TBML methods are:

- Falsify the price of goods: Invoice Manipulation
- Falsify the quantity of goods shipped: Over, short, and phantom shipment of goods
- Falsify the quality or type of goods or services: Falsely described goods and services

### 15.4. METHODS AND SCOPE OF TBML IN BANGLADESH

The three stages of TBML as observed are:

- Placement: Dirty money becomes goods.
- Layering: Trade goods move across borders.
- Integration: Resale of goods.

### 15.5. THE REGULATORY FRAMEWORK GOVERNING FOREIGN TRADE

Over the years Bangladesh government has taken some significant initiatives to prevent TBML. Such as the Money Laundering Prevention Act, 2012 has been enacted, separate national intelligence body has been formed and many more. Money Laundering Prevention Act, 2012: As per section 2 (v) (ii) of Money Laundering Prevention Act, 2012 smuggling of money or property is money laundering while section 2 (a) of the Act defines “smuggling of money or property” as-

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

The law of the land, therefore, prohibits smuggling of money or property in the strictest term and provides stringent punishment for the offence.

A number of Acts, regulations and instructions from competent authorities form the regulatory framework of trade services in Bangladesh. The Foreign Exchange Regulation Act, 1947 lays the foundation of regulatory framework by which the Bangladesh trade is mostly governed. The Import and Export Control Act, 1950 controls the import and export of goods to and from Bangladesh, while the Customs Act, 1969 defines the operational customs procedures of import and export in Bangladesh. The Bangladesh Bank Order, 1972 empowers Bangladesh Bank (BB) as the Central Bank of the country to formulate and implement intervention policies in the foreign exchange market and to hold and manage the official foreign reserves of Bangladesh. The Importers, Exporters and Indentors (Registration) Order, 1981 empowers the Chief Controller of Import and Export (CCI&E) to issue license as Import Registration Certificate (IRC),

Export Registration Certificate (ERC), Import Permit (IP) and Export Permit (EP) to importer and exporter of Bangladesh to perform trade. The Government of Bangladesh formulates import and export policy for the country namely the Import Policy Order (IPO) and the Export Policy for a three-year period. BEPZA, BEZA, EZ and PEZ regulations regulate the import and export of Special Economic Zones. Various Ministries, Departments and Divisions of Govt. import against permission of these authorities. Apart from these, BB issues instructions under FERA in the form of FE circulars and FE circular letters from time to time to regulate foreign exchange market of the country. Guidelines for Foreign Exchange Transactions (GFET) summarizes all the instructions issued for authorized dealers (ADs) and money changers. These local regulations primarily construct the regulatory framework of Bangladesh.

Since trade involves extra-territorial parties, some international rules, regulations and practices are also part of the broader regulatory framework. Notable of them are regulations designed by the General Agreement on Tariffs and Trade (GATT), Uniform Customs and Practice for Documentary Credits (UCPDC-600), Uniform Rules for Bank-to-Bank Reimbursements under Documentary Credits (URR- 725), Uniform Rules for Collections (URC-522), International Standard Banking Practices (ISBP-745), International Standby Practices (ISP-98), Uniform Rules for Demand Guarantees (URDG-758), and Inco terms 2020. It is to be noted that the local regulations generally prevail over the international ones. The Guidelines for Foreign Exchange Transactions (GFET) and Import Policy Order have made specific mandatory requirement for ensuring pricing competitiveness prior to any international trade transactions:

**Import Policy Order 2015-2018: Chapter 2 “General Provisions for Import”, Section 5(4) “Import at competitive rate”:**

- a) Import shall be made at the most competitive rate and it is obligatory for the importers, at any time, to submit documents to Import Control Authority regarding the price paid or to be paid by them;
- b) or indentors representing at least two source countries: Provided that this condition shall not apply for opening LC up to Tk. one lac; and
- c) for import at the most competitive rate by the public sector importers, quotations have to be invited before opening letter of credit, and goods shall be imported at the most competitive price.

**Guidelines for Foreign Exchange Transactions (GFET), 2018: volume-1 Chapter 7, Para 20: “Verification of import price etc.”**

“Before opening of LC or issuing LCAF, the AD shall have to take usual and reasonable cautionary measures to ensure that both the exporter and importer are bona fide business person of the goods concerned, the exporting country is the usual exporter of the goods concerned and the price of the goods concerned is competitive in terms of prevailing price in the international market on the date of contract and/or similar imports in contemporary period. ADs are advised to verify the above, if needed, with the help of concerned Bangladesh Mission abroad.

**“Chapter 8, Para 7 “Certification of EXP forms by ADs”:**

In order to avoid any loss of foreign exchange to the country, ADs shall not certify any EXP form unless they have satisfied themselves with regard to the followings:

(iv) Bona fides of the buyers/consignees abroad and their credentials etc. where necessary, ADs should make discreet enquiries in this regard through their correspondent abroad etc., greater care should be taken particularly in cases of shipments against contract alone and shipments on CAD/DA basis. Where ADs doubt the bona fides and standing of the buyers/consignees abroad or where owing to common interest or otherwise they suspect collusion with the intent of delaying or avoiding repatriation of export proceeds ADs should report such cases promptly to Bangladesh Bank. Similarly, ADs should report to Bangladesh Bank cases where it comes to their knowledge that the exporters are directly or indirectly connected with or have any financial or other interest in the buyer/consignee abroad. Where felt necessary, discreet enquiry about the bona fides and credentials of the charter party should also be made in case the shipment is to be against a charter party Bill of Lading so as to avoid loss of cargo/foreign exchange.

These are only few examples of regulatory instructions. In fact, there are many other regulatory instructions relevant to combating TBML.

**Import Procedure and Some Avenues for TBML**

- a) Import procedure in Bangladesh generally begins by obtaining an Importer Registration Certificate (IRC) from the Office of the Chief Controller of Import and Export (CCIE) under the Importers, Exporters and Indentors (registration) Order, 1981. According to this Order, an importer can get one IRC for commercial and one for industrial import. Importers may take the opportunity to have more than one IRC to use one in TBML as throughout the import procedure and reporting of the transactions importers are identified through IRCs not through their names. Moreover, family members of a trader having same business address may obtain IRCs and abuse them to commit TBML.
- b) Letter of Credit Authorization Form (LCAF) is mandatory for importer as it is the declaration of amount, value, HS code and the description of the goods as per Customs First Schedule and terms of import. After declaration of LCAF, importers are allowed to open/issue LC/Contract by the ADs. On the basis of the LC/Contract declaring on IMP by the importers ADs can sale/make payment of LC/Contract documents. Though importers are strictly prohibited from making payment in excess of LCAF value, sometimes abusing FC/ERQ accounts or other means, they pay more than the value of the LCAF or of expire value and thus facilitate TBML.
- c) Major portion of imported goods are imported on CFR basis in Bangladesh where freight charges are invoiced to the importer. In some cases it has been found that freight charges reached several times of the FOB value. In fact, freight and other charges can also be a medium of TBML.
- d) Value of goods to be imported can be medium of TBML as value can be quoted less than the actual price (Under invoicing) of the goods with a deliberate intention to evade import duties and taxes. Generally most of the amount of under invoiced import is paid through hundi or hawala. Evasion of taxes and duties i.e. custom related offenses is the predicate offence of ML in Bangladesh according to MLPA, 2012. On the other hand, capital machinery and raw materials (of which import duties are lower) can be imported quoting more than the actual price (Over invoicing) of goods as a medium of TBML.
- e) Banks are responsible to make payment against the import documents if found in order and no discrepancy arises. Yet, documents can be received directly by the importer and the goods can be released from the customs. In that case, banks may make payment based on the customs certified bill of entry (BE) submitted by the importer. This practice takes place while releasing goods with copy documents. TBML can occur in these situations as there are opportunities to fabricate the import documents and related BE by the mala fide importer.
- f) Banks are permitted to make advance payment against import without prior approval of BB based on a repayment guarantee from a bank abroad. This guarantee is not needed for remittance up to USD 5,000 (and USD 25,000 from ERQ accounts). Moreover, fabricated/fake/false bank guarantee can create a scope of TBML through payment of advance remittance against import.

- g) After making payment against the goods to be imported, importers are liable either to import the goods or to bring back the amount remitted in proper banking channel (Article 4(3), FERA, 1947). BB marks out the duration of the process 4 months after the date of making payment. Failure to transport the goods within the prescribed duration makes the related Bill of Entry (BE) overdue and no importer can get any import facility (opening LC/making advance payment, or enhancement of existing LC/Contract value) from any bank in Bangladesh having overdue BE against any of its previous import without the prior approval of BB. Importers may take the opportunity to surrender the IRC (intended to avoid the import liability and also to be involved in TBML) against which BE is being overdue and get another IRC for a fresh start.
- h) The incidence of loss or damage of the goods-in-transit or before release as well as cancellation of shipment may be used as a medium of TBML. Compensation against the damaged goods or return of the remittance against cancelled shipment can be received from sources/third parties directly not related to the exporter of the goods.
- i) The ADs are allowed to open back-to-back (BTB) import LCs against export LCs operating under the bonded warehouse system, subject to observance of domestic value addition requirement. Misuse of the bonded warehouse facility (intended to evade tax) by selling the imported goods to the local market can also be an example of TBML in import. Again, BTB LCs opened against arranged/fake master LCs can also be used in TBML where no export occurs showing some 'valid' reasons though raw materials imported duly against the BTB LCs.
- j) ADs are allowed to open deferred (Under Chapter 7, Para 33(a) of GFET, 2018), or usance basis L/C. As there are instances and vulnerabilities of abuse of suppliers' and buyer's credit, utmost care should be given to those payments where payments are settled through buyers' credit or suppliers' credit.
- k) Exporters are allowed to export on CMT (Cutting, Making and Trimming) basis as well as to import the raw materials on Free of Cost (FOC) basis. Since this FOC import does not require any bank endorsement and there is no matching of bill of entry with the value, customers can manipulate the FOC items.
- l) Import of non-physical goods (software and others) can be a medium of TBML as keeping track of import process of such non-physical goods is difficult for any reporting/regulatory agency.
- m) Import Policy Order allows actual users to import up to a certain limit (USD 7,000.00 per year) for their personal consumption. As AD banks have no control to monitor this limit through any system individuals might import through different ADs exceeding the limit and sell them commercially to the market illegally.

Consumers can purchase goods online by making payment through international credit or debit cards or unused portion of Travel Quota and later receive goods through courier. Criminal proceeds might be transferred through this online payment.

### Export Procedure and some avenues for TBML

- Export procedure in Bangladesh generally starts with obtaining Exporter Registration Certificate (ERC) from the CCI&E under the Importers, Exporters and Indentors (registration) Order, 1981. According to the order, an exporter can get only one ERC for export. Exporters may take the opportunity to have more than one ERC to use one in TBML, as throughout the export procedure and reporting of the transactions, exporters are identified through ERCs not through their names.
- Value of goods to be exported can be a medium of TBML as value can be quoted less than the actual price (under invoicing) of the goods intended to siphon money abroad.
- After shipment of the goods for export, exporters are liable to repatriate export proceeds in full (Section 12 of FERA, 1947). BB marks out the duration of the repatriation of export proceeds within 4 months after the date of shipment. Failure to receive the full export proceeds within the prescribed duration makes the related Export Bill overdue. Exporter can be out of track having huge amount of overdue export bills intended to commit money laundering through export.
- Commission, brokerage fee or other trade charges to be paid to foreign importers/agents (of which up to 5% ADs can allow) may also sometimes be abused for TBML.
- Payments in Foreign Exchange may be made through international cards (debit/ credit/ prepaid etc.) which are categorically mentioned in Chapter 19 of GFET, 2018. ADs should meticulously monitor the issuance and end-use of those cards.
- Partial drawing of export bill/Advance Receipt against export can be abused for TBML. It is the responsibility of the ADs to follow up each such case and to ensure that the balance amount is also realized within the prescribed period.
- Shutting out of a shipment by a particular vessel and re-shipment in another vessel should be checked. This is because there are opportunities of TBML as transshipment through one or more jurisdictions for no apparent economic reason is suspicious.
- The incidence of loss or damage of the exported goods in-transit or before release as well as cancellation of shipment (for which payment has not already been received) may be used as a medium of TBML. Compensation against then damaged goods can be received from other sources/third parties directly not related to the importer of the goods.
- Export of non-physical goods (software and others) can be a medium of TBML as keeping track of the export process of the non-physical goods is difficult for any reporting/regulatory agency.
- Buying House Arrangement/Buyer Nominated Supplier Arrangement can be a medium of TBML. Shipment of goods can illicitly be delayed by the buying houses through 'arranged game' for getting discount on the exported value. Again, buyer nominated supplier can quote higher price for the raw materials and thus money laundering can take place.
- Transaction in large volume through other than banking channel such as exchange house etc. is vulnerable to TBML. In the name of export proceeds wage earners' remittance may be brought into Bangladesh to claim cash incentives.
- Inward remittance may be brought from the countries where Bangladeshis have direct/indirect business and cash incentive may be claimed.
- The facility that ADs are allowed to discount the usance bill (para 25, chapter 8). Care shall be taken while discounting or purchasing foreign documentary export bills.

**Remittance of Royalty, Technical Assistance Fees etc.**

Under Section 18 of Bangladesh Investment Development Authority Act, 2016, approved industrial enterprises shall have to take approval from Bangladesh Investment Development Authority (BIDA) and other competent authorities for payment of royalty, technical know-how, operational service fees, management fees and technical assistance and franchise fees.

**15.6. TRADE BASED MONEY LAUNDERING -EXAMPLES CONT'D**

<b>Import / Export</b>	<b>Method</b>	<b>Qualifications</b>	<b>Shifting of Value</b>
Import	Over Invoicing	Expensive Imports	In Money Abroad
	Under Invoicing	Lucrative Imports	In Goods to the Homeland
Export	Over Invoicing	Lucrative Exports	In Goods to the Homeland
	Under Invoicing	Cheap Exports	In Goods Abroad

**15.7. SOME CONVENTIONAL AVENUES FOR TBML THROUGH OBUS, EPZS, EZS AND PEZS**

Trade finance through OBUs and different mode of international trade practiced in the EPZs, EZs, PEZs may be abused for TBML. Since OBUs can borrow funds from banks and FIs from both home and abroad they are more vulnerable to TBML.

In case of companies in Special Economic Zones, directors' liabilities are limited by shares. When the company falls into trouble due to taking more exposure through more foreign/local loan or trade gap, they may transfer, sell or even wind up the company keeping the outstanding liabilities in Bangladesh. The situation arises sometimes that the company makes payment for import without entry of the goods, or export is done but the proceeds are not realized. Keeping these liabilities pending owners/directors transfer, sell or wind up the company and leave the country. The Bank shall provide proper information to regulators in time before winding up of these companies. The Bank shall apply enhanced due diligence while providing trade and other services to these companies of Economic Zones. In Bangladesh context the letter of credit is assumed safe compared to other mode of trade (such as Open Account, Cash in Advance etc.) in TBML perspective. However, it is also undeniable that TBML risk may arise under LC if the LC is between parent and affiliates or if the trade is just an arranged game. Hence, TBML risk mitigation measures shall be stringent, otherwise trade should be facilitated by banks through LC applying adequate due diligence only.

## **15.8. KEY CHALLENGES AND DIFFICULTIES IN PREVENTING TRADE BASED MONEY LAUNDERING**

The globalization opens up various particular risks for TBML that would be difficult to detect. Moreover, it is reasonable to assume that as TBML schemes become more sophisticated, the use of services for money laundering will become more common. To monitor billions of transactions, encompassing millions of containers, in a cost-effective and efficient way is the great, gross challenge of TBML/TF enforcement. Although there would likely be some benefits in extending the AML/CTF regime to trade, the costs and logistics of implementation raise major concerns, particularly as TBML remains an under-researched area with a lack of data. However, some major challenges in preventing TBML in Bangladesh context as faced by banks and bankers are discussed below-

### **a) Price Verification for Financial Crime Control**

According to Import Policy Order, importers are obligated to import goods at competitive prices. Banks are advised in the GFET, 2018 to take usual and reasonable cautionary measures to ensure that the price of the goods concerned is competitive in terms of prevailing price in the international market on the date of contract and/or similar imports in contemporary period. They are also advised to verify the above, if needed, with the help of concerned Bangladesh Mission abroad. Due to lack of relevant business information, such as the terms of business relationship, volume discounting or specific quality, or feature, specifications of goods involved bankers have to be cautious in making meaningful determinations about the appropriateness of the unit price. Moreover, many products are not traded in public markets and their market prices are also not publicly available. Even where goods are publicly traded, the current prices may not reflect the agreed price used in any contract of sale or purchase and these details will not usually be available to the banks involved due to competitive sensitivity of such information.

### **b) Transfer Pricing**

Transfer pricing is a related party transaction commonly used by transnational corporation as part of their financial and tax planning strategy. Multinational organizations use transfer pricing to shift taxable income from jurisdictions with relatively high tax rates to jurisdictions with relatively low tax rates to minimize income tax. Similar strategies are also employed in relation to import duties and value added tax. TBML can occur when international trade is abused for transfer pricing. This poses a significant challenge which needs to be overcome.

### **c) Limited Skilled Manpower**

Performing the foreign exchange activities involves proper communication with the client, various banks of the country as well as abroad. A single error may cost thousands of dollars. In Bangladesh there are limited skilled manpower who are able to understand and handle the foreign exchange dealings very well. As such, skill development through proper training is a must to address TBML risk.

### **d) Extreme Competition**

Unhealthy competition is driving bankers to constantly hunt for aggressive business and profit target. Thus working under pressure of such target combined with the fear of losing customers and presence of other competitor banks officials sometimes ignore minor trade related due diligence which makes the bank as victim to TBML. Unhealthy competition poses a challenge to combating TBML.

### **e) Absence of Co-ordination**

Absence of coordination is also one of the major challenges in combating TBML. A coordinated Risk Management Unit/Division in combination of all concerned agencies may be framed to ensure co-ordination & concerted efforts. Besides, National Board of Revenue (specially the Valuations and Audit unit)/, Customs and Bangladesh Banks may also work to assess the value of the imported or exported goods/ commodities/ services. Arrangements may be in place so that customs authority and banks may be aware through mutual information sharing mechanism when there is abnormal increase in the number and value of LC of a particular company/firm etc., risky import of goods such as Reconditioned Capital Machinery, Software, Chemicals where complexity exists in determining price and description of the products, cases where importer and exporter are related, when import and export goods are inconsistent with the nature of trade of the customer, inconsistency in price exists, when an LC is frequently amended, where beneficiary desires payment in third country or party, when Bill of Lading does not mention container number, does not bear invoice number, where miscellaneous charges such as freight, lading charge etc are abnormal etc.

### **f) Absence of Management Information Systems (MIS) and a Central Data Base**

Lack of MIS and a central data base or uniform price list of various commodities is also a hindrance to preventing under invoicing and over-invoicing by those engaged in trade operations.

### **g) Duty/Tax structure**

At times, bankers sometimes disagree with the quoted price in the Proforma Invoice (PI), because they fail to match the given price which is sometimes far away from the actual price of the commodity in the international market. In some items of imports importers may quote higher price in line with customs' rate of duty even though the price may be less than the price mentioned in NBR's minimum price list. Though there is no scope of tax/VAT evasion against such imports, it may be abused for TBML.

## **15.9. CHALLENGES AHEAD**

The most significant challenge is that TBML, like other types of money laundering, will continue to develop and new typologies will undoubtedly emerge. In a statement as apt today as when it was made, FATF observed that:

“There are likely to be illicit financing methods being used that have not been detected by financial institutions or law enforcement, and so will not show up in the data gathered from criminal investigations or financial institution currency or transaction reporting. And there may be other illicit financing options that even the criminals have not yet discovered. In the absence of data or case studies identifying these methods, financial institutions and competent authorities must rely on creative intuition and a careful analysis of potential systemic weaknesses.”

This statement highlights several important points which are borne out by this research. First, the evolving, and often ingenious, nature of money laundering highlights the need to anticipate new developments and trends. Second, it emphasizes the importance of information and analysis in informing and shaping an effective AML/CTF strategy.

These points indicate that to be most effective, ongoing monitoring and assessment of TBML will be necessary to address potential new developments, such as the move from money laundering using international merchandise trade to services and from international trade to domestic trade. New trading forums such as virtual trading will also need to be considered. The trading in online gaming and social network environments, such as virtual currency (bit coin etc.) can be used for money laundering purposes. At present there is little known about these areas but they may be likely areas for the next evolution of TBML.

### **Trade Based Money Laundering-Challenges-**

- TBML involves transferring of goods as a substitute to money and occurs outside the Bank.
- Banks must leverage all the information available to them to determine whether their customers' transactions are consistent with their businesses.
- Trade finance brings its own unique challenges and whether the documents are reviewed manually, or the information regarding the trade is input into a system and alerts are thrown out properly. There is a difficulty in detecting complex relationships between trading operations, operators, and money movements. Three key barriers make it tough to detect trade based money laundering:
  - The tremendous **volume** of trade makes it easy to hide individual transactions;
  - The **complexity** that is often involved in multiple foreign exchange transactions; and
  - The limited **resources** available to agencies wanting to detect the fraud.

### **15.10. TRADE OPERATIONAL STRUCTURE OF BKB**

The trade operation of BKB is conducted centrally. There are one central establishments to operate the trade . BKB has no offshore banking. Trade transactions of 16 AD Branches along with related non-AD Branches are processed at ID Dhaka. The KYC and CDD of the trade customers are done at the Branch level.

#### **15.10.1. Products & Services offered by Bangladesh Krishi Bank related to Foreign Trade**

Bangladesh Krishi Bank deals with various products and services related with to Foreign Trade. Though exhaustive list of trade related products and services are not practicable, some indicative examples of products or services that fall within the scope of the Guidelines are:

- a) All types of Commercial Letters of Credits
- b) All types of Bank Guarantees
- c) All types of Standby LCs
- d) All types of Bills for Collections
- e) Open Account Transactions
- f) Cash in Advance
- g) All kinds of trade finance and payments
- h) Import and export of services and software

Trade finance products (such as factoring, forfeiting, etc.) which do not exist or are not allowed in Bangladesh have not been covered in these guidelines. Before such products are allowed by the Bank, ML & TF risks of these products shall be assessed and consulted with BFIU.

### 15.10.2. Scope/Definition of Customer

Any person or entity maintaining an account or a business relationship of any type, the beneficial owner of the account or business relationship, the person or entity involved in a financial transaction that may pose reputational or other risk to the Bank is a customer. In any single transaction through the banking channel, there must be at least two parties involved. Depending on the nature of transaction, there may be engagement of three or more parties in a single transaction.

### 15.10.3. Parties Involved and Their Role in Trade

Many parties actively participate in international trade in various points and they differ from one country to another based on the local regulatory requirements involved in the process. Even the parties involved in import are slightly different from those in export.

### 15.10.4. Major Parties and their Role in Import

The importer is the primary player in the import market and other participants have their respective roles. Roles are as under:

- a) Buyer and seller furnishes sale/purchase contract.
- b) Exporter supplies the goods/services as per the terms agreed in the LC/Contract.
- c) Shipping Lines/Airlines/Transport Agency transports the goods from exporter's end to the importer's end.
- d) Port Authority is the custodian of the goods till those are released properly.
- e) Customs Authority is responsible to assess collect duties-taxes, issue release order for the imported goods and combat trade based money laundering.
- f) Clearing Agent acts as the agent of importer to release the goods from the customs.
- g) Indentor is the agent of exporter.

### 15.10.5. The process flow in a documentary credit

Among the trade payment methods mostly followed in Bangladesh are documentary credit and documentary collection. In a documentary credit process, the issuing banks have primary obligations in the transaction. The process flow is as under:

- a) The Buyer (importer) and the seller (exporter) furnish sale/purchase contract.
- b) The applicant (Buyer) requests the issuing bank to open documentary credit on account of the buyer.
- c) The Issuing Bank issues the credit in favor of the beneficiary and transmits through the advising bank (usually).
- d) The advising bank advises the credit to the beneficiary (Seller).
- e) The beneficiary ships the goods, prepares, collects & collates the required documents under the credit and presents to the nominated bank (usually).
- f) The nominated bank forwards documents to the issuing bank/confirming bank. Nominated bank can honor/negotiate documents i.e. make payments and claim reimbursement if documents are in order as per LC terms.
- g) Issuing bank on receipt of complying presentation and /or obtaining documents effects payment to the beneficiary and/or nominated bank, as the case may be.
- h) The applicant releases documents from the issuing bank.
- i) The applicant clears the goods from the customs through his appointed clearing agent.

### 15.10.6. Major Parties and their Role in Export

Though the process of export is literally the reverse to the import, some participants change their roles in the process. However, the exporter is obviously the primary player in the market and the other players in the process support export surrounding the primary player. The roles of the parties are as follows:

- a) Buyer and seller furnishes sale/purchase contract.
- b) LC issuing Bank issues the LC.
- c) LC Advising Bank advises the LC to the exporter/supplier.
- d) Exporter ships the goods to the importer/buyer or named destination.
- e) Forwarding Agent acts as the agent of exporter to arrange shipment of the goods.
- f) Shipping Lines/Airlines/Transport Agency transports the goods from supplier's end to the buyer's end.
- g) Exporter prepares, collects and submits docs to the nominated bank.
- h) Port Authority is the custodian of the goods.
- i) Customs Authority is responsible to assess, collect duties-taxes and allow goods to export from exporting country and permits goods to release.
- j) LC Nominated Bank honors/negotiates/prepays/purchases/discounts the documents.
- k) LC issuing bank makes payment to the nominated/negotiating bank/exporter as per the terms agreed in the LC.

### 15.10.7. The process flow in a documentary collection

Under documentary collection, Banks involve in the transaction without incurring its own payment undertaking & the process flow (from exporter perspective) is as under:

- a) The Buyer (importer) and the seller (exporter) furnishes sale/purchase contract
- b) The exporter ships the goods & submits documents to the remitting bank
- c) The remitting bank sends documents to the collecting bank
- d) The collecting bank sends documents to the presenting bank [most of the time collecting and presenting bank are same]
- e) The presenting bank releases documents to the drawee (the importer) as per collection instructions, and
- f) The drawee clears the goods from the customs through his appointed clearing agent

### Instructing Parties

In a trade finance transaction, banks are not always involved into transactions at the request or instruction from its own customer. In addition to bank's own customer, the instructing party may be, for example, but not limited to.

For	Instructing party	Instructing party Commercial Bank's role as instructed party
Documentary Credit	Issuing Bank	Advising Bank, Nominated Bank, Confirming Bank, Transferring Bank
	Advising Bank	2nd Advising Bank
Documentary Collection	Remitting Bank	Collecting and/or presenting bank (if collecting bank and presenting bank are the same)
	Collecting Bank	Presenting Bank (if collecting bank and presenting bank are not the same)
Cash In advance	Ordering/ Customer/ institution	Inward remittance receiving bank
Guarantee backed by counter guarantee including standby LC	Counter guarantor/ Issuer/ Guarantor	Guarantor, Advisor, Confirmer, Nominated person etc.

### Counter Parties

There must be at least one counter party in a trade finance transaction. Counter party may be for instances but not limited to as under:

For	Counter Parties
Documentary Credit	Issuing Bank, Nominated Bank, Confirming Bank, Advising Bank, 2nd Advising Bank, Beneficiary, and Applicant etc.
Documentary Collection	Principal, Remitting bank, Collecting bank, Presenting bank, Drawee etc.
Cash in Advance	Ordering Institution, Customer, Exporter etc.
Guarantee/Stand by LC	Issuer, Counter guarantor, confirmer, guarantor etc. Counter parties in trade finance transaction can be broadly categorizes in two forms: <ul style="list-style-type: none"> <li>• Banks or financial institutions</li> <li>• Any party other than banks or financial institutions</li> </ul>

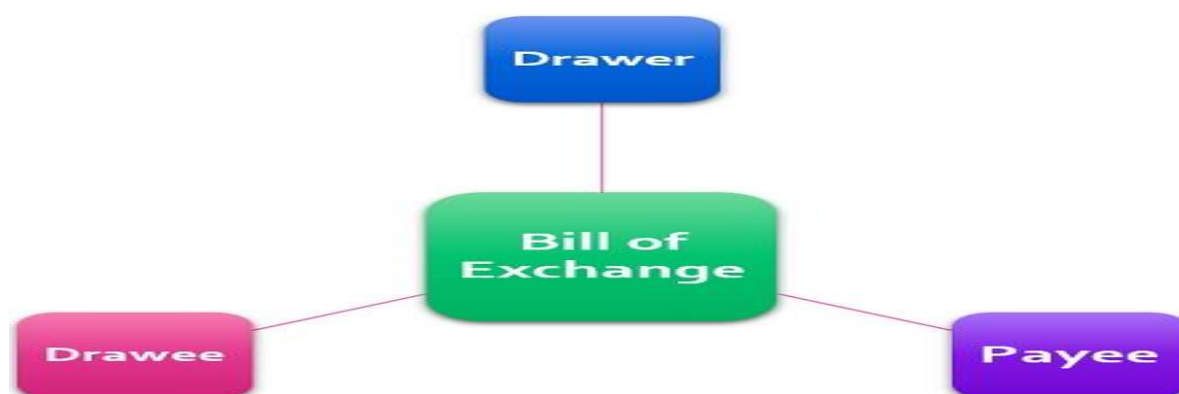
Depending on the risk and vulnerabilities of the instructing and counter parties mentioned above, the Bank shall frame the detailed due diligence measures in line with this guidelines, relevant BFIU circulars, local regulations and international best practices.

### Related Parties to Trade

In order to execute a trade transaction, there are inherently more parties involved other than buyer and seller. For the purpose of this guideline, those parties are called “related parties to trade”. “Related parties to trade” include traders, brokers, shipper/consignor, notify parties, shipping lines, freight forwarders etc.

### Trade of Services

Lion share of trade is backed by underlying goods, however, trade of service items such as software, data entry; repair/renovation/refilled/overhauling, transporting, carrying, delivering etc. is also on the rise. Service import and export therefore should be dealt with adequate due diligence as scope and vulnerability of service items to TBML is increasing day by day. All the documents and invoices should be verified and checked whether the competitive price of the service has been quoted or not. In software and service trade, certificate issued by BASIS and documents evidencing customs assessment and payment of duties and taxes will not be enough. Genuineness and reliability of the importer and supplier should be ensured so that transactions arising out of such arrangement may not pose ML, TF and PF threats. The Bank will guide trade processing staff on how to ensure them.



### 15.11. NATIONAL LAW

Initially, Bangladesh enacted laws to prevent money laundering in 2002, and to combat financing of terrorism in 2009. Subsequently, these laws were amended to be in line with the international standards and lastly, Money Laundering Prevention Act, 2012 was passed with effect from January 16, 2012 and The Anti-Terrorism Act (ATA), 2009 was amended in 2013. Lastly the government has enacted The Money Laundering Prevention Rules-2019. BFIU, to combat TBML/TF formulated the Guidelines on TBML making some recommendations to guide effective control measures; without modifying any applicable laws, regulations and requirements applicable to all banks operating in Bangladesh. The following Laws, Rules, Regulations and Guidelines are related with to the BKB Policy Guidelines on TBML:

- a) Money Laundering Prevention Act, 2012;
- b) Money Laundering Prevention Rules, 2019;
- c) Anti-Terrorism Act, 2009;
- d) Anti-Terrorism Rules, 2013;
- e) Foreign Exchange Regulations Act, 1947;
- f) Customs Act, 1969;
- g) The Import and Export Control Act, 1950;
- h) Importers, Exporters and Indentors (Registration) Order, 1981;
- i) Value Added Tax Act, 1991;
- j) Import Policy Order and Export Policy in force;
- k) Rules, Govt. SROs, Circulars, Circular letters, Guidelines, instructions issued by relevant authorities /regulator.

Some other initiatives as taken by the government are below:

- a) Bangladesh Government has formed the National Coordination Committee headed by the Finance Minister along with other fourteen members.
- b) Bangladesh Government has formed the Working Committee with designated senior level government officials.

**As per Section 2 (v) of Money Laundering Prevention Act, 2012 of Bangladesh, Money Laundering is definition-**

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

- Knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:
- Concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
- Assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
- Smuggling money or property earned through legal or illegal means to a foreign country;
- 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
- Concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
- Converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
- Acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
- Performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
- Participating in, associating with, conspiring, attempting, abetting, instigating or counseling to commit any offences mentioned above.

**15.11.1. Responsibilities of the Reporting Organizations under the MLP Act, 2012**

The Act defines the responsibilities of reporting organizations for the purpose of prevention of money laundering in Sub-Section 25(1) as follows:

- **KYC Requirement:** To retain correct and full information used to identify their customers [Clause 25(1)(Ka)];
- **Record Keeping:** To retain transaction records at least for 5 (Five) years after termination of relationships with the customers [Clause 25(1)(Kha)];
- **Providing Information on Demand:** To provide customer identification and transaction records to Bangladesh Bank on demand from time to time [Clause 25(1)(Ga)]; and
- **STR Reporting:** To send a Suspicious Transaction Report (STR) to the Bangladesh Bank where they observe any suspicious transaction or attempt for such transaction [Clause 25(1)(Gha)].

### **15.11.2. According to Section 16 of Anti-Terrorism (Amendment) Act, 2009, Bank's responsibilities to combat financing of terrorism are:**

- Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to the Bangladesh Bank without any delay.
- The Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under Section 15, which are applicable to the reporting agency, have been complied with or not.

### **15.11.3. Penalties for Non-Compliance with the Responsibilities of Reporting Organizations**

The MLP Act also provides penalties in Sub-Section 25(2) for non-compliance with the above responsibilities of the reporting organizations as follows:

#### **i. Cash Penalty:**

If any reporting organization fails to comply with its above-mentioned responsibilities defined under Sub-Section 25(1) of the Act, then Bangladesh Bank may impose cash penalty of minimum Tk. 50 (Fifty) thousand up to maximum Tk. 25 (Twenty Five) lacs upon that reporting organization [Clause 25(2)(Ka)];

#### **ii. Cancellation of Permission or License:**

In addition to the above-mentioned cash penalty, Bangladesh Bank may cancel permission or license of that reporting organization or any of its branch, service center, booth or agent's business, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Clause 25(2) (Kha)].

### **15.11.4. Penalties for Non-Compliance with the Directives of Bangladesh Bank**

The Act also provides penalties in Sub-Sections 23(3), 23(4), 23(5), 23(6), 23(7) and 23(8) for failure to provide information on demand, for providing erroneous/false information, or for failure to comply with Bangladesh Bank instructions as follows:

#### **i. Failure to Submit Information within Deadline:**

If any reporting organization fails to submit within deadline information sought by Bangladesh Bank under Sub-Section 23(1) of the Act, then Bangladesh Bank may impose cash penalty of Tk. 10 (Ten) thousand per day up to maximum Tk.5 (Five) lacs upon that reporting organization [Sub-Section 23(3)]; and if any reporting organization faces cash penalty for more than 3 (Three) times in a financial year, then Bangladesh Bank may withhold registration or license of that reporting organization or any of its branch, service center, booth or agent's business in Bangladesh, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Sub-Section 23(3)].

**ii. Submitting Erroneous or False Information or Statement:**

If any reporting organization submits erroneous or false information or statement on any subject sought by Bangladesh Bank under Sub-Section 23(1) of the Act, then Bangladesh Bank may impose cash penalty of minimum Tk. 20 (Twenty) thousand up to maximum Tk. 5 (Five) lacs upon that reporting organization [Sub-Section 23(4)]; and if any reporting organization faces cash penalty for more than 3 (Three) times in a financial year, then Bangladesh Bank may withhold registration or license of that reporting organization or any of its branch, service center, booth or agent's business in Bangladesh, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Sub-Section 23(4)].

**iii. Failure to Comply with any Instruction of Bangladesh Bank:**

If any reporting organization fails to comply with any instruction issued by Bangladesh Bank under the Act, then Bangladesh Bank may impose cash penalty of Tk. 10 (Ten) thousand per day up to maximum Tk. 5 (Five) lacs for each noncompliance issue upon that reporting organization [Sub-Section 23(5)]; and if any reporting organization faces cash penalty for more than 3 (Three) times in a financial year, then Bangladesh Bank may withhold registration or license of that reporting organization or any of its branch, service center, booth or agent's business in Bangladesh, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Sub-Section 23(5)].

**iv. Failure to Comply with Account Freezing or Suspension Order of Bangladesh Bank:**

If any reporting organization fails to comply with the freezing or suspension order on any account issued by Bangladesh Bank under Clause 23(1)(Ga) of the Act, then Bangladesh Bank may impose cash penalty equal to the balance of that account as a minimum, which will not be more than twice of the balance of that account on the order date [Sub-Section 23(6)].

**v. Realization of Penalty by Bangladesh Bank:**

If any person or entity or reporting organization fails to pay the amount of penalty imposed by Bangladesh Bank under Sections 23 and 25 of the Act, then Bangladesh Bank may realize the same by debiting the account maintained in the name of that person or entity or reporting organization with any bank or financial institution or with Bangladesh Bank. If any portion of the penalty amount still remains unpaid, then Bangladesh Bank may appear before the Court for realizing the same and the Court shall pass order as it deems appropriate [Sub-Section 23(7)].

**vi. Additional Penalty for Responsible Owner(s), Director(s), Employee(s) or Contractual(s):**

If any penalty is imposed upon any reporting organization under above-mentioned Sub-Sections 23(3), 23(4), 23(5) and 23(6) of the Act, then Bangladesh Bank may impose cash penalty of minimum Tk. 10 (Ten) thousand up to maximum Tk. 5 (Five) lacs upon the responsible Owner(s), Director(s), Employee(s) or Contractual Employee(s) of that reporting organization, and if necessary, may instruct the reporting organization for necessary disciplinary action against the responsible person [Sub-Section 23(8)].

## 15.12. INTERNATIONAL INITIATIVES

To combat TBML, different international and national bodies working to develop an effective mechanism such as -

- International standard setting body Financial Action Task Force (FATF) has started its work for combating TBML since 2006.
- After that The Asia Pacific region is also continuously working against TBML
- A number of supervisory authority in some countries like the Singapore, Hong Kong and Bangladesh have established Risk based control for Financial Institution for alleviating TBML risk.
- Several private bodies like The Wolfsberg Group, ICC and BAFT are active to develop sound standard for mitigating TBML risk.
- Over the last decade, there have been significant initiatives across the globe to combat TBML. The US Government and the European Union have both developed widespread AML/CTF programs and through transnational agencies, such as FATF, there has been a push to establish coordinated and interconnected AML/CTF strategies, with an emphasis upon compliance with FATF's 40+9 Recommendations (although the level of compliance by individual countries is varied). Although how successful the global AML/CTF response has been is not conclusive, its possible effectiveness in limiting certain avenues of TBML, primarily using financial systems to launder money and finance terrorist activities has been attributed to the apparent rise in TBML.

### 15.12.1. The Financial Action Task Force (FATF): In response to mounting

International concern about money laundering, the Financial Action Task Force (FATF) on money laundering was established in 1989. The FATF is an inter-governmental body that sets international standards and develops and promotes policies to combat money laundering and terrorist financing. FATF has recognized misuse of the trade system as one of the main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy.

### 15.12.2. FATF Guidelines on Trade Based Money Laundering -2006

The international trade system is clearly subject to a wide range of risk and vulnerabilities. As the anti-money laundering (AML) and counter-terrorist financing (CFT) standards that have been applied to other money laundering techniques have become increasingly effective, such abuse of the trade system is expected to become increasingly attractive. However, currently, many customs agencies, law enforcement agencies, financial intelligence units (FIU), tax authorities and banking supervisors (i.e. competent authorities) appear less capable of identifying and combating trade-based money laundering than they are in dealing with other forms of money laundering and terrorist financing.

### 15.12.3. FATF Best Practices Paper on Trade Based Money Laundering-2008

The Financial Action Task Force (FATF) has recognized misuse of the trade system as one of the main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. As the anti-money laundering (AML) and counter-terrorist financing (CFT) standards that have been applied to other money laundering techniques have become increasingly effective, such abuse of the trade system is expected to become increasingly attractive.

#### **15.12.4. FATF Document on Money Laundering Vulnerabilities in Free Trade Zone-2010**

FTZs are designated areas within jurisdictions in which incentives are offered to support the development of exports, foreign direct investment (FDI) and local employment. These incentives include exemptions from duty and taxes, simplified administrative procedures and the duty-free importation of raw materials, machinery, parts and equipment. In addition to boosting economic opportunity, these incentives can result in a reduction in finance and trade controls and enforcement, creating opportunities for money laundering and the financing of terrorism.

#### **15.12.5. Wolfsburg**

The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of FCRs, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies. The Wolfsberg Group consists of the following financial institutions: Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Ltd, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Société Générale, Standard Chartered and UBS. The Group recognizes the TBML in global trade has not only increased over the past few years, but that it has shifted away from relying solely on the preventative measures from banks and that this is leading to more cooperation between regulators, law enforcement and banks; either directly or via industry groups.

#### **15.12.6. APG Typology Report on Trade Based Money Laundering-2012**

The APG's TBML study aims to build on the existing studies, in particular those of the FATF, in order to study the extent of the prevalence of TBML and highlight current methods, techniques and modus operandi for TBML as well as to identify 'red flags' to detect and respond to TBML. In determining the magnitude of TBML, the study considered why so few cases of TBML have been detected since the FAT's 2006 study. The paper has sought to clarify and furnish explanations for terms and processes of 'trade finance' which are comprehensible to Money Laundering (ML) investigators. This paper has focused on TBML occurring in the course of international trade in goods. The study does not include in its scope capital flight, tax evasion, trade in services and domestic trade. The features of the dynamic environment that distinguish TBML from other forms of ML are its occurrence through intermingling of the trade sector with the trade finance sector in cross-border transactions. The foreign exchange market and the long supply chain make international trade particularly vulnerable to TBML. The study included circulation of questionnaire to APG and FATF members seeking statistically significant indicators. The paper sets out a number of case studies to illustrate trends of TBML. Simplified explanations of the terms and processes of trade finance have been attempted through interaction with the private sector. A brief review of the literature on the subject generated by the FATF, FSRBs and other authors has been made.

#### **15.12.7. Guidance Paper on Combating Trade-based Money Laundering-2016: The Hong Kong Association of Banks**

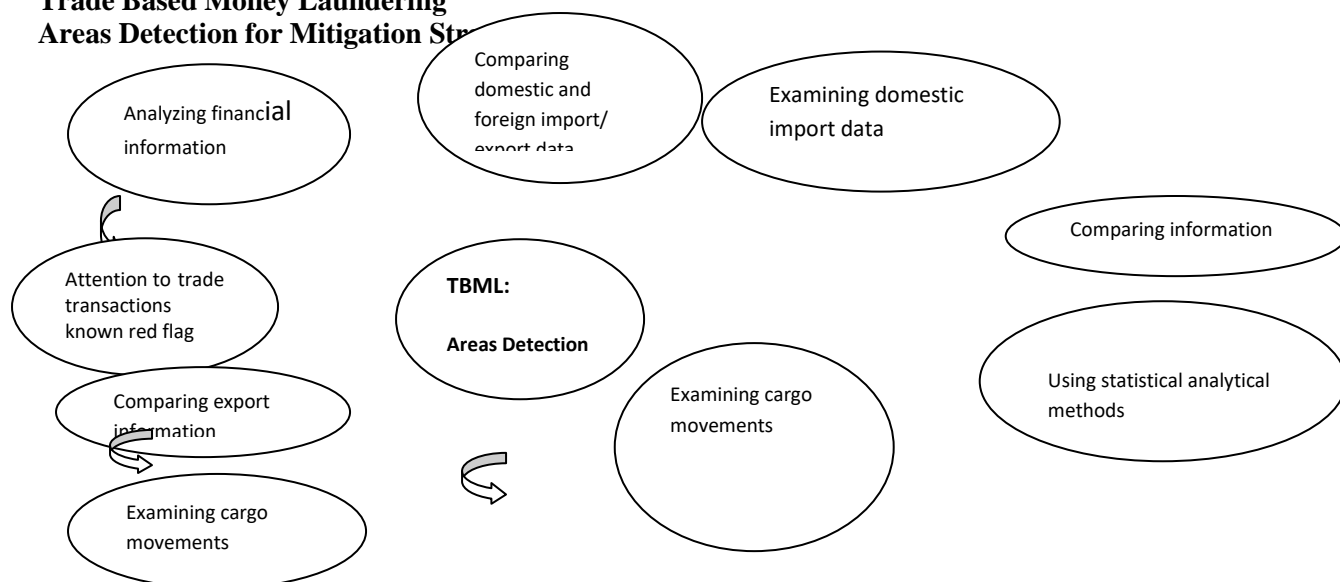
Guidance Paper on Combating Trade-based Money Laundering-2016 has been developed by The Hong Kong Association of Banks (HKAB) with input from Hong Kong Monetary Authority (HKMA). However, the HKMA considers that the adoption of these practices will assist authorized institutions (AIs) in not only meeting the legal and regulatory obligations under the Anti-Money and the AMLO Guideline, but also in implementing effective measures to further mitigate their money laundering and terrorist financing (ML/TF) risk. AIs should also take appropriate measures to ensure compliance with Hong Kong's sanctions regime, and obligations under Hong Kong law in respect of weapons of mass destruction (WMD) proliferation. In addition to meeting requirements under Hong Kong laws, these practices will also help AIs operating internationally to meet relevant overseas sanctions regimes that are applicable to them.

### 15.13. TBML RISK ASSESSMENT & MITIGATION MECHANISM

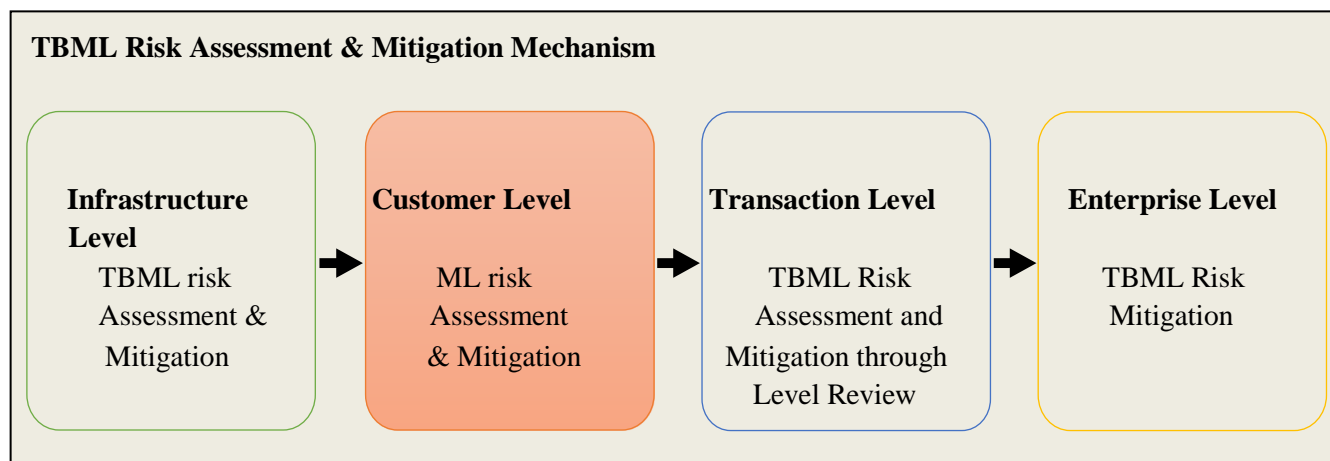
A Bank shall have to assess its TBML risks and develop trade control mechanism. The risk assessment should be documented, reviewed from time to time and updated accordingly.

A risk-based approach requires financial institutions to have systems and controls that are commensurate with the specific risks of money laundering and terrorist financing facing them. Assessing this risk is, therefore, one of the most important steps in creating a good AML/CFT compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk—whether low, medium or high—must be identified and mitigated by the application of controls, such as verification of customer identity, customer due diligence policies, suspicious activity monitoring and economic sanctions screening. Bank shall assess its TBML risks and develop trade control mechanism. The samples mechanism will be vetted by BFIU. The risk assessment shall be documented, reviewed from time to time and updated accordingly. The Bank will conduct a comprehensive risk assessment of the trade finance business, taking into account their customer base, geographical locations, products offered and emerging risks.

#### Trade Based Money Laundering Areas Detection for Mitigation Str



Trade based Money Laundering risk may arise and affect due to inadequate infrastructure of a bank, inaccurate assessment of the customer before on board, poor identification and handling of TBML alert while conducting trade transaction by the officials concerned and; overall for failure of a bank to address the risk at the enterprise or institute level. Hence, the bank has establish TBML risk assessment and mitigation at infrastructure level, customer level, transaction level and at enterprise level as shown in the flowchart below.



First comes the infrastructure risk assessment and mitigation as it is impossible to implement mitigation measures without adequate infrastructure.

Secondly, high risk customers with dubious trade transaction give birth to trade fraud. Hence knowing and assessing customer before on board for trade transaction shall be of great use to combating TBML.

Thirdly, TBML risk assessment and mitigation at the transaction level is the most important and vital to combating this offense as it is at this level that the TBML takes place. And finally a holistic approach by the entire institution can be effectively implemented through senior management engagement in TBML risk assessment and mitigation at enterprise level. Details are described below.

#### 15.14. INFRASTRUCTURE LEVEL RISK ASSESSMENT

The Bank has developed its own infrastructure for transaction monitoring and screening in line with their exposure to international trade and will maintain price verification. The Bank shall at a minimum establish the following to combat trade based money laundering:

- Automated Sanction screening process;
- Procedure of manual screening process;
- Own data base based on transactions;
- Subscribe for publically available online commodity pricing website;
- Vessel tracking system

**15.15. CUSTOMER LEVEL TBML RISK ASSESSMENT AND MITIGATION MECHANISM**

- a) **General ML/TF Risk Assessment and Mitigation:**

The customer level risk assessment starts with the establishment of customer relationship. While establishing business relationship/account opening with the trade customer, general ML/TF risk assessment and mitigation measures as outlined in relevant BFIU circular and ML & TF risk management Guidelines issued for banks by BFIU shall be followed.
- b) **Risk Assessment related to Trade:**

As in most cases there are some products and commodities, various delivery channels and jurisdictions through which TBML occurs it is quite convenient to have a risk based approach. Risk assessment should be done following the sample model given by the Bank (subject to vetting by BFIU) depending on their respective risk exposure and experience. Banks should design a standard format to collect the required information for this sample model. For fresh/new customers the assessment may be done on the projection submitted in the format by the customers and for the existing and old customers historical data may be chosen.
- c) **Independent Evaluation:**

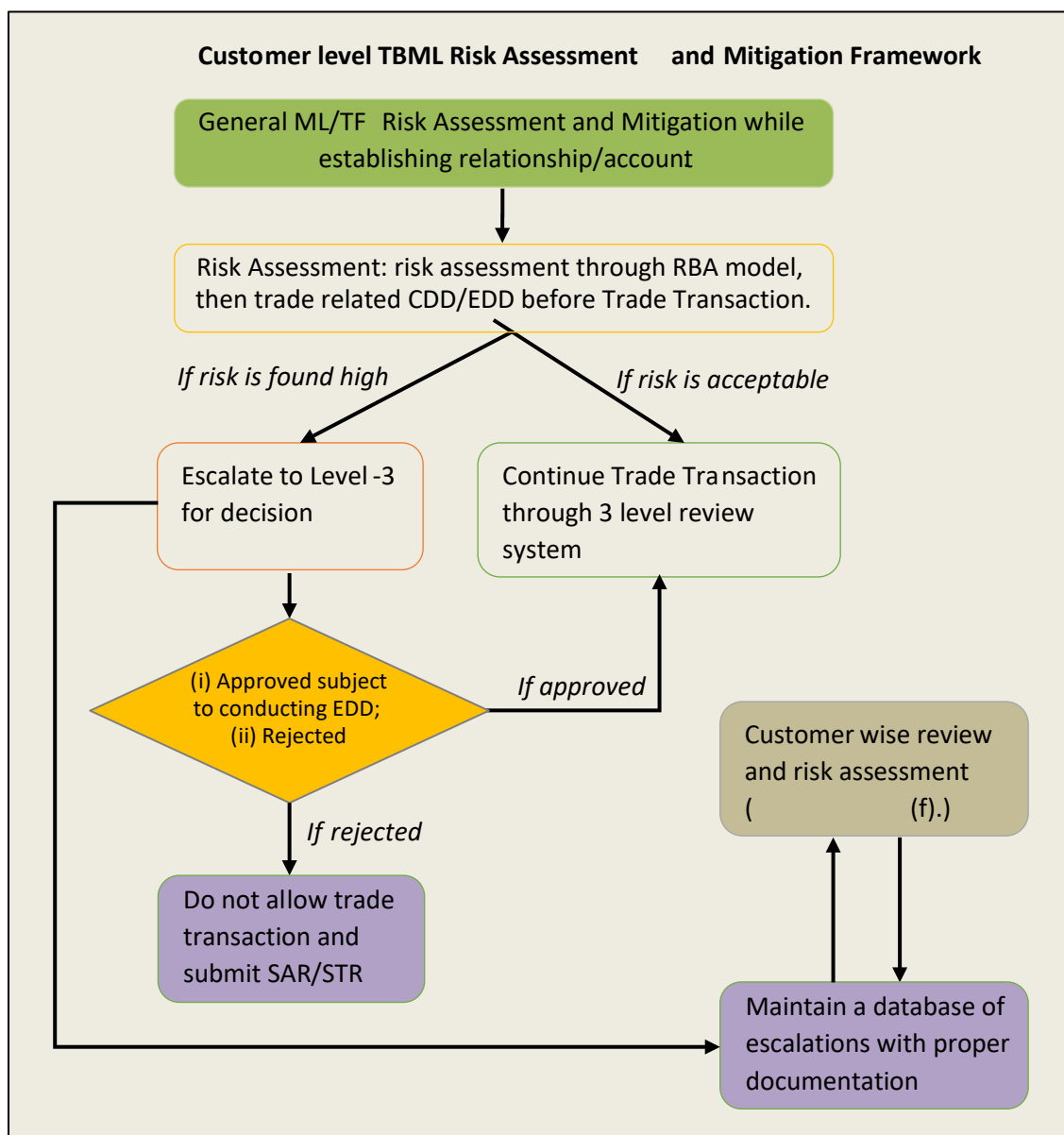
As recommended by the BFIU the Bank will ensure independent evaluation/assessment of importers and exporters by their own staff and ensure/examine, to the extent practicable, the relationship between importers and exporters through third parties. Customer level risk assessment for newly on-boarded trade customer is to be done before initiation of trade transactions. For existing trade customers, customer level risk assessment will be done as early as possible but should not be later than next periodic review of KYC in pursuance with BFIU circular 26.
- d) **Trade related CDD/EDD:**

If a customer's risk level is found low or medium, the Bank will conduct CDD for the trade customers before trade transaction takes place. However, if a customer is assessed as high risk, this should be escalated to Level 3 for further scrutiny and verification. If Level 3 is satisfied, they may approve the customer for transaction after conducting EDD. If Level 3 is not satisfied considering the magnitude of risk, the Bank's risk appetite and internal policy, they may reject the customer for trade transaction. After completion of CDD/EDD, the customer will be allowed to go for trade transaction.
- e) **Trade Transaction through 3 Level Review Systems:**

When a customer is allowed for trade transaction, trade transaction will take place following Three Level Review System.
- f) **Maintaining a database of escalations with proper documentation:**

A database should be established with customers assessed as high risk to facilitate yearly customer wise review and assessment.
- g) **Review and Assessment of Customers:**

For high risk customers review and assessment frequency shall be one year, for medium risk customers this frequency shall be every three years and for low risk customers it shall be 5 years. The review system mentioned above will facilitate input for the enterprise wide risk assessment and assist the Bank to update TBML trend and typology and devise appropriate policy and strategy at the enterprise level.



**15.16. CUSTOMER LEVEL RISK ASSESSMENT**

The framework as detailed below is a sample for guidance and reference only. The Bank may opt for qualitative and quantitative assessment, should design their own feasible scoring model depending on their respective risk exposure and experience and get the model vetted by BFIU.

Risk Components	SL	Risk Parameters	Risk Level			Risk Score (0-3)		
			Low	Obtained score	Max score	Obtained score	Max score	
Trade Customer Demographic	1	Business History	5 years and above	Less than 5 years	New Client			
	2	Payment Behavior	All payment made on due time	1-10% of total payment not made on due time	More than 10% of total payment not made on due time			
	3	Adverse Media Report	No adverse media report	Adverse report on social media or in other than daily newspaper	Adverse media report published in daily newspapers or electronics media			
	4	Law Suit Filed	No Law Suit	The client has been involved in litigation in past, but no adverse judgments and not current under litigation	Adverse judgment in past or the client is currently involved in litigation			
	others							
	5	Business entity	Government	Private limited	proprietorship/partnership/others			
	6	Export proceeds	Advance TT	Letter of credit	Collection/contract			
	7	PEPs/ IPs in management /owner	Have no PEPs/IP	Having PEPs/IPs before 36 month before	Having PEPs/IP.			
<b>Sub Total</b>								
Geographic location of trade Transaction	8	Basel AML index	Countries are ranked from 51-rest	Countries are ranked from 11-50	Countries are ranked from 1-10			
	9	FATF public documents	-	Jurisdictions no longer subject to monitoring list	Jurisdiction under increased monitoring list			
	10	Corruption perceptions Index of Transparency International	Countries are ranked from 1-20	Countries are ranked from 21-150	Countries are ranked from 151-rest			
	11	Port location	All Sea port except adjacent to sanction countries	Sea port Adjacent to sanction country	Land port/port of Landlocked country			
	12	Complexity	only 1 counterparty jurisdiction in a Trade Transaction	2 counter party jurisdiction in a Trade Transaction	More than counterparty jurisdiction in a Trade Transaction			
	<b>Sub Total</b>							

Risk Components	SL	Risk Parameters	Risk Level			Risk Score (0-3)	
			Low	Obtained score	Max score	Obtained score	Max score
Geographic location of trade Transaction	13	Food Grain	Import by Government	Import Commercially	Import Industrial		
	14	Industrial Raw Materials	-	Industrial Raw Materials Imported by Industrial importer	Industrial Raw Materials Imported by commercial importer		
	15	Industrial Raw Materials	-	Import under Not Bonded Warehouse facilities	Import under Bonded Warehouse facilities		
	16	Capital Machinery	govt. related Energy/power sector machinery	Textile/leather/ jute/ garment/ Agro food processing industry	Energy/power/ Agro food Machinery		
	17	Trading Goods	TTI 0-30%	TTI 31-50%	TTI 51% and above		
	18	Service Import or Service Export	-	Service related with import goods	Only service		
	19	Defense-Goods	Import by Government	Import by government Authorized representatives	Import privately		
	20	Dual-Use Goods	No Dual use goods	The client deals in low risk dual use goods (such as Common electronic parts, computer equipment, home appliances electronic parts)	Some activities with high risk dual use goods (such as iron, ammonium nitrate)		
	21	Other products (if any)	-	-	-		
	22	Multiple Products	Less than 5 products	Products range 5-10	More than 10 products		
	23	Export Goods	Cash Incentive 0-5%	Cash Incentive 5-20%	Cash Incentive above 20%		
	24	Export Goods	Traditional item	-	Non Traditional item		
<b>Sub Total</b>							

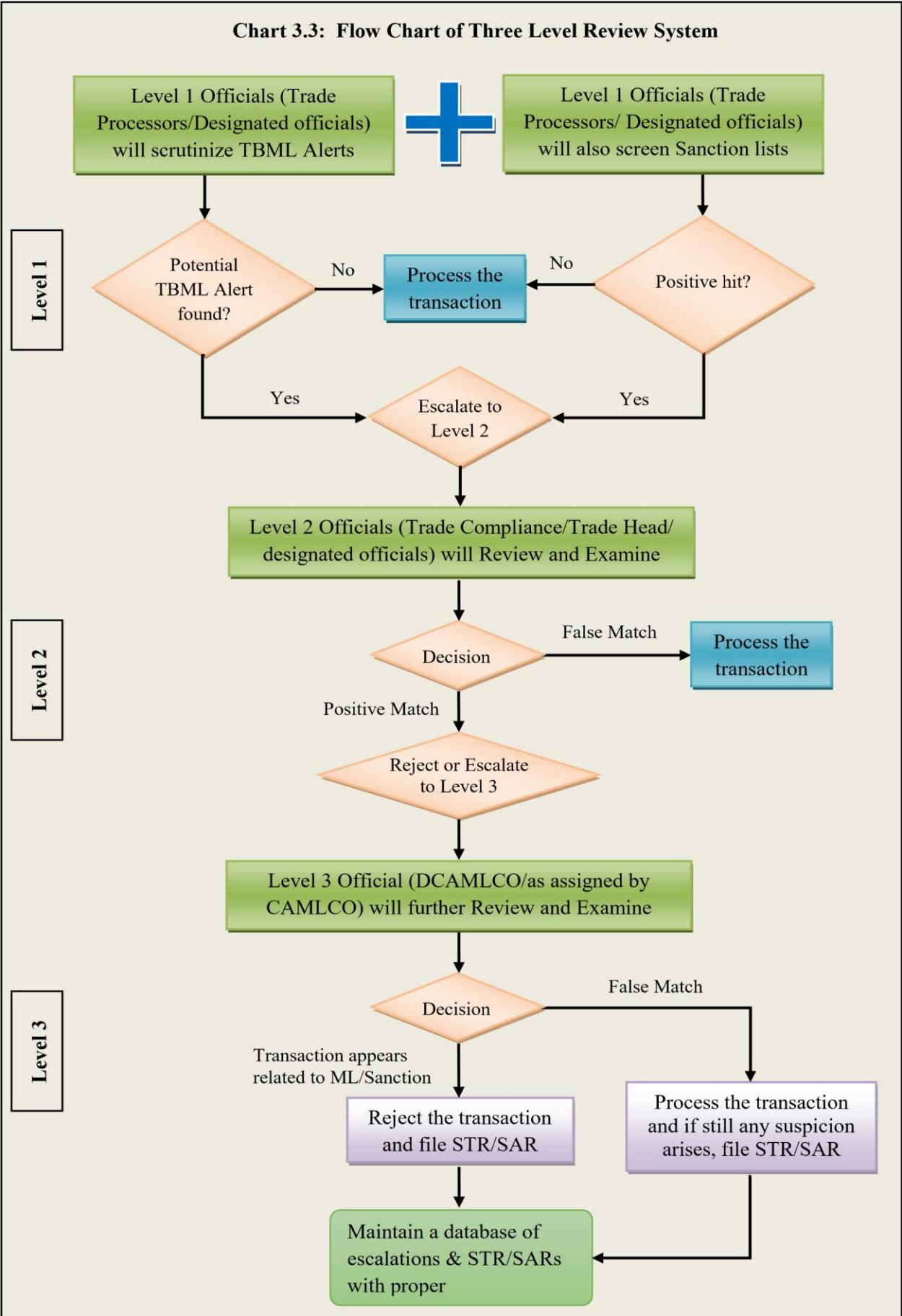
Risk Components	SL	Risk Parameters	Risk Level			Risk Score (0-3)	
			Low	Obtained score	Max score	Obtained score	Max score
Transactions trend/ history	25	Value of trade transactions (commercial)	Less than USD 200000.00 in past year in total trade	More than USD200000 to less than USD 200000 in past year in total trade	More than USD 200000 past year in total trade		
	26	Value of trade transaction (industrial)	Less than USD 100000.00 in past year in total trade	More than USD100000 to less than USD 200000 in past year in total trade	More than USD 200000 past year in total trade		
	27	Number of trade transactions (commercial)	1-20 per year	21-50 per year	over 50 per year		
	28	Number of trade transactions (industrial)	1-200 per year	201-500 per year	over 500 per year		
	29	Number of escalated TBML alerts	1 to 10	11 to 20	more than 20		
	30	Number of STR	0	1 but last two year ago	At least 1 within two years		
	<b>Sub Total</b>						
<b>Comprehensive Risk Level</b>				75 % and above			
High Risk				50 % and above but below 75 %			
Medium Risk				Below 50%			

**15.17. TRADE RELATED CDD REQUIREMENTS**

The Bank will conduct CDD in line with risk based framework and consider the following requirements as suggested below. The Bank may decide on whether the trade related CDD requirements will be performed at the time of establishing relationship/opening account with the customer along with conducting general CDD or separately before starting trade transaction-

1. Collection of required documents & information such as:
  - a) Nature of business including major goods, services and jurisdictions the customer deals with;
  - b) Usual delivery / transportation mode for goods or services;
  - c) Major suppliers and buyers;
  - d) Products and services to be utilized from the bank;
  - e) Existing/anticipated account activities;
  - f) Usual methods and terms of payment and settlement;
  - g) Any observations/ratings on the customer by concerned departments of the bank;
  - h) Any previous suspicious transaction/activity reports to BFIU;
  - i) Other information from the relevant staff; and
  - j) Trade Transaction Profile.
2. Verification of the documents & information mentioned in 1 above through reliable and independent sources.
3. Ascertaining and verifying the identity of the beneficial owners of the trade customer.
4. Conducting enhance due diligence if required.
5. Record Keeping.
6. Understanding business, production capacity, end-use of goods, 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.
7. Updating CDD information in accordance with BFIU Circulars and ML & TF Risk Management Guidelines.
8. Maintaining customer wise trade transaction profile (TTP) including items of goods, value, volume, nature of business, and principal counterparty country etc. TTP should be made available to Level 1, 2 & 3 so that they can easily check that a transaction is within the agreed profile of the customer. Until TTP is integrated within core banking system, it may remain offline outside of the core banking system. Level 2 shall conduct TTP review and decide on certain transactions escalated by Level 1. If necessary Level 3 may also consult TTP while taking ultimate decision on transactions escalated by Level 2. Post facto review of TTP against trade transactions may be conducted at least annually to identify TBML Alerts.
9. 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. Objective behind updating of the CDD profile is to ensure that the information in the CDD profile is current. The 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.
10. Bank has developed own process of “customer/transaction level risk assessment” based on their risk exposure.
  - a) Ensure that the customer has a current, approved KYC record and TTP in place before processing transactions.
  - b) Perform TBML Alert analysis and Sanction screening and execute transaction.
  - c) Escalate TBML Alerts/Potential hits of the transactions to Level 2, where required.
  - d) Escalate Suspicious Transactions/Activities to Level 2.
  - e) Keep record properly.

Chart 3.3: Flow Chart of Three Level Review System



### 15.18. INTEGRATED TBML CONTROLS WITH EXISTING AML/CTF PROGRAM

BKB as a reporting organization is subject to the AML & CFT laws. In line with the requirement of the laws and as per BIFU's directives, it will accomplish and maintain an effective TBML prevention program to keep the Bank risk free from money laundering and terrorist financing. The Bank will follow "Integrated TBML controls with existing AML/CTF program" in preventing TBML. "Stay alone" theory is not effective to combat TBML. The Bank deals with various lines of banking business such as Corporate, SME, Retail, MFS, and Foreign Trade etc. So, it is assumed that an integrated TBML control will be successful in combating TBML. The commencement of "Integrated TBML Control" should be a combined effort of the Customer selection, Customer Identification, Customer On-boarding, Conduction and making of the robust KYC profile of the customer, complying with the Customer Due Diligence requirements, and specific TBML and sanction controls initiated by trade operation people of the Bank.

### 15.19. KYC PROFILE AND TBML

Knowing the Customer adequately is the fundamental for TBML control. The Know You Customer

(KYC) program for trade customer is not only limited only knowing the customer but also:

- The source of fund;
- Nature of Business;
- Business history including Nature of goods traded;
- Trade cycle;
- Adverse media news;
- Ownership structure of the business;
- Relationship between the nature of business and Service/Product to be Imported/Exported;
- The demand and supply of the Service/Product in the country to be Imported/Exported etc.
- Trading partners or counterparties of the customer (including buyers, sellers, shippers, consignees, notifying parties, shipping agents, etc.);

#### i. Trade control- Specific Customer Due Diligence

- Collect customer information related to trade-based activities;
- Regularly update customer information related to trade-based activities;
- Get more information when inconsistencies are identified: A robust information sharing system will be established among relevant Department, Unit, Branches and management to be ahead of time;
- Performed on all parties to the transaction: The transaction monitoring will be done "each and every" basis, rather, sample test theory.

### ii. General

Establish policies and procedures based on a written risk assessment: The Bank periodically review the Policy Guidelines on TBML taking into account changes in the operating environments and regulatory developments. The Policy Guidelines on TBML will be reviewed annually, and if necessary the Policy Guidelines will be updated incorporating the necessary changes/updates. The updated Policy Guidelines will be implemented without delay.

### iii. 1st Line of defense

Front office staff knows clients normal trade activity;

### iv. 2nd Line of defense

Compliance trade/finance unit Review and analyze business plans and finance requests to determine legitimacy;

### v. 3rd Line of defense –

Internal audit Review effectiveness of anti-TBML controls.

### Roles and responsibilities

- Appoint a compliance officer;
- Staffing Expertise in the TBML combat;
- Train appropriate staff;
- Conduct an independent TBML audit;
- Monitor for suspicious transactions and red flags;
- File SARs as appropriate.

### Some of the Trade Controls the Bank will consider are:

- All relevant staff and officials of the Bank will be made aware and remain updated of trade controls. Dissemination through regular correspondence should also be emphasized.
- To assess the effectiveness and adequacy of the trade controls, independent review shall be done from time to time. Frequency of review should be based on ML/TF risks faced by the Bank, emergence of any particular or special need arising out of changes in regulatory instructions etc.
- Trade Controls should address all possible difficulties that relevant officials may face in combating TBML.
- The Bank shall make use of rule based alert/exception reports or detection scenarios to the extent reasonably practicable. Some examples of detection scenarios based on TBML Alerts.
- Trade Controls should ensure clear division of roles and responsibilities and ownership of risks relating to critical functions.
- Trade Controls should require decisions relating to trade transactions, work flow procedures and TBML Alerts to be documented appropriately for audit trail purposes, having regard to the record keeping standards as mentioned in MLPA, 2012, GFET, 2018 and ML & TF Risk Management Guidelines. They should also include mechanism to ensure that customer information including applicable trade processes and relevant updates is captured in the relevant bank's customer database, in order to facilitate the assessment and ongoing monitoring of customer activities.

- Apart from the yearly review of strategy and policy by senior management the Bank will involve senior management in planning and implementation of Trade Controls. Considering size and exposure to TBML risks, banks may decide the period of such review.
- The trade transactions conducted through any IT or Technological Platform of a bank will be governed under the directives of Bangladesh Bank issued from time to time.
- Relevant senior officials having awareness of contemporary intelligence & knowledge on geopolitics and other cross border regulatory restrictions which are not as much stringent as that of Sanction but may lead to regulatory and legal hassle should guide the transaction level officials on due diligence measures to be exercised in such situations.
- Trade Controls should be readily identifiable by and made known to all relevant officials engaged in trade related activities.

### Sanction Screening System

Economic sanctions are a way to financially isolate a target. Increasingly, countries are using economic sanctions instead of military force as an instrument of foreign policy. Sanctions can generally fall into one of the following categories.

- a) **Targeted sanctions:** Aimed at specifically named individuals, such as key leaders in a country or territory, named terrorists, significant narcotics traffickers and proliferators of weapons of mass destruction. These sanctions often include the freezing of assets and travel bans where possible.
- b) **Sectorial sanctions:** Aimed at key sectors of an economy to prohibit a very specific subset of financial dealings within those sectors to impede future growth.
- c) **Comprehensive sanctions:** Generally prohibit all direct or indirect import/export, trade brokering, financing or facilitating against most goods, technology and services. These are often aimed at regimes responsible for gross human rights violations and nuclear proliferation.

Bangladesh Krishi Bank will deploy the automated sanction screening system. The Bank will also continue its efforts to have automated real time Vassal Tracking System. Dedicated expertise will be employed to monitor both the systems, review and escalate applicable issues to the higher level.

Most jurisdictions impose sanctions regimes, particularly to comply with sanctions imposed by the United Nations and for members, the European Union. As expected,

- 1) Sanction screening shall be conducted on individual, entity, banks, insurer, NGO/NPO, country, port, flag, vessel etc. The screening should also be conducted on all the parties involved in the transaction and geographic location to the transaction, such as seller of the goods, the shipping company, any agents or third parties, countries or ports etc. that appear in the transactions.
- 2) For sanction screening it is important to ensure that there is no “risk based approach” –i.e. only screening certain transaction or parties. All parties (known to the bank) related to the transactions at the time and additional parties that come into the picture as the transaction progresses are required to be screened.
- 3) BKB has subscribed to the extensive Loyds Vessel Tracking System which facilitates Vessel tracking (origin port, transshipment, destination port) and its voyage history are tracked to determine whether it has docked at embargoed countries during its previous voyage and dealt with sanctioned entities or embargoed goods. It should be borne in mind

that vessels may change their names but cannot change their IMO number; hence cross-checking IMO number through a reliable source is recommended.

## **Chapter 15: TBML**

- 4) Beneficial owner, commercial operator and registered owner of the vessel involved in the transaction to trace the history of former ship owners with focus on country of residence;
- 5) Port of loading, ports-of-call and port of discharge (including whether the goods originate from, or are sold to any sanctioned country) and the trade routes proposed to be used;
- 6) Care should also be taken to PEPs/IPs screening, adverse media screening, High Risk Country screening;
- 7) A combination of automated and manual controls will be relevant in the context of AML and counter-terrorist financing (CTF) efforts.

### **15.20. TYPICALLY THE FOLLOWING ELEMENTS ARE, BUT NOT LIMITED TO, CHECKED VIA AUTOMATED /MANUAL PROCEDURE:**

- i. Unit prices
- ii. Number of items shipped
- iii. Shipping marks
- iv. Trade term – often an Incoterms rule followed by a place
- v. Commercial contract
- vi. The documentary credit applications
- vii. The guarantee applications
- viii. The documents presented under import documentary credits
- ix. The documents presented under export documentary credits
- x. The documents presented under import documentary collections
- xi. The documents presented under export documentary collections
- xii. Guarantee demands
- xiii. All incoming and outgoing SWIFT messages etc.

### **The Bank shall at minimum designate officials to handle:**

- i. Sanction screening results analysis/escalation
- ii. Vassal tracking report analysis/escalation
- iii. TBML related transaction monitoring alert analysis/escalation.

### **The key factors the Bank will consider regarding Sanction Screening**

One of the key components of a successful Sanctions Screening Program is a strong technology framework that can process data quickly and efficiently, employ an efficient and effective matching algorithm, and possess a clear audit trail of observations and resolutions. The Sanction Screening system of the Bank shall consider-

- Appropriate data shall be collected and consistent data formats maintained;
- Multiple versions of customer and related party records will be maintained;
- Applicable watch lists shall be kept current;
- All indicia in the watch lists should be utilized in the Sanctions Screening process;
- Matching algorithms should consider multiple parameters;
- Alerts should be risk rated or prioritized;
- Methodology for alert escalation and disposal should be clearly defined;
- Case management feature;
- Ability for ad hoc screening;
- Customizable KPI reports;
- A strong Business Continuity Plan etc.

### **Capacity Building**

Capacity building is a continuous process. Combined efforts of knowledge, skill and good practices can ensure sustainable enhancement of capacity of human resources. The global trend in implementing technology and innovative ideas to manage TBML risk has made fierce challenge for the expertise to be updated. Formal training, research/analysis, maintaining the approved standard can assure some comfort to build the capacity of the officials.

### **Training on Trade Based Money Laundering**

The AML division of the Bank will arrange training on TBML in association with the Training Institute. Training related records should also be retained properly. At a minimum the following issues will be considered:

- a) The Bank will arrange effective training/workshop time to time training on TBML. The main objective is to ensure that concerned officials understand the trade based money laundering in both national and international context, bank's exposure to TBML and its own Trade Controls;
- b) The Bank will conduct training need assessment on preventing TBML. For level 1, 2, 3 officials training is essential. Training should be designed in such a way that the trainees are able to provide, or contribute to, training depending on their background, role and experience;
- c) For officials involved in day to day trade processes role based training shall also be included. Objective behind such training should be to impart training to them on TBML specific risks and responsibilities;
- d) Role-based training will be included for staff involved in day-to -day trade processes. Such staff may include, for example, relationship managers and trade-related operations teams. The goal of role-based training is to educate staff about the specific risks and responsibilities applicable to them, to assist in preventing, identifying, mitigating and reporting potential trade-based money laundering. For example, a document checker in trade operations will require greater in-depth training on irregular data that may be found on invoices, L/Cs and other trade finance-related documents, which they would be expected to handle on a day-to-day basis;

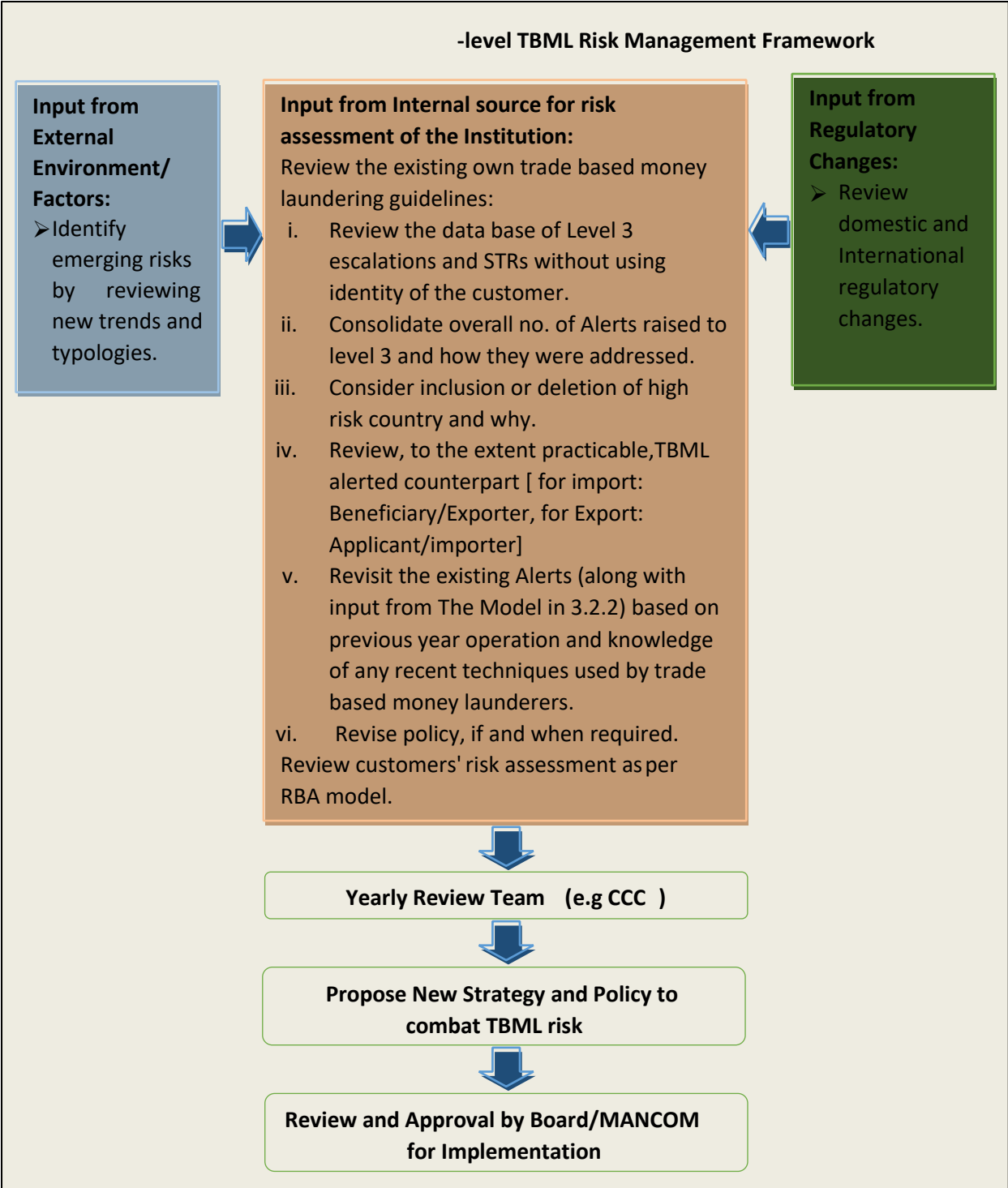
- e) The trade-based money laundering training should be be spoke. To this end, Staff training will be refreshed at regular intervals and relevant training records shall be properly retained to make the program effective and fresh. This will assist the employee to remain aware about the latest scenario of TBML and will also help them to understand about the expanded illicit utilization of the banking channel, risk prone area etc.;
- f) The Bank may consider providing foreign training for its employee if needed.

### **Suspicious Transaction/Activity Reporting**

- a) STR/SAR reporting shall be done in accordance with the procedure. Before submission, the STR/SAR will be escalated to DCAMLCO/level and CAMLCO to ensure compliance with instructions of relevant BFIU circular. Risk of tipping off shall also be managed.
- b) In complex situations the Banks may seek opinion from BFIU.

### **Price Verification**

The Bank will develop its own database and frame clear policies and procedures to guide trade processing staff in performing price checks. The policies should, at a minimum, mention the level of acceptable price variance and escalation procedures when significant price difference is identified. Provision of different threshold for different types of underlying goods and services may be allowed on the basis of periodic market price assessment. To enhance the effectiveness of the price checks, the process may be centralized or automated; otherwise care should be taken to ensure avoidance of any conflict of interest. With the growth of global trade and digitization fueling the next leg up of the trade finance business, the traditional documentary trade business will become more efficient as companies start leveraging technologies such as block chain, electronic bills of lading and electronic issuance to reduce or even entirely eliminate manual processes. While these developments evolve, it is vital for the banks to establish a strong foundation for mitigating the regulatory compliance risks, which is a combination of processes, controls, sound data model and technologies, so that all relevant transactional data is captured, managed and analyzed to ensure effective monitoring of TBML. Banking industry have a tough road ahead; however, the collective efforts of banks, regulatory authorities and technological advancements are paving the way to reach a state where effective and largely automated TBML monitoring would be a new normal.

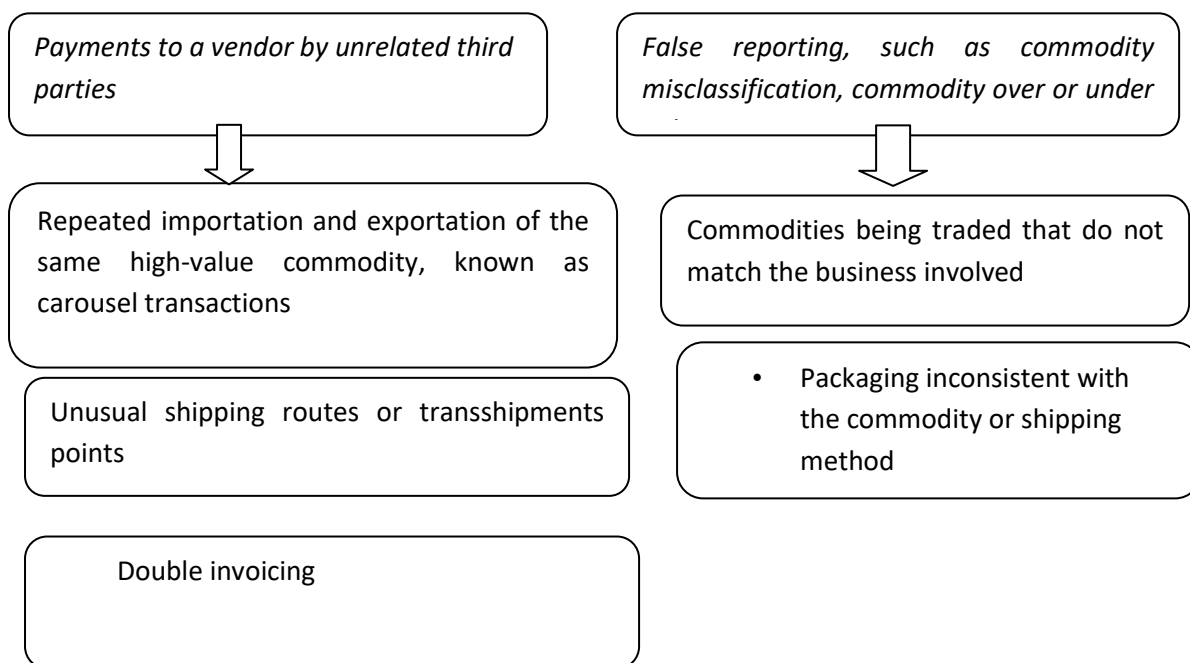


### 15.21. RED FLAGS FOR TRADE BASED MONEY LAUNDERING

- Incapability of a bank customer to produce trade documentation to back up a requested bank transaction.
- 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 transported.
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- Shipment locations or description of goods that is inconsistent with the letter of credit.
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to Customs or paid by the importer.
- A transaction that involves the use of amended or extended letters of credit that are amended significantly without reasonable justification or that include changes to the beneficiary or location of payment.
- A third party paying for the goods.
- A consignment that is inconsistent with the business (eg a steel company that starts dealing in paper products, or an information technology company that suddenly starts dealing in bulk pharmaceuticals).
- Customers conducting business in high-risk jurisdictions. Although not specifically identified by the regulatory/law enforcement agencies may be added to the list of high-risk jurisdictions.
- The commodity is transshipped through one or more jurisdictions for no apparent economic reason.
- Customers involved in potentially high-risk activities, including those subject to export/import restrictions such as equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as, metals, ore and crude oil.
- Customer seeks trade financing on the export or import of commodities whose stated prices are substantially more or less than those in a similar market situation or environment.
- Letter of Credit covers goods that have little demand in importer's country.
- Letter of Credit covers goods that are rarely if ever produced in the exporter's country.
- Documents arrive without title documents.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- A transaction structure that appears unnecessarily complex so that it appears designed to obscure the transaction's true nature.
- A shipment that does not make economic sense (eg; the use of a large container to transport a small amount of relatively low value merchandise).
- The method of payment appears inconsistent with the risk characteristics of the transaction, for example the use of an advance payment for a shipment from a new supplier in a high-risk country.
- A transaction that involves receipt of cash or payment of proceeds (or other payments) from third-party entities that have no apparent connection with the transaction or which involve front or shell companies.
- A transaction that involves commodities designated as high risk for money laundering activities, such as goods that present valuation problems or high value, high turnover consumer goods.

- Customer makes changes to a letter of credit beneficiary just before payment is to be made.
- Customer changes the place of payment in a letter of credit to an account in a country other than the beneficiary's stated location.
- Customer's standby letter of credit is used as a bid or performance bond without the normal reference to an underlying project or contract, or designates unusual beneficiaries.

Below are some of the red flag checks of potential TBML activity which the Bank will potentially look for introducing in their pre- and post-transaction screening processes classified by various areas requiring scrutiny.



**Business structure:**

- The type of item being shipped is not in line with the exporter's or importer's regular business activities, e.g., manufacturer of toy exporting IT equipment;
- The size of the shipment appears inconsistent with the scale of the exporter's or importer's regular business activities e.g., a third of the turnover;
- Customers conducting business in high-risk jurisdictions;
- Customers in high-risk activities, including those subject to export/import restrictions such as weapons, chemicals, metals, gems, crude oil.

**Transaction, goods and payments structure:**

- Transaction structure appears unnecessarily complex to obscure the transaction's true nature, e.g., the use of multiple intermediaries/parties or shipment locations;
- Goods do not comply with applicable import or export regulations, or involve dual-use and high-risk goods
- Obvious over or under pricing of goods and services relative to fair market value, example gold jewelry at \$500 an ounce when the market value is at \$950 per ounce;
- Deal involves receipt of cash (or other payments) from third-party entities that have no apparent connection with the transaction;

- Frequent amendments to LCs without a reasonable justification; or that include changes to the beneficiary or location of payment;
- LCs are routinely cancelled or utilized;
- Method of payment inconsistent with risks e.g., advance payment for a new supplier in a high- risk country;
- Multiple or double invoicing;
- Obvious misrepresentation of quantity or type of goods imported or exported;
- Unusual trigger point of LC payments e.g., before goods are shipped without documentation. Shipment structure:
- Shipping which uses small Non-Vessel Operating Common Carrier(NVOCC) with the potential of collusion, or high-risk/sanctioned vessels;
- Shipping via high-risk or transshipment jurisdictions or unconnected subsidiaries;
- Shipment by firms/individuals from foreign countries other than city of exporter;
- Shipment that does not make economic sense (e.g., the use of a 40-foot container to transport a small amount of relatively low-value goods);
- Mismatch in port of loading with vessel location check;
- Shipment locations or description of goods those are not consistent with LC.

**Documentation:**

- Packaging inconsistent with commodity or shipping method;
- Difficulty in determining the ultimate consignee (recipient) (i.e., via agent);
- Shows a higher/lower value or cost than declared to customs or paid by the importer;
- Significant discrepancies between the descriptions of the goods on BL, invoice, or other documents (i.e., certificate of origin, packaging list, etc.);
- Significant discrepancies between the actual goods shipped and the descriptions of the goods on the BL and/or invoice (can only know through inspections);
- Common red flags for LC fraud including incorrect use of banking terms, spelling mistakes, and error in grammar and composition.

**Intermediaries/deal parties/third party:**

- Transactions from unrelated parties in high-risk jurisdictions;
- Transactions involving third parties which are highlighted during sanctions screening as having unacceptably high risk;
- Negative news on parties;
- A transaction that involves front or shell companies;
- Connected applicant/beneficiary e.g., beneficial ownership, signers, shell companies, common shareholders, etc.;
- Originators and recipients of payments have ties to high-risk countries;
- Transactions from unrelated parties in high-risk jurisdictions;
- Transactions involving third parties which are highlighted during sanctions screening as having unacceptably high risk
- Negative news on parties
- A transaction that involves front (or shell companies)
- Connected applicant/beneficiary (e.g., beneficial ownership, signers, shell companies, common shareholders, etc.)

**The TBML Alerts may be sub-divided into the following categories, i.e.**

- a) The transactions
- b) The goods and size of shipment
- c) Transport
- d) Payment
- e) Country
- f) Party/parties
- g) Discrepancies
- h) Unusual documentation

Some of the important Products specific TBML alerts are given below. They do not laminate the alerts mentioned in Appendix B.

TBML Alerts common to almost all the products below and therefore should be guarded against are:

- a) Under Invoicing (against market price)
- b) Over Invoicing (against market price)
- c) Underlying goods is not in line with the customer's line of business.
- d) Descriptions of the goods are not clear or are coded or disguised.
- e) The method of payment appears inconsistent with the risk characteristics of the transaction.
- f) The transaction involves sanctioned entities.

# **Chapter 16**

## **Recruitment, Training and Awareness**

### **16.1. APPOINTMENT AND TRAINING**

One of the major purposes of combating money laundering and terrorist financing activities is to protect from risks arising out of money laundering and terrorist financing. To meet this objective, Bank shall have to undertake proper screening mechanism in different appointment procedures so that the Bank do not face money laundering and terrorist financing risks by any of the staff.

### **16.2. TRAINING FOR THE OFFICIALS**

To ensure proper compliance of anti-money laundering and anti-terrorism activities Bank will arrange suitable training by the training Institute and Central Compliance Unit for all officials. To deter siphoning of legally or illegally earned money abroad, TI shall also arrange trade based money laundering training along with anti-money laundering and anti-terrorism financing related training for the officials dealing in foreign exchange transactions. A general training program should include the following:

- Legal framework, how AML/CFT related laws apply to FIs and their employees;
- Institution's policies and systems with regard to customer identification and verification, due diligence, monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

#### **16.2.1. New Employees**

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

#### **16.2.2. Education and training for customers**

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

#### **16.2.3. AML/CFT Compliance Officer**

The AML/CFT Compliance Officer should receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, Bangladesh Bank directives and internal policies. In addition, the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

### 16.2.4. Training Procedures

The trainers can take the following steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick "why are they here" assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.
- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file.

### 16.2.5. Refresher Training

In addition to the above compliance requirements, training may have to be tailored to the needs of specialized areas of the institution's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Such training may provide on an annual basis; or may choose a shorter or longer period. Training should be conducted ongoing basis, incorporating trends and developments in an institution's business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicious activity.

### 16.3. Obligations under Circular

Obligations under BFIU Circular-26; dated 16/06/2020 : To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, bank should follow proper Screening Mechanism in case of recruitment and ensure proper training for their officials.

### 16.4. EMPLOYEE SCREENING

Bangladesh Krishi Bank is subject to ML & TF risk from its customers as well as from its employee in absence of proper risk mitigating measures. ML & TF risks arose by or through its employees can be minimized if the bank follows fair recruitment procedure. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment but also include the judgment of good character. For this, Bangladesh Krishi Bank should follow the following measures:

- Reference check
- Background check
- Screening through or clearance from Law Enforcement Agency
- Personal interviewing
- Personal guarantee etc.

Before assigning an employee in a particular job or desk, bank shall examine the consistency and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

### 16.5. KNOW YOUR EMPLOYEE (KYE)

Institutions and businesses learn at great expense that an insider can pose the same ML/TF threat as a customer. It has become clear in the field that having co-equal programs to know your customer and to know your employee is essential. In an effort to identify and anticipate trouble before it costs time, money and reputational damage, FIs should develop program to look closely at the people inside their own organizations.

A Know Your Employee (KYE) program means that the institution has a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job description, code of conduct/ ethics, levels of authority, compliance with personnel laws and regulations, accountability, dual control, and other deterrents should be firmly in place. Background screening of prospective and current employees, especially for criminal history, is essential to keep out unwanted employees and identifying those to be removed. It can be an effective risk management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. Used effectively, the pre-employment background checks may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. An institution should verify that contractors are subject to screening procedures similar to its own. His sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications. The extent of the screening depends on the circumstances, with reasonableness the standard.

# Chapter17

## Record Keeping

### 17.1. RECORD KEEPING

All documents collected or gathered for establishing relationship must be filed in with supporting evidence. Where this is not possible, the relevant details should be recorded on the applicant's file. Institutions which regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records.

#### 17.1.1. Legal Obligations

Obligations under MLPA, 2012	:	The reporting organizations shall have to preserve previous records of transactions of any close account for at least 5(five) years from the date of such closure and provide with the information maintained under the clause to Bangladesh Bank.
Obligations under MLP Rules, 2013	:	<p>The bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners:</p> <ol style="list-style-type: none"> <li>(1) Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;</li> <li>(2) The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction;</li> </ol> <p>The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order.</p>

#### 17.1.2. Reporting to BFIU

##### Legal Obligations

Obligations under MLPA, 2012	:	The reporting organizations shall have to report any suspicious transaction (defined in Section 2(Z) of MLPA, 2012 and Section 2(16) of ATA, 2009) to the Bangladesh Bank immediately on its own accord.
Obligations under MLP Rules, 2013	:	Every bank is obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self-assessment, independent testing procedure etc.) to Bangladesh Bank without any delay or in due time. Besides they have to produce any documents that are sought by Bangladesh Bank.

**17.1.3. Suspicious Transaction Reporting**

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.

Anti-Terrorism Act, 2009 defines suspicious transaction as follows-

‘Suspicious Transaction’ means such transactions –

- which is different from usual transactions;
- which invokes presumption that,
  - it is the proceeds of an offence under this Act,
  - it relates to financing of terrorist activities or a terrorist person or entity;
- which is any other transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.

**17.2. RECORDS KEPT BY BANGLADESH KRISHI BANK**

- Records to be kept for the aforementioned purposes, BKB will cover-
- Customer information
- Transactions
- Internal and external suspicion reports
- Report from CCC/CAMLCO
- Training and compliance monitoring
- Information about the effectiveness of training Transaction Monitoring
- Close accounts / transactions
- CTR Reports
- TP & KYC up-gradation
- Internal and External Audit Reports
- Policy, Manual, Circulars and Instructions both BFIU and BKB.

### 17.2.1. Walk-In/ One Off/Online Customer

The Branch should collect complete and correct information while serving Walk-in customer, i.e. a customer without having account. Banks should know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT. The Branch 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 banks should identify sources of funds as well.

### 17.2.2. 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.

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

### 17.2.4. Domestic Wire Transfers

In case of threshold domestic wire transfers of at least BDT 50,000/- (fifty thousand), 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. For providing Mobile financial services the concerned 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/instruction.

### 17.3. CUSTOMER INFORMATION

Branch shall obtain following information while opening accounts or establishing other relationships with individual customers:

- Correct name and/or names used;
- Parent's names;
- Date of birth;
- Current and permanent address;
- Details of occupation/employment and sources of wealth or income
- Contact information, such as – mobile/telephone no.

The original, certified copy of the following Photo ID also play vital role to identify the customer:

- Current valid passport;
- Valid driving license;
- National ID Card;
- Employer provided ID Card, bearing the photograph and signature of the applicant;

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

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

#### 17.3.1. Appropriateness of documents

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

### 17.4. TRANSACTIONS

All transactions carried out on behalf of or with a customer in the course of relevant business shall 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 shall be maintained in a form so that a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer shall be retained for a period of five years from the date on which the transaction is completed. As mentioned before the records will still be retained even after elapsing of five years should there is an investigation ongoing about the particular customer.

### 17.5. INTERNAL AND EXTERNAL REPORTS

BKB shall make and retain-

- Records of actions taken under the internal and external reporting requirements
- 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 shall be retained for five years. Records of all internal and external reports shall be retained for five years from the date the report was made. Mentionable that if any investigation is under process but five years time have been elapsed, the records have to be maintained till closure of the investigation process even after elapsing the time bar i.e. five years.

### 17.6. OTHER MEASURES

BKB records shall include-

#### a) **Training Related**

- 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 with evaluation.
- Managing Director & CEO's Commitment

#### b) **Compliance Monitoring Related**

- Reports by the CAMLCO to Senior Management, and
- Records of consideration of those reports and of any action taken as a consequence.

### 17.7. DOCUMENTS VERIFYING EVIDENCE OF IDENTITY AND TRANSACTION RECORDS

Records relating to verification of identity will generally comprise of-

- A description of the nature of all the evidence received relating to the identity of the verification subject.
- The evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such copy Records relating to transactions will generally comprise of.
- Details of personal identity, including the names and addresses, etc. as prescribed by Bangladesh Bank/BFIU under various circulars and subsequent directives pertaining to.
- The customer
- The beneficial owner of the account or product
- The non-account holder conducting any significant one-off transaction
- Any counter-party
- Details of transaction including-
- The nature of such transactions
- Customer's instruction(s) and authority(ies)
- Source(s) and volume of funds
- Destination(s) of funds
- Book entries
- Custody of documentation
- The date of the transaction
- The form (e.g. cash, cheque) in which funds are offered and paid out

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

- The carrying out of the one-off transaction, or the last in a series of linked one-off transactions, or
- The conclusion of the business relationship, or
- The commencement of proceedings to recover debts payable on insolvency

### **17.8. WIRE TRANSFER TRANSACTIONS**

Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of telegraphic transfers (TT) and electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in a TT and electronic payment message instruction. Following the recent focus on terrorist financing, relevant financial businesses are required to include accurate and meaningful originator (name, account number and where possible address) and beneficiary information (account name and/or account number) on all outgoing funds transfers and related messages that are sent and this information shall remain with the transfer or related message throughout the payment chain. Institutions shall conduct enhanced scrutiny of and monitor for suspicious incoming funds transfers which do not contain meaningful originator information. The records of electronic payments and messages shall be treated in the same way as any other records in support of entries in the account and kept for a minimum of five years after closure of the same.

### **17.9. INVESTIGATIONS**

Where any Branch of BKB has submitted a report of suspicious activity to Bangladesh Bank /BFIU as per Bank's AML Policy or where it knows that a client or transaction is under investigation, it shall not destroy any relevant records without the agreement of the Bangladesh Bank even though the five-year limit may have been reached. Branches of BKB shall maintain a register or tabular records of all investigations made to it by the Bangladesh Bank / BFIU and all disclosures to the Bangladesh Bank. The register shall be kept separate from other records and contain as a minimum the following details-

- The date and nature of the enquiry
- Details of the account(s) involved
- Be maintained for a period of at least 5 years

### **17.10. TRAINING RECORDS**

The Bank shall arrange training for its officials to comply with regulations and maintain records there of which include-

- Details of the content of the training programs provided
- The names of officer who have received the training
- The date on which the training was delivered
- The results of any testing carried out to measure officer understanding of the money laundering requirements, and
- An on-going training plan.

### 17.11 BRANCH LEVEL RECORD KEEPING

To ensure the effective monitoring and demonstrate their compliance with the concerned regulations, Branches of BKB have to ensure the keeping or availability of the following records at the branch level either in hard form or electronic form-

- Information regarding Identification of the customer,
- KYC information of a customer,
- Transaction report,
- Suspicious Transaction/Activity Report,
- Exception report,
- Training record,
- Return submitted or information provided to the Head Office or competent authority.
- All Internal / External Audit inspection report.

# Chapter 18

## BKB & Miscellaneous

### 18.1. WHISTLE BLOWING

Whistle blowing is the term used when a worker passes on information concerning wrongdoing. In this guidance, we call that “making a disclosure” or “**blowing the whistle**”. The wrong doing will typically (although not necessarily) be something they have witnessed at work.

Few definition and sections are given bellow from —The public interest Information Disclosure Act (provide protection) 2011, published in Bangladesh Gazette, Additional issue, 22 June, 2011

- **Whistleblower** means the person who discloses the public interest information to a competent authority.
- **Competent Authority** means the chief of any agency or chief or chief executive of divisional, regional, zila, upazila or union office of any department, directorate or office subordinate to it and the following persons or office-bearers shall also be included, as-
  - a) For persons holding constitutional posts, President
  - b) For member of parliaments, Speaker
  - c) For any member from judiciary, Register of Supreme Court
  - d) If related to corruption, Anti Corruption Commission
  - e) If related to public money, Comptroller and Auditor General, and
  - f) For illegal and unethical deeds, Officer-in-Charge of respective police station
- **Public interest** means the job undertaken by the government or by its directions for the interest of public or for a part of them;
- **Public interest information** or **information** means is such an information of any agency which expresses that, any officer was, is or may be involved in-
  - a) Irregular and unauthorized use of public money
  - b) Mismanagement of public resources
  - c) Misappropriation or misuse of public money or resources;
  - d) Abuse of power or maladministration;
  - e) Committing criminal offense or illegal or prohibited acts;
  - f) A conduct that is harmful or dangerous for public health, safety or to the environment corruption
- **Section-4 Public interest disclosure**
  1. Any whistleblower can make public interest disclosure, if considered reasonable, to a competent authority.
  2. Any whistleblower, for fulfilling the purpose of this Act, will be considered that he made public interest disclosure, if—
    - a) He believes on reasonable ground that the information is true; or
    - b) If there is no reasonable ground to believe the truth of the information, but he believes that the information may be true and is of sufficient significance to justify its disclosure so that its truth may be investigated.
  3. Any information mentioned in the sub-section (1), can be sent for disclosure, to a competent authority, in written—directly hand-to-hand, by post or via any electronic means.
  4. Each disclosed information shall be supported by such documents or materials that would substantiate it preliminarily.

- **Section-5 Whistleblower's protection**
  - a) If any whistleblower discloses any authentic information under sub-section (1) of section 4, his identity cannot be divulged without his consent.
  - b) For making disclosure of public interest information, no criminal or civil, or, where applicable,
  - c) Departmental suit can be filed against the whistleblower.
  - d) If the whistleblower is a service holder, only for disclosing public interest information- demotion, harassment transfer or forced retirement or any other measures cannot be taken against him that would incur loss of his psychological, financial or social standing or no departmental actions can be taken against him or he cannot be treated discriminatorily.
  - e) Subject to sub-section (6), information disclosed under section 4 cannot be produced as a proof in any civil or criminal case or the whistleblower cannot be presented as a witness in any civil or criminal case and nothing can be publicize in the case proceedings by which the identity of the whistleblower would or may be revealed.
  - f) If there is anything in a book, record or a document included in the witness's evidences of a civil or criminal case which contains the identity of the whistleblower, then the court will not allow permission to any person to visit the segment of that book, record or document which contains that identity.
  - g) Notwithstanding anything contained in this section, during the hearing of a case, if it is clear to the court that, the whistleblower intentionally disclosed false and baseless information or fair trial cannot be ensured without revealing the identity of the whistleblower, then the court can reveal the identity of the whistleblower and for disclosing false and baseless information it can take actions against him under section 10.
  
- **Section-10 Punishment for disclosing false information**
  - a) Being aware of the falsity or without being completely confirm about the truthiness of the information, if a whistleblower purposely discloses any baseless information, which is not of public interest or there is a possibility to conduct inquiry or trial proceedings based on that information under this Act, he shall be deemed to have been disclosed false information.
  - b) If any whistleblower discloses false information mentioned in the sub-section (1), he shall be deemed to have been committed crime under this Act and he shall be sentenced to imprisonment for a minimum 2 (two) years or maximum 5 (five) years or pay a fine or both.
  - c) If the whistleblower is a government officer and he discloses any false information mentioned in sub-section (1), departmental actions shall have to be taken against him along with the punishment mentioned in sub-section (2).

### **As per Money Laundering Prevention Act, 2012**

- a) Section (25) (d) of MLPA, 2012 imposes to raise STR willingly by Reporting Organization (RO) without any delay to BFIU Bank/ branches should raise STR/SAR if any suspicion found in transactions or activities of customer and send the report to BFIU through CCC. Bank must obtain EDD on those customers also.
- b) Section (28) of MLPA, 2012 provides the safe harbor for persons submitting suspicious report.

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

### **18.2. CORPORATE VEHICLES**

Corporate vehicles provide opportunities for those involved in serious or organized crime to manage and obscure the source of their wealth and hide their identity.

Corporate vehicles means legal entities through a wide variety of commercial activities are conducted and assets are held, including corporations, trusts and partnership. Corporate vehicles are an essential part of a capitalist, free-market economy as they are the means by which investment are made, enterprises are run and wealth is managed and inherited. Though they are deployed legally, but they can also be used for illegal purposes. By hiding the existence of assets, they can prevent their seizure or taxation. They can also be used to launder money concealing the proceeds or payments of bribery. Bank must take AML & CFT precautions as bank not be used by such entities.

### **18.3. VIRTUAL CURRENCY (VC)**

Virtual currency is currency held within the block chain network that is not controlled by a centralized banking authority. Virtual currency is different than digital currency since digital currency is simply currency issued by a bank in digital form. FATF Recommendation 15 should be applied for VC/VA (Virtual Assets). Bit coin is an example of VC.

### **18.4. FinTech & RegTech**

Today, FinTech has entered a phase of rapid development marked by the proliferation of startups and other new entrants, such as IT and ecommerce firms that have fragmented the financial services market. This new era presents fresh challenges for regulators and highlights why the evolution of FinTech necessitates a parallel development of RegTech. In particular, regulators must develop a robust new framework that promotes innovation and market confidence, aided by the use of regulatory "sandboxes."

Currently in its second stage of development, RegTech is being used by both institutions and regulators to address increasingly cumbersome compliance processes. But regulators have yet to unlock the transformative potential of RegTech. We argue that certain RegTech developments today are highlighting the path toward another paradigm shift, which will be typified by a reconceptualization of the nature of financial regulation. This "RegTech 3.0" will involve a regulatory approach that is as data centric as the markets it monitor.

FinTech, the word, is a combination of financial technology. FinTech describes new technology that seeks to improve and automate the delivery and use of financial services. Any company which integrates the financial services with technology is considered as a FinTech company. For example, PayPal provides the services of money transaction and online payment using technology which makes PayPal a FinTech company. RegTech refers to applications of innovative technologies that support compliance with regulatory and reporting requirements by regulated financial institutions.

### 18.5. E-KYC

The KYC terminology is an old banking one that refers to knowing a customer's identity, their financial activities and the risks they pose, especially in areas such as money laundering. Today, with the wide usage of mobile devices that have high quality cameras and scanners, coupled with technologies such as document verification, facial recognition and biometrics, e-KYC has become the norm in countries like China.

E-KYC is the expression used to describe the digitalization and electronic and online conception of KYC processes. e-KYC (Electronic Know Your Customer) is the remote, paperless process that minimizes the costs and traditional bureaucracy necessary in KYC processes.

Falsification of identity, signatures and phishing is very common. Specialist businesses dedicated technological compliance solutions have developed completely secure e-KYC processes with zero margins for the commission of these counterfeiting offences and related crime.

The regular e-KYC would be required for agent banking customers who perform transactions with branches as regular customers-

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

**(b) Regular e-KYC:** Where a customer can be on boarded and verifying customer identity electronically, a prescribed digital KYC required be filling in and storing as well as a risk grading exercise required to be documented. Based on the risk grading exercise where customer rated as high risk or some specific scenarios (for example. PEPs), some Enhanced Customer Due Diligence (EDD) required to be undertaken.

#### 18.6.1. Security measures

The financial institution may use additional security measures in the customer onboarding process which may contains checking the phone number by generating PIN codes and other measures as deemed necessary. Additionally, security of the data recorded and preserved under this e-KYC should be maintained properly by the financial institution so that no customer data to be hacked or compromised. This Guideline also suggest to preserved customer data locally hosted server or cloud sever and put in place necessary data protection and data security measures as prescribed by the prudential and self-regulators and/or by the government of Bangladesh.

#### 18.6.2. Objectives of promoting e-KYC

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

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

The data provided by the institutions showed that the e-KYC can save time of on boarding from 4-5 days to 5-6 minutes, cost of customer on boarding and KYC reduces 5-10 times and the growth of business (in particular to the client base) is around 25% compared to the traditional on boarding and KYC mechanism.

### **Conclusion**

Banks or the banking sectors are under the AML obligations because they are at risk of financial crime. AML regulations contain measures that companies must take to detect and prevent financial crimes, and these regulations are determined by AML regulators and are a guide for businesses.

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

## SUSPICIOUS TRANSACTION REPORT (STR) FORM

**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? 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/FDR/loan/other, pls. specify) 4. Nature of ownership:  
(Individual/proprietorship/partnership/company/other, pls. specify) 5. Date of opening/ Transaction: 6. Address: **D. Account holder details:**1. Name of the account holder: 2. Address: 3. Profession: 4. Nationality: 5. Other account(s) number (if any): 6. Other business: 7. Father's name: 8. Mother's name: 9. Date of birth: 10. Place of birth: 11. Passport No. 12. National Identification No.

13. Birth Registration No.	<input type="text"/>
14. TIN:	<input type="text"/>
1. Name of the account holder:	<input type="text"/>
2. Relation with the account holder mention in sl. no. D1	<input type="text"/>
3. Address:	<input type="text"/>
4. Profession:	<input type="text"/>
5. Nationality:	<input type="text"/>
6. Other account(s) number (if any):	<input type="text"/>
7. Other business:	<input type="text"/>
8. Father's name:	<input type="text"/>
9. Mother's Name:	<input type="text"/>
10. Date of birth:	<input type="text"/>
11. Place of birth:	<input type="text"/>
12. Passport No.	<input type="text"/>
13. National Identification No.	<input type="text"/>
14. Birth Registration No.	<input type="text"/>
15. 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 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)

<p><i>(Mention summary of suspicion and consequence of events) [To be filled by the BAMLCO]</i></p>
---

**G. Suspicious Activity Information**

Summary characterization of suspicious activity:

- a.  Corruption and bribery
- b.  Counterfeiting currency
- c.  Counter fitting
- d.  Deeds and documents extortion
- e.  Fraud
- f.  Forgery
- g.  Illegal trade of firearms
- h.  Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication
- i.  Illegal trade in stolen and other goods
- j.  Kidnapping, illegal restrain and hostage taking
- k.  Murder, grievous physical injury
- l.  Trafficking of women and children
- m.  Black marketing
- n.  Smuggling of domestic and foreign currency
- o.  Theft or robbery or dacoity or piracy or hijacking of aircraft
- p.  Human trafficking
- q.  Dowry
- r.  Smuggling and offences related to customs and excise duties
- s.  Tax related offences
- t.  Infringement of intellectual property right
- u.  Terrorism or financing in terrorist activities.
- v.  Adulteration or the manufacture of goods through infringement of title
- w.  Offences relating to the environment
- x.  Sexual exploitation
- y.  Insider trading and market manipulation
- z.  Organized crime, and participation in organized criminal groups
- aa.  Racketeering
- ab.  Other (Please specify)

H. Transaction/Attempted Transaction Details:			
Sl. no	Date	Amount	. Type*

\*Cash/Transfer/Clearing/TT/etc.  
Add paper if necessary

I. Counter Part's Details (Where Applicable)					
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 5. Others

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

## **COMMON INDICATORS OF SUSPICIOUS TRANSACTIONS**

**The following red flags can be used as indicators of Suspicious Transaction or Suspicious Activities:**

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 encashed 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.

## Short KYC for Walk-in/One-off Customers

According to the BFIU circular no-26, date-16.06.2020; as an Walk-in/One-off Customer, you are therefore kindly requested to provide the following details, with appropriate documentary evidence, to make the transaction 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 (Present / Permanent):

### **B. Identification Detail:**

1. NID Card number (verified):
  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

**Bangladesh Krishi Bank**  
 .....**Branch**  
 ..... **Region**

**BAMLCO Nomination Form**

According to the BFIU (Bangladesh Financial Intelligence Unit) circular no-26, Dated-16-06-2020, the following person is being proposed as Branch Anti Money Laundering Compliance Officer (BAMLCO). His/ Her related information is given bellow:

1. Name :  
 2. PF Index :  
 3. Designation :  
 4. Date of join in the Bank :  
 5. Joining Designation :  
 6. Date of join at the present Branch :  
 7. NID Number :  
 8. Date of Birth :  
 9. Mobile Number :  
 :

10. Number of Training obtained regarding AML & CFT related issues:

- i)  
 ii)

11. Select (✓) the subject (s) in which the proposed officer /executive has experience:

- A/C Opening & KYC maintenance       Remittance /Foreign Remittance (inward/outward)  
 CTR analyzing       Clearing, BACH Operation, Cheque Payments, RTGS  
 STR/SAR Reporting       Foreign Exchange & International Trade  
 Credit Operation       BAMLCO

12. Select (✓) the subject (s) in which the proposed officer required to has sufficient knowledge:

- |  | Has obtained             | Has to obtain            |
|--|--------------------------|--------------------------|
| ▪ Money Laundering Prevention Act-2012 (with amendment-2015) | <input type="checkbox"/> | <input type="checkbox"/> |
| ▪ Anti-Terrorism Act-2009 (with amendment-2013)              | <input type="checkbox"/> | <input type="checkbox"/> |
| ▪ AML Policy of Bangladesh Krishi Bank                       | <input type="checkbox"/> | <input type="checkbox"/> |
| ▪ AML related circulars issued by BFIU                       | <input type="checkbox"/> | <input type="checkbox"/> |
| ▪ Aware of Sanction Screening Criteria                       | <input type="checkbox"/> | <input type="checkbox"/> |

Signature:

Name:

Date:

(Seal)

N: B: This Nomination Form must be preserved in the AML/CFT related files no: 4 and one copy of nomination must be sent to the related department.

**Bangladesh Krishi Bank**  
 (Anti Money Laundering Cell)  
 Head Office, 83-85, Motijheel C/A, Dhaka-1000

Phone :  
 Email: dcamlco@krishibank.org.bd

### Account Opening Officer mination Form

According to the BFIU circular no-26, Date-16-06-2020, the following person is being selected as Account opening officer of this Branch. His/Her related information is given bellow:

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. NID Number:
6. Mobile Number:
7. Number of training obtained regarding AML & CFT related issues:
8. Selected officer /executive has experience in –
  - # AC Opening & KYC maintenance
  - # Remittance /Foreign Remittance (Inward, Outward)
  - # Over all General Banking
  - # Credit Operation
  - # Clearing, BACH Operation, Cheque Payments, RTGS
  - # Foreign Exchange & International Trade
9. Whether the nominated officer/ Executive is aware of Sanction Screening Criteria - # YES # NO
10. The Nominated Officer has/has to obtain sufficient knowledge on the following-
  - # Money Laundering Prevention Act-2012 (with amendment-2015)
  - # Anti-Terrorism Act-2009 (with amendment-2013)
  - # AML Policy of Bangladesh Krishi Bank.
  - # AML related Circulars issued by BKB & BFIU (Bangladesh Financial Intelligence Unit).

Signature:  
 Name:  
 Date:  
 (Seal)

N:B: This Nomination Form must be preserved in the AML/CFT related files no:5. And one copy nomination must be sent to this department.

### 1. 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

### 2. 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.

### 3. 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.

### 4. Asia/Pacific Group on Money Laundering (APG)

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

### 5. Egmont Group of Financial Intelligence Units

The Egmont Group of 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.

### 6. 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.

### 7. 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 counterterrorist 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.

## 8. 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.

## 9. 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.

## 10. 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.

## 11. 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.

## 12. 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.

## 13. 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.

## 14. 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.

## 15. 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

## 16. 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.

## 17. 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.

## 18. 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.

## 19. 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.

## 20. 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.

## 21. 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.

## 22. Red Flag

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

## 23. 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.

## 24. 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.

## 25. Structuring

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

## 26. 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.

## 27. 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.