POLICY AND GUIDELINES FOR

MONEY LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT

(September, 2024 Revision, Version–10
Approved on 19 September, 2024)

Published by

Money Laundering & Terrorist Financing Prevention Division
Islami Bank Bangladesh PLC
(Based on Islamic Shari'ah)

Policy and Guidelines for Money Laundering and Terrorist Financing Risk Management

Published by Money Laundering & Terrorist Financing Prevention Division
Islami Bank Bangladesh PLC.

Money Laundering & Terrorist Financing Prevention Division, IBBPLC

Tenth Edition : September, 2024

Ninth Edition : May, 2023

Eighth Edition : June, 2022

Seventh Edition : March, 2021

Sixth Edition : September, 2019

Fifth Edition : November, 2017

Fourth Edition : June, 2016

Third Edition : December, 2013

Second Edition : August, 2010

First Edition : September, 2006

PREAMBLE

An efficient and stable banking system is the prerequisite for overall development of the country. To maintain stability and integrity of international financial system, Financial Action Task Force (FATF), an inter-governmental body, established by G-7 in 1989, has set 40 recommendations for preventing Money Laundering (ML) & Terrorist Financing (TF) & Proliferation Financing.

To oversee the implementation of these recommendations in Asia Pacific region, the Asia/Pacific Group on Money Laundering (APG), FATF-style regional body, was founded in 1997, of which Bangladesh is a founding member. APG as the regional member of FATF evaluates the member countries and publishes their report on the AML & CFT status of the same. Mentionable that APG conducted 3rd round mutual evaluation of Bangladesh in 2016. Besides, Wolfsberg Group (a non-governmental organization & an organizations of a 13 Global Banks founded in 2000), Egmont Group (the association of FIUs of the world founded in 1995), BASEL Committee for Banking Supervisions (founded in 1974), Transparency International (founded in 1993) play a vital role to set the international standard & issue suggestions & recommendations for prevention of ML & TF. Wolfsberg Group issued Correspondent Banking Due Diligence Questionnaires (CBDDQ) & Anti Bribery & Corruption Compliance (ABC) Questionnaires that are two effective tools for evaluation of Banks AML & CFT Programs before establishing Correspondent Banking relationship.

In line with the international initiatives and standards, Bangladesh has also enacted Money Laundering Prevention Act (MLPA), 2012 (Amendment- 2015) and Anti Terrorism Act (ATA), 2009 (as amended in 2012 & 2013) and issued Money Laundering Prevention Rules-2019 & Anti Terrorism Rules-2013. The new Acts & Rules address all the deficiencies identified in the Mutual Evaluation of Bangladesh conducted by APG to determine the extent of its compliance with the global standard. Both the Acts have empowered Bangladesh Financial Intelligence Unit (BFIU) to perform the anchor role in combating ML & TF through issuing guidance and directives for reporting agencies including Commercial Banks, as defined in section 23&24 of MLPA, 2012 (Amendment-2015).

Later on, Bangladesh Financial Intelligence Unit (BFIU) issued different comprehensive circulars incorporating details procedures/ programs/ suggestions for prevention of ML&TF considering the changed pattern in ML&TF regime & complying with international standard like, BFIU Master Circular 10 dated 28.12.2014, BFIU Circular No. 19 issued on 17.09.2017 & lastly, BFIU issued Circular No. 26 on 16 June, 2020. BFIU also issued different guidelines & guidance notes like, Money Laundering & Terrorist Financing Risk Management Guidelines vide BFIU Circular Letter No. 05/2015 dated 10.09.2015, Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations, Guidance on Reporting Suspicious Transaction Report for the Reporting Organizations (January-2019), Guidance Notes on Beneficial Ownership, Guidelines on Electronic Know Your Customer (e-KYC), Guidelines for prevention of Trade Based Money Laundering (2019), etc.

Islami Bank Bangladesh PLC, in compliance with the regulatory requirement and maintaining of international standard, introduced Anti Money Laundering Policy for 1st time in September,

2006. Thereafter, the AML Policy of IBBPLC was revised for 4th time in June 2016 changing its name as "Policy and guidelines for Money Laundering and Terrorist Financing Risk Management of IBBPLC" in accordance with the Money Laundering & Terrorist Financing Risk Management Guidelines issued by BFIU in 2015.

Meanwhile, pattern of Money Laundering & Terrorist Financing has changed in many folds and evolve time to time. Due to prevent the changed pattern of Money Laundering & Terrorist Financing, provide priority & emphasis in some banking business by international standard setter, change in volume, nature of the products/ services as well as in the Account Opening Procedures of IBBPLC (AOF, KYC & Risk Grading, etc.), AML Policy of IBBPLC has further been revisited and modified. Board of Directors in its 342nd meeting held on 19 September, 2024 approved the change & modification of AML Policy with immediate effect. All concerned shall require to abide by the same compulsorily. The AML Policy shall be reviewed at least once in a year on getting due approval from the Board of Directors of the Bank.

TABLE OF CONTENTS

ACRONYM

A&ID	Audit & Inspection Division
ABC	Anti Bribery and Corruption Compliance
ACC	Anti Corruption Commission
ADD	Alternative Delivery Division
AML	Anti Money Laundering
APG	Asia Pacific Group
ARS	Alternative Remittance System
ATA	Anti Terrorism Act
ATM	Automatic Teller Machine
ATO	Anti Terrorism Ordinance
ATR	Anti Terrorism Rule
AWCA	Al-Wadeah Current Account
BACH	Bangladesh Automated Clearing House
BAMLCO	Branch Anti Money Laundering Compliance Officer
BB	Bangladesh Bank
BCU	Branch Compliance Unit
BEFTN	Bangladesh Electronic Funds Transfer Network
BFIU	Bangladesh Financial Intelligence Unit
BFIU	Bangladesh Financial Intelligence Unit
BGMEA	Bangladesh Garment Manufacturers and Exporters Association
BIDA	Bangladesh Investment Development Authority
BJMA	Bangladesh Jute Mills Association
BKMEA	Bangladesh Knitwear Manufacturers and Exporters Association
BM&DC	Bangladesh Medical & Dental Council
CAMLCO	Chief Anti Money Laundering Compliance Officer
CCC	Central Compliance Committee
CDD	Customer Due Diligence
CFT	Combating Financing of Terrorism
CTR	Cash Transaction Reporting
DCAMLCO	Deputy Chief Anti Money Laundering Compliance Officer
DNFBPs	Designated Non-Financial Businesses and Professions
DUDAR	‘Durniti Domon Commission’ refer to ACC.
EDD	Enhanced Due Diligence
e-KYC	Electronic Know Your Customer
E-TIN	Electronic Tax Identification Number
ETP	Effluent Treatment Plan
EU	European Union
FATF	Financial Action Taskforce
FIU	Financial Intelligence Unit
FT	Financing of Terrorism
HRW	Human Resources Wing

IBBPLC	Islami Bank Bangladesh PLC
IBTRA	Islami Bank Training & Research Academy
ICCW	Internal Control & Compliance Wing
IPs	Influential Persons
IT	Information Technology
KYC	Know Your Customer
KYCC	Know Your Customers' Customer
KYE	Know Your Employee
MER	Mutual Evaluation Report
ML	Money Laundering
MLPA	Money Laundering Prevention Act
MLPO	Money Laundering Prevention Ordinance
MLPR	Money Laundering Prevention Rule
MLTFPD	Money Laundering & Terrorist Financing Prevention Division
MSA	Mudaraba Savings Account
NBR	National Bureau of Revenue
NGO	Non Government Organization
NID	National Identity
NPO	Non Profit Organization
OECD	Organization for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
OFSI	Office of Financial Sanctions Implementation
PEPs	Politically Exposed Persons
PF	Proliferation Financing
PIN	Personal Identification Number
RDD	Rural Development Division
REHAB	Real Estate and Housing Association of Bangladesh
RO-FI	Reporting Organization-Financial Institution
SAR	Suspicious Activity Reporting
SOP	Standard Operating Procedures
STR	Suspicious Transaction Reporting
TBML	Trade Based Money Laundering
TIN	Tax Identification Number
TM	Transaction Monitoring
ToT	Trainers of Trainee
TP	Transaction Profile
UAMLCO	Unit Anti Money Laundering Compliance Officer
UN	United Nations
UNSCR	United Nations Security Council Resolution
WTP	Water Treatment Plan
ZAMLCO	Zonal Anti Money Laundering Compliance Officer
ZCU	Zonal Compliance Unit

AML & CFT Policy Statement

Islami Bank Bangladesh PLC (IBBPLC) pays special attention on Anti-Money Laundering and Combating Financing of Terrorism. IBBPLC has set a comprehensive AML & CFT policy and procedures, which has been approved by the Board of Directors and implemented accordingly. These policy and procedures comply with the relevant acts, orders & the Circulars of the appropriate regulators.

This policy statement is a brief description of general principles to which IBBPLC will adhere to, as follows:

1) To comply with applicable anti-money laundering and combating the financing of terrorism laws and regulations as established by the Central Bank of Bangladesh and respective Central Banks in each jurisdiction that is in accordance with the recommendation of the Financial Action Task Force (FATF) on Money Laundering and Terrorist Financing.
2) To maintain a written AML and CFT policy and related procedures, and apply it to all business units including Sub-Branches & Agent Banking Outlets.
3) To obtain all account opening documentation requirements as per laws.
4) To obtain necessary documents while conducting transaction for Non-Account Holders.
5) To apply the Risk Based Approach & Framework in dealing with the AML & CFT activities as per the set policies & procedures of the Bank.
6) To apply appropriate screening process while on boarding the customers.
7) To risk assessment, categorization & scoring of the products, customers etc. as per the set procedures.
8) To apply Enhanced due diligence for high-risk customers.
9) IBBPLC will not conduct business with Shell Bank. In addition to this, IBBPLC won't offer services of opening anonymous accounts.
10) IBBPLC shall maintain correspondent banking relationship with a number of banks and comply with the due processes like conducting CDD, EDD & KYC renewal, adverse media screening etc. for maintaining such relationship.
11) To retain all the customer related documents for a period specified as per local laws in each jurisdiction.
12) To monitor all the transactions systematically to identify the suspicious activity and transactions following the set norms and using the technical tools, where applicable.
13) To report all identified suspicious activities to the extent that it can do so under all applicable foreign and domestic laws.
14) To cooperate fully with law enforcement and regulatory agencies to the extent that it can do so under all applicable foreign and domestic laws.
15) To train up the staff on AML & CFT policies and new AML & CFT laws and regulations.
16) To maintain a system of internal controls to ensure ongoing AML & CFT compliance by a designated person(s) and take appropriate action, once suspicious activity is detected, a proper and thorough process for filing Suspicious Transaction Report (STR) is followed as per the requirements of Central Bank and applicable laws.
17) To comply with the circulars/guidelines/guidance notes issued by the Central Bank, BFIU and other Regulatory Authorities and as a part of the Risk Management, update the same from time to time (at least once in a year) incorporating all the changes brought into the AML & CFT compliance program during the interim period.

CHAPTER – I

Introduction

1.1 Preamble

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

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

The process of money laundering and terrorist financing (ML/TF) is very dynamic and ever evolving. The money launderers and terrorist financers 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 Local & international initiatives, Bangladesh has also acted on many fronts. Islami Bank Bangladesh PLC is an important partner in such emergent initiatives.

1.2 Scope of Application

These guidelines pertain to all the organs & branches already functioning or the future organs and branches including Sub-Branches & Agent Banking Outlets of the Bank expected to be accommodated by the Competent Authority from time to time. This Policy also shall be applied in the foreign Branches/ Subsidiaries complying all the Acts/ Rules/ Regulations of the Foreign Country where it is doing business. The risk management process described in these guidelines is supplementary to the standards set by the legislative requirements and previously issued manuals, guidelines and policies etc. This document does not replace or supersede them.

1.3 Objectives of the Guideline

i) To enable IBBPLC to ensure that only legitimate and bona fide customers are accepted.

ii) To aid IBBPLC in verifying the identity of customers using reliable and independent documentation.

iii) To enable IBBPLC to monitor customers' financial dealings. This would help the bank to mitigate the risk of its channels being used for Money Laundering.

iv) To enable IBBPLC in implementing processes to effectively manage the risks posed by customers trying to misuse facilities.

v) To prevent criminal elements from using IBBPLC for money laundering and terrorist financing activities.

vi) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws and regulations, and procedural guidelines.

vii) To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML/CFT procedures.

1.4 Definition of Money Laundering

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

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

The Financial Action Task Force (FATF), which is recognized as the international standard setter for anti-money laundering (AML) efforts, defines the term "money laundering" as "the processing of criminal proceeds to disguise its illegal origin" in order to "legitimize" the ill-gotten gains of crime.

1.5 Stages of Money Laundering

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

- Placement – Placement is the first stage of the money laundering process, in which illegal funds or assets are brought first into the financial system directly or indirectly.
- Layering - Layering is the second stage of the money laundering process, in which illegal funds or assets are moved, dispersed and disguised to conceal their origin. Funds can be hidden in the financial system through a web of complicated transactions.
- Integration - Integration is the third stage of the money laundering process, in which the illegal funds or assets are successfully cleansed and appeared legitimate in the financial system.

1.6 Definition of Terrorist Financing

Terrorist financing can simply be defined as financial support, in any form, to 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:

'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 as depicted in the International Convention for the Suppression of the Financing of Terrorism adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December, 1999; or

b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

1.7 The Link between Money Laundering and Terrorist Financing

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

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

1.8 AML & CFT Risk Associated in different Banking Products & their mitigation

a) Investment backed Money Laundering

Process to launder illegal fund (fund from smuggling, gambling, fraud & forgery, bribery, arm trafficking, etc) through the investment/ credit/ loan facility to the white fund is called credit backed money laundering with the intension to hide its origin or source.

Process of Investment backed Money Laundering

i) Taking investment for different purposes and adjust the same before maturity than the schedule time or adjust in lum-sum or as per schedule with the black fund.
ii) Illegal fund held with the offshore unit and issue/ arrange investment to the local business of the launderer. In this way the money not only returning home but also in a completely non-taxable form. While the investment customers adjust the loan/ investment, the same return to the tax heaven area.
iii) Launderers establish anonymous companies in countries where the right to secrecy is guaranteed. They are then able to grant themselves make investment out of the laundered money in the course of a future legal transaction. Furthermore, to increase their profits, they will also claim tax relief on the loan repayments and charge themselves interest on the loan.

iv) Repatriation can be done through investment back method using value of the account as collateral. Ironically, launderers often gain tax advantage too for their apparently legal operations, using the interest expense from the investments as tax deductions.

v) Credit Card is an important vehicle to launder black fund. Launders deposit fund in advance in their Credit Card Account. Therefore, they withdraw the same gradually to hide the sources of fund.

Responsibilities of IBBPLC:

- Ensure Customer Due Diligence (CDD) & Enhanced Due Diligence (EDD) as per the risk grading of the customers.
- Constant Monitoring of the Investment deals and its nature of adjustment as well as the customers' nature to adjust the deals.
- Monitoring shall also be done for deployment of investment fund according to nature of business and sources of fund used to deploy the fund.
- Offshore Unit shall also monitor the fund circulation of the customers and if any suspicious nature is detected in the customer's dealings, reporting shall be done as STR/ SAR.
- If any suspicious nature is detected in the customer's dealings, reporting shall be done to ML & TF Prevention Division as STR/ SAR as per Guidelines for reporting of Suspicious Transactions Reporting issued by BFIU. Confidentiality of the issue as per rules of Tipping off shall be maintained**.**

b) FinTech Services

FinTech provides an avenue for the customers for proving services by the Banks/ FIs through the technology in an easiest way. It includes, Internet Banking, Card Banking, Booth Banking, etc. Customer do not need to contact to the Bank physically for getting services, rather they can make transactions at their home or business center or from the booths/ agents. Therefore, FinTech is vulnerable in terms of money laundering and terrorist financing issues.

Responsibilities of IBBPLC

- Conduct Risk Grading of the customers as per the Risk Based Approach of the Bank
- Ensure Customer Due Diligence as per Risk of the Customers
- Ensure confidentiality of the customers security PIN/ Key/others
- Conduct Monitoring of transactions
- Screening of Sanctions, Local Black List & Adverse Media Report, etc.
- File STR/ SAR if any suspicious transaction is detected.

c) Virtual Currency:

IBBPLC does not offer any virtual currency business. Besides, IBBPLC shall take precautionary measure and ensure Enhanced Due Diligence for making Correspondent Banking relationship/ remittance drawing arrangement with any banks/ financial institutions those offers virtual currency business.

A virtual or digital currency (VC) is a medium of exchange that operates in the digital space such as Bitcoin. It can be firstly of 02 (two) types-

- Centralized: Centralized virtual currency has an administrator & repository.

- Decentralized: Decentralized virtual currency has no repository and administrator but works as peer to peer media of exchange without any need for an intermediary.

Further the virtual currency can be divided into following 02 (two) categories-

- Convertible: Convertible virtual currency can be converted into fiat currency or national currency of a jurisdiction.
- Nonconvertible: Non convertible virtual currency can not be converted into fiat currency but can be converted into another virtual currency as a future contract.

Vulnerability of Virtual Currency:

Decentralized systems of virtual currency are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body and no AML software currently available to monitor and identify suspicious transaction patterns.

Bangladesh Bank vide a notice advised the peoples to refrain themselves to transact in Virtual Currency (crypto currency like Bitcoin, Etherum, Ripple, Litecoin, etc), help in any of this transaction and its publicity

d) Whistle blowing:

Definition:

A whistle blowing is the activity or process to disseminate information to the appropriate authority of any illegal activity or activity which is/was harmful or which may cause in the institution's financial, reputational, legal loss to secure the institution and not for whistle blowers personal interest or for the interest of any individual or entity.

Scope of Reporting:

Any irregularity and mis-conduct, including but not limited to the following activities:

a. Fraud or Dishonesty
b. Breaches of Policies, Procedures and applicable Laws and Regulations
c. Bribery, Corruption
d. Abuse of Power
e. Theft or Embezzlement
f. Insider Trading
g. Misuse of Bank's Property and Information
h. Harassment, Sexual Harassment and/or
i. Intimidation

Guidelines of reporting:

- Reporting shall be done for the Banks interest only not for the interest of the whistleblower or for the interest of any individual/ entity.

- Reporting shall be done firstly to the immediate reporting boss or the Officials/ Executive who will be assigned to deal in such process through mail/ phone or any other means that shall be instructed from time to time maintaining the confidentiality.
- The whistleblower is responsible to ensure that the disclosure is made in good faith, free from malicious intent, and is not for personal gains.
- This procedure strictly prohibits frivolous, bogus disclosure for personal gain or with personal agenda.
- If the subsequent investigation reveals that the disclosure was made with malicious intent, appropriate action can be taken against the whistleblower as per rules of Bank.
- Bank shall accord protection of confidentiality to the whistleblower to the extent reasonably consistent with the need to conduct an adequate investigation.
- Bank shall take all reasonable steps to protect the whistleblower against any discrimination, retaliation or harassment, corresponding to its internal policies and scope under its purview and jurisdiction as per instruction of regulatory authority.

CHAPTER - 2

International, National & IBBPLC Initiatives on AML and CFT

In response to the growing concern about money laundering and terrorist activities, the international community has acted on many fronts. This part of this Guideline Notes discusses the various international organizations that are viewed as the international standard setters. It further describes the documents and instrumentalities that have been developed for anti-money laundering (AML) and combating the financing of terrorism (CFT) purposes. In the line of the International Initiatives Bangladesh has also furnished a frame work and chalked out different plan & procedure for AML & CFT. IBBPLC itself as a reporting organization also has furnished a frame work and chalked out different programs complying the international & national AML & CFT rules/ regulations set out by national & international organizations for the purpose.

A. International Initiatives

i) The United Nations

The United Nations (UN) was the first international organization to undertake significant action to fight money laundering on a truly world-wide basis. Some steps of United Nations against AML & CFT are mentioned below:

The Vienna Convention

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

The Palermo Convention

Palermo Convention has come into force from 29th September 2003, having been signed by 147 countries and ratified by 82 countries 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 i) Criminalize money laundering and include all serious crimes as predicate offenses of money laundering ii) Establish regulatory regimes to deter and detect all forms of money laundering iii) Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities & iv) Promote international cooperation.

International Convention for the Suppression of the Financing of Terrorism

The convention came into force on April 10, 2002, with 132 countries signing the convention and 112 countries which ratify the member countries 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.

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).

Security Council Resolution 1373

The UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to i) deny all forms of support for terrorist groups ii) suppress the provision of safe haven or support for terrorist iii) prohibit active or passive assistance to terrorists and iv) cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.

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.

ii) 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 34 countries and territories and two regional organizations. For prevention of ML & combating of TF, FATF set out 40 recommendations, a pin picture of the same is mentioned below:

Summary of 40 recommendations of FATF

Group	Topic	Recommendations
A	AML/CFT Policies and Coordination	1-2
B	Money Laundering and Confiscation	3-4
C	Terrorist Financing and Financing of Proliferation	5-8
D	Preventive Measures	9-23
E	Transparency and Beneficial Ownership of Legal Persons and Arrangements	24-25
F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	26-35
G	International Co-operation	36-40

iii) The Basel Committee on Banking Supervision

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

iv) 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 with the purpose is to provide a forum for FIUs to improve support for each of their national AML programs and to coordinate AML initiatives. Bangladesh got membership in the Egmont Group in the year 2013.

v) Asia Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 40 members and a number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units.

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

vi) Wolfsburg Group

The Wolfsburg Group is an association of 13 global banks comprising of Banco Santander, Bank of America, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, MUFG Bank, Société Générale, Standard Chartered Bank, UBS.

The aim of the Wolfsburg Group is to develop financial services industry standards and guidance related to Know Your Customer, Anti-Money Laundering and Counter-Terrorist Financing policies. The Wolfsburg Group, which has no enforcement powers, issued the guidelines to manage its members’ own risks, to help make sound decisions about clients and to protect their operations from criminal abuse. The Group first came together in 2000 at the Wolfsburg castle in Switzerland, accompanied by representatives of Transparency International, to draft anti-money laundering guidelines for private banking that, when implemented, would mark an unprecedented private-sector assault on the laundering of corruption proceeds.

Wolfsburg Group among others introduced Questionnaire for making correspondent banking relationship to know about the nature of business of the correspondent & respondent bank

and Anti Bribery & Corruption (ABC) Policy to prevent the bribery and corruption over the bank.

B. National Initiatives

In line with international efforts, Bangladesh has also taken many initiatives to prevent money laundering and combating financing of terrorism and proliferation of weapons of mass destructions considering their severe effects on the country. Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997.

i) Legal Framework

Bangladesh is the first country in the South Asia that has enacted Money Laundering Prevention Act (MLPA) in 2002. To address the shortcomings of the MLPA, 2002 and to meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER), Bangladesh has again enacted Money Laundering Prevention Act in February, 2012 repealing MLPA, 2009. Money Laundering Prevention Rules, 2019 has been framed for effective implementation of the act. Money Laundering Prevention Act further has been modified in 2015 under title "Money Laundering Prevention (Amendment) Act-2015 complying with the international standard.

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

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

ii) Bangladesh Financial Intelligence Unit

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

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

BFIU as the Regulatory Authority for AML & CFT compliance provides different guidelines, instructions to maintain international standard/ best practices in the compliance Program by issuing different Circulars time to time.

iii) 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.

C. IBBPLC Initiatives:

i) Compliance Program

The compliance program of IBBPLC has been chalked out covering all related areas of ML & TF and the same may be redesigned & restructured considering the size and range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by IBBPLC. The program includes-

Components of AML & CFT Compliance Program

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

ii) Compliance Structure

Compliance structure of IBBPLC is an organizational setup that deals with AML & CFT compliance of the same and the reporting procedure. This includes-

- Central Compliance Committee (CCC),
- Chief Anti-Money Laundering Compliance Officer (CAMLCO),
- Zonal Anti Money Laundering Compliance Officer (ZAMLCO)
- Branch Anti-Money Laundering Compliance Officer (BAMLCO).

iii) Customer Due Diligence (CDD)

The CDD program of IBBPLC should include following minimum compulsory elements:

- Know Your Customer (KYC)
- Transaction Profile (TP)
- Definition & Acceptance of the Customer

- Risk Grading of Customer
- Transaction Monitoring
- Investigating unusual transaction
- Reporting of CTR
- Filing of STR
- Record Keeping.

CHAPTER –3

Compliance Program

The compliance program of IBBPLC has been chalked out covering all related areas of ML & TF and the same may be redesigned & restructured considering the size and range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by IBBPLC. The program includes-

3.1 Components of AML & CFT Compliance Program

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

3.2 Development of AML & CFT Compliance Program

In developing the AML & CFT compliance program, IBBPLC considered all relevant laws, regulations, guidelines relating to AML & CFT and also the practices related to corporate governance. In drafting the compliance program, IBBPLC has involved all its relevant Wings/Divisions/Departments like Operations Wing (general banking), Investment Wing, International Banking Wing (foreign exchange), Information & Communication Technology Wing (information technology, Alternative Delivery Channels), Internal Control & Compliance Wing and above all Central Compliance **Committee (CCC)**. Their involvement has been documented or reflected in the compliance program. Proper attention is given to the size and range of activities, complexity of operations, customer base, use of technology, diversity of product, delivery channel, external linkage, geographic location and the output of ML & TF risk assessment. The Program will be reorganized, restructured, amended and changed from time to time depending on regulatory desires and changing environment.

3.3 Senior Management Role

For the purposes of preventing ML, TF & PF, senior management includes members of the Board of Directors of IBBPLC, the Chief Executive Officer (CEO) or the Managing Director (MD) and the others senior Executives of the bank and their role in this regard shall be as under:

Role of Senior Management

Board of Directors of IBBPLC shall-

- ❖ approve Bank's AML & CFT Policy and Guidelines
- ❖ approve AML & CFT compliance program and ensure its implementation;
- ❖ issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- ❖ take reasonable measures through analyzing self assessment report and independent testing report summary;
- ❖ understand ML & TF risk of the bank, take measures to mitigate those risk;
- ❖ get the CEO or/and MD issue statement of commitment to prevent ML, TF & PF in the bank;
- ❖ Ensure compliance of AML & CFT program;
- ❖ shall develop risk appetite commensurating the risk assessment report and take steps to raise capital where necessary to mitigate the risk.
- ❖ Allocate enough human and other logistics for effective implementation of AML & CFT compliance program.

Senior management of IBBPLC shall convey a clear signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of its AML & CFT policy, IBBPLC shall communicate clearly to all employees on an annual basis by a statement from the CEO or MD that clearly sets forth its policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement shall evidence the strong commitment of IBBPLC to comply with all laws and regulations designed to combat money laundering and terrorist financing.

Besides, the Managing Director & CEO of IBBPLC shall furnish/ issue a commitment to all Employees of the Bank at the very outset of each year including **directives to implement commitments and ensure the implementation of the same.** The Commitment & directives shall include among others the followings:

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

The Managing Director & CEO of the Bank shall also ensure the implementation of the directives on the above issues.

Senior management of IBBPLC will ensure that the policy, process and procedures towards AML & CFT are appropriately designed and implemented, and are effectively operated to minimize the risk of the bank being used in connection with ML & TF.

Senior management of IBBPLC will ensure the adequacy of the human and other resources devoted to AML & CFT. Moreover, they need to ensure the autonomy of the designated officials related to AML & CFT. Senior management shall take the report from the **Central Compliance Committee (CCC**) into consideration which will assess the operation and

effectiveness of the bank's systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner.

HR Policy of IBBPLC shall be modified for ensuring the compliance of AML & CFT measures by the employees of the bank which shall cover the followings:

- Proper administrative action for non-compliance of AML & CFT measures;
- Proper weight shall be given in the annual performance evaluation of employees for extra ordinary preventive action vis a vis for non-compliance;
- Written procedure to recover the fined amount from the concerned employee if the fine imposed on Bank/ Employee by the BFIU;
- shall include a comprehensive KYE process;
- Other disciplinary measures as per HR Policy of the Bank shall be taken in case of non-compliance by the same.

Senior management of IBBPLC will be responsive of the level of money laundering and terrorist financing risk when the bank is exposed to and take a view whether the bank is equipped to mitigate that risk effectively; this implies that decisions on entering or maintaining high-risk business relationships must be escalated to senior management.

3.4 Policies and Procedures

The AML & CFT Policy of IBBPLC has been tailored on the basis of assessment of the money laundering and terrorist financing risks, taking into account the bank's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering and terrorist financing.

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

It also includes a description of the roles of the AML&CFT Compliance Officers(s)/Unit and other appropriate personnel will play in monitoring compliance with and effectiveness of AML&CFT policies and procedures. The program continuity shall be going on at its own pace despite changes in management or employee composition or structure.

The AML & CFT policies of IBBPLC shall be reviewed time to time and updated as & when necessary and at least annually as a part of the Risk Management based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing AML&CFT related rules and regulations or business.

In addition, the policy emphasizes the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and shall set forth the consequence of non-compliance with the applicable laws and IBBPLC's HR Policy including the criminal, civil and disciplinary penalties.

This policy includes the following 4 (four) key elements;

- ❖ High level summary of key controls and Operational controls;
- ❖ Objective of the policy (e.g. to protect the reputation of the institution);
- ❖ Scope of the policy (A statement confirming that the AML/CFT policy applies to all areas of the business);
- ❖ Waivers and exceptions- procedures for obtaining exemptions from any aspects of the policy shall be carefully controlled;

3.4.1 Procedures

The standard operating procedures are often designed at a lower level in the organization and modified as needed to reflect the changes in products, personnel and promotions, and other day to day operating procedures. The procedure is to be more detailed than policies. Standard operating procedures translate policy into an acceptable and working practice. In addition to policies and procedures, there shall also be a process to support and facilitate effective implementation of procedures and that shall be reviewed and updated regularly. However, the procedural instructions of IBBPLC regarding AML & CFT shall be issued through different operational manuals, instruction circulars, circular letters, etc.

3.5 Customer Acceptance Policy

IBBPLC has a separate Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The primary objectives of the Customer Acceptance Policy are –

1. to manage any risk that the services provided by the Bank may be exposed to;

2. to prevent the Bank from being used, intentionally or unintentionally, for ML/TF purposes; and

3. to identify customers who are likely to pose a higher than average risk.

While crafting Customer Acceptance Policy of IBBPLC, a great care has been taken to strike the appropriate balance between risk aversion regarding criminal activities and the willingness to take on new clients. As such, IBBPLC's Customer Acceptance Policy has been designed in such a manner wherein neither the socially disadvantaged are excluded nor general public are restricted to the access of financial services.

Customer acceptance policy of IBBPLC includes-

- ❖ No account in anonymous or fictitious name or account only with numbers shall be opened;
- ❖ No banking relationship shall be established with a Shell Bank; and
- ❖ No account in the name of any person or entity listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance adopted under Chapter VII of the Charter of UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government shall be opened or operated.
- ❖ Individuals/ Entities rejected from being accepted as customers of IBBPLC shall be properly recorded in an automated manner.

A separate chapter on Customer Acceptance Policy of IBBPLC has been annexed in this Guideline.

3.6 Customer Rejection Policy

In addition to the customer acceptance policy, IBBPLC has adopted a customer rejection policy wherein the causes and procedures of customer rejection are depicted.

3.7 Standard Operating Procedures (SOPs)

Standard Operating Procedures (SOPs) is the set rules, procedures or guidelines to perform different Banking activities in IBBPLC in effective and efficient manner to minimize the AML & CFT risks of the Bank. SOPs of IBBPLC vetted by Kroll Advisory Solution, a renowned consultancy firm on AML & CFT, shall be complied in every dealing of Banking activities with utmost due responsibility by the Employees of Bank.

3.8 Onsite and Offsite Supervision:

To trigger the AML & CFT compliance program in every unit of IBBPLC and keep those in the right track, ML & TF Prevention Division of IBBPLC shall conduct onsite & offsite supervision in each year as per decision of the Competent Authority of the Bank. Summary of the findings with recommendations against those shall be placed before the Competent Authority of the Bank through proper channel.

3.9 Introduction of Electronic Know Your Customer Program (e-KYC):

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

An electronic customer on-boarding involves multiple activities. An efficient customer on-boarding starts from clients' identity information and can be segmented into following steps:

a. Data capture and generation;
b. Identity verification;
c. Sanction and other screening;
d. Account opening;
e. Customer profiling (e-KYC Profile); and
f. Customer risk grading (as applicable).

Guidelines on Electronic Know Your Customer **(e-**KYC) issued by BFIU shall be complied with to implement e-KYC program in IBBPLC.

CHAPTER –4

Compliance Structure

Compliance structure of IBBPLC is an organizational setup that deals with AML & CFT compliance of the same and the reporting procedure. This includes-

- Central Compliance Committee (CCC),
- Chief Anti-Money Laundering Compliance Officer (CAMLCO),
- Deputy Chief Anti-Money Laundering Compliance Officer (D-CAMLCO),
- Zonal Anti Money Laundering Compliance Officer (ZAMLCO),
- Branch Anti-Money Laundering Compliance Officer (BAMLCO).

4.1 Central Compliance Committee (CCC).

The Central Compliance Committee (CCC) of IBBPLC shall be headed by a high official, who will be known as the Chief Anti Money Laundering Compliance Officer (CAMLCO). In this case, 'High official' will be considered as an official up to 2 (two) steps below of the Managing Director/ Chief Executive Officer. IBBPLC shall inform of any change of the CAMLCO to BFIU without delay. It will also ensure the involvement of CAMLCO regarding AML & CFT activities in case of assigning him to other duties of the bank.

IBBPLC will also nominate one **Deputy Anti-Money Laundering Compliance Officer (D-CAMLCO) not below the rank of Senior Vice President.** The CAMLCO and D-CAMLCO have to have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing Money Laundering & Terrorist Financing.

Under the guidance of the Central Compliance Committee (CCC), Money Laundering and Terrorist Financing Prevention Division shall issue instructions for the branches, where obtaining KYC, transaction monitoring system, internal control system, policies and procedures will be included to prevent Money Laundering and Terrorist Financing.

4.1.1(a) Formation of CCC

CCC shall be formed consisting of at least 7 (Seven) members wherein Heads / Senior officials from different Wings/Divisions/ Departments of Head Office (like Human Resources Wing, ICT Wing, Retail Investment Wing, Corporate Investment Wing, International Banking Wing, Branches Control Division, Card Division) etc along with CAMLCO & DCAMLO will be included . The members of the CCC need to have enough knowledge on AML & CFT measures of Bangladesh including MLPA, ATA and the related rules and instructions issued by BFIU or Bangladesh Bank. There shall be a Board approved separate Terms of Reference (ToR) of CCC for smooth functioning of the same.

4.1.1(b) Holding of Meeting by CCC

At least 04 meetings of CCC shall be conducted on quarterly basis in a year. But if feels required, CCC may call any number of meetings at any time.

4.1.2 Authorities and Responsibilities of the CCC

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

- develop bank's policy, procedure and strategies in preventing ML, TF & PF;
- coordinate bank's 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 **and submit a copy of the same to BFIU within 02 months from the end of the respective period;**

For shouldering these responsibilities, Bank authority of IBBPLC has given 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.

4.1.3 Separation of CCC from Conflicting Organs

For ensuring the independent audit function in the bank, CCC shall be completely separated from Internal Control & Compliance Wing. Either the Division or unit may perform same job but in different and independent way. In this regard, ICCW shall also examine the performance of CCC and the bank's AML & CFT compliance program. To ensure this autonomy, there shall not be any member from IC&CW to CCC and vis-a-vis; but there shall be enough co-ordination and co-operation in performing their responsibility and information exchange. There shall not be any impediment to transfer employee from IC&CW to CCC and vis-à-vis 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 "Money Laundering & Terrorist Financing Prevention Division" headed by the D-CAMLCO shall be placed under the Central Compliance Committee (CCC) to provide all sorts of secretarial assistance to the CCC with sufficient manpower & logistic supports considering the number of branches, expansion & size of business, number of customers & corporate risk for ensuring effective AML & CFT compliance of the Bank. There shall be a Board approved separate Terms of Reference (ToR) of Money Laundering & Terrorist Financing Prevention Division for smooth functioning of the same.

4.2 Chief Anti Money Laundering Compliance Officer (CAMLCO)

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

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

All staffs engaged in the bank at all levels shall be made aware of the identity of the CAMLCO, his deputy and the staff and branch/unit level AML&CFT compliance officers, and the procedure to follow when making a suspicious transaction/activity report. All relevant staffs must be aware of the chain through which suspicious transaction/activity reports shall be passed to the CAMLCO.

The CAMLCO will establish the basis on which a risk-based approach to the prevention of money laundering/terrorist financing is put into practice.

4.2.1 Authorities and Responsibilities of CAMLCO

Authorities-

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

Responsibilities-

- CAMLCO must ensure overall AML&CFT compliance of the bank;
- CAMLCO shall be liable to MD & CEO for proper functioning of CCC;
- CAMLCO shall review and update ML & TF risk assessment of the bank;
- ensure that corrective actions have been taken by the bank to address the deficiency identified by the BFIU or Bangladesh Bank.

4.3 Zonal Anti Money Laundering Compliance Officer (ZAMLCO)

A high officials experienced in overall banking operations shall be nominated as the Zonal Anti Money Laundering Compliance Officer (ZAMLCO). ZAMLCO 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, etc. A clear job description and responsibility of ZAMLCO shall be mentioned in his/her appointment letter. ZAMLCO shall perform his duties among others the followings:

- Communicate and follow-up activities of the BAMLCOs & BCU
- Motivate the BAMLCOs to submit STR proactively
- Take initiative for updating KYC/TP/Risk grading of all accounts
- Activate & operate ZCU properly & efficiently
- Escalate any true match hit of UN sanction screening to CAMLCO
- Any other work as and when assigned by the Competent Authority.

4.4 Branch Anti Money Laundering Compliance Officer (BAMLCO)

The Manager, Manager Operations 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. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her appointment letter.

BAMLCO shall arrange AML & CFT (BCU) 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,
- Training,
- Implementation of Local Sanction List alongwith resolutions of UN Security Council.
- Activities regarding Self Assessment Reporting
- Sending Minutes of BCU Meeting to Money Laundering & Terrorist Financing Prevention Division on quarterly basis.

4.4.1 Authorities and Responsibilities of BAMLCO

For preventing ML, TF & PF in the branch, the BAMLCO shall perform among others the following responsibilities:

- ensure that the KYC of all customers have been done properly and for the new customer KYC is being done properly;
- ensure that the UN Security Council and domestic sanction list is being checked properly before establishing business relationship with a customers or before providing any banking facilities to the existing customers both local and international transaction.
- 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. IBBPLC 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 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 Money Laundering & Terrorist Financing Prevention Division;
- accumulate the training records of branch officials and take initiatives including reporting to Money Laundering & Terrorist Financing Prevention Division, Central Compliance Committee (CCC), Human Resources Wing (HRW) and Islami Bank Training & Research Academy (IBTRA);

- ensure all the required information and document are submitted properly to Money Laundering & Terrorist Financing Prevention Division and any freeze order or stop payment order are implemented properly;
- follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO shall make an STR/SAR;
- ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements;
- ensure that corrective actions have been taken by the branch to address the deficiency identified by the BFIU, or IBBPLC's internal/ external audit/ visit.

4.5 Internal Control and Compliance

Internal Control and Compliance Wing shall have an important role for ensuring proper implementation of IBBPLC's AML & CFT Compliance Program. IBBPLC will ensure that ICCW is equipped with enough manpower and autonomy to look after the prevention of ML&TF. The ICCW 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, IBBPLC shall assess the program regularly and look for new risk factors.

IBBPLC's 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 IBBPLC 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 tellers' cash proof sheets;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned unit/ person;
- examine that corrective actions have been taken on deficiency identified by the BFIU or IBBPLC'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 ongoing education, training and compliance,
    - employee accountability for ensuring AML&CFT compliance,
    - comprehensiveness of training, in view of specific risks of individual business lines,
    - training of personnel from all applicable areas of the bank,

- frequency of training,
- coverage of bank policies, procedures, processes and new rules and regulations,
- coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
- penalties for noncompliance and regulatory requirements.

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

1) Audit & Inspection Division (A&ID) shall assess the Self-assessment received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the Money Laundering & Terrorist Financing Prevention Division.
2) While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the A&ID 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 A&ID 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.
3) The A&ID shall send a copy of the report with the rating of the branches inspected/audited by the A&ID to the Money Laundering & Terrorist Financing Prevention Division of the bank.
4) The A&ID shall conduct inspection/audit activities on at least 10% cash points/m-Cash agents on a yearly basis to review the compliance status of AML and CFT activities related matters of the cash points/m-Cash agents.

4.6 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 June, 2020.

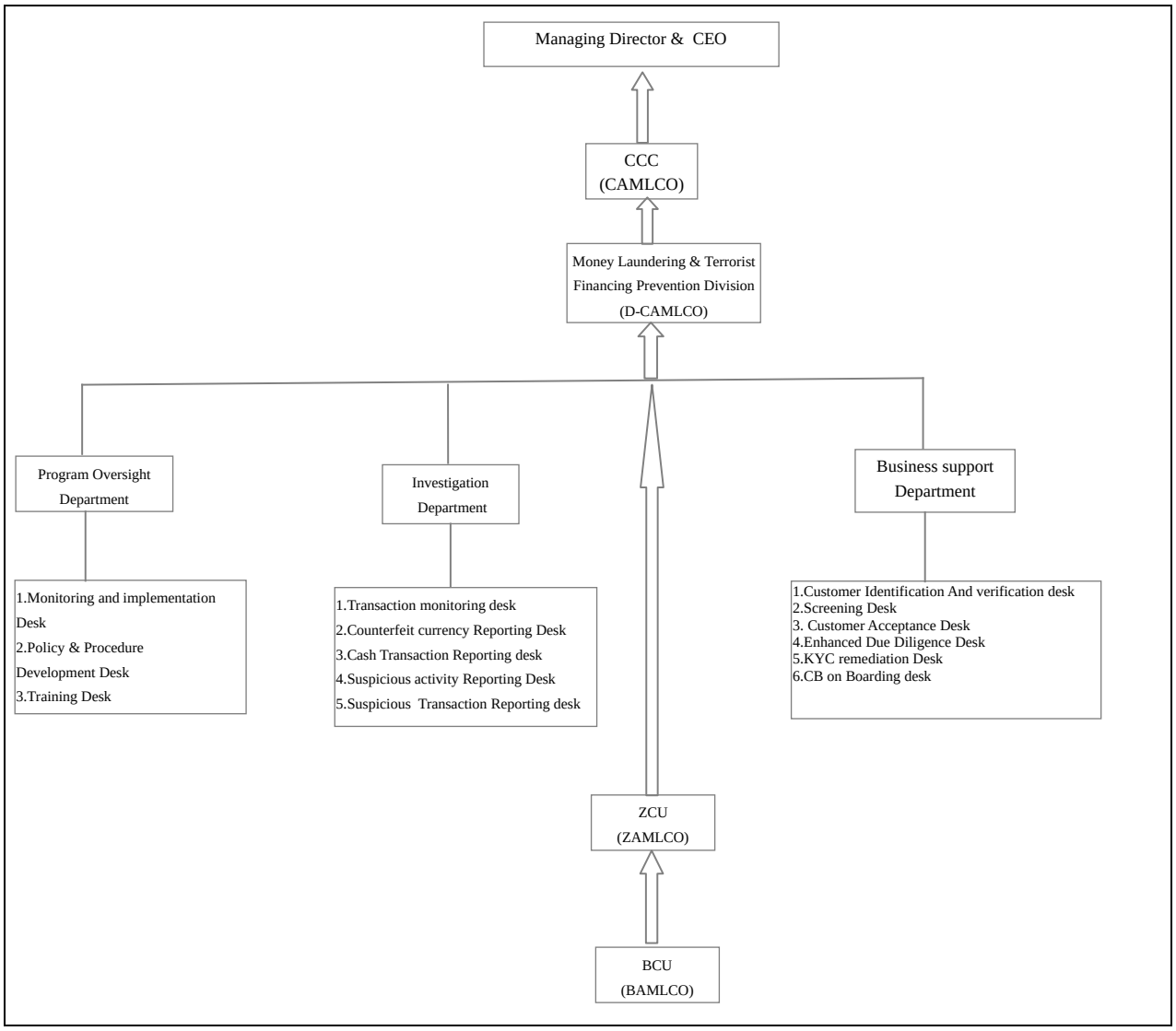
4.7 Fixing up the responsibilities

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

Function	Role / Responsibilities
Officer Responsible for Account Opening / Central on-boarding	❖ Perform due diligence on prospective clients prior opening an account ❖ Be diligent regarding the identification (s) of account holder and the transactions relating to the account ❖ Ensure all required documentation is completed satisfactorily ❖ Ensure all types of screening done ❖ Complete the KYC Profile for the new customer ❖ Ongoing monitoring of customer‘s KYC profile and transaction activity ❖ Obtain documentary evidence of large cash deposits ❖ Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO ❖ Escalate any true match hit of UN sanction screening to BAMLCO
Customer Service Of-	❖ Support the Account Officer in any of the above roles

ficer	❖ Perform the Account Officer roles in their absence
Manager Operations	❖ Ensuring that all control points are completed prior to transaction mon itoring ❖ Ongoing diligence on transaction trends for clients ❖ Update customer transaction profiles in the ledger/ system
BAMLCO	Manage the transaction monitoring process ❖ Report any suspicious activity to Branch Manager, and if necessary to the Money Laundering & Terrorist Financing Prevention Division ❖ Provide AML training to Branch officers ❖ Update policy with local AML & CFT regulations and communicate to all officers ❖ Submit Branch returns to Money Laundering & Terrorist Financing Division on Bi-monthly & Quarterly basis ❖ Clear the AML compliance link messages regarding UN sanction screening
Head of Branch	❖ Ensure that the AML program is effective within the branch/unit ❖ First point of contact for any AML issues
Risk Management /Investment Officer/Foreign Exchange Officer/ Internal Control Officer	❖ Perform AML Risk Assessment for the Business ❖ Perform periodic Quality Assurance on the AML program in the unit ❖ Communicate updates in AML laws and internal policies
Operations & Technology Manager	❖ Ensure that the required reports and systems are in place to maintain an effective AML program
ZAMLCO	❖ Communicate and follow-up activities of the BAMLCOs & BCU ❖ Motivate the BAMLCOs to submit STR proactively ❖ Take initiative for updating KYC/TP/Risk grading of all accounts ❖ Activate & operate ZCU properly & efficiently ❖ Escalate any true match hit of UN sanction screening to CAMLCO
Head of Zone	❖ Overall responsibility to ensure that the branches have an AML & CFT program in place and that it is working effectively
DCAMLCO	❖ Report suspicious clients to BFIU on Institution's behalf ❖ Inform Controller of Branches/BAMLCOs of required actions (if any) ❖ Confirm AML & CFT programs are implemented at branch level.
CAMLCO	❖ Develop bank's anti-money laundering & terrorist financing policies & programs ❖ Ensure proper functioning of the CCC ❖ Ensure bank's AML & CFT compliance
Managing Director & CEO	❖ Overall responsibility to ensure that the Business has an AML/CFT program in place and that it is working effectively.

4.8 Organization chart for the purpose of AML & CFT:



CHAPTER - 5

Customer Due Diligence

Customer Due Diligence (CDD) is the combination of the followings:

- Confirmation of the Know Your Customer (KYC) based on collected information & documents from reliable and independent sources,
- Verification of KYC related information and documents as well as source of fund &
- Conducting ongoing monitoring on KYC data/documents as well as Account's transactions.

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

I. Type of customers;
II. Business relationship with the customer;
III. Type of banking products;
IV. Transaction carried out by the customer and
V. Geographic location to and from the business conducted.

The adoption of effective KYC standards is an essential part of IBBPLC's risk management policies. IBBPLC, therefore, shall carry out customer due diligence for two broad reasons:

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

In case of on-boarding, Account Opening Form so circulated from the BRPD, Bangladesh Bank shall be used. But, considering the efficiency, modern technology as mentioned in the "Guidelines on Electronic Know Your Customer (e-KYC)" issued from Bangladesh Financial Intelligence Unit shall be used in appropriate cases. Where on-boarding is not possible electronically, hard copy of Account Opening Form may be used.

5.1 General Rule for CDD

Completeness and Accuracy

IBBPLC requires to be certain about the customer's identity and underlying purpose of establishing relationship with the bank, and shall collect sufficient information up to its satisfaction. **"Satisfaction of the bank"** means satisfaction of the appropriate authority that is necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

It is an obligation for IBBPLC to maintain **complete** and **accurate** information of their customer and person acting on behalf of a customer. '**Complete**' refers to combination of all information for verifying the identity of the person or entity. For example: name and detail address of the person, profession, source of funds, Passport/National Identity Card/Birth Regis-

tration Certificate/acceptable ID card with photo, phone/ mobile number etc. '**Accurate**' refers to such complete information that has been verified for accuracy.

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

The verification procedures establishing the identity of a prospective/existing customer shall basically be the same whatever type of account or service is required. It would be best to obtain the identification documents from the prospective customer which is the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity, so verification will generally be a cumulative process.

Where IBBPLC is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, unable to identify the beneficial owner taking reasonable measures, unable to obtain information on the purpose and intended nature of the business relationship, it shall not open the account, commence business relations or perform the transaction; or shall terminate the business relationship following the due process; and shall consider making a suspicious transactions report in relation to the customer.

Ongoing CDD measures (Review and update of KYC)

Concerned units of IBBPLC shall take necessary measures to **review** and **update** the KYC of the customer after a certain interval. This procedure shall have to be conducted in every **five years** in case of low risk customers. Furthermore, this procedure shall have to be conducted in every year in case of high risk customers. But, IBBPLC shall update the changes in any information on the KYC as soon as bank gets to be informed. Moreover, IBBPLC shall update KYC information anytime if there is any particular necessity realized. Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay. Besides, a process shall be available to detect the accounts that shall be transformed from low risk to high risk.

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

IBBPLC shall collect the announcement of customer about the Transaction Profile of customer account in the specified form. After reviewing the nature of the customer, the source of money in the account and the nature of transaction, IBBPLC shall bring necessary amendment in the Transaction Profile of the respective customer within 6 (six) months of establishing business relation and assessing the effectiveness with a justifying consideration.

Enhanced Due Diligence

In case of High Risk rated customers as assessed through the Risk Assessment report, IBBPLC 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.

IBBPLC shall 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 terrorist financing (such as enlisted in "Jurisdictions under Increased Monitoring" and "High-Risk Jurisdictions subject to a Call for Action" by Financial Action Task Force). In such a case, Counter measures of FATF shall be ensured for appropriate cases.
- STR submitted Accounts;
- In-house investigated suspicious accounuts.
- Privilege Banking Services (Presently IBBPLC does not offer any Privilege Banking Service).

Simplified Customer Due Diligence

Simplified Customer Due Diligence shall be ensured for the Low Risk customers or customers conversant with the indicators of Low Risk which combines the following measures:

- 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 alongwith the telephone number of the applicant(mobile number, if telephone number is not available) shall be collected.
- If the transaction amount is above Tk.50,000/-(fifty thousand) but less than Tk.5,00,000/-(five lakh), Attested copy of Photo paste ID of the Sender/ Applicant/ Depositor/ With-drawer 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).
- For ensuring Simplified Customer Due Diligence instructions laid down in the Guidelines on e-KYC issued by BFIU shall be followed.

5.2 Timing of CDD

i. IBBPLC shall apply CDD measures when it does any of the following:

- ❖ establishing a business relationship;
- ❖ carrying out occasional transactions amounting to TK. 5.00 lakh and above by the Walk-in-customers;
- ❖ Conducting of occasional transactions through wire transfer.
- ❖ Suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification.
- ❖ Suspecting money laundering or terrorist financing and in such a case, if there is a possibility of 'Tipping-Off of submitting STR/ SAR, completion of CDD is not required/ may be relaxed.

ii. Existing CDD measures as ensured by IBBPLC shall be reviewed for an on-going basis.

iii. On-going CDD measures shall be conducted to detect the inconsistency among the nature of business, magnitude of risk or sources of income (if felt appropriate). High Risk Customers information shall be updated after proper verification & review.

iv. KYC information of Customer or Beneficial Owners (if applicable) shall be obtained/ verified while establishing of business relationship or before withdrawal of fund from the account. In case of Walk-in Customers, KYC information shall be verified at the time of making transaction. In case of low risk customers or where the risk control system of the identified risk is available or where there is no necessity to held up/ cancel the business relationship, KYC information shall be verified within shortest possible time.

v. Beneficial Owner (s) of each account shall be identified. KYC information of the Beneficial Owners shall be ensured taking information from the independent & reliable sources as per satisfaction of concerned authorities considering the followings:

a) If any customer operates any account on behalf of another person, KYC information shall be ensured for that person from reliable & independent sources alongwith the customer.
b) If any Customer seems to be controlled by another person, complete & accurate information shall be ensured for that person.
c) In case of company, if any person (s) has/ have the ownership/ controlling interest, complete & correct information shall also be ensured for those persons.
d) To comply with the instructions set above at clause no. a) & b), if there is not possible to identify any natural person(s), CDD shall be ensured for the Chief Executive/ Management Head collecting information from reliable & independent sources.
e) To identify the Beneficial Owners and taking necessary steps for the same, Guidelines on Beneficial Ownership issued from BFIU can be followed.
f) For establishing of correspondent banking relationship (RMA) with foreign banks, Money Laundering & Terrorist Financing status of countries or jurisdiction shall be considered.

5.3 Others instructions for CDD:

i. IBBPLC shall preserve the account information and documents of the customers completing the KYC & ensuring CDD for account opening. For the purpose, digital prescribed form as laid down in Guidelines for e-KYC or where e-KYC is not possible prescribed hard copy of KYC shall be used.
ii. Prescribed hard copy of KYC Form shall not be treated as a part of the Account Opening Form and shall not be filled in by the customer.
iii. If any Customer has more than one account in different branches of IBBPLC, a Unique Identification Code shall be provided to avoid the duplicity in KYC process and ease the transaction monitoring.
iv. IBBPLC shall furnish Transaction Profile of the Customer and prepare a transaction nature of the customers considering past 6 to 12 months transactions and using this nature, IBBPLC shall monitor the customers' transactions. If significant changes are found in the nature of transaction, investigation shall be conducted and if necessary Transaction Profile shall be modified and if the transaction seems to be suspicious, STR shall be filed. In such a case, it shall carefully be looked after so as to the customer do not fall into any harassment.

5.4 In case where conducting the CDD measure is not possible

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

(a) not to carry out a transaction with or for the customer through a bank account;

(b) not to establish a business relationship or carry out an occasional transaction with the customer;

(c) to terminate any existing business relationship with the customer;

(d) branch shall preserve the information and documents of such A/c and send the same to Money Laundering & Terrorist Financing Prevention Division and they shall circulate the same to the branches for their information and necessary cautionary measures.

(e) to consider whether it ought to be making a report to the BFIU through an STR.

IBBPLC shall always consider whether an inability to apply CDD measures is caused by the customer. In this case, the IBBPLC 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 IBBPLC 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 IBBPLC 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.

5.5 Transaction Monitoring

IBBPLC shall continuously monitor the transactions of customers. The complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized during monitoring to detect the suspicious transactions/ activities.
In this respect instructions laid down in the Guidance on reporting of Suspicious Transactions and Guidelines for Prevention of Trade Based Money Laundering (TBML) shall be considered**.** In this regard, the system to be developed/ outsourced by the bank or any updates in the system to be brought from time to time shall be used to identify and review the risky, unusual & suspicious transactions and activities; and according to the review, Enhanced Due Diligence has to be maintained for accounts involved with such transactions. In this regard, the system to be developed/ outsourced by the bank or any updates in the system to be brought from time to time shall be used to identify and review the risky, unusual & suspicious transactions and activities; and according to the review, Enhanced Due Diligence has to be maintained for accounts involved with such transactions.

Monitoring shall be conducted by all Divisions of Operations Wing (OW), International Banking Wing (IBW), Corporate Investment Wing (CIW), Retail Investment Wing (RIW), Corporate & Social Responsibility Division (CSR) of Development Wing (DW), m-Cash/ Agent Banking, Alternative Delivery Division (ADD) of Information & Communication Technology Wing (ICTW), Rural Development Division (RDD) or any other Divisions/Departments involved with such transactions so as to report potential unusual/ suspicious activity/ transaction to the Central Compliance Committee (CCC), Head Office.

5.6 Screening System of IBBPLC

Sanctions Screening is the process of reviewing various international sanction list or local black lists to check if any investor/client in bank's Fund/business is involved in financing crime or terrorism, so that the bank can take the appropriate action. Sanctions are used for a number of purposes, including pressurizing a particular country or regime or financial institution to change their behaviour, or to prevent terrorist financing. There are many different types of international sanctions including travel bans, asset freezes, trade embargoes and other restrictions which are being imposed by United Nations, Office of Foreign Assets Control(OFAC), USA, European Union, OFSI under HM Treasury, UK etc. at international level. Besides, any black list from local regulatory authorities or adverse media reports shall be screened to detect or deter Money Laundering and Terrorist Financing & Proliferation Financing. IBBPLC shall establish an automated screening system which will compulsorily comply/ screen the UN sanction in international level along with other international sanctions as and when required as well as national/internal sanctions/ blacklists while establishing new business relationship or providing any banking facility to the existing customers.

5.7 Exception when opening a bank account

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

a) the account is not closed;

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

5.8 Customer Identification

Customer identification is an essential part of CDD measures. A customer includes:

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

5.9 Verification of Source of Funds

IBBPLC shall collect and verify the document supporting sources of funds 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 shall request the person to produce E-TIN (Electronic Tax Identification No) certificate which declares taxable income.

5.10 Verification of Address

IBBPLC shall 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 or through a phone contact & SMS. IBBPLC will collect any other document (recent utility bill or any other such documents mentioning the name and address of the customer) as per their satisfaction.

Verification of the information obtained shall 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 shall see originals of any documents involved in the verification.

5.11 Walk-in/ One off Customers

Bank shall collect complete and correct information while serving Walk-in customer, i.e. a customer without having account. Bank shall know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT or any other such transaction which do not require to be an account holder of the Bank. Bank shall 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 bank shall identify sources of funds as well.

5.12 Non Face to Face Customers

Non face to face customer' refers to "the customer who opens and makes transaction in the accounts through internet or bank's agent or his professional representatives (lawyers/ accountants) without having physical presence at the Bank's Branch."

Where there is no face-to-face contact, photographic identification would clearly be inappropriate procedures to identify and authenticate the customer. Bank/Branch would ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check shall be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID card where there is no face-to-face contact, then a certified true copy shall be obtained. IBBPLC Branches shall not allow non face to face contact to a resident Bangladeshi in establishing relationship.

IBBPLC shall assess money laundering and terrorist financing risks while providing service to non face to face customers. Bank may consider the following steps for identification of non face to face customers but not limited to:

- if the proposed customer is an existing customer of the Bank, the referred account may be verified;
- initial deposit can be taken through a cheque of the customer's any other account with any other banks; In such case identification can be ensured through the respective bank;
- customer must produce such identity documents which can be verified by the Bank from the 3rd party or in any electronic means;
- In case of transactions, two factor authentication can be ensured;
- Must be introduced by such a person who is well known to the Bank;

- The signature to be used must be similar with the signature already put in any other acceptable documents;
- The local address can be verified by the banker or any other 3rd party reliable to the Bank;
- Certified copies of the documents by an acceptable person to the Bank;
- Or any other acceptable means to be adopted by the respective official of the Bank for satisfaction of the customer's identity.
- Guidelines for e-KYC shall be used for opening of accounts or providing any service (if applicable).

5.13 Customer Unique Identification Code

IBBPLC shall use unique identification code for any customer maintaining more than one accounts 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. To ensure this, IBBPLC can use its system like auto searching through NID, Name, Date of Birth, Mother's name or any other references of the customers which are unique in nature.

5.14 Correspondent Banking

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

IBBPLC shall establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank through collection of information through the prescribed form or **if required, necessary additional information may be collected by using 'Open Sources' as per BFIU circular-26 dated 16 June, 2020**. IBBPLC shall also obtain approval from the CAMLCO before establishing and continuing any correspondent relationship. IBBPLC shall be sure about the effective supervision of that foreign bank by the relevant regulatory authority. IBBPLC shall 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.

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

The countries and territories that do not meet international standard or countries/ territories that have huge lacking in preventing money laundering and terrorist financing (such as enlisted in "Jurisdictions under Increased Monitoring" and "High-Risk Jurisdictions subject to a Call for Action" by Financial Action Task Force) Enhanced Due Diligence (EDD) shall be ensured for making business relationship with any Individual/ Entity of those countries and counter measures of FATF shall be ensured for appropriate cases.

AML & CFT Compliance status of the countries/ territories shall be verified before making any business relationship with the foreign Banks located in that country.
There shall be a monitoring mechanism for Correspondent Banking and other FI relationships to check for adverse media news against any CB/ FI or any other emerging news. Simultaneously, due diligence shall be done on Senior Management and Beneficiaries of CB/ FI during on-boarding or renewal of relationship. In doing so, if any adverse result is found at any stage, it has to be reported to the CAMLCO for decision.

5.15 Agent Banking

IBBPLC shall follow the policy / procedures regarding Agent Banking Operations which are among others as under:

- Ensure KYC procedures including Screening Mechanism while on-boarding the Agent
- Ensure effective Training for the Agents
- Ensure proper internal Auditing and Reporting to the Agent Banking Operations
- Publishing update list of the Agents in Bank's own website on (January-June) basis
- Publishing the list of rejected Agents in Bank's own website on (January-June) basis
- Mentionable that all the responsibilities in connection with AML & CFT compliance program shall totally be bestowed on the Bank alongwith the Agent.
- In case of Agent Banking, Guidelines on e-KYC issued by BFIU shall be complied with.

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

All clients must be subject to an assessment to determine whether they are 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 (PEP's, 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.

5.16.1 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 Head of State or of gov-

ernment, 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 legislatures;
- 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.

5.16.2 CDD Measures for PEPs

IBBPLC will identify whether any of their customer is PEP. In this regard, IBBPLC shall use an updated list of such PEPs in the screening solutions for easy, accurate and prompt identification of the customers concerned. Once identified banks need to apply enhanced CDD measures. Moreover, they need to perform the following-

- Bank has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a PEP;
- obtain additional information related to KYC of the customer from independent and reliable sources;
- obtain CAMLCO's approval before establishing such business relationship;
- take sufficient measures to identify the PEPs / IPs physically and financially based on information / data and documents obtained from reliable and independent sources while on-boarding;
- in every investment proposals, the PEPs column shall be filled up with specific and concrete answer; Vague words like 'unknown', 'not applicable', 'not found' etc. shall be avoided;
- monitor their transactions on regular basis; and
- all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly .
- Instructions laid down in Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations issued by BFIU shall be complied with.

5.16.3 Definition of Influential Persons

'**Influential persons'** refers to, "Individuals who are or have been entrusted with prominent public functions domestically, for example Head 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:

- heads and deputy heads of state or government;
- senior members of ruling party;
- ministers, state ministers and deputy ministers;
- members of parliament and/or national legislatures;
- members of the governing bodies of major political parties;
- Secretary, Additional secretary, joint secretary in the ministries;
- Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

- Governors, Deputy Governors, Executive Directors and General Managers of Central Bank;
- heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
- heads of state-owned enterprises;
- members of the governing bodies of local political parties;
- ambassadors, **chargés d'affaires** or other senior diplomats;
- city mayors or heads of municipalities who exercise genuine political or economic power;
- 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 shall not be classified as an influential person. In this regard, Bank shall use an updated list of such PEPs in the screening solutions for easy, accurate and prompt identification of the customers concerned.

5.16.4 CDD Measures for Influential Persons (IP)

IBBPLC will identify whether any of their customer is an IP. Once identified they will apply enhanced CDD measures. Moreover, they will perform the following-

- To adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is an IP;
- obtain CAMLCO's approval before establishing such business relationship in applicable cases;
- take reasonable measures to establish the source of fund of a IP's account;
- monitor their transactions in a regular basis; and
- report anything found suspicious
- Instructions laid down in Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations issued by BFIU shall be complied with.

5.16.5 CDD Measures for Chief Executives or Top Level Officials of any International Organization

IBBPLC will identify whether any of their customer is a CEO or top level officials of any International Organization. In this regard, Bank shall use an updated list of such senior officials in the screening solutions for easy, accurate and prompt identification of the customers concerned. Once identified banks need to apply enhanced CDD measures. Moreover, they will perform the followings-

a) 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 CAMLCO's approval before establishing such business relationship in applicable cases;
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.
f) Instructions laid down in Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations issued by BFIU shall be complied with.

5.16.6 Close Family Members and Close Associates of PEPs

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

- the PEP's spouse (or any person considered as equivalent to the spouse);
- the PEP's children and their spouses (or persons considered as equivalent to the spouses); and
- the PEP's parents;

There may be exceptional circumstances where the individual shall not be classified as a 'Close Family Member' of the PEP, 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 PEP, they shall also be classified as PEPs.

A Close Associate of a PEP includes:

I. 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 PEP; and
II. 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 PEP.

In addition, it shall 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 PEP.

5.16.7 CDD Measures for Close Family Members and Close Associates of PEPs

IBBPLC shall identify whether any of their customers is a family member or close associates of a PEP. Once identified bank needs to apply enhanced CDD measures. Moreover, they need to perform the following-

a) To adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a family member or close associates of a PEP
b) obtain CAMLCO's approval before establishing such business relationship in applicable cases;
c) take reasonable measures to establish the source of fund of the account of a family member or close associates of a PEP;
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 .

5.17 Wire Transfer

5.17.1 Cross-Border Wire Transfers

- Under general or special consideration in case of threshold cross-border wire transfers of 1000 (one thousand) or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected, preserved and has to be sent to

intermediary/beneficiary bank. Among these information customers account number, Unique Transaction Reference Number (if account number is not available) shall be included so that it can be identified in future. Besides, In the Beneficiaries information, Beneficiaries account number, Unique Transaction Reference Number (if Beneficiaries account number is not available) shall be included so that it can be detected in future.

- Furthermore, below the above mentioned threshold, Customers & Beneficiaries information which shall not be needed to verify like, Name, Address, account number or Unique Transaction Reference Number (where account number is not available) shall be included so that it can be identified in future.
- In case of making any payment under cross-border wire transfer, beneficiaries' information shall be obtained.
- 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, IBBPLC shall include the account number of the originator.

5.17.2 Domestic Wire Transfers

In case of threshold domestic wire transfers of at least 25000/- (twenty five thousands) BDT, full and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank/institutions. Furthermore, for domestic wire transfers below the threshold full and meaningful originator information has to be preserved. For providing money of domestic wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved. In case of Mobile financial services, IBBPLC shall 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.

5.17.3 Duties of IBBPLC as Ordering, Intermediary and Beneficiary Bank in Case of Wire Transfer

Ordering Bank:

Being the ordering bank, IBBPLC shall 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. Mentionable that if any of such transaction is under investigation of BFIU or any other competent regulatory authority, the records have to be preserved even after 5 years of the transaction concerned even though the depicted time was over. Besides, Ordering Bank shall not make any transaction without complying the instructions laid down in Chapter-7 (Criteria for Rejection of Customers) & clause no. 13.6 of Chapter 13 of this AML Policy.

Intermediary Bank:

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

tion). Mentionable that if any of such transaction is under investigation of BFIU or any other competent regulatory authority, the records have to be preserved even after 5 years of the transaction concerned even though the depicted time was over.

As an intermediary Bank, IBBPLC shall 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 shall be consistent with straight-through processing.

Beneficiary Bank:

Being a beneficiary financial institution, IBBPLC shall initiate risk based procedure to identify wire transfers that lack required originator or required beneficiary information. In case of insufficient originator information concerned parties shall collect that information through mutual communication or using any other means. During the payment to receiver/beneficiary, IBBPLC shall collect complete and accurate information of receiver/beneficiary and shall preserve those information for 5 (five) years. Mentionable that if any of such transaction is under investigation of BFIU or any other competent regulatory authority, the records have to be preserved even after 5 years of the transaction concerned even though the depicted time was over.

5.18 CDD for Beneficial Owners

IBBPLC shall 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 shall put in place appropriate measures to indentify 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. In this regard, the **prescribed KYC form** for Beneficial Owner shall be used. IBBPLC shall consider the following aspects while identifying beneficial ownership:

- 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 bank shall consider other means to determine controlling interest or ownership of a legal entity or arrangements. In addition to that bank shall also consider reasonable measures to verify the identity of the relevant natural person who holds senior management position;
- Any person or entity who has controlling or 20% or above share holding within any or legal entity.
- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercises control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) shall consider for other types of legal arrangements.
- In case of failure of the identification of the natural person of the beneficial owners, accurate and complete information of the CEO of that Organization shall be obtained.

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

activities/transaction done by the beneficial owners shall also be brought under effective monitoring.

5.19 Reliance on Third Party

IBBPLC could rely on the third parties to perform the CDD measures with the prior permission of Bangladesh Bank which may include i) identify and verify customer identity; ii) identify the beneficial ownership and control structure; and iii) identify the purpose and nature of the business relationship under the following criteria:

- A third party shall immediately obtain necessary information related to i) -iii) as mentioned above;
- All necessary data and documents held with the third party must be available for the bank without any delay;
- IBBPLC shall satisfy that third party is regulated, supervised and monitored for, and has taken appropriate measures in compliance with CDD and record keeping requirements set out in this Policy and Guidelines for Money Laundering and Terrorist Financing Risk Management.

5.20 Management of Legacy Accounts

Legacy accounts refer those accounts opened before 30 April, 2002 and yet to update KYC procedures. These legacy accounts shall be treated as "Dormant". No withdrawal shall be permitted in those accounts; however, deposit can be permitted. These accounts will be fully functional only after conducting proper CDD measures.

5.21 Individual Customers

Where verification of identity is required, the following information shall be obtained from all individual applicants for opening accounts or other relationships, and shall be independently verified by the Bank itself through maker/ checker process:

- true name and/or names used;
- parent's names;
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of wealth or income
- Contact information, such as – mobile/telephone number.

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

(i) Valid passport;
(ii) Valid driving license;
(iii) National ID Card;
(iv) Employer provided ID Card, bearing the photograph and signature of the applicant;

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, certificate from any local government organs, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures shall be plainly legible. Where applicants put forward documents with which IBBPLC is unfamiliar, either because of origin, format or language, the Bank shall take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. The Bank shall also be aware of the authenticity of passports.

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 NID with Election Commission;
- checking the Telephone Directory/ Cell Phone Number.
- record of home/office visit.
- sending thanks letter
- Sending balance confirmation SMS through Cell Phone

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

5.22 Appropriateness of documents

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

5.23 Joint Accounts

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

5.24 Change in address or other details

Any subsequent change to the customer‘s name, address, or employment details shall 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.

5.25 Introducer

To identify the customer and to verify his/her identity, an introducer may play an 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 shall be recorded on the customer's file. However, personal introductions without full verification shall 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. Besides, introduction shall not be placed under exception on any form of plea in KYC procedures. While accepting introduction in favour of a potential customer, the followings shall be considered:

1) Introduction of those customers can only be accepted who had been maintaining an equivalent or superior nature of regular accounts for at least 6 months of time.
2) While opening of a new account by an existing similar or superior nature of account holder can be exempted from introduction by others upon satisfaction of the account opening officers

3) While opening a staff account by the employee of the Bank, the data card maintained by the HRM System may be considered as introduction and in this case, the account opening official shall be given privilege to access the HRM System's data card of each employee.
4) Introduction of the customers can also be exempted for any other valid grounds/documents upon satisfaction of the BAMLCO & CCC. In such case, the reason of such exemption shall have to be recorded duly.

For effective KYC & Due Diligence procedure, IBBPLC shall determine threshold(s) from time to time depending on the nature and grounds of introduction for generating necessary red flags on the basis of number of introduction. Upon satisfaction of the concerned officials, the red flags may be settled, if justified, with adequate supporting records/evidences both in the system as well as in the respective file.

5.26 Minor

For minor, the normal identification procedures set out above shall be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s). Under normal circumstances, a family member or guardian who has an existing relationship with the Bank 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, shall be verified. All other procedures as mentioned in the section 6, Chapter V of the General Banking Manual shall be followed.

5.27 Corporate Bodies and Other Entities

The principal requirement for corporate bodies 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 shall 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.

The following documents shall normally be obtained from companies:

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

Where the business relationship is being established in a different name from that of the applicant, the branch shall also satisfy itself that the reason for using the second name makes sense.

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

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

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

When authorized signatories change, care shall 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. All other procedures as mentioned in the section 11, Chapter V of the General Banking Manual shall be followed.

5.28 Companies Registered Abroad

Particular care shall be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, IBBPLC shall carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature/ presence of the business.

5.29 Partnerships and Unincorporated Businesses

In the case of partnership and other unincorporated businesses whose partners/directors are not known to the Bank, the identity of all the partners or equivalent shall 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 shall be obtained.

Evidence of the trading address of the business or partnership shall be obtained along with a copy of the latest report and accounts (audited where applicable).

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

procedures as mentioned in the section 09, 10 and 14, Chapter V of the General Banking Manual shall be followed

5.30 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 guarantor of the power of attorney and third party mandates. Records of all transactions undertaken as per a power of attorney shall be kept in accordance.

5.31 Internet, Online Banking and adoption of new technologies/ services

Islami Bank Bangladesh PLC offers Internet Banking or Online Banking through i-banking, m-Cash account, Visa Card/ Debit Card, Khidmah Card, agent banking, etc. IBBPLC shall apply necessary CDD measures to prevent Money Laundering, Terrorist Financing & Proliferation Financing through these online/ internet products.

Prior to adoption of new technology/ services (Internet Banking, Electronic Card, e-KYC, SWIFT, Transaction Platform, etc.), the concerned authority of IBBPLC shall conduct AML/CFT risk assessment, evaluate the risk and take necessary steps to mitigate the same. Mentionable that above mentioned procedures shall be done before introduction of the new technology/ service.

5.32 Know Your Employee (KYE)

It is learnt 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, IBBPLC shall look closely at the people inside their own organizations as per the Human Resources Policy and its amendments from time to time.

A Know Your Employee (KYE) program means that IBBPLC shall have a program in place that would allow 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 shall 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. IBBPLC shall verify that contractors are subject to screening procedures similar to its own.

The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which shall include verification of references, experience, education and professional qualifications. The extent of the screening depends on the circumstances, with reasonableness the standard. In this regard, the prescribed **KYE Form** shall be executed during on-boarding its employees.

5.33 CDD for CSR Beneficiary

CDD procedure for CSR Beneficiary shall include the following among others,

- the acceptance and rejection policy
- EDD Process for institutional beneficiary, adverse media/UN Sanction List/ internal black list/ local government black list/ rejection record verification/contact point verification
- execution of the prescribed **Know Your Beneficiary (KYB) Form**
- Risk categorization on the basis of beneficiary, purpose, amount, etc.

5.34 Third Party (ies)

Third party shall mean an individual/ entity/ group who is/are not directly involved with Bank's business but provides some supports to the Bank on its behalf to accomplish the job like Panel Lawyers, Insurers, Surveyors, m-Cash Agents, C&F Agents, Suppliers, Vendors, etc. Their CDD process shall be done depending on the nature of party and business relationship which shall among others include adverse media report screening, UN & other local and international Sanction List screening, PEPs/ IPs/ Brass Plate Firms screening, etc.

5.35 Duties for the Foreign Branch (es)/ Subsidiary (ies):

Foreign Branch/ subsidiary shall comply with the instructions of MLPA 2012 (Amended in 2015) & ATA 2009 (Amended in 2012 & 2013), Money Laundering Prevention Rules-2019 & Anti Terrorism Rule-2013 and the instructions/ circulars issued by BFIU time to time.

If any Foreign Branch/ Subsidiary is unable to comply with the stipulations of Money Laundering Prevention Act 2012 (Amended in 2015) & Anti Terrorism Act 2009 (Amended in 2012 & 2013) and Money Laundering Prevention Rules-2019 & Anti Terrorism Rule-2013, necessary initiative shall be taken to manage/ mitigate the risk of ML & TF and inform the same to BFIU without any delay.

This instruction shall also be applicable for the Offshore Banking Unit licensed by Bangladesh Bank.

5.36 Central Customer On-boarding

To ensure the accuracy and to maintain international standard in Customer Due Diligence, IBBPLC has introduced Central On-boarding process. Branches shall exercise vigilance during the on-boarding process of the customer and shall cooperate with the Central On-boarding Team as and when required. Duties and Responsibilities of different parties in connection with the Central On-boarding process is laid down in the Standard Operating Procedures circulated vide Circular No. AMLD/7690 dated 22.03.2017 and detailed instructions related to opening accounts through the Central on-boarding process was issued vide circular letter No. MLTFPD/13089 dated 25.08.2020 which shall be meticulously complied with all concerned.

CHAPTER –6

Customer Acceptance Policy

6.1 Who is a Customer?

Clause No. 3.1 of BFIU Circular No. 26 dated 16 June, 2020 defines customer as under:

Under the Money Laundering & Terrorist Financing Risk Management, Customer means the following individuals & entities:

1) Individual or Entity who maintain (s) account or has business relationship with Bank.
2) Beneficial Owner of the Account(s) or Business Relationship (Person(s)/ Entity on whose be half account/ relationship is maintained)
3) Professional Intermediary(ies), i.e, Lawyer(s), Consultancy Firm, Chartered Accountant(s), etc. who is/ are appointed to operate the account(s) of Account Holder(s), Trust or Beneficiary(ies) of the Transactions under the prevailing structure.
4) Any Individual/ Entity conducts high value occasional transaction in a single entry or any Individual/ Entity may create risk for the Individual/ Entity or abolish the reputation.
5) Any Individual/ Entity is declared as customer by BFIU.

The Basel Committee defines a customer as:

- A person or entity who maintains an account with a financial institution or on whose behalf an account is maintained (i.e., beneficial owners);
- Beneficiaries of transactions conducted by professional intermediaries (e.g., agents, accountants, lawyers); and
- A person or entity connected with a financial transaction who can pose a significant risk to the bank.

A crucial aspect of customer identification is to establish whether the customer is acting on his, her or its own behalf, or whether there is a beneficial owner of the account that may not be identified in the documents maintained by the financial institution. If there is any reason to suspect that the customer is acting on behalf of another person or entity, appropriate due diligence measures shall be instituted.

Sound Know Your Customer (KYC) procedures are critical elements in the effective management of banking risks. Sound KYC procedures have particular relevance to the safety and soundness of financial institutions, in that:

- they help to protect financial institution's reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;

- they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks:

Reputational risk poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution.
Operational risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

Legal risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

Market/ Concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity.

6.2 Know Your Customer (KYC) 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.

IBBPLC 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.

6.3 Know Your Customer (KYC) Procedure

Money Laundering Prevention Act, 2012 (Amendment-2015) requires all reporting agencies to maintain complete and accurate 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 obtaining information on the purpose and intended nature of the business relationship, it shall not open the account, commence business relations or perform the transaction; or shall terminate the business relationship; and shall consider making a suspicious transactions report in relation to the customer. IBBPLC shall follow the above observations/ recommendations in conducting KYC procedure of the Bank.

6.3.1 Know Your Customers' Customers (KYCC)

Simultaneously, IBBPLC shall obtain minimum number of information, data & documents regarding true identification of the customers's customers along with its sources of funds/ nature of business to set up an effective preventive measures.

Screening of management, beneficiaries, major vendors/ suppliers and others interested parties shall be done at the proposal stage of an investment while developing a business relation or providing investment facilities.

6.3.2 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 Bank shall be ascertained at the outset to establish what might be expected later as normal activity. This information shall be updated as appropriate, and as opportunities arise. In order to judge whether a transaction is or is not suspicious, institutions need to have a clear understanding of the business carried out by their customers.

6.3.3 Identifying Real Person

IBBPLC shall establish to get 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 shall be interviewed personally. This will safeguard against opening of fictitious account.

6.3.4 Document is not enough

The best identification documents possible shall 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 the Branches of IBBPLC 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.

6.4 Salient features of Customer Acceptance Policy

Taking among others the above into consideration, IBBPLC's **Customer Acceptance Policy (CAP)** is introduced whose salient features are as under:

Sl. No.	Particulars	Policy	Procedures
1	**Common procedures/ documents to be required for all types of Accounts**	CDD & EDD will be ensured including identification of the persons/ Entity & verification of Address/ Sources of Fund and uses of fund with proper documentation.	CDD/ EDD shall be ensured by the following process: ❖ AOF in force to be filled in 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 all Individual/ Entity address by Utility Bill, Physical Verification, etc (where applicable). ❖ 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. ❖ Introduction of the proposed customer shall be ensured. ❖ The prospective customer must be mentally sound and capable to make a contract.
1.1	**Accounts Introduction Policy**	Introduction shall be ensured for the Customers	Introduction of the proposed customer shall be ensured under the following ways- a. All Individual Accounts (Natural Person) shall be opened without introduction who have valid NID as per BRPD Circular-02 dated 23.02.2020. b. Individuals who haven't valid NID may be allowed to open an account based on the introduction by such a person having valid NID. In that case signature of the introducer shall be similar with that of the signature inserted in NID as per BRPD Circular-02 dated 23.02.2020. c. Entity accounts shall not require any introduction, but their update license/enrollment documents issued by the competent authority may be accepted by the introduction as per BRPD Circular-02 dated 23.02.2020. ❖ In absence of stipulation set above at para (c), Managers/Executives of IBBPLC shall be allowed to introduce AWCA Accounts under a special circumstances but staff below the rank of Senior Officer shall not be allowed to introduce any accounts.
1.2	**Photo Paste ID**	Photo Paste ID shall be collected from Customers/ Beneficiaries/ Beneficial Owner/ Operators of the Accounts	Photo paste ID means- ❖ Copy of the National ID Card/ Valid Passport/ valid Driving License or any other Photo Paste ID Card acceptable to the Bank (i.e. ID card of Arm 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.

Sl. No.	Particulars	Policy	Procedures
1.3	**Nomination**	Proper Nomination shall be ensured for the customers	❖ Nomination must be ensured in case of Individual & Joint Accounts as per BRPD Circular-2 dated 23.02.2020. ❖ Nominee's details and photo paste ID alongwith 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 alongwith his/ her Photo Paste ID & recent Passport size Photograph shall be obtained in addition to the Birth certificate, recent passport size photograph & particulars of the Minor Nominee.
2	**Individual Account including Joint Account**	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).	CDD is to be ensured taking the following documents: ❖ 2 (two) copies of passport size recent photograph attested by the introducer for each Account holder. ❖ Copy of National ID Card/ Valid Passport/ Driving License or any other photo paste ID Card. 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. ❖ Nominee's details 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. ❖ Copy of the latest (note more than 03 months past) utility bill (Gas, Electricity, WASA, Telephone) of the customers as a proof of present address (if any) or any other reliable means shall be applied. ❖ Photocopy of up-to-date TIN Certificate (if any). ❖ In case of Student Account (Student Mudaraba Savings Account & others) valid Student ID/ Testimonial/ others Certificate that indicate the identity of the student from the institutions authority. ❖ In case of Farmers Accounts (Mudaraba Farmers Savings Accounts & others) Agriculture Card/ Farmers Card/ Certificate from competent authority. ❖ In case of Industrial Employee Account valid job ID/ Certificate from the Employer. **Additional documents required for non residential customers:** ❖ Copy of valid passport alongwith 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).

Sl. No.	Particulars	Policy	Procedures
3	**Non Individual Accounts (Sole Proprietorship/ Partnership /Private Limited Company/ Public Limited Company/ Others Entity**	Following usual practices Bank can open this type of account.	Common Documents to be required to ensure CDD: ❖ 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 paste 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. ❖ Beneficial owner KYC shall be ensured in case of having 20% share of each shareholder of the company. ❖ Copy of recent utility bill (Gas, Electricity, WASA, Telephone) as a proof of mailing address in case of high risk account (if any). ❖ Photocopy of up-to-date TIN/BIN Certificate (where applicable).
3(i)	**Sole Proprietorship Firm.**	Following usual practices Bank can open this type of account.	CDD shall be ensured taking the following special documents as a Proprietorship concern: ❖ All necessary papers must be submitted in the letter head 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. ❖ Beneficial owner KYC shall be ensured. ❖ Financial statement of last year. ❖ All other necessary procedures and documents as mentioned in Sl. No. 1, 2 & 3 are applicable for on-boarding of this type of customers. ❖ IRC/ERC from CCI&E (where the client is an exporter/importer)
3(ii)	**Partnership Firm**	Following usual practices Bank can open this type of account.	CDD shall be ensured taking the following special papers/ documents as partnership firm: ❖ Partnership Deed. ❖ Resolution for opening and operating of accounts. ❖ Financial Statement of last year, if applicable. ❖ All necessary papers must be submitted in the letter head pad of the firm with Seal & signature by the Managing Partner. ❖ Beneficial owner KYC shall be ensured in case of having 20% share of each shareholder of the firm. ❖ 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. ❖ IRC/ERC from CCI&E (where the client is an exporter/importer)

Sl. No.	Particulars	Policy	Procedures
3(iii)	**Private Limited Company**	Following usual practices Bank can open this type of account.	CDD 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. ❖ Beneficial owner KYC shall be ensured in any shareholder having 20% of the company. ❖ Audited Financial Statement of last 03 years. ❖ 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. ❖ IRC/ERC from CCI&E (where the client is an exporter/importer)
3(iv)	**Public Limited Company**	Following usual practices Bank can open this type of account.	❖ 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. ❖ Beneficial owner KYC shall be ensured in any shareholder having 20% of the company. ❖ Audited Financial Statement of last 03 years. ❖ 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	**Co-operative Society/ Samity.**	Following usual practices Bank can open this type of account.	CDD 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/ bye-laws certified by competent Authority. ❖ Copy of the approval letter from the Concerned Authority to run the business. ❖ List of office bearers (with address) alongwith their Bio data. ❖ 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. ❖ Bye laws and Certificate of Registration from Zila/Upazila Somobay Office required. ❖ As if with run microcredit program, Certificate of Registration from Microcredit Regulatory Authority as per MRA Act-2006 required.

Sl. No.	Particulars	Policy	Procedures
5	**Trust/ Waqf Organization.**	Following usual practices Bank can open this type of account.	CDD 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) alongwith 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	**Minor**	Legal Guardian on behalf of minor can open the account.	❖ 2 (two) copies of recent passport size photograph attested by the introducer of both Minor and operator(s). ❖ Operators details shall be obtained in the AOF alongwith all necessary papers/ documents as a customer. ❖ Nominee's details and photo paste ID of the Nominee alongwith 1 (one) copy of recent passport size photograph for each nominee to be attested by the applicant ❖ 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	**Illiterate Person**	Illiterate Person can open account with the bank following the norms in practice.	❖ Physical presence is required for withdrawal of money. ❖ Apply EDD for high risk clients. ❖ All others necessary documents as mentioned in Sl. No. 1, 2 shall also be applicable for this type of accounts.
8.			

8.1	**PEPs (Politically Exposed Persons):**	PEPs can open account complying Circular Letter BCD(AMLD)/6584 date: 21.10.2015 but prior approval to be taken from Head Office.	❖ 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. ❖ Besides, Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations shall be complied with.

Sl. No.	Particulars	Policy	Procedures
8.2	**IPs (Influential Persons)**	IPs can open account complying Circular Letter BCD(AMLD)/6584 date: 21.10.2015 but prior approval to be taken from Head Office.	❖ 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 (Where applicable). ❖ Besides, Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations shall be complied.
9	**Non Residential Bangladeshi and Foreign National.**	Non Resident Bangladeshi and Foreign Citizen can open account as per usual norms & practice.	❖ 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	**Pardansheen Women**	Pardansheen Women can open account as per usual norms & practice.	Women who are not interested to unveil their face: ❖ All other appropriate documents required to open an individual/ joint accounts & Foreign Residence as mentioned in Sl. No. 1 & 2. ❖ "The Woman", if educated, has to be introduced by the client known to the Bank and if illiterate, 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 sanctions screening, conduct risk grading and apply EDD for high risk clients.
11(i)	**Blind Man**	Blind man can open account as per usual norms & practice.	❖ 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 prevention regulations. ❖ No cheque book & ATM card shall be issued against this account. Withdrawal shall be executed through debit voucher.
11 (ii)	**Deaf & Dump Person**	Deaf & Dump Person can open account as per usual norms & practice.	❖ 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 with-

			drawal. Apply all other ML, FT & PF prevention regulations. ❖ No cheque book & ATM card shall be issued against this account. Withdrawal shall be executed through debit voucher.

Sl. No.	Particulars	Policy	Procedures
12	**NGO/NPO/ Club or Association**	Bank can open such account as per usual terms & practices.	1. Appropriate documents as mentioned in Sl. No. 1, 3, 4 & 5 shall be applicable for this account 2. 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. • Permission from NGO Affairs Bureau shall mandatorily be obtained. • 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/ sanctions, proper documents to be obtained. 3. Regular monitoring of their transaction to be done. 4. Apply all other ML, FT & PF prevention regulations.
13	**Travel Agency/ Hajj Agency/Recruiting Agency**	Concerned Documents to be obtained	❖ Appropriate documents mentioned in Sl. No. 1, 3 shall be obtained. ❖ Besides following documents must be obtained to ensure CDD/ EDD: ❖ Hajj License from Ministry of Religion Affairs. ❖ Approval of Hajj Agency Association of Bangladesh (HAAB) required. ❖ Civil Aviation License from Ministry of Civil Aviation and Tourism. ❖ International Air Transportation Association (IATA) Certificate. ❖ Association of Travel Agency of Bangladesh (ATAB**).** ❖ License from Ministry of Expatriates' Welfare & Overseas Employment in case of Manpower export.
14	**Garments /Manufacturing Industry**	Accounts of Manufacturing Industry shall be opened following necessary procedures of the Bank	❖ Appropriate documents mentioned in Sl. No. 1, 3 shall be obtained. ❖ Besides following documents must be obtained to ensure CDD/ EDD: ❖ ETP/WTP for Dying Industry. ❖ Environmental Certificate for Brick Field, Green Field, Ship Breaking, CNG Station Real state and others (where applicable). ❖ IRC/ERC from CCI&E.
15	**Export/ Import related Business**	Accounts of Export/ Import related Business shall be opened following necessary procedures of the Bank	❖ Appropriate documents mentioned in Sl. No. 1 & 3 shall be obtained. ❖ IRC & ERC from CCI&E. ❖ Membership Certificate. ❖ VAT Registration Certificate, TIN Certificate.
16	**NPO/ Educational/ Religious Institutions.**	Branch will open such accounts except UN/ OFAC sanction listed institutions or prohibited by Bangladesh Government.	❖ Appropriate documents as mentioned in clause no. 6.4 (Customer Acceptance Policy), Sl. No. 1, 3, 4 & 5 shall be obtained. ❖ Branch must ensure getting full identification of the members of Governing Body or Managing Committee, Resolu-

			tion for account opening, source of fund and destination/ using of fund etc. ❖ Apply all other ML, FT & PF prevention regulations.

Sl. No.	Particulars	Policy	Procedures
17	**Companies Registered Abroad**	Accounts opened in the name of companies registered abroad may be opened with all formalities including verification of supporting documents.	i. All other necessary documents as mentioned in Sl. No. 1 & 3 shall be applicable for this account. ii. Photocopy of Agreement with Agent with regard to open & operate the account by the Agent. iii. Documents showing evidence of registration of the companies with the concerned regulatory bodies abroad depending on their nature. iv. Documents verified/ attested by Bangladeshi High Commission/ Embassy to that country where the entity is registered. v. Documents verified by the High Commission/ Embassy of the License giving country working in Bangladesh. vi. Any other 3rd party verification (if required). vii. All other AML & CFT and prevention of PF regulations to be complied with.
18	**Foreign National/Entity**	Accounts in the name of foreign nationals may be opened with all formalities including verification of supporting documents	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) for Entities Accounts and Work permit for Individuals Accounts issued by Competent authority.
19	**Diagnostic Center/ Hospital or others Medical Service Providers including Medical College**	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	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).
20	**Publication (Print & Electronic Media including online newspapers)**	Accounts in the name of Publication (Print & Electronic Media including online newspapers) may be opened with all formalities including verification of supporting documents	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.	**Executor/ Administrator/ Liquidator.**	Following usual practices Bank can open this type of account.	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. All other ML & TF and PF prevention regulations to be complied with
22.	**Correspondent Banking**	Correspondent Banking to be established after obtaining information about respondent bank's commitment to prevent	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, Transaction monitoring, AML training, etc. are established.

		money laundering and combat terrorist financing.	All other ML & TF and PF prevention regulations to be complied with

Sl. No.	Particulars	Policy	Procedures
23.	**Shell Banking.**	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).	No Accounts shall be opened in the name of Shell Bank/Company.
24.	**Mobile Banking (mCash) Accounts**	The Mobile Banking account will be opened & operated through Bank's panel agents.	Specific terms and conditions are applicable for the KYC, TP (in agents a/c), Photograph & Identifying documents shall be collected for each and every account holder.
25.	**Internet Banking.**	The Internet Banking is a registration based service. No Internet Banking service will be provided without IBBPLC transaction account. Through internet banking a customer will be entitled View accounts, Fund transfer, iRecharge, Wimax Recharge, Utility bill pay, Transaction summery, etc.	To access in Bank's internet banking facilities, a customer having personal internet access must register and setup some password for customer verification. The customer will link to the customer number any of those accounts which the customer controls, which may be cheque, savings, investment, credit card and other accounts. To access internet banking, the customer would go to the bank's website and enter the internet banking facility using the customer number and password. Two facto authentication to be ensured. Source of fund and purpose of transaction to be ensured and recorded. Stricter monitoring of transactions to be ensured.
26.	**Walk-in Customer**	The customers who do not maintain any account with the bank is entitled to get some specific services by following KYC profile.	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.
27.	**On-line/ Non face- to- face Customer.**	On-line customer is one 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.	Branches shall confirm to obtain satisfactory evidence of identification of applicants/ depositors/ withdrawal holders through Short KYC including name, address, mobile number, occupation, relationship with beneficiary, source of fund etc. All other procedures to be maintained as mentioned in section 5.3 of the policy.
28.	**Account of undercharged insolvent**	No account shall be opened in the name of an Undercharged Insolvent or a person of Unsound Mind.	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. All other AML & CFT and prevention of PF regulations to be complied with

Sl. No.	Particulars	Policy	Procedures
29.	**Accounts of Banks, Govt. Officials and**	Branches shall not open accounts for Banks which are not established	While under the existing arrangements, Government servants authorized to maintain Banking Accounts in their official capacity shall have their accounts with Bangladesh Bank or Son-

	Military Funds.	at their own stations nor shall they enter into any agency arrangements with other banks without prior approval of the Head Office.	ali Bank and these restrictions do not apply to Government Official's personal accounts. Regimental and Non public funds may be so deposited subject to certain conditions and prior consent of the respective Controllers of Accounts. All other ML & TF and PF prevention regulations to be complied with
30.	**Accounts of Local Authorities.**	Before opening the account of any Government or semi Government Organisation or a local Body, a certified copy of the Statute or any other law by which the body is formed and governed shall be obtained.	Such accounts shall not be opened or allowed to be operated in contravention of this provision of the rules governing the accounts of those corporations. The accounts of Local Authorities, Municipal corporations, District Council, etc. shall be opened in Mudaraba Savings A/C, Al-Wadeeah Current A/C, Special Notice Deposits Account and related AOF shall be used for opening accounts. KYC will be obtained of every individual of operator of those accounts. All other AML & CFT and prevention of PF regulations to be complied with
31	**Locker, i-Banking, ADD or any other such services**	No such services shall be provided without opening a mother account.	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.
32	**Induction of Investment Clients**	No investment facilities shall be allowed to any customer without having satisfactory deposit account conduct.	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	**MSBs, CBS, C&F Agents etc.**	Due process to be followed	KYC, DD & Screening process to be executed for on-boarding and renewal.
34	**CellFin/ Others Internet based Banking**	CellFin is an omni-channel platform of Islami Bank Bangladesh PLC (IBBPLC) for all types of digital services and transactions. Any Bangladeshi citizen can create CellFin account. All you need is a smartphone with active SIM, a National Identification (NID) card, and get onboard in minutes, get a virtual VISA card, send/receive money, make payment, pay bills, receive foreign remittance and more	❖ Specific instruction as mentioned in the CellFin operations Manual/eKYC Guidelines shall be complied with to ensure CDD/ EDD of the customers. ❖ Besides, Instructions for Internet Banking as mentioned in the Sl. No. 25 shall also be complied.
35	**Pharmacy Account**	AWCA account shall be opened. But, for valid reason others accounts may also be opened.	Following Documents shall be obtained to ensure CDD/ EDD: ❖ Appropriate documents as mentioned in Sl. No. 1 & 3 shall be obtained. ❖ Valid Drug License in favor of the pharmacy/ proprietor/ partners shall be obtained from Drug Administration Department under Ministry of Health & Family Welfare.
36	**Filling Station & Distributor, supplier & retailers of Gas & Cylinder**	AWCA account shall be opened. But, for valid reason others accounts may also be opened.	Following Documents shall be obtained to ensure CDD/ EDD: ❖ Appropriate documents as mentioned in Sl. No. 1 & 3 shall be obtained. ❖ Fire License from Fire Service & Civil Defense ❖ LP Gas preservation certificate from department of Explosives in specific format from Chemist and Druggist Department under Ministry of Home Affairs.

6.5 KYC Documentation

To ensure proper KYC documentation, an additional checklist shall be consulted while establishing new business relationship or providing banking services/facilities to the existing customers as lying in the General Banking Manual Chapter V.

Besides, all other rules & regulations regarding Account Opening as stipulated at Chapter-V of the 'Manual for General Banking Operations' of IBBPLC and its subsequent modifications shall have to be followed.

6.6 KYC Exception

The Customer Acceptance Policy of IBBPLC shall not be used against the disadvantaged people or the people who have not proper identification document. Customer Acceptance Policy of IBBPLC shall encourage the ultimate goal of transparent, accountable and inclusive financial system.

CHAPTER –7

Customer Rejection Policy

Islami Bank Bangladesh PLC (IBBPLC) is strongly committed to ensure meticulous compliance of AML & CFT issues of the bank under the purview of local and global regulatory stipulations/bindings. As such, IBBPLC has adopted a policy that shall deter establishing new business relationship or providing banking services or facilities to the existing customers if he/she/it is fallen under following criteria:

I. No account will be opened in anonymous or numbered or fictitious name(s) and all concerned shall take necessary initiatives to prevent opening of such accounts.
II. No account will be opened through on-line beyond physical presence of a customer inside Bangladesh.
III. No account will be opened & operated in the name of persons/ institutions included in the UN sanction list, OFAC sanction list, and local Govt. black list, etc.
IV. No account will be opened in the name of license less Bank/ Financial Institution/ Money Changer.
V. Unwilling Customer to provide required information/data.
VI. Internally black listed clients
VII. Customers under frequent STR/ SAR shall be barred from opening another new account in any branch of IBBPLC.
VIII. Customers listed by Bangladesh Bank as the fraudster one shall not be allowed to open any account with IBBPLC.

Any rejection so made shall properly be recorded and an automated system shall be introduced in CBS so that all the branches give posting the detail information of the rejected customers including the reasons for rejection. No account or transaction shall be opened or conducted unless screening this rejection list. If any individual/entity found in the rejection list, the concerned branch shall not allow any banking facility to the customer provided getting due approval from the competent authority of the Bank.

However, the branches of IBBPLC shall also follow the undernoted instructions while establishing new business relationship or providing banking services or facilities to any existing customers:

01 Account Opening Form, KYC Profile and Transaction Profile forms shall be properly filled up.
02 Documentation formalities shall be completed in favor of customer identification.
03 Branch will verify the genuineness of customer's source of fund.
04 Branch will follow the rules of Money Laundering Prevention ACT, 2012 (Amendment-2015) and Anti Terrorism Act, 2009 (along with its amendment of 2012 & 2013), MLP Rules-2013, ATA Rules-2013.
05 Terminate an existing account or not to open an account where the bank is unable to apply appropriate customer due diligence measures i. e. bank is unable to verify the identity 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 bank. It may, however, be necessary to have suitable built safeguards to avoid harassment of the customer under any legal complication. In the case of discontinuation of relationship, the due process to be strictly followed and the proceeds of the account to be sent to the actual account holder.
06 Necessary precautions to be taken before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations or involved in Money Laundering offence.

07 Branches/ offices shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/ financial status, nature of business activity, information about his clients, business and their location etc.

08 Confirmation/verification of related data/ information obtained :

7.1 IBBPLC shall verify information by at least one of the following methods (in case of persons):

- ❖ confirming the date of birth from an official document (e.g. birth certificate, passport, id card, social security records);
- ❖ confirming the address (e.g. utility bill, tax assessment, bank statement, a letter from a publ thority);
- ❖ contacting the customer by telephone, by letter or by e-mail to confirm the information su after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect address should warrant further investigation);
- ❖ confirming the validity of the official documentation provided through certification by an a ized person (e.g. embassy official, notary public).

7.2 IBBPLC shall verify information by at least one of the following methods (in case of business entities):

- for established corporate entities - reviewing a copy of the latest report and accounts (audited, if available);
- conducting an enquiry by a business information service, or an undertaking from a reputed and known firm of lawyers or accountants confirming the documents submitted;
- undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- utilizing an independent information verification process, such as by accessing public and private databases;
- obtaining prior bank references;
- visiting the corporate entity, where practical;
- contacting the corporate entity by telephone, mail or e-mail.

7.3 IBBPLC shall verify information by at least one of the following (in case of other types of institution):

- obtaining an independent undertaking from a reputed and known firm of lawyers or accountants confirming the documents submitted;
- obtaining prior bank references;
- accessing public and private databases or official sources.

Incompleteness/inadequacy of the above stated information particularly for non cooperation from the customers' end may lead to the Bank to reject any transaction or discontinue the relationship as stated in sections 5.6 and 5.7 of the policy.

CHAPTER – 8

Transaction Monitoring

Transaction Monitoring is the main tool to arrest the suspicious transactions. All concerned shall monitor the transactions of customer on regular basis. The complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be emphasized more during monitoring to detect the Suspicious Transactions. In this respect instructions laid down in the Guidance on reporting of Suspicious Transactions Reporting and Guidelines for Prevention of Trade Based Money Laundering shall be followed. Presently, Transaction Monitoring of IBBPLC is being conducted through both Automated Transaction Monitoring Tool named 'SAS' Transaction Monitoring Tool and Manual Process.

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

- Transactions in local currency;
- Transactions in foreign currency & transactions conducted electronically;
- Transactions above the designated threshold determined by the branch
- Cash transactions under CTR threshold to find out structuring;
- Transactions related with international trade;
- Transaction screening with local and UN Sanction list.
- transactions conducted electronically;
- Transactions conducted in the account of the alleged person(s)/ entity (ies) against whom Adverse Media Report has been published.

To run branch transactions on right way ignoring any STR/ terrorist financing/ illegal financing, an automated monitoring process for the transaction accounts shall be introduced or linked with the CBS through which transaction monitoring shall be done smoothly and perfectly by the Branch Compliance Unit (BCU) as well as by the Central Compliance Committee.

AML & CFT programs depends on a well designed and effective transaction monitoring system and hence every branch must initiate a strong transaction monitoring to identify any transaction that may lead to money laundering and terrorist financing so as to protect the bank from regulatory/pecuniary obligations. In this regard, Red flag, threshold, scenario, logic and intelligence based Transaction Monitoring System shall be in place.

The transaction monitoring system shall be dynamic and able to control an ongoing basis to monitor the relevant activities in the course of the business relationship. Possible areas to monitor may be considered:

a. TP declaration
b. transaction trend in a particular account
c. transaction type
d. source of income
e. professional status
f. regulators' inquiry
g. local punishable incidents
h. predicate offences
i. transaction frequency
j. unusually large amounts
k. structuring

l. suspicious activity scenarios & logics
m. geographical origin/destination
n. changes in account signatories
o. Freeze order
p. Dormant & unclaimed account transactions etc
q. High risk related accounts.

While monitoring/ examining of Transactions following issues shall also be considered:

- United Nation's Security Council resolutions
- Persons/ Entities enlisted in Bangladesh Government Black List
- Countries which can not maintain international standard/ have significant lacking for implementation of AML & CTF program.
- OFAC Sanction
- EU Sanction

The transaction monitoring system shall have to be optimized in terms of false positive and false negative. Automated signaling for SAR/STR shall be generated on the basis of different logics and scenarios. The system shall be capable to produce role based report for effective monitoring and supervision.

It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture and properly trained, vigilant officer through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course. Computerized approaches may include the setting of "floor levels" for monitoring by amount. Different "floor levels" or limits may be set for different categories of customers.

The Customer Category is assigned at account inception and may be periodically revised and is documented on the Transaction Profile. Transaction Limits are established by the business subject to agreement by BAMLCO. The Customer Categories and Transaction Limits are maintained in the computer systems.

Designated officer will review and sign-off on such exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer. The concerned officer will document their review by putting initial on the report and where necessary will prepare internal Suspicious Transaction Reports (STRs) with action plans having adequate records and matters for treating or releasing the transaction from/to suspects.

BAMLCO will review the STRs and responses from the Designated Officer or other concerned officer. If the explanation for the exception does not appear reasonable then the Branch shall review the transactions prior to considering submitting them to the ZAMLCO or CAMLCO.

Apart from the above, the monitoring shall be done in dealing with all types of Investment operations, Import Business, Export Business, Foreign Remittances, procurements, etc. and the reporting of STR/SAR shall be practised by the CAMLCO of the concerned Wing / Divisions of IBBPLC, Head Office to the Central Compliance Committee (CCC) for onward submission of the same to Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank. In this regard, CAMLCO shall maintain all the supporting records and documents of the decisive factors.

Basically, Branches shall monitor all the unusual transacted accounts. But, following accounts must be monitored on regular and continuous basis:

- High Risk accounts
- PEPs/ IPs accounts
- Trust, NGO & NPO accounts
- Charity & Social organization Accounts
- Walk-in Customers
- Beneficiary who does not maintain accounts.
- Accounts opened through different digital platform under e-KYC
- Transactions of Trade Customers
- Transactions & Trend (Nature of adjustment, destination of fund, etc.) of Investment Customers
- CTR generated accounts
- Accounts are running with Beneficial Owner's Fund
- Importer & Exporter's account
- Defaulter's account.
- Accounts which are transacted by 3rd party.
- Transaction Profile violated accounts.
- Transaction in dormant & unclaimed accounts
- STR submitted Accounts
- Internet Banking Accounts
- M-Cash Accounts
- Agent Banking Accounts
- Negative Media affected Accounts
- Mother A/C of Locker A/C holder
- Under any regulatory (ACC, NBR, BFIU) investigation Accounts

Following Red Flags may be consulted to detect the suspicious transactions of the accounts:

Banking Transactions

Cash transactions

- ❖ Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
- ❖ Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- ❖ Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.
- ❖ Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).
- ❖ Customers who constantly pay in or deposit cash to cover requests for payment order, bankers drafts, money transfers or other negotiable and readily marketable money instruments.
- ❖ Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
- ❖ Branches that have a great deal more cash transactions than usual. (Head Office statistics detect aberrations in cash transactions.)
- ❖ Customers whose deposits contain counterfeit notes or forged instruments.
- ❖ Customers transferring large sums of money to or from other locations with instructions for payment in cash.
- ❖ Large cash deposits using Deposit Machine facilities, thereby avoiding direct contact with bank or building society officer.

- ❖ Frequent remote cash deposit of similar amount and nature which have sufficient ground to suspect.

Accounts

- ❖ Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominee names.
- ❖ Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
- ❖ Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).
- ❖ Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.
- ❖ Customer's reluctance or refusal to disclose other banking relationships.
- ❖ Home address or business location is far removed from the Branch where the account is being opened and the purpose of maintaining an account at your Branch cannot be adequately explained.
- ❖ Reluctance or refusal to provide business financial statements.
- ❖ Information provided by the customer in the Transaction Profile does not make sense for the customer's business.
- ❖ A visit to the place of business does not result in a comfortable feeling that the business is in the business they claim to be in.
- ❖ Customers who appear to have accounts with several financial institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.
- ❖ Matching of payments out with credits paid in by cash on the same or previous day.
- ❖ Paying in large third party cheques endorsed in favor of the customer.
- ❖ Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- ❖ Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
- ❖ Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.
- ❖ Companies' representatives avoiding contact with the branch.
- ❖ Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
- ❖ Customers who show an apparent disregard for accounts offering more favourable terms
- ❖ Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.
- ❖ Insufficient use of normal banking facilities, e.g. avoidance of high interest rate facilities for large balances.
- ❖ Large number of individuals making payments into the same account without an adequate explanation.

International banking/trade finance

- ❖ Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.
- ❖ Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

- ❖ Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bonafide transactions to, or receive regular and large payments from: countries which are commonly associated with the production, processing or marketing of drugs; proscribed terrorist organizations; [tax haven countries].
- ❖ Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held in other locations.
- ❖ Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.
- ❖ Frequent requests for TCs, foreign currency drafts or other negotiable instruments to be issued.
- ❖ Frequent paying in of TCs or foreign currency drafts, particularly if originating from overseas.
- ❖ Customers who show apparent disregard for arrangements offering more favourable terms.
- ❖ Customer makes changes to a Letter of Credit beneficiary just before payment is to be done.
- ❖ Payment made by wire transfers from third parties unconnected to the underlying transactions
- ❖ Letter of Credit covers goods that have little demand in importing country
- ❖ Letter of Credit is received from countries with a high risk for money laundering
- ❖ Commodities are shipped through one or more jurisdictions for no apparent economic or logistic reasons
- ❖ Frequent dollar endorsement for traveling abroad

Institution's employees and agents

- ❖ Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.
- ❖ Changes in employee or agent performance, e.g. the salesman selling products for cash have a remarkable or unexpected increase in performance.
- ❖ Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

Secured and unsecured lending

- ❖ Customers who repay problem investment unexpectedly.
- ❖ Request to borrow against assets held by the financial institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
- ❖ Request by a customer for a financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.
- ❖ Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earning capacity or asset base.
- ❖ Customers who are always interested to repay the investment dues in cash instead of cheque.

Merchant Banking Business

New business

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

Dealing patterns and abnormal transactions

Dealing patterns

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

Abnormal transactions

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

Settlements

Payment

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

Delivery

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

Disposition

- Payment to a third party without any apparent connection with the investor.
- Settlement either by registration or delivery of securities to be made to an unverified third party.
- Abnormal settlement instructions including payment to apparently unconnected parties.

Pointing to Financing of Terrorism

Behavioural Indicators:

- ❖ The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- ❖ Use of false corporations, including shell-companies.
- ❖ Inclusion of the individual or entity in the United Nations 1267 Sanctions list.
- ❖ Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
- ❖ Beneficial owner of the account not properly identified.
- ❖ Use of nominees, trusts, family members or third party accounts.
- ❖ Use of false identification.
- ❖ Abuse of non-profit organization.
- ❖ In-transparent Nominee relationship

Indicators linked to the financial transactions:

- ❖ The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
- ❖ The transaction is not economically justified considering the account holder's business or profession.
- ❖ A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
- ❖ Transactions which are inconsistent with the account's normal activity.
- ❖ Deposits were structured below the reporting requirements to avoid detection.
- ❖ Multiple cash deposits and withdrawals with suspicious references.
- ❖ Frequent domestic and international ATM activity.
- ❖ No business rationale or economic justification for the transaction.
- ❖ Unusual cash activity in foreign bank accounts.
- ❖ Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- ❖ Use of multiple, foreign bank accounts.

SAS Automated Transaction Monitoring System:

Suspicious Transactions are being identified under 40 (forty) scenarios under SAS. Branch shall cooperate with the Central SAS Automated Transaction Monitoring Team, ML & TF Prevention Division.

Specific responsibilities of the Branches including Sub-Branches, Agent Banking Outlets for SAS Automated Transaction Monitoring System:

- ▪ Head of Branch shall assign specific official (s) issuing office order for automatic transaction monitoring process.
- ▪ BAMLCO or assigned person shall log in TM Tools on regular basis to observe whether any query/ information are asked from the central TM Team.
- ▪ Assigned Officials shall reply the Central TM Team uploading necessary papers/ documents/ information in the specific fields of SAS TM Tool.
- ▪ He shall keep records of all the documents/ communication held for Transaction Monitoring process.

- Assigned official (s) shall update the information of the customers as asked by the Central TM Team (if necessary).
- If any suspicious transaction is detected, STR shall be reported to MLTFPD for filing the same to BFIU.

CHAPTER - 9

Trade Based Money Laundering (TBML)

"Trade-Based Money Laundering" is the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.

Trade Based Money Laundering (TBML) was recognized by the Financial Action Task Force (FATF) as one of the three main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy.

There is a growing concern on how the rapid growth in the global economy has made international trade an increasingly attractive avenue to move illicit funds through financial transactions associated with the trade in goods and services. TBML is a complex phenomenon since its constituent elements cut across not only sectoral boundaries but also national borders. The dynamic environment of international trade allows TBML to take multiple forms. Under this backdrop, IBBPLC has taken comprehensive measures to prevent TBML through using its system.

TBML Compliance program of IBBPLC shall be conducted as per the Guidelines for Prevention of Trade Based Money Laundering issued by Bangladesh Financial Intelligence Unit.

9.1 TBML Compliance Program in IBBPLC:

TBML Compliance program of IBBPLC will be conducted as per the Guidelines for Prevention of Trade Based Money Laundering issued by Bangladesh Financial Intelligences Unit as well as IBBPLC.

9.2 How Trade Based Money Laundering (TBML) can be done

Money launderers can move money out of one country by simply using their illicit funds to purchase high-valued products, and then exporting them at very low prices to a colluding foreign partner, who then sells them in the open market at their true value. In some instances, the situation may reverse. To give the transactions an air of legitimacy, the partners may use a financial institution for trade financing, which often entails letters of credit and other documentation. Trade-based money laundering involves using of the following techniques to disguise the illicit origin of money:

1. Over-and under-invoicing of goods and services;
2. Over and under shipment of goods
3. Multiple invoicing of goods and services; or
4. False description of goods and services.

9.2.1 Tools use for Trade Based Money Laundering (TBML)

The following tools are used for Trade Based Money Laundering (TBML):

Under invoicing

The act or practice of stating the price of goods on an invoice as being less than the price actually paid. Under invoicing occurs if the importer and/or exporter wish to reduce a tariff or if a buyer and/or seller wish to reduce their apparent profits so as to pay less in taxes.

Over invoicing

An invoice with a price listed that is higher than a company actually intends to charge a client. The overpayment is returned to the customer in the form of liquid or various benefits. The advantage of over-invoicing is obviously tactful exit of illegal money.

Multiple invoicing of goods and services

By providing multiple invoices for the same transaction, a money launderer or terrorist financier can justify multiple payments for the same goods or services. In addition, by using a number of financial institutions to make these multiple payments, a money launderer or terrorist financier can increase the level of complexity of the transaction and complicate efforts at detection. If the transaction is detected, a launderer can offer a number of plausible explanations that compound efforts by officials to detect the activities.

9.2.2 Shell Bank

A Shell bank is a corporate entity that looks like bank, but is not really bank. The purpose is to deceive others into thinking the company is a bank. It conceals the identity of the beneficial owner of the funds, and the company records are often more difficult for law enforcement to access because they have no physical presence in any country.

9.2.3 Correspondent Banks

Correspondent Bank carries out transactions on behalf of customers of respondent bank. This indirect relationship means that the correspondent bank provides services for individual or firms for which it has neither verified the identities nor obtained first hand knowledge about the end client.

9.2.4 Payable Thorough Accounts (PTAs)

Payable-through account is an arrangement where the respondent bank’s customers are allowed to conduct their own transactions - such as sending ware transfers, making and withdrawing deposits and maintaining checking accounts- through the respondent’s bank correspondent account without needing to clear the transactions through the respondent bank.

9.2.5 Bank Capture

In extreme cases, money launderer may have a controlling interest in a bank, allowing them to move funds without scrutiny.

9.3 Red Flags for Trade Based Money Laundering

1. Inability of a bank customer to produce trade documentation to back up a requested bank transaction.

2. Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.
3. Significant discrepancies appear between the description of the goods on the bill of lading or invoice and the actual goods transported.
4. Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
5. Shipment locations or description of goods that are inconsistent with the letter of credit.
6. Documentation showing a higher or lower value or cost of merchandise than that which was declared to Customs or paid by the importer.
7. 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.
8. A third party paying for the goods.
9. 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).
10. 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.
11. The commodity is transshipped through one or more jurisdictions for no apparent economic reason.
12. 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 defence articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as, metals, ore and crude oil.
13. 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.
14. Letter of Credit covers goods that have little demand in importer's country.
15. Letter of Credit covers goods that are rarely if ever produced in the exporter's country.
16. Documents arrive without title documents.
17. Obvious misrepresentation of quantity or type of goods imported or exported.
18. A transaction structure that appears unnecessarily complex so that it appears designed to obscure the transaction's true nature.
19. 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).
20. 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.
21. 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.
22. 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.
23. Customer makes changes to a letter of credit beneficiary just before payment is to be made.
24. Customer changes the place of payment in a letter of credit to an account in a country other than the beneficiary's stated location.

25. 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.

9.4 Measures to prevent Trade Based Money Laundering (TBML)

To prevent Trade Based Money Laundering (TBML), the following preventive measures will be taken by IBBPLC in line with the Bangladesh Bank policy guidelines and international best practices:

9.4.1 As the trade is centralized in the Bank, there should be tools/techniques, to the some extend in automation form, in place to determine the prices of importable items is 'competitive' and the price of exportable item is 'fair' to guard the over-pricing and under pricing of both imports and exports.

9.4.2 Establishing, continuing or re-establishing of correspondent relationship with Shell Banks or Establishing, continuing or re-establishing of correspondent relationship with those banks who are continuing the relationship with shell banks is prohibited. Overseas Banking Division will ensure that the Bank do not maintain any relationship with Shell Banks.

9.4.3 IBBPLC will not permit Payable-through accounts (PTAs) arrangement with any of its customers, subsidiaries, overseas branches if any.

9.4.4 IBBPLC will ensure proper KYC/CDD/EDD procedures both for on-boarding correspondent relationships and existing correspondent relationships to prevent TBML through correspondent networks.

9.4.5 To detect the Bank Capture, one of the basic tools for TBML, during the procedures of CDD, the Bank will properly ensure the shareholding structures of correspondent banks and also structures of the major shareholding firms of that bank.

9.4.6 Before providing correspondent banking service or continuing the existing CB relationship on renewal basis, approval from the CAMLCO must be obtained on being satisfied about the nature of the business of the respondent bank through collection of information as per the instructions issued by Bangladesh Bank/ IBBPLC time to time. If required necessary addition al information may be collected by using Open Sources.

9.4.7 IBBPLC shall establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.

9.4.8 IBBPLC shall pay particular attention when maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries and territories and Territories list). Enhanced due diligence shall be required in such cases. Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.

9.4.9 Enhanced Due Diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customers to transact business on their be half (i.e. payable through account)

9.4.10 All instructions issued from BFIU/ IBBPLC shall be applicable for arresting TBML.

9.5 Record Keeping for Trade based Money Laundering (TBML)

All records related to trade transactions must be preserved up to 05 (five) years from the date of transactions or closing of any of trade transaction accounts.

9.6 Screening

To prevent the trade transactions with under sanctioned country, institutions, individual, ports, vessels etc., all of the trade transactions should be screened by the "Real Time Sanctions Screening Solutions" vendored by Accuity.

9.7 Reporting of STR/SAR

All AD Branches dealing with Foreign Exchange business and Foreign Trade Processing Division shall monitor the trade transactions and anything found suspicious shall be filled STR/SAR to the Central Compliance Committee (CCC) complying all necessary instruction while filling STR/SAR.

9.8 Exception review and monitoring

Upon obtaining Exceptions report through STR/SAR, Central Compliance Committee (CCC) shall monitor the scenario to prevent further occurring such exceptions.

9.9: Training & motivation for TBML

General Training on TBML for all employees shall be ensured. Besides, need based training on TBML shall be conducted for the selected Executives/ Employees of the Bank. In addition, a course in the foundation training program shall be included on TBML.

CHAPTER -10

Record Keeping

Record keeping is an essential component of the audit trail that the Laws and Regulations seek to establish in order to assist in any financial investigation and to ensure that criminal funds which are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

IBBPLC shall retain records concerning customer identification and transactions as evidence of the work it has undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

10.1 Records to be kept

For the aforesaid purposes, IBBPLC's records shall 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 IBBPLC

10.2 Customer Information

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

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

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

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.

10.3 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 from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer shall be retained for a period of **five years** from the date on which the transaction is completed.

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.

10.4 Internal and External Reports

IBBPLC shall make and retain:

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

In addition, copies of any STRs made to the BFIU 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.

10.5 Other Measures

IBBPLC's records shall include:

(a) in relation to training:

- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate with evaluation.
- Managing Director's Commitment

(b) in relation to compliance monitoring

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

10.6 Formats and Retrieval of Records

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

It is not always necessary to retain documents in their original hard copy form, provided that the bank has reliable procedures for keeping records in electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, IBBPLC may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on the bank itself and the responsibility is thus on the bank to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required.

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

For more clarifications, the records prepared and maintained by bank's customer relationships and transactions shall be such that:

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

Where there has been a report of a suspicious activity concerning to a client or a transaction, records concerning to the transaction or the client shall be retained until confirmation is received that the matter has been concluded.

10.7 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:

  (1) the customer;
  (2) the beneficial owner of the account or product;
  (3) the non-account holder conducting any significant one-off transaction;
  (4) any counter-party;

- details of transaction including:

  (5) the nature of such transactions;
  (6) Customer's instruction(s) and authority(ies);
  (7) source(s) and volume of funds;
  (8) destination(s) of funds;
  (9) book entries;
  (10) custody of documentation;
  (11) the date of the transaction;
  (12) 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 :

i. the carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
ii. the ending of the business relationship; or
iii. the commencement of proceedings to recover debts payable on insolvency

10.8 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.

10.9 Investigations

Where any Branch of IBBPLC 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 IBBPLC 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:

I. the date and nature of the enquiry,
II. details of the account(s) involved; and
III. be maintained for a period of at least 5 years

10.10 Training Records

The Bank shall arrange training for its officials to comply with regulations and maintain records thereof which include:
i. details of the content of the training programs provided;
ii. the names of officer who have received the training;
iii. the date on which the training was delivered;
iv. the results of any testing carried out to measure officer understanding of the money laundering requirements; and
v. an on-going training plan.

10.11 Branch Level Record Keeping

To ensure the effective monitoring and demonstrate their compliance with the concerned regulations, Branches of IBBPLC have to ensure the keeping or availability of the following records at the branch level either in hard form or electronic form:

1) Information regarding Identification of the customer,
2) KYC information of a customer,
3) Transaction report,
4) Suspicious Transaction/Activity Report,
5) Exception report,
6) Training record,
7) Return submitted or information provided to the Head Office or competent authority.
8) All Internal / External Audit inspection reports.

CHAPTER – 11

Reporting of STR and CTR

11.1 Suspicious Transaction Reporting

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;
- 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.

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

Generally, STR/SAR means a formatted report of suspicious transactions/activities where there is reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seems to be usual manner. Such report is to be submitted by banks to the competent authorities i.e. to BFIU. Suspicion basically involves a personal and subjective assessment. IBBPLC shall assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

11.2 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. Guidance on reporting of suspicious transactions shall be followed for identification of Suspicious Transactions and Reporting thereof. Generally the detection of something unusual may be sourced as follows:

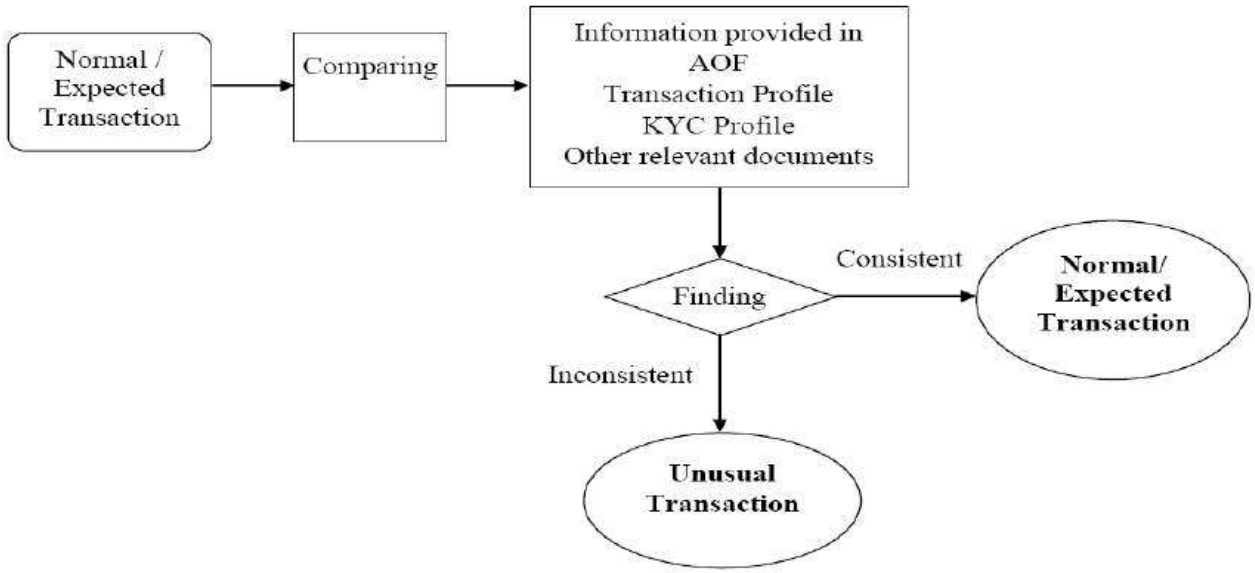
- Comparing the KYC profile, if any inconsistency is found and there is no reasonable explanation;

- By monitoring customer transactions;
- By using red flag indicator.

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

All suspicions reported to the ML&TFPD 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/SAR-



As 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:

11.3 Identification

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

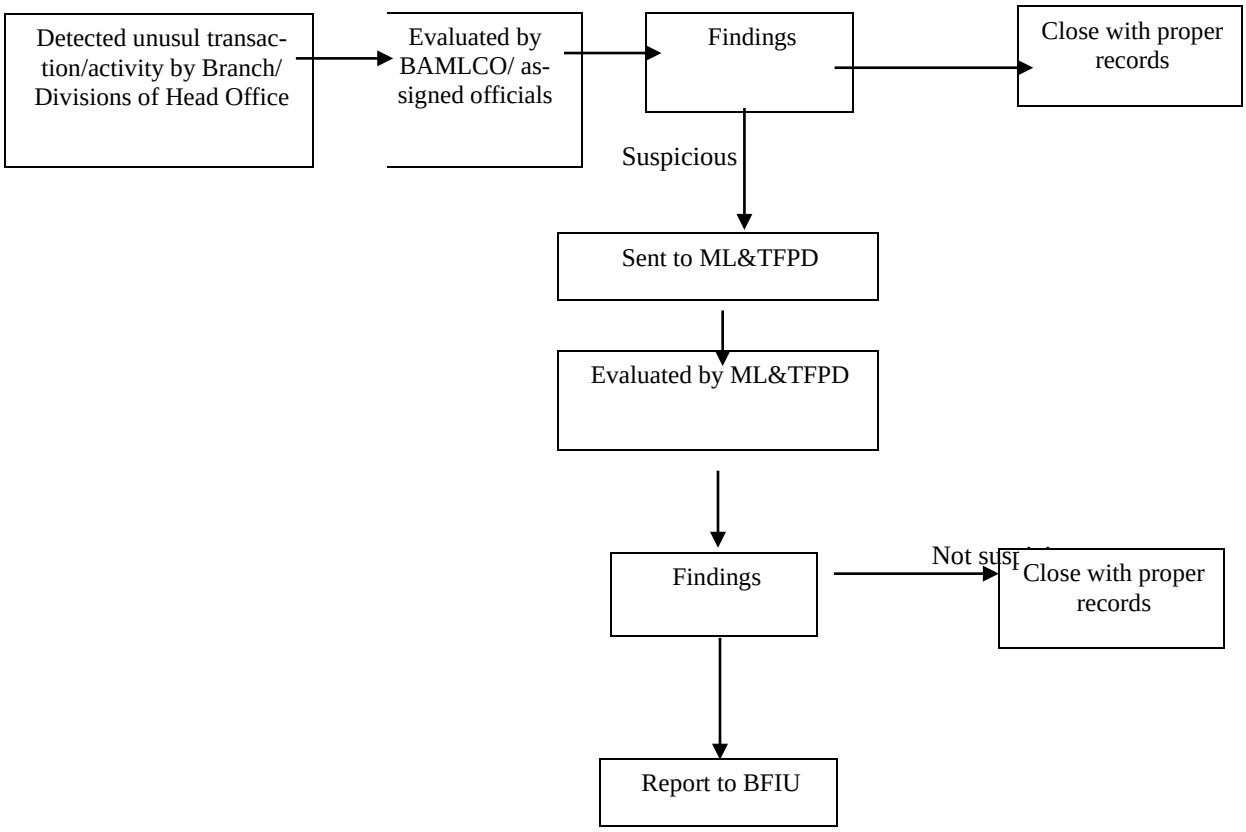
11.4 Evaluation

This part must be in place at branch level and Central Compliance Committee (CCC). After identification of STR/SAR at branch level, BAMLCO shall evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. If BAMLCO is not satisfied, he shall forward the report to CCC. After receiving report from branch, CCC shall check the sufficiency of the required documents. Every stages of evaluation (whether reported to BFIU or not), bank shall keep records with proper manner.

11.5 Disclosure

This is the final stage and banks shall submit STR/SAR to BFIU if it still looks suspicious.

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



11.6 Cash Transaction Report

System will generate Branch-wise monthly cash transaction report and CCC shall have access to the Central MIS to review the report. Simultaneously, branches of IBBPLC need to identify whether there is any suspicious transaction reviewing the cash transactions. If any suspicious transaction is found, the branch of IBBPLC will submit it as 'Suspicious Transaction Report' to the CCC. If no such transaction is identified, it needs to inform to the CCC as 'No suspicious transaction has been found' while reporting the CTR. Besides, every branch of IBBPLC needs to preserve its CTR in their own records.

The Central Compliance Committee (CCC) needs to prepare the accumulated CTR with the assistance of IT received from its all branches. The CCC must ensure the accuracy and timeliness while reporting to BFIU. Moreover, it has to review all the cash transactions from the branches above the threshold and search for any suspicious transaction. If any suspicious transactions are found, the branch will submit it as 'Suspicious Transaction Report' to the BFIU. CCC has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR. Moreover, CCC must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

Mentionable that if any of such transaction is under investigation of BFIU, the records have to be preserved even after 5 years of the transaction concerned even though the depicted time was over.

11.7 Reporting of Suspicious Transactions

There is a statutory obligation on all officials to report suspicions of money laundering. Section 25(1)(Gha) of MLPA-2012(Amendment-2015) contains the requirement to report to the Bangladesh Bank. Guidance on Reporting Suspicious Transaction Report for the Reporting Organization issued by BFIU shall be followed for reporting of Suspicious Transactions.

It has to be ensured:

- ❖ that each relevant employee knows to which person they shall report suspicions, and
- ❖ that there is a clear reporting chain under which those suspicions will be passed without delay to the Chief Anti Money Laundering Compliance Officer (CAMLCO).

11.7.1 The following steps shall be taken for submitting STR

- At the time of submitting STR, the Branch Anti-Money Laundering Compliance Officer (BAMLCO) shall examine that whether all formalities were observed or not for opening of the account, whether KYC procedures are maintained or not, whether the transactions are consisting with the Transaction Profile or not. The Branch shall collect updated information from the client, if necessary. After observing all formalities, if it is determined as suspicious, then the Branch shall report to the Central Compliance Committee (CCC) as STR. If the transaction determined as usual, the issue shall be settled at branch level.
- To comply with the instructions of Anti Terrorism Act, 2009 if identified a reasonable cause to believe that the transaction or effort of transaction of the client is related to any proceeds of crime and terrorist financing then the Branch shall report to the Cen-

tral Compliance Committee (CCC) as STR instantly on same day with the comments of BAMLCO.

- **Adverse Media Report:**
  Adverse Media Report is an indicator of Suspicious Transaction as per the Guidance on Reporting Suspicious Transaction Report issued by BFIU. Concerned officials of the Bank shall ensure whether the alleged person/ entity is maintaining any account with IBBPLC or not. If any account is being maintained in the name of alleged person/ entity, Suspicious Transaction/ Activity Report shall be filed to MLTFPD/ Central Compliance Committee.
- Upon receipt an STR from the Branch, the CCC shall submit the same to BFIU within 03 (three) working days after proper examination through goAML software of BFIU.

11.7.2 Necessary papers / documents for STR

1. Separate forwarding letter to be issued for every STR.
2. Copy of the related Account Opening Form to be submitted with STR.
3. Copy of the related KYC, TP & other papers shall be submitted with STR.
4. Related Account statement for minimum 01 (one) year to be enclosed.
5. Related Investigation Report to be submitted with STR.
7. Copy of at least two related vouchers shall be submitted

Where it is impossible in the circumstances to refrain from executing a suspicious transaction before reporting to the BFIU or where reporting it is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operations, the branches shall apprise the BFIU immediately afterwards. While it is impossible to spell out in advance how to deal with every possible contingency, in most cases common sense will suggest what course of action is most appropriate. Where there is doubt, the advice of the Anti Money Laundering Compliance Officers may be sought.

It is the Chief Anti Money Laundering Compliance Officer (CAMLCO) who will have the responsibility in the bank for communicating reports of suspicious transactions to BFIU and who will act as the liaison officer between the IBBPLC and the BFIU.

The CAMLCO must take steps to validate the suspicion in order to judge whether or not a report shall be submitted to BFIU. In making this judgment, he shall consider all other relevant information available within the Bank concerning the person or business to which the initial report relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the relationship and referral to identification records held. If, after completing this review, the CAMLCO decides that there are no facts that would negate the suspicion, then he will disclose the information to BFIU.

The determination of whether or not to report implies a process with at least some formality attached to it. It does not necessarily imply that the CAMLCO must give reasons for negating and therefore not reporting any particular matter, but it clearly would be prudent for internal procedures to require that written reports are submitted and that he shall record his determination in writing. Clearly in cases where there is a doubt it would be prudent for the CAMLCO to make a report to the BFIU.

The CAMLCO will be expected to act honestly and reasonably and to make his determinations in good faith. Provided the CAMLCO or an authorized deputy does act in good faith in

deciding not to pass on any suspicions report, there will be no liability for non-reporting if the judgment is later found to be wrong.

Care shall be taken to guard against a report being submitted as a matter of routine to BFIU without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

11.8 Internal Reporting Procedures and Records

Reporting lines shall be as short as possible, with the minimum number of people between the person with the suspicion and the CAMLCO. This ensures speed, confidentiality and accessibility to the CAMLCO.

Supervisors shall also be aware of their own legal obligations. He has a legal obligation to report to the BAMLCO.

All suspicions reported to the BAMLCO shall be documented (in urgent cases this may follow an initial discussion by telephone). The report shall include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

The BAMLCO shall acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. “tipping off”. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, shall be documented.

On-going communication between the BAMLCO and the reporting person/department is important. It is particularly important that the BAMLCO is informed of all communication between the investigating officer and the branch concerned at all stages of the investigation.

Records of suspicions shall be retained for five years from the date of the transaction. Records of suspicions which the BFIU has advised are of no interest shall be retained for a similar period. Records of suspicions that assist with investigations shall be retained until the branch is informed by the BFIU that they are no longer needed.

11.9 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.

At the time of CTR any educational degree or title of the client such as Mr, Mrs, Dr, Al-Haj etc. will not be used but his original name only be used.

IBBPLC 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.

11.10 Tipping off:

Bank officials need to consider the confidentiality of the reporting of STR/SAR. They shall not make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious. Besides, the STRs already reported/ filed to BFIU shall not be subject to any internal/ external auditors. But, the same may be disclosed or handed over upon being warranted by a Competent regulatory/ court authority.

All concerned shall be aware of maintaining confidentiality of the information related to the identification of suspicious transaction/ activity & reporting thereof and the information asked by BFIU time to time. In this connection, instruction laid down in the BFIU circular No. 01 dated 22.04.2018 shall be complied with.

CHAPTER - 12

Training and Awareness

FATF recommendation 18 suggests that a formal AML/CFT compliance program shall include an ongoing employee training program. The importance of a successful training and awareness program can not be overstated. Employees in different business functions need to understand how the IBBPLC's policy, procedures, and controls affect them in their day to day activities. As per AML circular, IBBPLC shall arrange suitable training for their officials to ensure proper compliance of money laundering and terrorist financing prevention activities.

12.1 Employee Screening

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

12.2 Know Your Employee (KYE)

Know-your-customer, an essential precaution, must be coupled with know-your-employees. There are a lot of instances that highlight the involvement of employees in fraudulent transactions and in most cases in association with customers. This therefore brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables. Policies, procedures, job descriptions, internal controls, approval levels, levels of authority, compliance with personnel laws and regulations, code of conduct/ethics, accountability, dual control, and other deterrents shall be firmly in place. And the auditor shall be conversant with these and other requirements, and see that they are constantly and uniformly updated. KYE requirements shall be included in the IBBPLC's HR policy.

12.3 Training for Employee

To ensure the effective prevention of ML, TF & Proliferation Financing, concerned authorities of IBBPLC shall comply with the followings:

- Appropriate Training shall be ensured for all the Employees of IBBPLC on Prevention of Money Laundering (ML), Terrorist Financing (TF) and financing in proliferation of weapons of mass destructions. 'Appropriate Training' means the basic training for prevention of ML, TF & PF for all the employees working under different departments/ Divisions/ Wings/Branches of IBBPLC, the training necessary to their respective desk to minimize the ML & TF Risk and the refresher training after a specific time interval.
- IBBPLC shall ensure at least 01 (one) AML & CFT training for the employees within each 2 (two) consecutive years.
- Appropriate training shall be provided to the CAMLCO & DCAMLCO and the others concerned employees to enhance the professional capability and/ or necessary arrangement shall be available for them to acquire Professional Certificates.
- Records of all trainings shall be preserved for at least 05 (five) years.

AML & CFT basic training of IBBPLC shall cover the followings-

- ❖ an overview of AML & CFT initiatives;
- ❖ relevant provisions of MLPA & ATA and the rules there on;
- ❖ regulatory requirements as per BFIU circular, circular letters and guidelines;
- ❖ CDD measures
- ❖ Transaction Monitoring
- ❖ KYC & TP upgrading program.
- ❖ STR/SAR reporting procedure;
- ❖ ongoing monitoring and sanction screening mechanism;

Besides, basic and refreshment AML & CFT training, IBBPLC shall arrange job specific training or focused training i.e., Trade based money laundering training for the trade professional employees who deal with foreign or domestic trade, UNSCR screening related training for all employees who deal with international transactions, customer relations and account opening; fraud through ATM Card/Visa Card/ Khidmah Card/ Traveler Card etc. and ML related training for all the employees who deal with investment of the bank; customer due diligence and ongoing monitoring of transaction related training for the employees who conduct transaction of customers. There shall have specific training for the concerned employees of ICCW on Independent Testing procedure.

12.4 Customer Awareness

Concerned units of IBBPLC shall ensure the following issues to grow customer awareness on prevention of Money Laundering, Terrorist Financing & Proliferation of weapons of mass destruction:

- At the time of customer on-boarding, concerned desk official (s) shall discuss with the customers for the justification of receiving customer information, documents & papers so that they become familiar with the AML & CFT program.
- To grow the customer awareness on the AML, CTF & Prevention of PF, leaflet distribution program shall be conducted.
- Posters on the AML & CFT issues shall be hung in the auspicious places.
- Concerned authority shall take proper initiatives for broadcasting awareness building advertisement and documentaries regarding prevention of money laundering and terrorist financing through different mass media under Corporate Social Responsibility (CSR) fund.

12.5 Awareness of Mass People

Prevention of ML & TF largely depends on awareness at all level. Public or mass people awareness on AML & CFT measures provides synergies to banks in implementing the regulatory requirement. For this, IBBPLC under the guidance of BFIU, BB, other regulators as well as the government shall arrange public awareness programs on AML & CFT issues like advertisements through billboard, poster, festoon and mass media, distribution of handbills, leaflet and so on which will continue in the next course of action.

12.6 The Need for Staff Awareness

Officials of IBBPLC shall be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All officers shall be trained up to co-operate fully and to provide a prompt report of any suspicious transactions.

It is, therefore, important that branches introduce comprehensive measures to ensure that all officer and contractually appointed agents are fully aware of their responsibilities.

12.7 Education & Training Program:

All officials shall be educated in the process of the "know your customer" requirements for money laundering prevention purposes. The training in this respect shall cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant officials shall be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

12.8 General Training

A general training program shall include the following:

- General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
- Legal framework, how AML/CFT related laws apply to Bank and employees;
- Internal policies and systems with regard to customer identification and verification, due diligence , monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees.

The person responsible for designing the training must identify which, if any, of these topics relate to the target audience. Effective training shall present real life money laundering schemes, preferably cases that have occurred at the institution or at similar institutions, including, where applicable, how the pattern of activity was first detected and its ultimate impact on the bank.

12.9 New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting any suspicious transactions to the Branch Anti Money Laundering Compliance Officer (BAMLCO) shall be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They shall 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.

12.10 Customer Service/Account Opening Officer/Tellers/Foreign Exchange Dealers

Officials dealing directly with the public are the first point of contact with potential money launderers and their efforts are vital to the organization's strategy in the fight against money laundering. They must be made aware of their legal responsibilities and shall be made aware of the organization's reporting system for such transactions. Training shall be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

It is vital that 'front-line' officials of IBBPLC are made aware of the organization's policy for dealing with non-regular (walk in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

12.11 Investment Officials

Training shall reflect an understanding of the Investment function. Judgments about collateral and investment require awareness and vigilance toward possible laundering and funding terrorists. Indirect funding programs and lease financing also call for KYC efforts and sensitivity to laundering risks.

12.12 Processing (Back Office) Officials

Those members of employees who receive completed Account Opening, Payment Order/DD/TT/MTDR application forms and cheques for deposit into customer’s account or other investments must receive appropriate training in the processing and verification procedures. Those employees who are in a position to deal with account opening, or to accept new customers, must receive the training given to cashiers and other front office officer above. In addition, the need to verify the identity of the customer must be understood, and training shall be given in the organization's account opening and customer/client verification procedures. Such officials shall be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Anti Money Laundering Compliance Officer whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

12.13 Trade Processing Officials

Those employees who are in a position to deal with all types of International Trade Processing including dealing with all sorts of Import & Export LCs, Foreign Remittances, etc.

12.14 Audit and compliance staff

These are the people charged with overseeing, monitoring and testing AML/CFT controls, and they shall be trained about changes in regulation, money laundering and terrorist financing methods and enforcement, and their impact on the institution.

12.15 Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures shall be provided to those with the responsibility for supervising or managing officer. This will include the offences and penalties arising from the Act for non-reporting and for assisting money launderers; internal reporting procedures and the requirements for verification of identity and the retention of records.

12.16 Senior Management and Board of Directors

Money laundering and terrorist financing issues and dangers shall be regularly and thoroughly communicated to the Board. It is important that the Money Laundering & Terrorist Financing Division has strong Board support, and one way to ensure that is to keep Board members aware of the reputational risk that money laundering and terrorist financing poses to the bank. Major AML/CFT compliance related circulars/circular letters issued by BFIU shall be placed to the Board to bring it to the notice of the Board members.

12.17 Anti Money Laundering Compliance Officials

The AML/CFT Compliance Officer of IBBPLC shall receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, BFIU 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.

12.18 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 shall be accompanied by a quick “why are they here” assessment. New hires shall 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 shall be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.

- ❖ Course evaluation shall be done to evaluate how well the message is received; copies of the answer key shall 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.

12.19 Refresher Training

In addition to the above compliance requirements, IBBPLC's training shall be tailored to the needs of specialized areas of the bank'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 official of IBBPLC does not forget their responsibilities. For some officials may provide such training on an annual basis; others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.

IBBPLC's Training shall be conducted ongoing basis, incorporating trends and developments in bank'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 importances when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.

12.20 General Policy of IBBPLC to the Training

i) No employee of IBBPLC shall remain out of AML & CFT Training
ii) All employees of IBBPLC shall be brought under AML & CFT Training once every two year
iii) Need base Training shall be provided on priority basis
iv) Central Compliance Committee of IBBPLC shall design/ prepare the AML Training schedules, modules, materials and questionnaires
v) Human Resources Division of IBBPLC shall issue necessary office order to the deserving participants and shall keep the record of AML training imparted to each employee in an automated manner
vi) A panel of the Trainers of Trainee (ToT) shall be prepared to conduct effective AML & CFT Training Program
vii) AML & CFT Training shall have an effect to the promotion of the employees
viii) Arranging of AML & CFT Training for the employees both home and abroad
ix) Introduction of AML e-learning system

CHAPTER -13

Terrorist & Proliferation Financing

13.1 Introduction:

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

The bank shall not knowingly go for any transactions proceeds of which involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activity, is committing a criminal offence under the laws of Bangladesh. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism.

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

13.2 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.

13.3 Movement of Terrorist Fund

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

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

Often, terrorist organizations 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.

13.3.1 Formal Financial Sector

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

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

13.3.2 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.

13.3.3 Cash Couriers

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

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

13.3.4 Use of Alternative Remittance Systems (ARS)

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

13.3.5 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.

13.4 Targeted Financial Sanctions

In recent years, the concept and strategy of targeted sanctions imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, have been receiving increased attention. 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.

To implement TFS in Bangladesh, the Government has issued Statutory Regulatory Order (SRO) under section 2 of the United Nations (Security Council) Act, 1948 (29 November, 2012) and amended the SRO to make it more comprehensive (June, 2013). To make the process enforceable, a separate section has been included in ATA, 2009 through amendment of ATA in 2013. Section 20(A) of ATA, 2009 covers all the requirements under UNSCR's tool were taken and will be taken under chapter VII of the charter of UN. Before that BFIU used to issue circular letters for reporting organizations to implement UNSCR resolutions.
For effective implementation of these provisions, detailed mechanism has been developed in Anti-terrorism Rules, 2013. Under rule 16 of AT rules, 2013, IBBPLC as a reporting agency has to maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. In case there is any fund or economic resources held by the listed individuals and entities, IBBPLC shall immediately stop payment or transaction of funds, financial assets or economic resources and report to the BFIU within the next working day with full particulars of the listed and/or the suspected individuals or entities or related or connected individual identities.

13.5 Automated Screening Mechanism of UNSCRs

For effective implementation of TFS relating to TF & PF, IBBPLC requires to have automated screening mechanism that could prohibit any listed individuals or entities to enter into the banking channel. The bank shall operate in such system whether they could detect any listed individuals or entities prior to establish any relationship with them. In particular, IBBPLC needs to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individuals or entities could not use the formal financial channel. In a word, the IBBPLC shall ensure that screening has done before-

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

For proper implementation of UN sanction list, every official of IBBPLC shall 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.

13.6 Role of IBBPLC in Preventing TF & PF

Following initiatives shall be taken to implement the Security Council Resolution 1267 & resolution adopted before it, Security Council Resolution 1373 of United Nations and Resolution for Proliferation of weapons of mass destruction & Financing thereof and its control & prevention:

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

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

- If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, IBBPLC 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.

- IBBPLC shall maintain a list of the persons/ entities in electronic form suspected for terrorism, terrorist financing & financing in proliferation of weapons of mass destruction by the United Nations and the black listed persons/ entities as declared by Bangladesh Government and ensure proper utilization of the same.

- IBBPLC shall run a check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009; individuals or entities owned or controlled directly or indirectly by such persons or entities, as well as persons and entities acting on behalf of, or at the direction of, individuals or en tities listed or scheduled under the Act are holding any funds, financial assets or eco nomic resources or related services or having any form of relationship with them.

- To identify the accounts maintained in the name of the persons/ entities or individuals or entities owned or controlled directly or indirectly by such persons as well as persons and entities acting on behalf of, or at the direction of whose name is enlisted in the UN Sanction List or the above mentioned persons who is black listed by Bangladesh Government, a regular activities shall be conducted and if necessary transactions shall be monitored. Besides, the 'False Positive' list as identified in the above process shall also be maintained. If any account or transaction is detected in the above process, the issue shall be communicated to BFIU with necessary information/ papers within next working day marking the account as 'freeze'.

- For compliance of the Resolutions of United Nations on terrorism, terrorist financing & proliferation of weapons of mass destruction, Guidance Notes for Prevention of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction shall be followed.

CHAPTER-14

Screening

Screening is the filtering of relevant individuals, entity or transactions prior to execution or on-boarding. This activity, together with the screening of client details both at on-boarding and at other points during the client relationship, is typically used for complying with embargoes and sanctions and can be most effectively used for the identification of payments to or from persons or entities for which relevant competent authorities have provided notice to the Bank.

In order to enhance the quality of real-time and other screening activity, IBBPLC believes that the following points are of the utmost importance:

- Real-time screening shall only be required for screening and filtering related to embargoes or sanctions, and the Bank should not be required to engage in real-time screening for names other than those specified by relevant competent authorities Institutions should screen during on-boarding and at appropriate points during the subsequent relationship (e.g.upon receipt of a revised list provided by a relevant competent authority)

- IBBPLC shall be able to rely on the quality and completeness of information provided by relevant competent authorities and other relevant parties such as data providers

- Being an intermediary bank, IBBPLC shall only screen information input by the originator of a payment or other instruction

- In order to minimize the production of a significant number of "false positives" (i.e.,apparent matches that prove to have been incorrect on substantive review) and thereby to maximize operational effectiveness and efficiency, it is essential that lists provided by relevant competent authorities to financial institutions conducting real-time screening contain acceptable amounts and types of information (including, where available, full name, date of birth and other relevant unique identifiers); and

- IBBPLC acting in an intermediary capacity with respect to a payment or other transaction rely, to the extent permissible by law, on the active cooperation and efficiency of their counterparties to avoid delays in completing the transaction by resolving potential issues related to sanctions, embargoes or potential money laundering in a timely manner

14.1 The Lists to be screened with

IBBPLC shall have standard and up to date databases to screen all of its customers with the following lists but not limited to:

IBBPLC shall have standard and up to date databases to screen all of its customers with the following lists but not limited to:

- UN sanction list
- OFAC Sanction List
- EU Sanction List
- High risk customer/PEPs/IP list
- Govt. black listed clients/companies
- Adverse media
- Rejected clients' List
- trustee/waqf/charitable/religious/club/societies organizations

- Non profit organizations
- Fraud database of Bangladesh Bank
- REHAB members list
- BoI registration list
- List of the companies registered with different associations (eg. BGMEA/BKMEA/BJMA etc.)
- List of RJSC & Firms
- FI data base including management/directors list
- Any other lists to be approved by the Management from time to time

14.2 Whom to be screened

- Every deposit client
- Every investment client
- Every remitter
- Every remittance beneficiary
- m-Cash agents
- m-Cash end customers
- 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
- 3rd parties
- Walk-in customers
- And any other potential customers

For screening of the customers with the standard lists of databases may be determined by the Management on Risk Based Approach and can change from time to time depending on the regulatory changes and desires.

14.3 Periodic Rescreening

IBBPLC shall conduct periodic rescreening of its entire customer base in a regular frequency to be determined by the Management from time to time.

CHAPTER-15

Risk Based Framework

A RBA to AML/CFT means that countries, competent authorities and financial institutions are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

When assessing ML/TF risk, countries, competent authorities, and financial institutions should analyze and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures.

The RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate ML/CFT risks, but it is still used for ML or TF purposes.

A RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low

In January 2014, the Basel Committee on Banking Supervision (BCBS) issued a document, entitled "Sound Management of Risks related to Money Laundering and Financing of Terrorism" which includes the following statement on the importance and conduct of Risk Assessments:

"Sound risk management requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied."

15.1 Risk Categorization – Based on Activity/KYC Profile

The risk assessment may be made using the KYC Profile Form in which following six risk categories shall be scored:

- Occupation or nature of customer's business
- Product/ Service and Delivery Channels
- Nature of on-boarding
- Jurisdiction Risk
- Relationship
- Transaction Related Risk
- Transparency Related Risk

The risk scoring of less than 15 indicates low risk and more than or equal 15 indicates high risk. The risk assessment scores are to be documented in the KYC Profile Form.
However, Branch Management may judiciously override this automatic risk assessment to "Low Risk" if it believes that there are appropriate mitigates to the risk. This override decision must be recorded (reasons why) and approved by the Branch Manager, and Branch AML

Compliance Officer. For automatic risk assessment, the Risk Register annexed with this guideline or its changes from time to time shall be utilized.

KYC Profiles and Transaction Profiles must be updated and re-approved at least annually for "High Risk" accounts (as defined above). There is no requirement for periodic updating of profiles for "Low Risk" transactional accounts. These shall, of course, be updated if and when an account is reclassified to "High Risk", or as needed in the event of investigations of suspicious transactions or other concern.

15.2 Obligation for ML & TF Risk Assessment and Management

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on anti money laundering (AML) and combating terrorist financing (CTF) states that countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks. Rule 21 of Money Laundering Prevention Rules (MLPR) 2013 states that every Reporting Organization-Financial Institution (RO-FI) shall conduct periodic risk assessment and forward the same to Bangladesh Financial Intelligence Unit (BFIU) for vetting. It also states that RO-FI shall utilize this risk assessment report after having vetted by BFIU.

As per Money Laundering Prevention Act, 2012 (Amendment-2015)empowers BFIU sufficiently to establish a sound and efficient AML & CFT regime, IBBPLC has to comply with the instructions issued by BFIU under the power of Money Laundering Prevention Act (MLPA), 2012 (Amendment-2015) and Anti Terrorism Act (ATA), 2009 (including all amendments). BFIU vide their Circular Letter No. 01/2015 dated 08.01.2015 issued a Risk Assessment Guideline for the Banks aiming to strengthen AML & CFT regime in Bangladesh. Therefore, it is obligatory for Islami Bank Bangladesh PLC to comply with this Guideline and based on this Guideline, IBBPLC has prepared its own Risk Management Framework.

15.3 Assessing Risk

Islami Bank Bangladesh PLC shall take appropriate steps to identify and assess their money laundering and terrorist financing risks time to time as per ML/TF Risk Assessment Guidelines for Banking Sector issued by Bangladesh Financial Intelligence Unit considering customers, products & services, delivery channels, countries or geographic locations. IBBPLC preserves the documents of those assessments in order to be able to demonstrate it's basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to the competent Authorities.

15.4 Risk Management and Mitigation

Islami Bank Bangladesh PLC shall adopt different policies such as AML & CFT Policy, Customer Acceptance Policy, AML & CFT Risk Assessment Policy and also circulate various instructions/ norms/rules/ procedures that enable the employees of every tier of the Bank to manage and mitigate effectively the risks that have been identified. All the policies, controls and procedures of IBBPLC have been approved by the Board of Directors, and the measures taken to manage and mitigate the risks (whether higher or lower) shall be consistent with national requirements and with guidance from the competent Authorities.

15.4.1 Definition of Risk

Risk means a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities and that may be avoided through preventive action.

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

15.4.2 Risk Management

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

15.4.3 Classification of Risks

As per Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector issued by BFIU, IBBPLC shall categorize Money Laundering (ML) & Terrorist Financing (TF) risks under the following ways:

Business risk :

Business risk is the risk that business may be used for Money Laundering (ML) & Terrorist Financing (TF) and thus the Management of the Bank must assess the following risks in particular to indentify the same:

i) Customer risks.
ii) Products or services risks.
iii) Business practices and/or delivery channels risks.
iv) Country or jurisdictional risks-Geographic location/ vulnerable area.

Regulatory risk:

Regulatory risk is associated with not meeting all obligations of the bank under the Money Laundering Prevention Act, 2012 (Amendment-2015), Anti Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two Acts and instructions issued by BFIU, such as, regulatory obligations like failure to report STR/SAR, inability or inappropriateness in verification of customers and lacking of AML & CFT program (how a business identifies and manages the ML & TF risk it may face), etc.

15.5 Risk Management Structure

For effective risk management, following principles shall be complied at every level of the Bank:

- Risk management contributes to the demonstrable achievement of objectives and improvement of performance, governance and reputation.

- Risk management is not a stand-alone activity that is separate from the main activities and processes of the bank. Risk management is the part of the responsibilities of management and an integral part of all organizational processes, including strategic planning.
- Risk management helps competent Authority of the Bank making informed choices, prioritize actions and distinguish among alternative courses of action.
- Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
- A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
- Risk management is based on the best available information.
- Risk management is aligned with the bank's external and internal context and risk profile.
- Risk management is transparent and inclusive.
- Risk management is dynamic, iterative and responsive to change.

In assessing and mitigating ML & TF risk, IBBPLC considers a wide range of financial products and services, which are associated with different ML/TF risks. These include, but are not limited to:

- Retail banking: where the bank offers products and services directly to personal and business customers (including legal arrangements), such as Current Accounts, Investments and Savings products;
- Corporate and investment banking: where the bank provide corporate finance and corporate banking products and investment (including Import & Export) services to the individuals, corporations, institutions and government;
- Investment services: where the bank provides products and services to manage their customers' wealth (sometimes referred to as privileged or priority banking); and
- Correspondent services: where banking services are provided by one bank (the "correspondent bank") to another bank (the "respondent bank").

15.6 Risk Management Framework

The Risk Management Framework of IBBPLC shall consist of the followings:

15.6.1 Internal & External Context

Establishing the internal and external context within which the designated service is, or is to be, provided. These may include:

- the types of customers;
- the nature, scale, diversity and complexity of their business;
- their target markets;
- the number of customers already identified as high risk;
- the jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML/CFT controls and listed by FATF;
- the distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;
- the internal audit and regulatory findings-causes/ types of irregularities found related to ML & TF.
- the volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.

- ❖ STR/SAR detected by the Branches and its type of predicate offences.

15.6.2 Risk identification

Islami Bank Bangladesh PLC shall evaluate/predict the vulnerability involved in its day to day activities in connection with its clients nature/ dealings, opportunities to misappropriation in products & distribution channels and also its strength to comply the regulatory issues through past performance/data and also prediction. Therefore, risks are identified from the same.

15.6.3 Risk assessment or evaluation

Islami Bank Bangladesh PLC shall assess the risks of its business & regulatory issues through a Risk Matrix which is a blending/ combination of Likelihoods of the risk and also the consequences/impact of those risks. Therefore, each risk is classified into one of 04 risk categories such as Extreme, High, Medium & Low.

15.6.4 Risk treatment

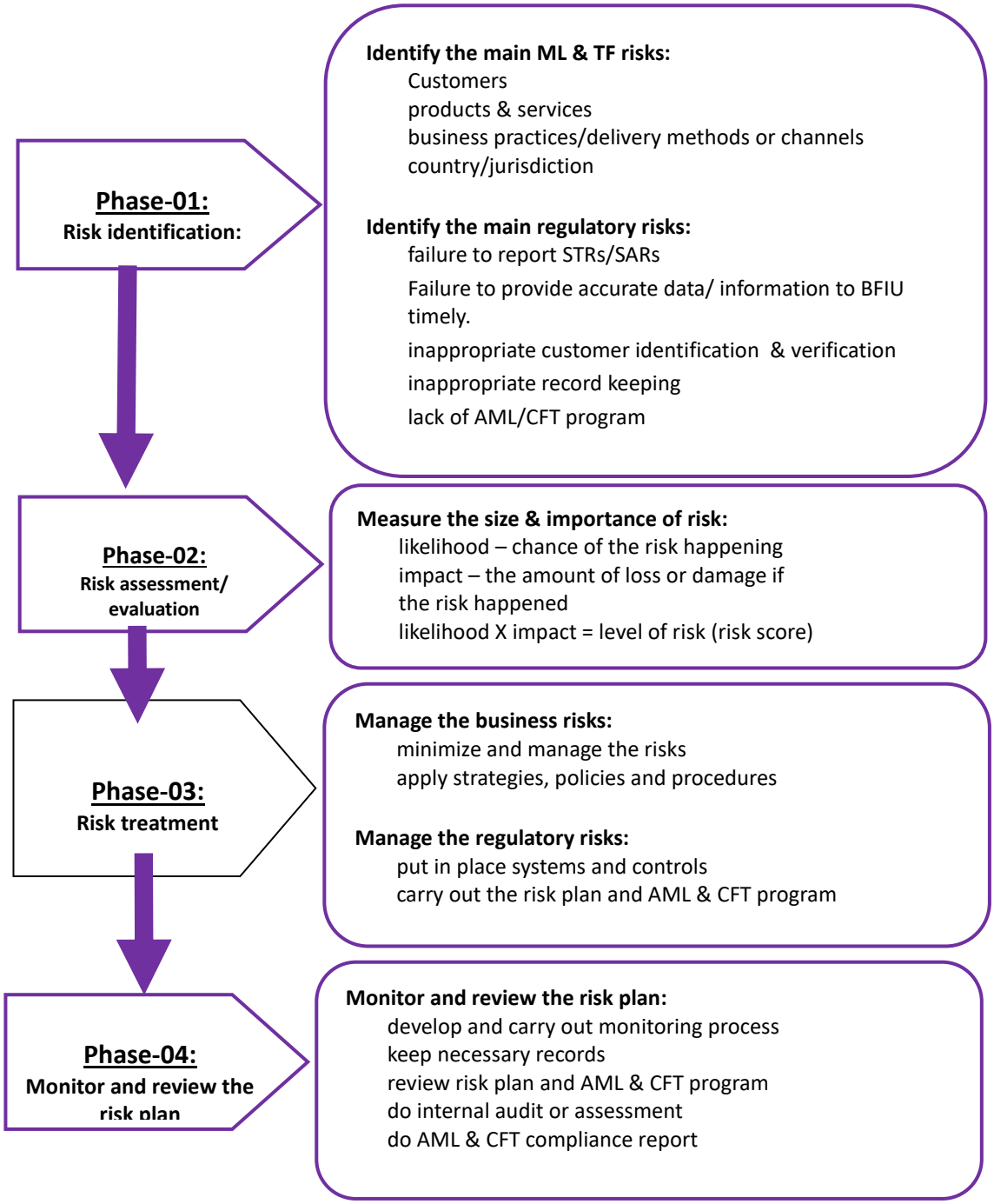
In order to guard against bank's reputational, operational, legal & concentration risk, customer identification is an essential element of an effective Customer Due Diligence (CDD). In terms of Money Laundering Controls, CDD means implementing adequate policies, practices & procedures that promote high ethical and professional standard for dealing with customers and are designated to prevent the bank from being used intentionally or unintentionally, by criminal elements.

Customer Due Diligence (CDD) includes among others the followings:

- ❖ Verification of customers' identification through collecting required/ related information
- ❖ Client's address
- ❖ Nature of business/ profession,
- ❖ Source of funds
- ❖ Uses of funds
- ❖ Volume of transactions, etc.

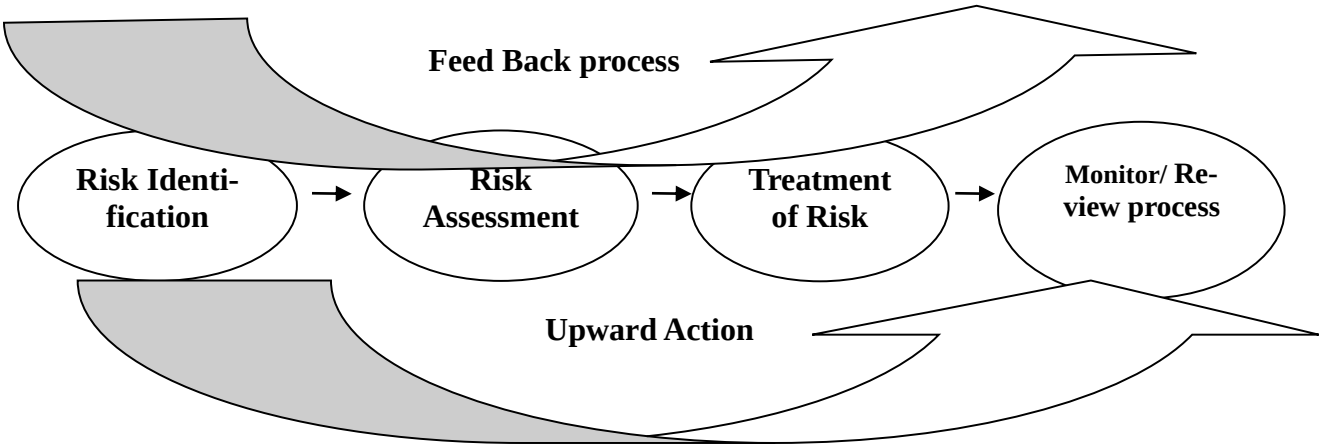
Besides, Enhanced Due Diligence (EDD) also helps financial institutions preventing Money Laundering and Terrorist Financing. EDD though prevails in CDD, means additional examination and cautionary measures aimed at identifying customers and confirming that their activities and funds are legitimate. Islami Bank Bangladesh PLC (IBBPLC) shall conduct its ML & TF risk mitigation process under the spirit mentioned above through applying proper CDD & EDD.

Given below a flow chart of the "Risk Management Framework" of IBBPLC:



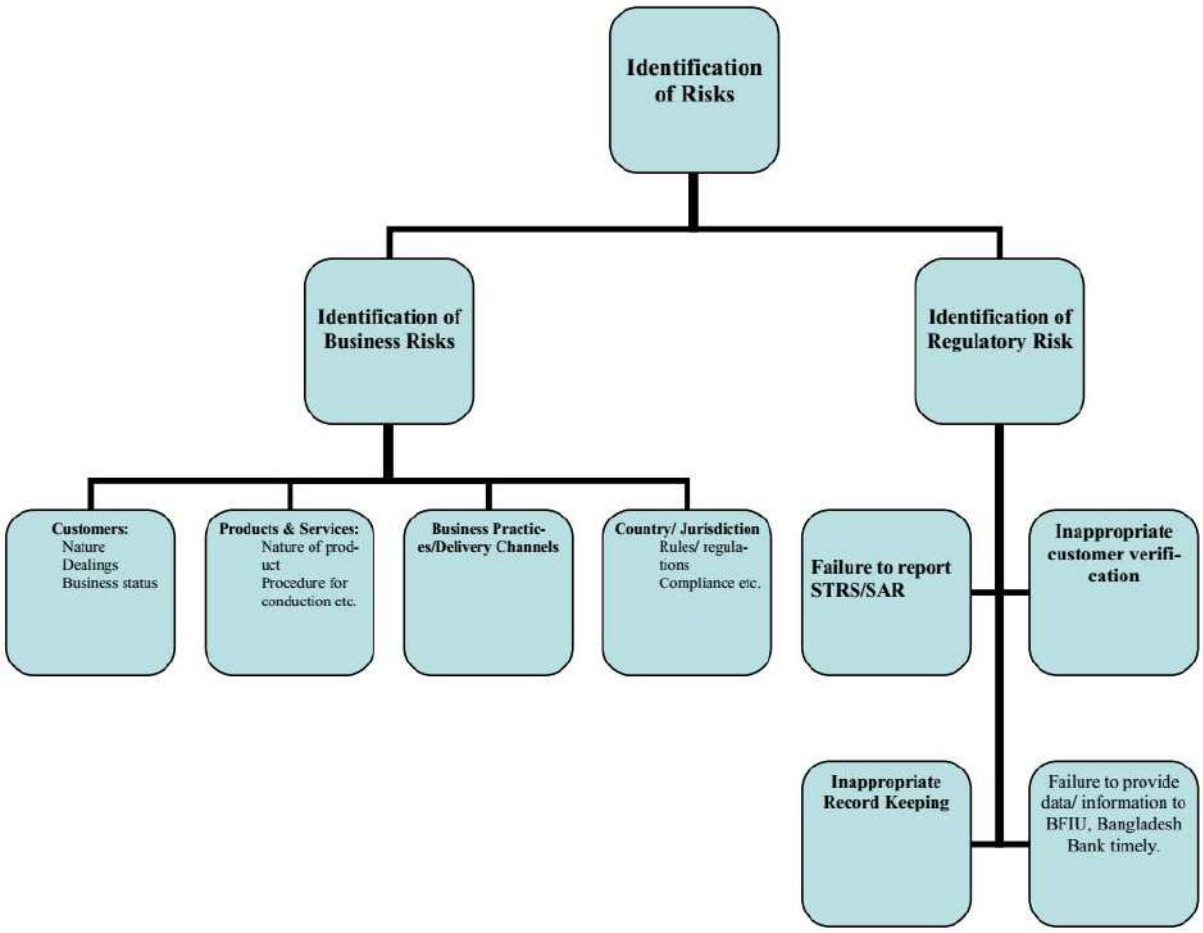
15.6.5 Risk Management Process

Risk Management Process is a continuous process. In a business life of an entity, it faces different problems/obstacles and changes, it's Management process accordingly taking into consideration organization's objectives, nature of business, clients involved and policies of controlling authorities. Islami Bank Bangladesh PLC has developed a four stage Risk Management Process including the followings-



15.6.5(a) Risk Identification

In the face of Risk Identification, Islami Bank Bangladesh PLC shall take into consideration the overall environment of the Industry highlighting the following arena of risks:



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

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

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

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

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

As previously discussed, there are two risk types: **business risk and regulatory risk.**

Business risk:

Islami Bank Bangladesh PLC shall consider the risk posed by any element or any combination of its business listed below:

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

Under these four groups, individual risks of IBBPLC shall be determined. While not an exhaustive list, some of these individual risks may include:

1. **Customers:** followings are some indicators (but not limited to) to identify ML & TF risk arises from customers of IBBPLC:

   New Customer:

   a) Accounts are opened without physical presence of the client (s).
   b) Genuineness of submitted documents is difficult to be verified.
   c) Account opening branch is far from the account holder's address without any valid reasons.
   d) Transaction is made by the beneficiaries through opening of the account in the name of their spouses/ children.
   e) Opening/ operations of the accounts in the name of Charity organizations, NGOs, Clubs, Societies, etc.
   f) High volume of transaction in the account does not match with the TP declaration/ nature of business of the clients.
   g) Counterfeiting of signature/ cheque/any other security documents.
   h) Transfer of account from one branch to another branch without any valid cause.
   i) Relationship of clients with the PEPs/ Influential Persons.
   j) Clients related to agency/ travel/money exchange/ import-export business.
   k) Induction of new clients who were refused by another bank earlier.

l) Clients objected by regulatory/ law enforcement authority.
m) Account open before 30 April, 2002.
n) Customer who is enlisted in UN/OFAC/EU sanction list.
o) PEPs.
p) IPs.
q) Customer who brings in large amounts of used notes/ small denomination.
r) Customers whose business address and registered office are in different geographic location.
s) Walk in Customer:

i) Transaction made for small amount/ denomination.
ii) Transaction made in favor of the Govt. /Reputed Organization.
iii) Transaction made for large amount/ denomination.
iv) Transaction made in favor of the non-reputed/ unknown organization.

2. Products:

a) Al-Wadeah Current Account
b) Mudaraba Savings Account
c) Mudaraba Special Notice Account
d) Mudaraba Special Savings (Pension) Account
e) Mudaraba Term Deposit Account
f) Mudaraba Savings Bond Account
g) Mudaraba NRB Savings Bond (MNSB)
h) Mudaraba Hajj Savings Account
i) Mudaraba Waqf Cash Deposit Account
j) Import-Export business
k) Investments

3. Alternative Delivery Channels:

a) ATM Cash Withdraw
b) ATM Fund Transfer
c) Salary Card
d) Travel Card
e) I Banking
f) SMS Banking
g) Mobile Banking/ m-Cash
h) Phone Banking
i) Online Banking
j) BACH
k) BEFTN
l) International Clearing Houses

4. Geographic/ Location:

a) The jurisdictions which have been identified for inadequate AML/CFT measures by FATF
b) Border Area
c) Publicly known vulnerable areas
d) Drug (Source, Destination & Trafficking Countries)

Regulatory Risk:

1) Failure to keep record properly
2) Failure to scrutinize staffs properly
3) Failure to train staff adequately
4) Not having an AML/CFT compliance program
5) Failure to report STR/SAR
6) Not submitting required report to BFIU
7) Not submitting required data/ information to BFIU timely.

8) Failure to do EDD for high risk customer
9) Not complying with Freezing order issued by BFIU
10) Not submitting accurate information instructed by BFIU

Fraud-Forgeries Risk:

1) Internal elements.
2) External elements.

15.6.5(b) Risk Assessment

For assessing risk, in this chapter we have used, the Table -1, which is a simple & generic table with Risk Score and Treatment. Risk Score can be found by blending likelihood and impact; the details will be explained later on. Table -1 is used, only the examples of customer risk assessment and developed phase by phase so that user can have a good idea of risk assessment.

Risk Group	**Customers**			
Risk	**Likelihood**	**Impact**	**Risk Score**	**Treatment/ Action**
New customer (example only)				
Customer who brings in large amounts of used notes and/or small denominations (example only)				
Customer whose business address and registered office are in different geographic locations (example only)				

Table 1: Risk Management Worksheet – risk

15.7 Calculation of Risk Score:

Risk Level/ Score is the blending of Likelihood and Impact of Risk.

LIKELIHOOD	X	IMPACT	=	RISK LEVEL/ SCORE

Likelihood **:** the chance of the risk happening

Impact (consequence) **:** the amount of loss or damage if the risk happened –

Likelihood Scale **:** Likelihood is measured under following 03 (three) Scales.

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

Table-2: Likelihood Scale

Impact Scale:

Impact is measured under following 03 (three) Scales.

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

Table-3: Impact Scale

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

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

Risk matrix and risk score:

Risk Score can be obtained by blending the "Likelihood" & "Impact of Risk" which are discussed in Table 1 & 2 and using the Rix Matrix which indicates the Risk Level & Risk Score at each combination of "Likelihood" & "Impact of Risk" .

Risk are classified into 04 levels-

Low	: Score-01
Medium	: Score-02
High	: Score-03
Extreme	: Score-04

Threat level for ML/TF risk

LIKELIHOOD					
A	**Very Likely**	**Medium 2**	**High 3**	**Extreme 4**
B	**Likely**	**Low 1**	**Medium 2**	**High 3**
C	**Unlikely**	**Low 1**	**Low 1**	**Medium 2**
What is the chance it will happen?		**Minor**	**Moderate**	**Major**
		A	**B**	**C**

IMPACT

How serious is the risk?

Table-4: Threat level

Risk Score

Rating	Impact – of an ML & TF risk
4 Extreme	**Risk almost sure to happen and/or to have very serious consequences.** **Response:** Do not allow transaction to occur or reduce the risk to acceptable level.
3 High	**Risk likely to happen and/or to have serious consequences.**

	Response: Do not allow transaction until risk reduced.
2 Medium	**Possible this could happen and/or have moderate consequences.** **Response:** May go ahead but preferably reduce risk.
1 Low	**Unlikely to happen and/or have minor or negligible consequences.** **Response:** Okay to go ahead.

Table-05: Risk score table

15.8 Risk Assessment and Management Exercise:

From the above discussion, an idea has been developed to calculate risk score by blending likelihood and impact, the risk matrix and risk score and can assess the risks of individual customer, product/service, delivery channels and risks related to geographic region by using the simplified risk management worksheet (Table-01). Now, IBBPLC can also fix up its necessary actions against the particulars outcomes of risks. All the exercises done by the banks would be called together **"Risk Register"**.

15.9 Risk Register of IBBPLC:

Considering the Nature of customers, products & services, delivery channels, Islami Bank Bangladesh PLC shall identify the ML & TF Risks of the Bank and shall formulate the action plan as per the risk grade to mitigate the same in its formulated Risk Register. This Risk Register of IBBPLC shall show the Risks, Likelihood, Impact Scale, Risk Score & Grade and Action Plan there against adopted/ chalked out by the Bank which is mentioned below:

RISK REGISTER

ML & TF Risk Register for Customers:

Risk	Likelihood	Impact	Risk Score	Treatment/ Action
Retail Banking Customer				
A new customer	Unlikely	Minor	1 Low	i) CDD shall be applied properly. ii) EDD shall also be applied for high risky clients & accounts opened without physical presence of the clients.
Walk-in customer (beneficiary is government/semi government/autonomous body/ bank & NBFI	Unlikely	Minor	1 Low	Obtaining proper KYC of the Remitter
Walk-in customer (beneficiary is other than government/semi government/autonomous body/ bank & NBFI	Likely	Moderate	2 Medium	i) Obtaining proper KYC of the remitter/ beneficiary ii) Reporting STR/ SAR if suspicious anything found. iii) May go ahead but preferably reduce risk.
Non-Resident customer (Bangladeshi)	Unlikely	Major	2 Medium	i) CDD shall be done ii) verification of necessary papers/ documents including work permit, passport & visa. iii) Transaction monitoring shall be done. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious. v) May go ahead but preferably reduce risk.
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	Likely	Moderate	2 Medium	i) CDD shall be applied properly. ii) Verifying the genuineness of the data/ information of the client. iii) Transaction monitoring shall be done. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious. v) May go ahead but preferably reduce risk.
A customer making series of transactions to the same individual or entity	Likely	Moderate	2 Medium	i) CDD shall be applied properly. ii) Verifying the genuineness of the data/ information of the client. iii) Transaction monitoring shall be done. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious. v) May go ahead but preferably reduce risk.
Customer involved in outsourcing business	Unlikely	Major	2 Medium	i) CDD shall be applied properly. ii) Verifying the genuineness of the data/ information of the client. iii) Transaction monitoring shall be done. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious. v) May go ahead but preferably reduce risk.
Customer appears to do structuring to avoid reporting threshold	Likely	Moderate	2 Medium	i) EDD shall be applied properly for the clients & also outsource partners. ii) Transaction monitoring shall be done. iii) STR shall be submitted to ML&TFPD if any transaction found suspicious. iv) May go ahead but preferably reduce risk.
Customer appears to have account with several banks in the same area	Likely	Moderate	2 Medium	i) CDD shall be applied properly for the clients & also outsource partners. ii) Transaction monitoring shall be done. iii) STR shall be submitted to ML&TFPD if any transaction found suspicious. iv) May go ahead but preferably reduce risk.
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Unlikely	Major	2 Medium	i) CDD shall be applied properly. ii) Activities & Transaction of the client will be monitored.

				iii) STR/ SAR shall be filed if any transaction found suspicious. iv) May go ahead but preferably reduce risk.
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Likely	Major	3 High	i. Business relationship shall not be established. ii. For existing client, information shall be provided the regulatory Authority through STR/ SAR. **Do not allow transaction until risk reduced.**
Negative news about the customers' activities/ business in media or from other reliable sources	Likely	Major	3 High	i. No such customer to be onboarded until risk is reduced. **For existing customers-** ii CDD/ EDD shall be applied properly. iii Court order/ instruction shall be followed. iv Transaction & activities of the client shall be monitored. v STR/ SAR shall be filed if any transaction found suspicious. vi **Do not allow transaction until risk reduced**.
Customer is secretive and reluctant to meet in person	Likely	Major	3 High	**i.** No business relationship will be made with such client. **ii. Do not allow transaction until risk reduced.**
Customer is a mandate who is operating account on behalf of another person/ company	Likely	Major	3 High	i) CDD/ EDD shall be applied properly. ii) Transaction & activities of the client shall be monitored. iii) STR/ SAR shall be filed if any transaction found suspicious.
Large deposits in the account of customer with low income	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) If necessary, TP shall be updated (if the case is genuine/ pertinent) iii) Constant Transaction monitoring shall be undertaken. iv) STR shall be submitted to ML&TFPD if the client fails to provide the accurate source of the fund. v) May go ahead but preferably reduce risk.
Customers about whom BFIU seeks information (individual)	Likely	Major	3 High	i) EDD shall be applied. ii) Transaction & activities of the client shall be monitored. iii) STR/ SAR shall be filed if any transaction found suspicious.
A customer whose identification is difficult to check.	Likely	Major	3 High	i) Business relationship shall not be established. ii) For existing client, information shall be provided to the regulatory Authority through STR/ SAR iii) Transaction shall be closely monitored. iv) **Do not allow transaction until risk reduced.**
Significant and unexplained geographic distance between the bank/ branch and the location of the customer	Likely	Moderate	2 Medium	i) CDD shall be done properly. ii) Proper justification for opening of such account shall be obtained from the client iii) Constant Transaction monitoring iv) STR shall be submitted to ML&TFPD if any transaction found suspicious. v) May go ahead but preferably reduce risk.
Customer is a foreigner	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Permission shall be obtained from competent Authority of the Bank. iii) Transaction shall be monitored. iv) STR/ SAR shall be submitted to ML&TFPD if any transaction found suspicious. v) May go ahead but preferably reduce risk.
Customer is a minor	Likely	Minor	1 Low	i) Proper CDD shall be applied ii) CDD shall also be applied for Beneficial Owner.

Customer is Housewife	Likely	Moderate	2 Medium	i) Proper CDD shall be applied ii) CDD shall also be applied for Beneficial Owner. ii) Transaction shall be monitored. v) STR/ SAR shall be submitted to ML&TFPD if any transaction found suspicious. v) May go ahead but preferably reduce risk.
Customers that are politically exposed persons (PEPs) or Influential Persons (IPs) or Chief/ Senior officials of international organizations and their family members and close associates	Likely	Major	3 High	i. EDD shall be applied. ii. Permission shall be obtained from Competent Authority of the Bank. iii. The official approval letter to open the account shall be obtained in case of Foreign PEPs. iv. Client's source of fund shall be verified. v. Transaction shall be monitored vi. STR shall be submitted to ML&TFPD if any transaction found suspicious.
Customer opens account in the name of his/ her family member who intends to credit large amount of deposit	Likely	Moderate	2 Medium	i) Obtaining full KYC of the beneficiaries including his source of funds. ii) Verifying the genuineness of the data including sources of fund applying EDD. iii) Transaction shall be done with constant monitoring of the account. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious. May go ahead but preferably reduce risk.
Customers doing significant volume of transactions with higher-risk geographic locations.	Likely	Major	3 High	i) KYC Procedures including physical verification of the client's information shall be done properly. ii) Transaction (specially sources & uses of fund) shall be monitored. iii) STR/SAR shall be made if anything found suspicious.
A customer who brings in large amounts of used notes and / or small denominations	Likely	Moderate	2 Medium	i) Proper KYC including the sources of fund shall be done/ obtained through EDD. ii) Verifying the given information iii) STR shall be done if anything found suspicious. iv) May go ahead but preferably reduce risk.
Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)	Likely	Major	3 High	i) EDD shall be applied ii) Verifying the genuineness of the data/ information of the client iii) Transaction monitoring shall be done. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious.
Customer is a money changer/ courier service agent/ travel agent	Likely	Major	3 High	i) For new customers, account shall not be opened until all obligatory data/ information are obtained through physical verification. ii) For the existing customers EDD shall be done. iii) Transaction shall be monitored. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious.
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above.	Likely	Moderate	2 Medium	i) EDD shall be done. ii) Transaction shall be monitored. iii) STR shall be submitted to ML&TFPD if any transaction found suspicious. May go ahead but preferably reduce risk.
Customer is involved in Manpower Export Business	Likely	Major	3 High	i) For new customers, account shall not be opened until all obligatory data/ information are obtained through physical verification. ii) For the existing customers EDD shall be done. iii) Transaction shall be monitored. iv) STR shall be submitted to ML&TFPD if any transaction found suspicious.
Customer has been refused to provide banking facilities by another bank	Likely	Moderate	2 Medium	i) Sufficient information of the client shall be collected through proper verification.

				ii) EDD shall be applied. iii) Proper justification of such refusal by the cli ent shall be obtained. iv) Other Banks information shall be collected. v) Transaction shall be monitored vi) STR shall be done, if anything found suspi cious May go ahead but preferably reduce risk.
Accounts opened before 30 April, 2002	Unlikely	Major	2 Moderate	i) KYC has to be updated with all required pa pers/ documents. ii) Dormant shall be marked in the account if KYC not done. iii) Deposit facility shall be provided but no withdrawal facility shall be allowed. iv) EDD shall be applied while allowing transac tion. v) SAR may be filed if anything suspicious found. vi) May go ahead but preferably reduce risk.
Customers with complex accounting and huge transaction	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Constant Monitoring of transactions. iii) Evaluating the Risk Grading. iv) STR/ SAR shall be filed if suspicious any- thing is found. v) May go ahead but preferably reduce risk.
Receipt of donor fund, fund from foreign source by micro finance insti- tute (MFI)	Likely	Major	3 High	i) For new customers, account shall not be opened until all obligatory data/ information are obtained through physical verification. ii) EDD shall be applied. iii) Sources of Fund & uses of fund shall be mon itored/ verified. iv) If the submitted documents are found ok, transaction shall be allowed with constant monitoring of the account. v) STR shall be submitted to ML&TFPD if any transaction found suspicious.
Customer which is a reporting organi- zation under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	Unlikely	Major	2 Moderate	EDD shall be applied. May go ahead but preferably reduce risk.
Wholesale Banking Customer				
Entity customer having operations in multiple locations.	Likely	Moderate	2 Medium	i. CDD shall be applied. ii. Transaction shall be monitored. iii. STR shall be filed if suspicious any- thing is found. iv. May go ahead but preferably reduce risk.
Customers about whom BFIU seeks information (large corporate)	Likely	Major	3 High	i. EDD shall be applied. ii. Transaction & activities of the client shall be monitored. iii. STR/ SAR shall be filed if any transact tion found suspicious.
Owner of the entity that are Influen- tial Persons (IPs) and their family members and close associates	Likely	Moderate	2 Medium	i) Permission shall be obtained from Competent Authority for making rela- tionship with the client. ii) EDD shall be applied. iii) Client's source of fund shall be veri- fied. iv) Transaction shall be monitored v) STR shall be submitted to ML&TFPD ifany transaction found suspicious. vi) May go ahead but preferably reduce risk.
A new customer who wants to carry out a large transaction. (i.e. transac- tion amounting 10 million or above)	Likely	Moderate	2 Medium	i) CDD shall be applied properly. ii) Verifying the genuineness of the data/ information of the client.

				iii) Transaction monitoring shall be done. iv) STR shall be submitted to ML&TFPD ifany transaction found suspicious. May go ahead but preferably reduce risk.
A customer or a group of customers making lots of transaction to the same individual or group (wholesale).	Likely	Moderate	2 Medium	i) CDD shall be applied properly. ii) Transaction monitoring shall be done. iii) STR shall be submitted to ML&TFPD ifany transaction found suspicious. iv) May go ahead but preferably reduce risk.
A customer whose identification is difficult to check	Likely	Moderate	2 Medium	i) Business relationship shall not be established. ii) For existing client, information shall be provided the regulatory Authority through STR/ SAR. iii) May go ahead but preferably reduce risk.
Owner of the entity/ institution that are Politically Exposed Persons (PEPs) or chief/ senior officials of International Organizations and their family members and close associates	Likely	Major	3 High	i) Approval from Head Office shall be obtained to set up such business relationship. ii) Client's documents/ identity, source of fund shall be verified. iii) Transaction shall be monitored iv) STR shall be submitted to ML&TFPD if any transaction found suspicious.
Charities or NPOs (especially operating in less privileged areas).	Likely	Major	3 High	i) For new customers, account shall not be opened until all obligatory data/ infor mation are obtained through physical verification. ii) EDD shall be applied. iii) Sources of Fund & uses of fund shall be monitored/ verified. iv) If the submitted documents are found ok, transaction shall be allowed with con stant monitoring of the account. v) STR shall be submitted to ML&TFPD if any transaction found suspicious.
Khidmah' Card Customer				
Customer who changes static data frequently	Likely	Moderate	2 Medium	i. EDD shall be applied. ii. Sources & uses of fund shall be verified. iii. Transaction shall be monitored. iv. STR shall be submitted if suspicious anything if found. v. May go ahead but preferably reduce risk.
Khidmah' Card Customer	Unlikely	Minor	1 Low	i. 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. ii. Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) iii. Confidentiality of Security option of the card including PIN Code shall be strictly maintained. iv. Multi factors authentication shall be introduced/ applied. v. Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions. vi. Transaction shall be monitored. vii. STR shall be submitted if anything found suspicious.
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	Unlikely	Minor	1 Low	Do
Prepaid Card Customer	Unlikely	Minor	1 Low	Do
International Trade Customer				

A new customer (Outward remittance-through SWIFT)	Likely	Moderate	2 Medium	**i)** EDD shall be applied. **ii)** Screening of the Transaction **iii)** STR shall be filed if suspicious anything is found. **iv)** May go ahead but preferably reduce risk.
A new customer (Import/ Export)	Likely	Moderate	2 Medium	i) Approval shall be obtained from the competent Authority for sanctioning limit ii) Proper KYC shall be done. iii) Physical visit/ verification of the client's personal/ business information/ establishment to check over/ under invoicing. iv) Proper documentation shall be ensured. v) Confirmation shall be obtained from the competent Authority to detect the fake invoices. vi) UN Sanction list shall be screened. vii) Constant monitoring and follow up to recover the fund. viii) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account. ix) May go ahead but preferably reduce risk.
A new customer (Inward remittance through SWIFT)	Likely	Moderate	2 Medium	i. EDD shall be applied. ii. Screening of the Transaction iii. STR shall be filed if suspicious anything is found.May go ahead but preferably reduce risk.
A new customer who wants to carry out a large transaction (Import/ Export)	Unlikely	Major	2 Moderate	i) Approval shall be obtained from the competent Authority for sanctioning limit ii) Screening shall be conducted. iii) Proper KYC shall be done. iv) Physical visit/ verification of the client's personal/ business information/ establishment to check over/ under invoicing. v) Proper documentation shall be ensured. vi) Confirmation shall be obtained from the competent Authority to detect the fake invoices. vii) Constant monitoring and follow up to recover the fund. viii) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account. ix) May go ahead but preferably reduce risk.
A new customer who wants to carry out a large transaction (Inward/ outward remittance)	Likely	Major	3 High	i) EDD shall be applied. ii) Sources of fund & uses of fund shall be verified. iii) Screening of the Transaction **iv)** STR shall be filed if suspicious anything is found v) **Do not allow transaction until risk reduced.**
A customer wants to conduct business beyond its line of business (Import/ Export/ Remittance)	Likely	Major	3 High	i) For new clients: business relationship shall not be made. ii) For existing customer: such transaction shall not be allowed.
Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	Likely	Major	3 High	i) Approval from Head Office shall be ob tained to set up such business relationship. ii) Client's documents/ identity, source of fund shall be verified. iii) Transaction shall be monitored iv) STR shall be submitted to ML&TFPD if any transaction found suspicious.
Correspondent Banks	Likely	Moderate	2 Medium	i) Permission from competent Authority shall be obtained.

				ii) KYC procedures shall be conducted. iii) Necessary formalities as per Correspondence banking & F.Ex regulation Act 1947 shall be followed. iv) May go ahead but preferably reduce risk.
Money services businesses (remittance houses, exchange house)	Likely	Moderate	2 Medium	a. For new customers, account shall not be opened until all obligatory data/ information are obtained through physical verification. b. For the existing customers EDD shall be done. c. Transaction shall be monitored. d. STR shall be submitted to ML&TFPD if any transaction found suspicious. May go ahead but preferably reduce risk.

ML & TF Risk Register for Products & Services

Risk	Likelihood	Impact	Risk Score	Treatment/ Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)	Likely	Moderate	2 Medium	i) CDD shall be maintained. ii) Sources of fund & uses of fund shall be verified. iii) STR shall be filed if suspicious anything is found. iv) May go ahead but preferably reduce risk.
Gift Cheque	Likely	Minor	1 Low	CDD shall be maintained.
Locker Service	Likely	Moderate	2 Medium	i) CDD shall be maintained. ii) Activity shall be monitored. iii) SAR shall be filed if suspicious anything is found. May go ahead but preferably reduce risk.
Foreign currency endorsement in Passport	Likely	Moderate	2 Medium	i) CDD shall be maintained. ii) Activity shall be monitored. iii) SAR shall be filed if suspicious anything is found. iv) May go ahead but preferably reduce risk.
Large transaction in the account of under privileged people	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Constant Transaction monitoring shall be undertaken. iii) STR shall be submitted to ML&TFPD ifthe client fails to provide the accurate source of the fund. iv) May go ahead but preferably reduce risk.
MTDRA (less than 2 million)	Likely	Minor	1 Low	i) CDD shall be maintained. ii) Sources of fund shall be verified. iii) STR shall be done if anything found suspicious.
MTDRA (2 million and above)	Likely	Moderate	2 Medium	i) EDD shall be done ii) Sources of fund shall be verified iii) In case of unauthenticated source of fund account shall be regretted or iv) STR shall be done. v) May go ahead but preferably reduce risk.
Special scheme deposit accounts opened with big installment and small tenure	Unlikely	Minor	1 Low	i. Proper KYC shall be done with obtain ing all required papers/ documents of the clients including source of income. ii. Physical verification of the information shall be ensured.
Multiple deposit scheme accounts opened by same customer in a branch	Likely	Moderate	2 Medium	i) CDD/ EDD shall be maintained. ii) Sources of fund & uses of fund shall be verified.

				iii) Transaction shall be monitored. iv) STR shall be filed if suspicious anything is found. May go ahead but preferably reduce risk.
Multiple deposit scheme accounts opened by same customer from different location	Likely	Moderate	2 Medium	i) CDD/ EDD shall be maintained. ii) Sources of fund & uses of fund shall be verified. iii) Transaction shall be monitored. iv) STR shall be filed if suspicious anything is found v) May go ahead but preferably reduce risk.
Open MSSA in the name of family member Or Installments paid from the account other than the customer's account	Likely	Moderate	2 Medium	i) EDD shall be maintained. ii) Sources of fund & uses of fund shall be verified. iii) Transaction shall be monitored. iv) STR shall be filed if suspicious anything is found. May go ahead but preferably reduce risk.
Stand alone DPS	Unlikely	Minor	1 Low	i) Proper KYC shall be done with obtaining all required papers/ documents of the clients including source of income. ii) Physical verification of the information shall be ensured.
Early encashment of FDR, special scheme etc.	Likely	Minor	1 Low	Proper CDD shall be maintained.
Non face to face business transaction	Likely	Major	3 High	i) EDD shall be applied. ii) Sources & uses of fund shall be verified. iii) Proper identification of the transaction maker. iv) Transaction shall be monitored. v) STR shall be filed if suspicious anything is found.
Payment received form unrelated/ unassociated third parties	Likely	Major	3 High	i) EDD shall be applied. ii) Sources & uses of fund shall be verified. iii) Proper identification of the transaction maker/ 3rd party. iv) Transaction shall be monitored. v) STR shall be filed if suspicious anything is found. vi) **Do not allow transaction until risk reduced.**
Retail Privilege Facilities				
Pre-Approved Khidmah' Card with BDT 300K limit				i) 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. ii) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) iii) Confidentiality of Security option of the card including PIN Code shall be strictly maintained. iv) Multi factors authentication shall be introduced/ applied. v) Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions. vi) Transaction shall be monitored. vii) STR shall be submitted if anything found suspicious. viii) Short KYC of the depositors/ withdrawers shall be obtained in case of online banking.
Enhanced ATM cash withdrawal Limit BDT 100K				Do

SME Banking Product				
What to open MTDR where source of fund is not clear	Likely	Minor	1 Low	i. CDD shall be maintained. ii. Sources of fund shall be verified. iii. STR shall be done if anything found suspicious.
Early encashment of MTDR	Likely	Minor	1 Low	Proper CDD shall be maintained.
Repayment of investment MPI from source that is not clear	Likely	Moderate	2 Medium	i) EDD shall be applied ii) Sources of fund shall be ascertained. iii) Activities of the client shall be monitored. iv) STR/ SAR shall be filed if suspicious anything is found. v) May go ahead but preferably reduce risk.
Repayment of full investment amount before maturity	Likely	Moderate	2 Medium	i) EDD shall be applied ii) Sources of fund shall be ascer tained. iii) Activities of the client shall be monitored. iv) STR/ SAR shall be filed if suspi cious anything is found. v) May go ahead but preferably re duce risk.
Investment amount utilized in sector other than the sector specified during availing the loan	Likely	Major	3 High	i) EDD shall be applied ii) Physical verification of clients es tablishment on regular interval/ sudden, if required. iii) Activities of the client shall be monitored. iv) Transaction shall be monitored. **v)** STR/ SAR shall be filed if suspi cious anything is found. vi) **Do not allow transaction until risk reduced.**

In case of fixed asset financing, sale of asset purchased immediately after repayment of full investment amount.	Likely	Major	3 High	i) EDD shall be applied ii) Physical verification of clients establishment on regular interval/ sudden, if required. iii) Activities of the client shall be monitored. iv) Transaction shall be monitored. v) STR/ SAR shall be filed if suspicious anything is found.
Sources of fund used as security not clear at the time of availing Investment	Likely	Moderate	2 Medium	i) EDD shall be applied ii) Sources of fund shall be ascertained. iii) Activities of the client shall be monitored. iv) STR/ SAR shall be filed if suspicious anything is found. v) May go ahead but preferably reduce risk.
Wholesale Banking Product				
Development of new product & service of bank	Likely	Moderate	2 Medium	i) Product vulnerability shall be ascertained. ii) Market accessibility shall be evaluated. iii) Examination of software, logistics related to the product. iv) May go ahead but preferably reduce risk.
Payment received from unrelated third parties	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Sources of fund shall be verified. iii) Proper identification of the transaction maker/ 3rd party.

				iv) Transaction shall be monitored. v) STR shall be filed if suspicious anything is found. vi) May go ahead but preferably reduce risk.
High Value MTDR	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Sources of fund shall be verified. iii) Proper identification of the transaction maker/ 3rd party. iv) Transaction shall be monitored. v) STR shall be filed if suspicious anything is found. vi) May go ahead but preferably reduce risk.
Term Investment, HPSM, Bai-Salam, Bai-Assharf, MDB, BBLC (SOD (FO), SOD (G-work order), SOD (Garment), SOD (PO), Loan General, Lease finance, Packing Credit, BTB L/C)	Likely	Moderate	2 Medium	i) Approval shall be obtained from the competent Authority for sanctioning limit ii) Proper KYC shall be done at the time of new induction/ renewal of the limit. iii) Physical visit/ verification of the client's personal/ business information/ establishment to assess his net worth. iv) Proper documentation shall be ensured. v) Constant monitoring and follow up to recover the fund. vi) STR shall be done if any illegal fund transfer/ transaction detected. May go ahead but preferably reduce risk.
BG (bid bond), BG (PG), BG (APG)	Likely	Moderate	2 Medium	i) CDD shall be maintained. ii) Proper documentation shall be done. iii) Verification of beneficiary's information. iv) May go ahead but preferably reduce risk.
L/C subsequent term loan, DP L/C	Likely	Moderate	2 Medium	Do
Pledge, Hypothecation, SOD (G-Business), STL	Likely	Moderate	2 Medium	i) Screening of on boarding process ii) CDD with proper documentation iii) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account. iv) May go ahead but preferably reduce risk.
OBU	Likely	Moderate	2 Medium	i) Screening of on boarding process ii) CDD with proper documentation iii) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account. iv) May go ahead but preferably reduce risk.
Syndication Financing	Likely	Moderate	2 Medium	i) Approval shall be obtained from the competent Authority for sanctioning limit ii) Proper KYC shall be done at the time of new induction/ renewal of the limit. iii) Physical visit/ verification of the client's personal/ business information/ establishment to assess his net worth. iv) Proper documentation shall be ensured. v) Constant monitoring and follow up to recover the fund. vi) STR shall be done if any illegal fund transfer/ transaction detected. vii) May go ahead but preferably reduce risk.

Khidmah' Card				
Supplementary Khidmah' Card Issue	Likely	Major	3 High	i) 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. ii) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) iii) Confidentiality of Security option of the card including PIN Code shall be strictly maintained. iv) Multi factors authentication shall be introduced/ applied. v) **Do not allow transaction until risk reduced.**
Frequent use of Card Cheque				
BEFTN Cheque or pay order as mode of payment instead of account opening at bank (Merchant)	Likely	Moderate	2 Medium	**i)** Beneficial owner identity must be ensured. **ii)** CDD with proper documentation **iii)** STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account. **iv)** May go ahead but preferably reduce risk.
Credit card issuance against ERG and RFCD accounts	Likely	Moderate	2 Medium	i. Screening of on boarding process ii. CDD with proper documentation iii. STR shall be done if over invoicing or any other means of illegal funds trans fer detected in the account. iv. May go ahead but preferably reduce risk.
International Trade				
Line of business mismatch (import/ export/ remittance)	Likely	Moderate	2 Medium	i) Approval shall be obtained from the competent Authority for sanctioning limit ii) Proper KYC shall be done. iii) Physical visit/ verification of the client's personal/ business information/ establishment to check over/ under invoicing. iv) Proper documentation shall be ensured. v) Confirmation shall be obtained from the competent Authority to detect the fake invoices. vi) UN Sanction list shall be screened. vii) Constant monitoring and follow up to recover the fund. viii) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account. ix) May go ahead but preferably reduce risk.
Under/ Over invoicing (Import/ Export/ Remittance)	Likely	Major	3 High	i) Approval shall be obtained from the competent Authority for sanctioning limit ii) Proper KYC shall be done. iii) Physical visit/ verification of the client's personal/ business information/ establishment to check over/ under invoicing. iv) Proper documentation shall be ensured. v) Confirmation shall be obtained from the competent Authority to detect the fake invoices. vi) UN Sanction list shall be screened. vii) Constant monitoring and follow up to recover the fund. **viii)** STR shall be done if over invoicing or

				any other means of illegal funds transfer detected in the account. ix) **Do not allow transaction until risk reduced.**
Retirement of import bills in cash (Import/ Export/ Remittance)	Likely	Moderate	2 Medium	i) Approval shall be obtained from the competent Authority for sanctioning limit ii) Proper KYC shall be done. iii) Physical visit/ verification of the client's personal/ business information/ establishment to check over/ under invoicing. iv) Proper documentation shall be ensured. v) Confirmation shall be obtained from the competent Authority to detect the fake invoices. vi) UN Sanction list shall be screened. vii) Constant monitoring and follow up to recover the fund. viii) STR shall be done if over invoicing or any other means of illegal funds transfer detected in the account. ix) May go ahead but preferably reduce risk.
Wire transfer	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Sources of fund shall be verified. iii) Proper identification of the transaction maker/ 3rd party. iv) Transaction shall be monitored. v) STR shall be filed if suspicious anything is found.
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/ inward remittance)	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Sources of fund shall be verified. iii) Proper identification of the transaction maker/ 3rd party. iv) Transaction shall be monitored. v) STR shall be filed if suspicious anything is found. May go ahead but preferably reduce risk.

Risk Register for Business practice/ delivery methods or channels

Risk	Likelihood	Impact	Risk Score	Treatment/ Action
Online (multiple small transaction through different branch)	Likely	Minor	2 Medium	i) 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. ii) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) iii) Confidentiality of Security option of the card including PIN Code shall be strictly maintained. iv) Multi factors authentication shall be introduced/ applied. v) Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions. vi) Transaction shall be monitored. vii) STR shall be submitted if anything found suspicious.

BEFTN	Likely	Moderate	2 Medium	i) CDD shall be done ii) STR shall be submitted if anything found suspicious.
BACH	Likely	Moderate	2 Medium	i) CDD shall be done ii) STR shall be submitted if anything found suspicious.
IDBP	Likely	Moderate	2 Medium	i) CDD shall be done ii) STR shall be submitted if anything found suspicious.
Mobile Banking	Likely	Minor	2 Medium	i) 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. ii) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) iii) Confidentiality of Security option of the card including PIN Code shall be strictly maintained. iv) Multi factors authentication shall be introduced/ applied. v) Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions. vi) Transaction shall be monitored. vii) STR shall be submitted if anything found suspicious.
Third party agent or broker	Unlikely	Major	2	i) Documents shall be verified. ii) Accounts will be monitored. iii) STR shall be submitted if anything found suspicious.
Khidmah' Card				
New Merchant sign up	Likely	Moderate	2 Medium	i) Documents shall be verified. ii) Accounts will be monitored. iii) STR shall be submitted if anything found suspicious. iv) May go ahead but preferably reduce risk.
Alternate Delivery Channel				
Large amount withdrawn from ATMs	Unlikely	Minor	1 Low	i) 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. ii) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) iii) Confidentiality of Security option of the card including PIN Code shall be strictly maintained. iv) Multi factors authentication shall be introduced/ applied. v) Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions. vi) Transaction shall be monitored. vii) STR shall be submitted if anything found suspicious.

Larger amount transaction from different location and different time (mid night)through ATM	Likely	Moderate	2 Medium	i) EDD shall be done at the time of opening of the related deposit accounts against which card/ service is issued/ provided. ii) Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) iii) Confidentiality of Security option of the card including PIN Code shall be strictly maintained. iv) Multi factors authentication shall be introduced/ applied. v) Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions. vi) Transaction shall be monitored. vii) STR shall be submitted if anything found suspicious. viii) May go ahead but preferably reduce risk.
Large amount of cash deposit in CDM	Likely	Moderate	2	i) Customer's identity & source of fund shall be verified with proper documentation ii) Monitoring shall be done whether the deposit is under or over threshold. iii) STR shall be submitted if anything found suspicious. iv)May go ahead but preferably reduce risk.
Huge fund transfer through internet	Likely	Moderate	2 Medium	**i)** EDD shall be done at the time of opening of the related deposit accounts against which card/ service is issued/ provided. **ii)** Besides, CDD shall be obtained from depositor/ withdrawer (if transaction is made other than account holder) **iii)** Confidentiality of Security option of the card including PIN Code shall be strictly maintained. **iv)** Multi factors authentication shall be introduced/ applied. **v)** Pre-cautionary measures shall be taken to ensure effective security of the instruments in case of online transactions. **vi)** Transaction shall be monitored. **vii)** STR shall be submitted if anything found suspicious. May go ahead but preferably reduce risk.
Transaction Profile updated through Internet Banking				N/A
Customer to business transaction-Online Payment Gateway-Internet Banking	Unlikely	Moderate	1 Low	i) CDD will be done. ii) Transaction will be monitored.
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Likely	Moderate	2 Medium	i) EDD shall be applied. ii) Screening of the Transaction iii) STR shall be filed if suspicious anything is found. iv) May go ahead but preferably reduce risk.
Existing customer/ other bank customer	Likely	Moderate	2	i. EDD shall be applied.

receiving remittance through SWIFT under single customer credit transfer (fin-103)			Medium	ii. Screening of the Transaction iii. STR shall be filed if suspicious anything is found. May go ahead but preferably reduce risk.

Risk Register for Country/ jurisdiction

Risk	Likelihood	Impact	Risk Score	Treatment/ Action
Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas	Likely	Major	3 High	i) EDD shall be maintained. ii) Proper documentation shall be maintained. **iii)** Screening shall be done. iv) **Do not allow transaction until risk reduced.**
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	Likely	Major	3 High	i) EDD shall be maintained. ii) Proper documentation shall be maintained. iii) Screening shall be done. **iv) Do not allow transaction until risk reduced.**
Customer belongs to High Risk ranking countries of the Basel AML index.	Unlikely	Major	1 Low	i) CDD shall be maintained. ii) Proper documentation shall be maintained. iii) Screening shall be done.
Customer belongs to the countries identified by the bank as higher-risk because of its prior experiences or other factors	Likely	Major	3 High	i) EDD shall be maintained. ii) Proper documentation shall be maintained. iii) Screening shall be done.
Any country identified by FATF or FSRBs-(FATF style Regional Body) as not having adequate AML & CFT systems	Likely	Major	3 High	i) EDD shall be maintained. ii) Proper documentation shall be maintained. **iii)** Screening shall be done. **Do not allow transaction until risk reduced.**
Any bank that allow payable through account	Very likely	Moderate	3 High	1) Proper CDD shall be maintained. 2) EDD shall be applied. **3)** If necessary STR shall be filed. **Do not allow transaction until risk reduced.**
Any country identified as destination of illicit financial flow	Likely	Major	3 High	No relationship will be established.
Branches in a Boarder Area	Likely	Moderate	2 Medium	**i)** Transaction shall not be allowed until reducing the risk at an acceptable level. **ii)** KYC Procedures including physical verification of the client's information as well as business premises shall be done properly. **iii)** Transaction shall be monitored. **iv)** STR/SAR shall be made if anything found suspicious.

Register for Regulatory Risk

Risk	Likelihood	Impact	Risk Score	Treatment/ Action
Not having AML/CFT guideline	Likely	Major	3 High	AML/ CFT guideline shall be chalked out/ updated regularly.
Not forming a Central Compliance Committee (CCC)	Likely	Major	3 High	Central Compliance Committee must be formed as per instructions of BFIU and will be communicated any changes if any occurred in the same.
Not having an AML & CFT Compliance Officer	Not likely	Major	2 Medium	AML & CFT Compliance Officer must be formed as per instructions of BFIU and will

				be communicated any changes if any occurred in the same.
Not having Branch Anti Money Laundering Compliance Officer	Likely	Major	3 High	Branch Anti Money Laundering Compliance Officer must be deployed.
No Senior management commitment to comply with MLP and AT Acts	Not likely	Major	2 Medium	Senior Management must be committed for implementation of MLPA & ATA.
Failure to follow the BFIU circulars, circular letters, instructions etc.	Likely	Major	3 High	AMLD/ BFIU instruction must be followed.
Unique account opening form not followed while opening account	Likely	Major	3 High	Unique AOF must be followed.
Non screening of new and existing customers against UNSCR Sanction and OFAC lists	Likely	Major	3 High	Screening process must be conducted for new & existing customers.
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Likely	Major	3 High	Foreign Exchange Regulation Act, 1947 must be complied.
Complete and accurate information of customer not obtained	Likely	Major	3 High	Complete and accurate information of customer must be obtained
Failure to verify the identity proof document and address of the customer	Likely	Major	3 High	Customer's information must be verified/ supported by documents.
Beneficial owner identification and verification not done properly	Likely	Major	3 High	Beneficial owner's KYC must be obtained
Customer Due Diligence (CDD) not practiced properly	Likely	Major	3 High	CDD must be maintained.
Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e, PEPs, family members and close associates of PEPs and influential person and senior official of international organization)	Likely	Major	3 High	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
Failure to complete KYC of customer including walk in customer	Likely	Major	3 High	CDD must be maintained.
Failure to update TP and KYC of customer	Likely	Major	3 High	TP & KYC of customer must be obtained.
Keep the legacy accounts operative without completing KYC	Likely	Major	3 High	Legacy Accounts will be marked as Dormant till completion of CDD.
Failure to assess the ML & TF risk of a product or service before launching	Likely	Moderate	2 Medium	Assessment shall be done on the ML & TF risk of a product or service before launching
Failure to complete the KYC of Correspondent Bank	Likely	Moderate	2 Medium	KYC procedures must be completed before making relationship.
Senior Management approval not obtained before entering into a Correspondent Banking relationship	Unlikely	Major	2 Medium	Senior Management approval must be obtained before making relationship.
Failure to comply with the instruction of BFIU by bank Foreign subsidiary	Not likely	Major	2 Medium	N/A
Failure to keep record properly	Not likely	Major	2 Medium	Records will be preserved properly
Failure to report complete and accurate CTR on time	Likely	Moderate	2 Medium	Complete and accurate CTR will be submitted in time.
Failure to review CTR	Not likely	Major	2 Medium	CTR must be reviewed.
Failure to identify and monitor structuring	Likely	Moderate	2 Medium	Structuring must be identified. SAR shall be filled if necessary.
Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Likely	Moderate	2 Medium	Structuring must be identified. SAR shall be filled if necessary.
Failure to conduct quarterly meeting properly	Not likely	Major	2 Medium	Meeting shall be conducted regularly.
Failure to report suspicious transactions	Likely	Major	3 High	Suspicious transaction must be detected and reported in time.
Failure to conduct Self Assessment properly	Not likely	Major	2	SAR shall be conducted

			Medium	properly.
Failure to submit statement/ report to BFIU on time	Likely	Major	3 High	Statement/ report shall be reported to BFIU on time.
Submit erroneous statement/ report to BFIU	Likely	Major	3 High	Accurate report shall be submitted to BFIU on time.
Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Likely	Major	3 High	BFIU's order/ instruction must be complied on time.
Not submitting accurate information or statement sought by BFIU or BB.	Likely	Major	3 High	Accurate information shall be reported to BFIU on time.
Not submitting required report to senior management regularly	Not likely	Major	2 Medium	Required reported must be submitted to senior Management.
Failure to rectify the objections raised by BFIU or bank inspection teams on time	Not likely	Major	2 Medium	BFIU's objection must be rectified on time.
Failure to obtain information during wire transfer	Not likely	Major	2 Medium	
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely	Major	3 High	Responsibilities of ordering, intermediary and beneficiary bank must be complied.
Failure to scrutinize staff properly	Not likely	Major	2 Medium	Staff will be scrutinized properly. May go ahead but preferably reduce risk.
Failure to circulate BFIU guidelines and circulars to branches	Not likely	Major	2 Medium	BFIU's instruction must be circulated to the branches on time. May go ahead but preferably reduce risk.
Inadequate training/ workshop arranged on AML & CFT	Not likely	Major	2 Medium	Proper training must be ensured. May go ahead but preferably reduce risk.
No independent audit function to test the AML program.	Not likely	Major	2 Medium	The must be an independent audit function to test the AML program. May go ahead but preferably reduce risk.

CHAPTER 16

Internal Audit, Independent Testing & Self Assessment

16.1 Why the audit function is necessary

To ensure the effectiveness of the AML/CFT program, IBBPLC shall assess the program regularly and look for new risk factors. FATF recommendation 15 suggests that a bank covered by laws shall establish and maintain policies, procedures and controls which shall include an appropriate compliance function and an audit function.

16.2 Why the audit function must be independent

The audit must be independent (i.e. performed by people not involved with the bank's AML/CFT compliance officer). Audit is a kind of assessment of checking of a planned activity. Only those will check or examine the branch who do not have any stake in it. To ensure objective assessment it is important to engage an independent body to do audit.

16.3 Whom they report

The individuals conducting the audit shall report directly to the Board of Directors/senior management.

16.4 The ways of performing audit function

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.

16.5 Internal audit

IBBPLC's internal auditors shall be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable. The 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.
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements.
- Determine personnel adherence to the financial 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 branch 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:

- The importance that the board and the senior management placed on ongoing education, training and compliance
- Employee accountability for ensuring AML/CFT compliance.
- Comprehensiveness of training, in view of specific risks of individual business lines.
- Participation of personnel from all applicable areas of the branch.
- Frequency of training.
- Coverage of bank's 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.

16.6 Requirement of Independent Testing

As per BFIU Circular No. 26 dated 16.06.2020, Independent Testing is to be conducted at least annually by Bank's internal audit department introducing separate chapter in their regular report. The test will cover the following areas:

- Branch Compliance Unit/BAMLCO
- Knowledge of officers/employees on AML/CFT issues
- Customer Identification (KYC) process
- Branch's receipt of customers' expected transaction profile and monitoring
- Process and action to identify Suspicious Transaction Reports (STRs)
- Regular submission of reports to CCC
- Proper record keeping
- Overall AML related activities by the branch

The tests include interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the anti-money laundering procedures of the branch.

- sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- test of the validity and reasonableness of any exemption granted by the Bank; and
- test of the record keeping system according to the provisions of the laws. Any deficiencies shall be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline.

16.7 Requirement of Self Assessment:

As per BFIU Circular No. 26 dated 16 June, 2020, each Bank shall establish half yearly self assessment procedure that will assess how effectively the Bank's AML/CFT program is working. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment shall conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions and recommendations. The self assessment shall advise management whether the internal procedures and statutory obligations of the Bank have been properly discharged.

Therefore, each Branch of IBBPLC will assess its AML/CFT activities covering the following areas on half yearly basis and submit the report to CCC within next 15 days:

- The percentage of officers/employees that received official training on AML/CFT;
- The awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and BFIU's instructions and guidelines;
- The arrangement of AML/CFT related meeting on regular interval;

- The effectiveness of the customer identification during opening an individual, corporate and other account;
- The risk categorization of customers by the branch;
- Regular update of customer profile upon reassessment;
- The monitoring of customers' transactions with their declared TP after categorizing the customers based on risk or transactions over specific limit;
- Identification of Suspicious Transaction Reports (STRs);
- The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees;
- The measures taken by the branch during opening of account of PEPs;
- Consideration of UN Sanction List while conducting any business.
- The compliance with AML/CFT weaknesses/irregularities, as the bank's Head Office and BFIU's inspection report mentioned.

Besides, All Wings/ Divisions/ Departments of IBBPLC's Head Office shall form an AML Compliance Team in their offices who will look after the AML compliance issues of the Wings/ Divisions/ Departments and report their activities on quarterly basis to the Central Compliance Committee (CCC) as per Self Assessment Format developed by themselves based on the nature of their business. Apart from, they will file unusual or suspicious activities or transaction report detected by them in their normal course of monitoring to the Central Compliance Committee as and when detected.

16.8 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 CCC or ICC to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFIU has established a Self Assessment Reporting system for the branches.

According to the instructions of BFIU, branches of IBBPLC shall conduct the Self Assessment to evaluate the Branch on a half yearly basis. Self Assessment has to be done through a checklist that is circulated by BFIU Circular No. 26 dated 16 June, 2020. Before finalizing the evaluation report, there shall have to be a meeting presided over by the branch manager with all concerned officials of the branch. In that meeting, there shall be a discussion on the branch evaluation report; if the identified problems according that report are possible to solve at the branch level, then necessary actions shall be taken without any delay to finalize it; and in the final report, recommendations shall have to be jotted down. In the subsequent quarterly meetings on preventing money laundering and terrorist financing, the progress of the related matters 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 (A&ID) of ICCW of the Head Office and the Central Compliance Committee within the 15th of the next month.

16.9 Independent Testing Procedure

The audit must be independent (i.e. performed by people not involved with the bank's AML&CFT compliance). Audit is a kind of assessment of checking of a planned activity.

Independent testing has to be done through a checklist that is circulated by BFIU circular no. 26; dated 16 June, 2020.

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

16.10 IBBPLC's Internal Audit & Inspection Division's Obligations Regarding Self Assessment Or Independent Testing Procedure

The Internal Audit & Inspection Division of IBBPLC shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the CCC.

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

16.11 Obligations of Audit & Inspection Division (A&ID)

- Necessary initiatives shall be taken to deploy sufficient skilled resources to evaluate the Self Assessment Report submitted by Branches and conduct Independent Testing on the Branch Performance.
- The Internal Audit & Inspection Division shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the CCC
- While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the Internal 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 Internal 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 A&ID shall send a copy of the report with the rating of the branches inspected/audited to the CCC of the bank.
- The A&ID shall conduct inspection/audit activities on at least 5% cash points/agent outlets on yearly basis to review the compliance status of AML and CFT activity related matters of the cash points/agent outlets and a copy of the report on the same shall be sent to ML&TFPD.

16.12 Branches' Obligations:

a) In order to execute the Self Assessment depending on the provided checklist, branches shall have to evaluate themselves in a half yearly basis;

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 draft Self Assessment Report of the Branch; If any problem is identified in the Self Assessment Report and the same is not possible to solve at the branch level, Branches shall forward the same to Audit & Inspection Division and ML & TF Prevention Division including their recommendations alongwith the Self Assessment Report for necessary guidance to solve the identified problems. In the subsequent quarterly BCU meetings on prevention of money laundering and terrorist financing, the progress of the recommendations so submitted to A&ID and ML&TFPD shall be discussed/ reviewed.

16.13 Obligations of Central Compliance Committee (CCC) regarding Self Assessment & Independent Testing

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 (branch wise 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; and
- Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as **unsatisfactory** and **marginal** in the received report.

Aforementioned report shall be included with the matter mentioned in section 1.3(3) of BFIU Circular No. 26 dated 16 June 2020:

The branch evaluation reports received from the branches shall have to be assessed and if there is any risky matter realized in any branch, there shall be an arrangement of immediate inspection by the A&ID in the branch and 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 A&ID, 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 CEO of the bank. With the comments of the 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.

16.14 Assessment of Internal Controls

Once the inherent risks have been identified and assessed, internal controls must be evaluated to determine how effectively they offset the overall risks. Controls are programmes, policies or activities put in place by the Bank to protect against the materialization of a ML risk, or to ensure that potential risks are promptly identified. Controls are also used to maintain compliance with regulations governing an organization's activities. Many of the same controls apply to various activities undertaken within the Bank and will be executed by both the Front Office (1st line) and Compliance (2nd line). The controls in place are evaluated for their effectiveness in mitigating the inherent money laundering risk and to determine the residual risk rating. AML controls are usually assessed across the following control categories:

- AML Corporate Governance; Management Oversight and Accountability
- Policies and Procedures
- Know Your Client ("KYC"); Client Due Diligence ("CDD"); Enhanced Due Diligence ("EDD")
- Previous Other Risk Assessments (local and enterprise-wide)
- Management Information/Reporting
- Record Keeping and Retention
- Designated AML Compliance Officer/Unit
- Detection and SAR filing
- Monitoring and Controls
- Training
- Independent Testing and Oversight (including recent Internal Audit or Other Material Findings)
- Other Controls/Others

Each area is assessed for overall design and operating effectiveness. There may be both a positive or negative indicator of control execution and these should be clearly documented in order to assess the operating effectiveness of each control. Additionally, controls should be linked to Key Performance Indicators or other metrics where possible.

One way in which control effectiveness may be assessed is by undertaking a focused self-assessment by business unit/business line. A self-assessment of this kind can be challenged independently using subject matter expertise as well as existing internal information, such as business risk reviews, audit testing and assurance testing. A specific control may be rated according to a pre-defined rating scale or based on qualitative factors, e.g. 'satisfactory', 'needs improvement' or 'deficient' for each of the above control factors.

Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk can be determined. Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML risks within the Bank are being adequately managed.

It is possible to apply a 3 tier rating scale, to evaluate the Residual Risk on a scale of High, Moderate and Low. Any rating scale could also be used, for example a 5 point scale of Low, Low to Moderate, Moderate, Moderate to High, and High. The following definitions could be considered to describe the level of residual risk applied to a 3 tier rating scale:

Low Residual Risk: The overall inherent risk of the FI/business unit/business Line, based on the clients, products/services, channels, geographies and other qualitative factors, is low-to-moderate and the mitigating controls are sufficient to manage this inherent risk;

Moderate Residual Risk: The overall inherent risk of the FI/business unit/business line, based on the clients, products/services, channels, geographies and other qualitative factors, is low-to-moderate and the mitigating controls are not adequate to manage this level of risk, OR the overall inherent risk of the FI, based on the clients, products/services, channels, geographies and other qualitative factors, is high and the mitigating controls are adequate to manage this inherent risk

High Residual Risk: The overall inherent risk of the FI/business unit/business line, based on the clients, products/services, channels, geographies and other qualitative factors, is moderate-to-high and the mitigating controls are not sufficient to manage this inherent risk.

16.15 Agent Banking Operations checking

Internal Audit and Inspection Division of IBBPLC shall bring the policy/ procedures to conduct audit in Agent Banking Operations which are among others as under:

i) To ensure preservation of the AML Policy of IBBPLC in Agent Outlets
ii) To ensure KYC in every customer/account in Agent Points
iii) To ensure having a Bank official from the concerned controlling Branch for supervision of Agent Outlets regarding AML & CFT Compliance.
iv) Internal Audit and Inspection Division shall prepare a check list like ITP to conduct audit on AML & CFT Compliance in Agent Outlet.
v) To check on going Transaction Monitoring in Agent Outlets
vi) To check the capability of the officers of Agent Outlet to detect STR/SAR and report it to the concerned BAMLCO proactively
vii) To ensure the better implementation of BFIU Circular-26 dated 16.06.2020.

CHAPTER 17

Anti Bribery and Corruption Compliance Program of IBBPLC

Islami Bank Bangladesh PLC is a welfare oriented and Islami Shariah' based Bank. By born it is committed to ensure bribery & corruption free dealings in all of its operations. So, IBBPLC has Zero tolerance for corruption and bribery. Therefore, it is proposed to introduce an "Anti Bribery and Corruption Compliance (ABC) Program in IBBPLC of which Salient features may be as under:

17.1. Introduction:

Bribe involves financial & non financial facilities which are offered for discharging legal, illegal activities in favor of the offerer that means giving or receiving an unearned reward to influence someone's behavior. As per Black's Law Dictionary, Bribery is as the offering, giving, receiving, or soliciting of any item of value to influence the actions of an official or other person in charge of a public or legal duty.

Corruption is the financial & non financial facilities acquired by applying illegal authority and power. Corruption is a form of dishonesty or criminal activity undertaken by a person or organization entrusted with a position of authority, often to acquire illicit benefit. Corruption may include many activities including bribery and embezzlement, extortion, fraud, deception, collusion, cartels, Money Laundering and others similar activities.

17.2: Importance of Anti Bribery and Corruption compliance in Banks/ Financial Institution:

Anti Bribery and Compliance program is very much important for any Bank and Financial Institution. Bribery and corruption is directly related with Banks business as well as fund management. So, non compliance of Anti Bribery and Corruption Compliance may result in the following risks-

- **Credit Risk:** Bank will fail to recover the investment due to wrong assessment of the customer/ project and its collateral.

- **Reputation Risk:** Fraud and forgery in the international trade may loss the reputation of the Bank which results in decrease in foreign business.

- **Legal Risk:** Banks may fall into legal action for losing public interest.

17.3. Scope of Bribery and Corruption in IBBPLC:

i) Induction/ on-boarding of customers:

Induction or on boarding of Black listed customers/ customers those are not beneficial such as defaulters, criminal and so on without getting approval from Competent Authority of the Bank for financial or non financial benefits.

ii) Allowing transaction violating the instruction of Regulatory Authorities:

Allowing the customers to make transactions violating the freeze order/ Stop payment order of the Regulatory Authorities like BFIU, BB, DUDAK, NBR, Hon'ble Court, etc. without taking consent from Competent Authority or convey confidential information to the related parties to make transaction before implementing the instruction.

iii) Issuance of Fake PO/DD/Guarantee on behalf of the Customers to be submitted to any other organization as security/bid bond and so on by the Customers.

iv) Sanction of excess/ additional Investment/ facilities:

Incorrect assessment, estimation of the customer, business and valuation of the security is done and sanction of excess/ additional investment/ facilities violating the Banks norms, rules and practices.

v) Allowing insufficient, false securities/ collateral:

Violating the Banks norms/rules, allow the customers to avail investment/ facilities against insufficient or false collaterals in spite of tracing false documents.

vi) Providing illegal facilities:

Provide special rate of return, zero or lower L/C margin or Guarantee Commission, re-scheduling, free online facilities violating the Banks norms or showing false/ manipulated statement.

vii) International Trade:

Allowing the customers to launder the black money through under invoicing/ over invoicing/ multiple invoicing and so on.

viii) Procurement and Selling:

Procurement and sales of goods and services is done without Tendering or arranging fictitious Tendering violating the Banks rules and norms or convey the confidential information to the Buyer/ Seller before procurement/ sale process.

ix) **Donation/ sponsorship:**

Donate to any charity, organization, Political Entity, Social Community where concerned Executives/ Employees have direct or indirect benefit violating the Banks norms or without getting approval from the competent Authority of the Bank.

x) **Gift, Hospitality & Expense:**

Taking any gift, service, hospitality by any Executive/ Employee of IBBPLC violating the Bank's norms or without getting due approval from the Competent Authority of the Bank. Incurring any Expense for any Executive/ Employee of IBBPLC violating the Banks norm.

xi) **Transfer & Posting, Recruitment, Promotion, Remuneration:**

Applying of illegal authority and power or influencing the concerned person for transfer & posting, recruitment, promotion, allowing special financial benefit/ facilities to the employees, executives of the Bank.

17.4. IBBPLC's initiatives to prevent Bribery & Corruption prevention/ mitigation

Governance:

IBBPLC's ABC Compliance Programs shall be overseen by a Senior Management Team under direct supervision of the Hon'ble Managing Director & CEO of the Bank.
The overall objective of ABC governance is to establish and maintain a Program which sets a standard of behavior of IBBPLC that achieves a culture of ethical business practices and compliance with ABC legal and regulatory requirements.

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

- **Board of Directors:**

  Board of Directors after proper verification will approve the policy including the modification/ changes that may take place as per requirement. They will ensure a control environment for the bribery and corruption compliance.

- **Executive Committee:**

  Executive Committee shall adhere to and promote compliance with this policy. The Committee will also consider and recommend changes to this policy to the Board of Directors.

- **Audit Committee:**

  Audit Committee shall ensure that the system of internal control is adequate to prevent the risk of Corruption and Bribery at IBBPLC and will report to the competent Authority on their findings.

- **Risk Management Committee:**

  Risk Management Committee will evaluate the risk of Bribery and Corruption Risk of the Bank and make necessary recommendation to the Competent Authority of the Bank to mitigate the same.

- **Human Resources Wing:**

  Human Resources Wing (HRW) of IBBPLC shall chalk out plan & formulate procedures to identify any bribery & corruption activities in light of clause No. 17.5 of this program that may happen by the employees working in the Bank.

  They shall circulate this program for information of all concerned with advice to be vigilant for any bribery and corruption activities by the employees working under Wing/Division/Zone/Branch and if any of such occurrence is detected/ unearthed, the same

shall be reported to HRW for communicating the same to the Competent Authority of the Bank to do the needful.

☞ **Audit and Inspection Division:**

Audit and Inspection Division (A&ID), IBBPLC shall pay special attention to evaluate the activities of Branch/ Zone/ Wing/ Division in this regard while conducting their routine audit and report the same accordingly alongwith intimation to Human Resources Wing and Central Compliance Committee.

17.5. ABC Compliance Program of IBBPLC

Anti Bribery and Corruption (ABC) Compliance Program of IBBPLC shall among others includes the followings:

- ☞ Prohibit the promising, offering, giving, solicitation or receiving of anything of value, directly or indirectly through third parties, if improperly intended to influence action or obtain an advantage.
- ☞ Prohibit falsifying or concealing any books, records or accounts that relate to the business of the firm, its customers, suppliers or other business partners.
- ☞ Define and identifies the heightened risk of interaction with Public Officials.
- ☞ Provide employees with the opportunity to report potential bribery in a confidential manner and protects employees from retaliation for good faith reports
- ☞ Notify employees of potential consequences of non-compliance.
- ☞ Obtain strong and visible commitment from Senior Management and the Board of Directors, including a public statement of such commitment by the Bank.
- ☞ Get the customer to be inducted verifying all necessary records, Past History and screening of Sanction List, Adverse Media Report and Local & Internal Black List.
- ☞ Get the all Employees of the Bank follow the instruction of the Regulatory Authority of the Bank like BFIU, BB, DUDAK, NBR, Hon'ble Court and maintain confidentiality of the same.
- ☞ Provide all facilities to the Customers as per prevailing rules and practices of the Bank.
- ☞ Ensure that before sanctioning the Investment, sufficiency, quality, ownership, nature of the collateral must be judged with utmost good faith including verification of the documents and papers. No nepotism and biasness shall be allowed in this regard.
- ☞ Ensure that Proper verification of the documents of the International trade shall be verified through independent sources like, international price list, shipper and competitors.
- ☞ Ensure that Procurement & selling process shall be done as per the set rules of the Bank and obtaining the approval from Competent Authority of the Bank. Verification of the Price/ documents shall be made from independent sources and confidentiality of the same shall be strictly maintained.
- ☞ Ensure that before sanctioning any donation, sponsorship, Expense and investment proper verification of the motive, ultimate beneficiary or relationship with the Direc-

tors/Executives/Employees and the concerned organization, Charity or Community shall be considered and ascertained.

- ☞ Ensure that before receiving any gift, benefits and hospitality by any Employee of IBBPLC, HR Policy of the Bank shall be strictly followed.
- ☞ Ensure that every dealing of the Banks operations including recruitment, transfer & positing, remuneration, benefit, training shall be done as per the HR Policy of the Bank.

17.6. Conclusion

All Employees of the Bank shall be brought under the ABC Compliance Program of IBBPLC and necessary Disciplinary measures as per the HR Policy of the Bank shall be taken against the concerned employee found non-compliant to the Anti Bribery and Corruption (ABC) Compliance Program of the Bank.

Chapter - 18

e-KYC Policy in IBBPLC

18.1 Preamble

Bangladesh Financial Intelligence Unit (BFIU) vide Circular No. 25 dated 08 January, 2020 issued an electronic Know Your Customer (e-KYC) guideline to open accounts in the financial sector without filling up any paper-based documents for bringing people under the financial services at financial institutions which shall be implemented within December, 2020. The new guideline on account opening will be applicable to the financial institutions including banks, non-bank financial institutions, insurance companies, capital market intermediaries, MFS, DFS and the other companies licensed by Bangladesh Bank within a limited transaction threshold and having the lower risk nature. In e-KYC process, applicants' photographs will be taken on spots and customer's identification data authenticated instantly. The thumb print will serve as the digital signature.

Based on the customers' risk exposures, the BFIU classified e-KYC into two categories: simplified e-KYC and regular e-KYC. Under the simplified e-KYC, digital financial services — mobile financial services, payment service providers and operators, and fintech companies — would be allowed to be registered for those services. Besides, financial inclusion products and agent banking products could be offered upon simplified e-KYC registration.

Banking products like deposit or withdrawal not exceeding Tk 1 lakh, term deposit up to Tk 10 lakh and special deposit scheme with maturity value up to Tk 10 lakh can be offered upon simplified e-KYC. Banks offering products to customers beyond the limit will have to be registered through regular e-KYC. The e-KYC guidelines said that the financial institutions should maintain all sorts of digital data and log until five years after the closure of the account or business relationship.

This e-KYC guideline contains a set of instructions for the financial institutions to enable them to conduct customer due diligence in a digital means. To implement BFIU Circular 25 dated 08 January, 2020, Islami Bank Bangladesh PLC (IBBPLC) requires formulating an e-KYC Policy/Guideline to be implemented across the bank which is as under:

18.2 Scope

This Guideline shall be known as **Electronic Know Your Customer (e-KYC) Policy** of IBBPLC which shall deal with electronic customer on-boarding, identification and verification of customer identity, creating of customer digital KYC profile as well as risk grading of customer in a digital means.

This Policy shall be applicable only for natural person, therefore, all legal persons or legal arrangements shall be excluded from the obligation of e-KYC.

For a low risk assessed customer simplified e-KYC and for a regular and higher risks customer regular and enhanced e-KYC shall be conducted.

In case of failure of attempting e-KYC due to any technical reason, traditional KYC approach shall be followed for natural person.

18.3 Objectives

The key objectives of promoting e-KYC in IBBPLC are to :

- Establish good governance within the bank
- Enhance the growth of financial inclusion
- Protect the bank from abuse of criminal activities
- Ensure integrity and stability of the bank
- Manage ML & TF risks
- Reduce cost related to customer on-boarding and managing CDD
- Promote fintech services and
- Participate in the national level well-being

18.4 e-KYC Process

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

The e-KYC module can be divided into following two types base on the customers' risk exposures:

a. **Simplified e-KYC :** In case of proven lower risk scenario, a customer can be onboarded electronically using simplified digital KYC form where no risk grading will be required. However, sanction screening shall be undertaken and KYC review shall be done every five years.

b. **Regular e-KYC :** Where a customer shall be on-boarded and verifying customer identity electronically, Branches Control Division (BCD) IBBPLC, HO shall formulate a digital KYC Form (Digital e-KYC Form) as per prescribed format given by BFIU in their e-KYC Guideline at Section 6.2. 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.

   However, e-KYC is a digital process where IBBPLC can open a customer account by filling up a digital form, taking photograph on the spot, and authenticate the customer's identification data (ID No., biometric information, address proof) instantaneously. Such bio-metric information or digital signatures or electronic signatures may be used for transaction authentication as well. The customer on-boarding process may undertake via followings means:

   - **Assisted customer on-boarding:** Where IBBPLC or its nominated agent or third-party visit customer or customer visit IBBPLC or its nominated agent or third party's premises and open account with the direct assistance of IBBPLC or its nominated agent or third party; and

   - **Self check- in:** Where customer can onboard at his own by using kiosk, smart phone, computer or other digital means abiding by the norms of this e-KYC Guidelines. Self check-in shall be allowed for face matching model only as described section in 5.8 of this Guideline.

18.4.1 Applicability

e-KYC shall only be applicable for natural persons who have valid NID document. Natural person without NID and a legal entity or arrangement shall follow the KYC norms as prescribed by the BFIU from time to time. Therefore, 'simplified' and 'regular' e-KYC norms shall be applicable based on threshold and risk mentioned in BFIU e-KYC Guideline. IBBPLC shall conduct paper based customer on-boarding and simplified or regular KYC and CDD measures if any customer unable to on board with this e-KYC mechanism.

18.4.2 Simplified e-KYC

The scope of simplified e-KYC covers the following products of IBBPLC which may be revised as per BFIU guideline from time to time:

a) Digital Financial services

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

b) Financial inclusion products

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

c) Agent banking products:

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

d) Banking products:

- ❖ Deposit or Withdrawal not exceeding BDT 1,00,000 per month in a checking account;

iv) Term Deposit upto BDT 10,00,000;

v) Special deposit scheme with maturity value exceeding BDT 10,00,000

e) Securities Market Products:

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

18.4.3 Regular e-KYC

The scope of regular e-KYC covers the followings:

a) Agent banking accounts:

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

b) Banking products:

- Other banking products except the banking products mentioned in section 4.2;

c) Non-Bank Financial institutions Products:

- Any type of NBFI products exceeding BDT 10,00,000;

d) Securities Market Products:

- Deposit to the BO account exceeds BDT 15,00,000 and above.

18.5 Customer On-boarding-Simplified

18.5.1 Customer on-boarding models

IBBPLC shall follow customer boarding under this e-KYC Policy which is based on national identification document, information stored within a specific NID plus any one of the bio-metric verification out of fingerprint matching, face matching, voice matching and iris matching. The customer on-boarding shall also be covered self check-in, check in with assistance of service providers and other relevant means as required necessary.
An electronic customer on-boarding involves multiple activities. An efficient customer on-boarding starts from clients' identity information and can be segmented into following steps:

a) Data capture and generation;

b) Identity verification;

c) Sanction and other screening;

d) Account opening;

e) Customer profiling (e-KYC Profile); and

f) Customer risk grading (where applicable).

For the purpose of undertaking e-KYC, this guideline suggests initially following two bio-metric based models of customer on-boarding which are as follows:

a. Customer on-boarding by using fingerprint; and
b. Customer on-boarding by matching face.

However, other two models i.e. voice matching and iris matching may also be used if there are sufficient infrastructural and logistics facilities available. Moreover, IBBPLC may also introduce other innovative models using bio-metric beyond these four models having prior approval from BFIU.

18.5.2Customer on-boarding by using fingerprint

The customer on-boarding by using fingerprint matching is one of the commonly used methods where customer fingerprint will be used as a main identifier of a person's identity. The minimum generic approach for this model will be as follows:

(a) **Step-one**

NID Number:.....

Date of Birth:
(DD/MM/YYYY).....

Bio-metric verification.....

Next

Total process shall be developed, maintained and managed by ICTW, IBBPLC, HO for smooth functioning of the same.

In this step, a customer shall approach to IBBPLC or to its agent for account opening or BO account opening using e-KYC. Then, the customer will provide his or her NID. IBBPLC or its agent inserts NID number and Date of Birth (DOB) into the specified template (to be developed and introduced by ICTW, IBBPLC, HO) and also collects fingerprint, then press Next button. After pressing Next, button the information of NID number, DOB and fingerprint data will be matched with NID database, if the data is matched, then next template will be appeared.

(b)Step-two

Applicant's Name:
.....

Mother's Name:
.....

Father's Name:
.....

Spouse Name:
.....

Gender (M/F/T): ……...

Profession: …….

Mobile Phone Number: ……..

Present Address: .....

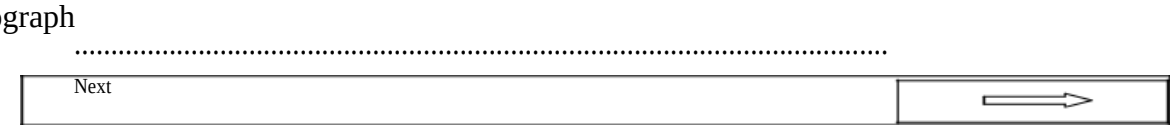
Permanent Address: .....

Nominee: ……Relation: …… Photograph: ……

Next

In step two, IBBPLC or its agent will insert or punch customer's personal information data as far as possible. It is encouraged to use the technology that enable data fetching from the NID and wherever required insert rest other information manually. On completion of personal information, Next option shall be pressed.

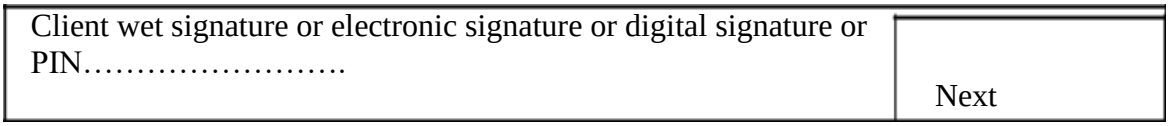
(c) Step-Three



In step three, IBBPLC or its agent or client shall capture or upload customer's photograph. However, when there is self check-in occurs, the live selfie with proper light and camera frame is required; therefore, Next option shall be pressed.

Concerned officials/ agent shall ensure that system only captured the real persons' picture only.

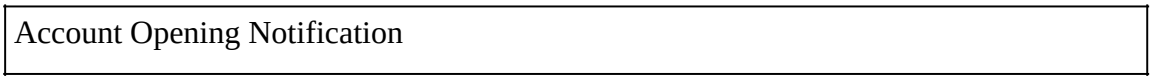
(d) Step-Four



Where necessary, the concerned officials/ agent may collect physical signature at the later stage and preserve it digitally for further use.

In step four, customer wet signature (signature using pen) or customer electronic signature (signature using devices) or digital signature or personal identification number (PIN) shall be required to be preserved for future reference.

(e)Step-Five



In step five, after completion of all the processes, system shall generate a notification of account opening in process. After completion of necessary sanction and other screening, account opening confirmation notification shall be sent to the customer.

The simplified customer on-boarding process shall be completed once the client gets notification from the IBBPLC. However, at any point of relationship, IBBPLC may ask for additional information from customer and shall preserve it in the digital KYC profile of customer.

In case of joint customer (more than one) on-boarding, the similar process shall be followed. All the fields mentioned in step- two is the minimum requirement, however, if necessary, IBBPLC may add few fields.

18.5.3 Required technology

The electronic customer on-boarding and e-KYC process shall require technology platform for its implementation. Therefore, based on the simplified e-KYC model at a minimum, following technology and instruments shall be used by IBBPLC to complete the process:

i) Software/App/Program compatible to the above process;

ii) Internet connection;

iii) Online connection to the NID verification server

iv) Fingerprint capturing devices;

v) Electronic signature capturing devices (where necessary) etc.

ICT Wing & Engineering Division of IBBPLC, (or Concern Wing/Division) Head Office with joint collaboration may take necessary initiatives to procure and install the above mentioned equipments/accessories for smooth functioning of the same.

18.5.4 Sanction and other screening

The full-fledged account procedures shall be completed by completion of sanction and other necessary screening which includes as follows:

i) UNSCRs/OFAC/EU/UK screening;

ii) Adverse media screening (where necessary); and

iii) Internal or external exit list (where necessary).

18.5.5 Audit trail of customer profile

To maintain an audit trail, IBBPLC shall preserve a digital KYC profile and relevant logbook, even for low risk or financial inclusion products, which shall include the followings:

i) Customer details (name, contact, address, etc) with photograph;

ii) Customer ID image (both side);

iii) Customer signature (where necessary);

iv) Customer risk review process (once in 5 years);

v) Transaction pattern etc; and

vi) Others information as deemed necessary to complete customer KYC.

IBBPLC shall maintain a digital log for all successful and unsuccessful client on-boarding, matching parameters etc. for further work and audit trail. All the data shall be preserved and stored digitally for further both for internal and external audit purposes. The sample e-KYC profile, at a minimum, is appended at Annexure-A

18.5.6 Matching parameters

As the electronic on-boarding requires matching customer's ID stored data with the national identification database, the following elements or information shall be required to be matched as per described percentile:

Particulars	Matching Percentage
Applicants' Name	≥ 80%
Date of Birth	100%
Fingerprint	≥ 80%
NID number	100%
Fathers' Name	≥ 80%
Mothers' Name	≥ 80%

18.5.7. Security measures

IBBPLC shall use additional security measures in the customer on-boarding process which shall contain 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 shall be maintained properly by the Bank so that no customer data to be hacked or compromised. IBBPLC shall also preserve customer data locally hosted server or cloud server 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.

18.5.8 Customer on-boarding by using face matching

IBBPLC may adopt customer on-boarding using face matching model where customer face Bio-metrics shall be used as a main identifier of a person's identity along with the national ID number. Following steps shall be required for on-boarding of a customer by using face matching model:

(a) **Step-one**

i) Taking picture of customer NID (original copy)-front page
ii) Taking picture of customer NID (original copy)-back page

Next ⇨

In this step, a customer approaches to IBBPLC or its agent or IBBPLC or its agent approaches to a customer or customer engaged in self check-in for account opening, or BO account opening by using e-KYC procedures. Then, it requires to capture photograph or scanning front page of the customer NID followed by the back page. An Optical Character Recognition (OCR) shall be used to capture the NID data both in Bangla and English. In the back end, all NID data shall be preserved within specific format.

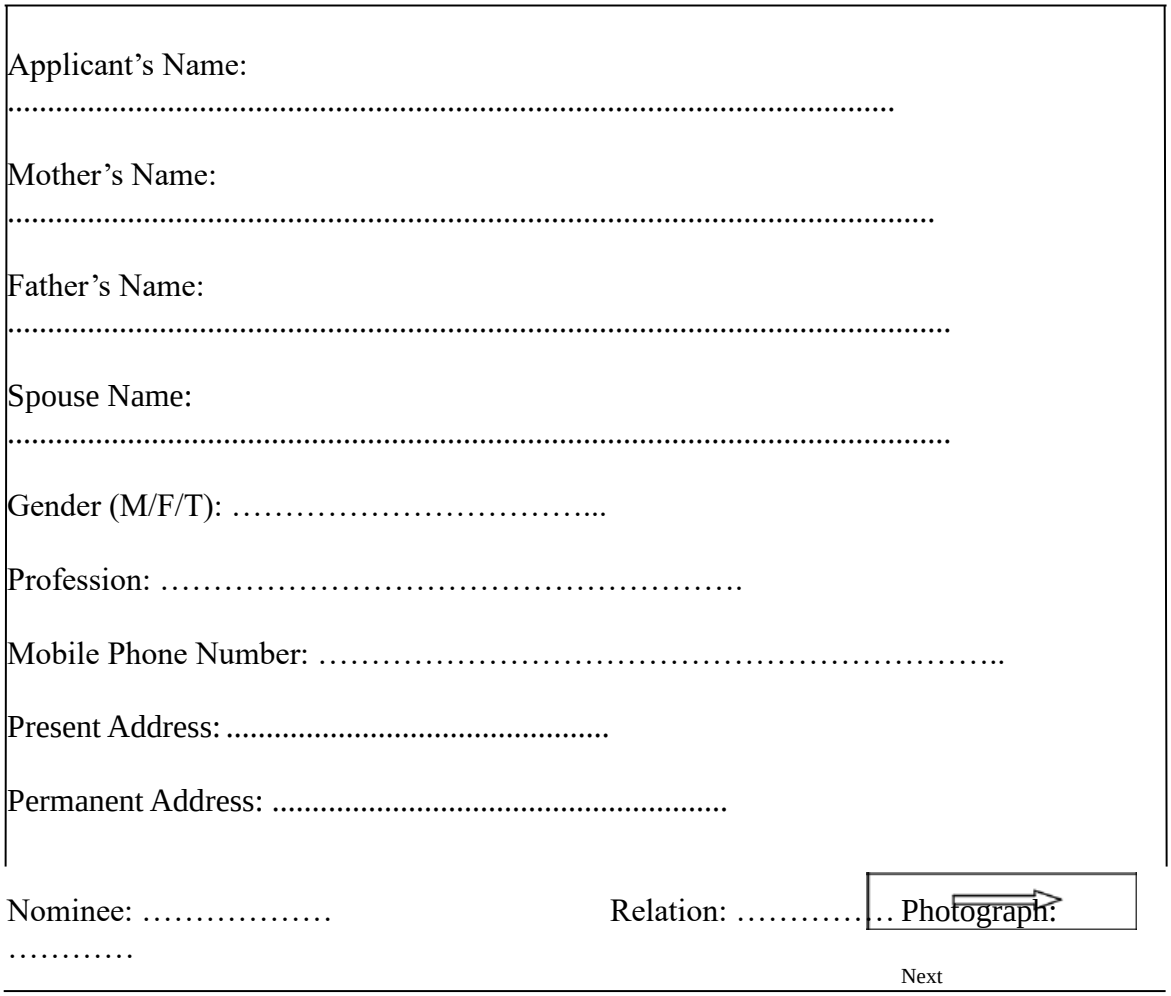
(b) Step-two

ii. Taking picture of customer face

Next ⇨

In step two, IBBPLC or its agent or client shall take an appropriate photograph of the customer's face by using high resolution camera or webcam. While taking picture agent or client shall be tactful enough to take the face only of the customer as well as visible quality of the photograph.

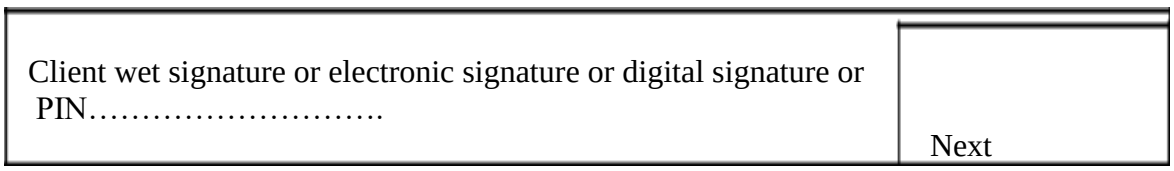
(c) Step-Three



In step three, all necessary information shall be fetched up in the above digital format. Furthermore, additional input shall be punched to fulfill the whole template.

Concerned officials/agent shall ensure that system only captured the real persons' pic ture only.

(d) Step-Four



In step four, customer wet signature (signature using pen) or customer electronic signature (signature using devices) or digital signature or personal identification number (PIN) is required to be preserved for future reference.

(e)Step-Five

Account Opening Notification

In step five, after completion of all the processes, system shall generate a notification of account opening in process. After completion of necessary sanctions and other screening, account opening confirmation notification shall be sent to the customer.

The simplified customer on-boarding process shall be completed once the client gets notification from IBBPLC. However, at any point of relationship, IBBPLC may ask for additional information from customer and will preserve it in the digital KYC profile of customer.

In case of joint customer (more than one) on-boarding, the similar process shall be followed. All the field mentioned in step two is the minimum requirement, however, IBBPLC may add few fields where necessary.

18.5.9. Required technology

At a minimum, the customer on-boarding via face matching model requires to use the following technology to complete the whole customer on-boarding process;

i. Software/App/Program compatible to the above process;

ii. Internet connection;

iii. Smart phone or desktop computer with high resolution webcam;

iv. Online connection to the NID verification server;

v. Electronic signature capturing devices (where necessary) etc.

Concern Division of IBBPLC, Head Office with joint collaboration may take necessary initiatives to procure as per procurement policy of the IBBPLC and install the above mentioned equipments/ accessories for smooth functioning of the same.

18.5.10 Sanctions and other screening

The full-fledged account procedures shall be completed by completion of sanction and other necessary screening which includes as follows:

- UNSCRs/OFAC/EU/UK screening;
- Adverse media screening (where necessary); and
- Internal or external exit list (where necessary).

18.5.11 Audit trail of customer profile

To maintain an audit trail IBBPLC shall preserve a digital KYC profile and relevant logbook, even for low risk or financial inclusion products, which include the followings:

- Customer details (name, contact, address, etc) with photograph;
- Customer ID image (both side);
- Customer signature (where necessary);
- Customer risk review process (once in 5 years);
- Transaction pattern etc; and
- Others information as deemed necessary to complete customer KYC.

IBBPLC shall maintain a digital log for all successful and unsuccessful clients on-boarding, matching parameters etc. for further use and audit trail. All the technology data shall be preserved and stored digitally for further both internal and external audit purposes. The sample e-KYC profile, at a minimum, is mentioned at annex -A.

18.5.12. Matching parameters

As the electronic on-boarding requires matching customer's ID stored data with the national identification database, the following elements or information shall be matched as per described percentile:

Particulars	Matching Percentage
Applicants' Name	≥ 80%
Date of Birth	100%
Fingerprint	≥ 80%
NID number	100%
Fathers' Name	≥ 80%
Mothers' Name	≥ 80%

18.5.13. Security measures

IBBPLC shall use additional security measures in the customer on-boarding process which shall contain 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 shall be maintained properly by the Bank so that no customer data to be hacked or compromised. IBBPLC shall also preserve customer data locally hosted server or cloud server 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 Customer on-boarding- Regular measure

IBBPLC shall use electronic on-boarding and e-KYC procedures for the products and services which are not fall under proven low risk or limited risks as well gradually as electronic on-boarding and e-KYC procedures are also applicable for any sorts of financial products.

Both the technology-based model i.e. fingerprints and faces matching technologies are applicable for regular on-boarding and managing KYC. Similarly, such on-boarding process only applicable for natural person who have valid NID.

Initially on-boarding process for the regular e-KYC is similar, however, it requires few modes of additional information and conduct additional customer due diligence compared to the simplified method. IBBPLC shall create digital customer KYC profile and risk grading exercise digitally during the regular e-KYC. This means similar step by step procedures shall be followed in case of different models (fingerprint and face matching) as discussed above to complete the regular e-KYC procedures.

Therefore, the component of regular e-KYC includes the following elements:

- A digital template with more information compared to simplified e-KYC;
- A more stringent KYC profile of the customer;
- Screening of customer other than UN Sanctions (for example: PEPs/IPs, Beneficial Owner, Adverse Media, Internal External list checking etc.); and
- Risk grading exercise.

Along with the process of digital on-boarding already discussed above, the digital information template at a minimum required for regular e-KYC would be as follows:

Account Name…… Account Type……

Account Number…….....Unique Account Number…….....

Applicant's Name: .....

Mother's Name: .....

Father's Name: .....

Spouse Name :.....

Gender (M/F/T)……... Date of Birth…….

Profession…… Monthly income…… Sources of Fund…….

Mobile Phone Number:……

Present Address:..... Nationality…….

Permanent Address: .....

Nominee:……Date of Birth……..
Relation……Photograph……

NB: (a) Incorporate 'add' button of similar field if there is more than one applicant;

(b) Incorporate 'add' button of similar field if there is more than one nominee;

(c) If applicant is minor, traditional method of account opening shall be followed.

(d) Incorporate 'add' the following field if nominee is 'Minor'

i) Name of minor nominee… ii) Name of Guardian… iii) Address…. iv) Relation….

v) NID of Guardian……. vi) Photograph of Guardian…….

The customer on-boarding process and instructions as discussed above for the simplified measures shall be similar for regular e-KYC. After opening Account IBBPLC shall collect additional information and customer wet signature to create full digital profile of the client.

18.6.1.Required technology

The same technologies mentioned for e-KYC also be applicable for regular e-KYC.

18.6.2.Sanctions and other screening

The screening mechanism for regular e-KYC is quite stringent compare to the simplified one. The full-fledged account procedures shall be completed by completion of sanctions and other necessary screening which includes as follows:

i) UNSCRs/ OFAC/EU/UK screening;

ii) PEPs/IPs Screening;

iii) Identification of beneficial ownership (if any);

iv) Adverse media screening;

v) Risk grading of customer;

vi) Customer Due Diligence template;

vii) Enhanced Due Diligence (if needed).

18.6.3. Audit trail of customer profile

To maintain an audit trail IBBPLC shall require to preserve a digital KYC profile and relevant log book or data which should include the followings:

a) Customer details (Name, contact, address, etc) with photograph;

b) Customer ID image (both side);

c) Customer signature (where necessary);

d) Risk grading of customer (where necessary);

e) Customer Due Diligence template (where necessary)

f) Customer transaction pattern; and

g) Others information as deemed necessary to complete customer KYC.

IBBPLC shall maintain a digital log for all successful and unsuccessful e-KYC on-boarding process for further work and audit trail. All the technology data shall be preserved and stored digitally for further audit purposes. The sample e-KYC profile, at a minimum is enclosed at Annexure-B.

18.6.4 Matching parameters

The similar matching parameters mentioned in the simplified e-KYC shall be applicable for regular e-KYC.

18.6.5 Security measures

IBBPLC shall use additional security measures in the customer on-boarding process which shall contain 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 shall be maintained properly by IBBPLC so that no customer data to be hacked or compromised. IBBPLC shall also preserve customer data locally hosted server or cloud server 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.

18.7 Other relevant issues

18.7.1 Record Keeping

IBBPLC shall maintain all sorts of digital data and log until five years after the closure of the account or business relationship. The digital data shall contain customer on-boarding, customer identity verification, KYC profile, risk grading exercise; transaction related data and their analysis; all sorts of correspondence with customer; data collected later for CDD purposes; and all other relevant files.

Digital fingerprint and log shall contain but not limited to information collected during clients' identity verifications and other relevant information related to the screening measures also required to be preserved. IBBPLC also shall collect other complementary data (such as, geo location, IP addresses, etc.) which could also support ongoing due diligence.

18.7.2 Reliance on third parties

To implement the e-KYC, IBBPLC may rely on the third-party technology providers either full or part to implement e-KYC. Though IBBPLC may engage with third party, the ultimate responsibility still lies with them. This means IBBPLC may rely on another entity or technology providers that satisfies the criteria described above to conduct customer due diligence which covers:

(i) customer identification and verification data from independent and reliable sources;

(ii) identify and understand who the beneficial owner(s) is; and

(iii) identify the purpose and intended nature of business and relevant CDD measures in a digital manner. Yet, IBBPLC itself shall ensure the reliability and authenticity of the

data collected. The following condition shall be applied while engaging with any third party for the financial Institutions:

(a) Immediately obtain the necessary information concerning the identity of the customer as mentioned in (i) –(iii) in the above.

(b) Take adequate steps to satisfy itself that the third party shall make available copies of identity evidence or other appropriate forms of access to the data or digital log as mentioned (i) –(iii) in the above and in this Guideline without delay.

(c) The activities of the third party shall be regulated under the e-KYC guideline of BFIU and shall be monitored by IBBPLC.

- Third party shall ensure customer and IBBPLC data protection according to the IT security policy of Bangladesh Government and the respective prudential and self regulators.
- Both the third party and the IBBPLC covered under this guidance shall ensure the customer data collected under this guidance shall not digitally transmitted or transferred outside Bangladesh without prior approval of the prudential regulators and/or BFIU. In this case, BFIU Circular No. 23 dated 31/01/2019 will be applicable.

18.7.3 Risk Assessment

IBBPLC shall conduct a risk assessment of new technology based electronic KYC mechanism to understand how it may be abused and put in place appropriate measures to prevent such abuse as per the circulars and Guidance issued by BFIU. IBBPLC shall also conduct customer risk assessment as per risk assessment format annexed at C(i) & C(ii).

18.7.4 Transformation of existing clients CDD

IBBPLC shall transform their existing clients CDD related documents into digital form following above mentioned procedures where applicable.

18.7.5 Implementation

This Electronically Know Your Customer (e-KYC) Policy of IBBPLC shall be a part of the Bank's existing the Manual for General Banking Operations and shall be inserted in the same accordingly. This Policy may be modified/ revised as per local regulatory requirements (if any in future) on getting due approval from the august Board of Directors of IBBPLC.

The e-KYC Policy of IBBPLC shall come into force with immediate effect and shall be applicable while conducting Customer Due Diligence (CDD) in the Bank.

Annexure-A

Sample output of the simplified e-KYC

Photo Customer	Photo Nominee

Applicant's Name:
.....
.....
Mother's Name:
.....
Father's Name
:.....
.....
Spouse Name----------

Date of Birth ……... Gender (M/F/T)……..

Profession…….

Mobile Phone Number……..

Present Address:.....

Permanent Address: .....

Nominee:…….: Relation…… Photo-graph…….

Specimen signature/digital signature (where necessary)
…….……

Front side of NID	Back side of NID

1. Has UNSCRs check done? (Yes) (No)
2. Has review of customer profile done (existing customer)? if so, date of review…..
3. What is the average range of customer transaction (over 6/12 months)?.....
4. Any other relevant field may be added here……..

Sample output of regular e-KYC

Photo Customer	Photo Nominee

Applicant's Name:.....

Account number:..... Unique account number.....

Mother's Name: .....

Father's Name :.....

Spouse Name: .....

Date of Birth ..... Gender (M/F/T).....

Profession:..... Monthly income..... Sources of Fund.....

Mobile Phone Number:..... Nationality..... TIN (if any): .....

Present Address: .....

Permanent Address:.....

Nominee:.....: Relation..... Photograph.....

Specimen signature.....

Front side of NID	Back side of NID

5. Has UNSCRs check done? (Yes) (No)
6. Has risk grading done? If assessed risk high then conduct EDD as per BFIU circular.

Risk Type	Overall Score
Regular (< 15)	
High (≥15)	

7. Is the customer is IPs/PEPs? If client is PEPs or IPs with higher risk, then conduct EDD as per BFIU circular.
8. Is there any adverse media news against the customer? If any then conduct EDD.
9. Has the source of und verified/justified? (Yes) (No)
10. Has the beneficial ownership checked? If there any beneficial owner found, then conduct CDD on beneficial owner. If beneficial owner is PEPs, then conduct EDD.
11. Are any other documents obtained.....?
12. Nominee details:.....
13. Has review of customer profile done (existing customer)? if so, date of review.....
14. What is the average range and usual pattern of customer transaction (over 6/12 months)?....
15. Any other relevant field may be added here .....

Annexure-C(i)

Form for Customer Risk Grading

1. Type of On-boarding	
Branch/Relationship Manager	2
Direct Sales Agent	2
Walk-in	3
Internet/Self check-in/Other non Face to Face	5
2. Geographic Risks:	**Score**
Client is--	
Resident Bangladeshi	1
Non-resident Bangladeshi	2
Foreign Citizen	3
For Foreigners:	
Risk classification of country of origin	
Does client's country of citizenship feature in FATF/EU/OFAC/UN Black List/Grey List?	
No	0
Yes	5
3. Type of Customer:	**Score**
Is client a PEP/Chief or High Official of International Organization, as per BFIU Circular?	
No	0
Yes	5
Is client's family/close associates related to PEP/Chief or High Official of International Organization?	
No	0
Yes	5
Is client a IP? or his family/close associates related to IP?	
No	1
Yes (based on assessed risk)	5

4. Product and Channel Risk:	**Score**
Type of Product	
Savings account	1
Current account	4
FDR	3
Deposit Scheme upto12 lac	1
Deposit Scheme above 12 lac	3
Forex account	5
S.N.D.	3
R.F.C.D.	5
5. Business and Activity Risk	**Score**
(a) Business	
Please pick Applicable from Annexure and put the relevant score in the next column	.....
(b) Profession	
Please pick Applicable from Annexure and put the relevant score in the next column	
	.....
6. Transactional Risks:	**Score**
What is the lient's Average Yearly Transactions Worth?	
<BDT 1 million	1
From BDT 1 million to 5 million	2
From BDT 5 million to 50 million (5 crores)	3
More than BDT 50 million (5 crores)	5
7. Transparency Risk	**Score**
Des client has Provided credible source of funds	
No	5
Yes	1

Annexure-C(ii)

Risk Grading for Business or Profession

Client Business	Score	Client Profession	Score
Jeweller/Gold/Valuable Metals Business	5	Pilot/Flight Attendant	5
Money Changer/Courier Service/Mobile Banking Agent	5	Trustee	5
Real Estate Developer/Agent	5	Professional (Journalist, Lawyer, Doctor, Engineer, Chartered Accountant, etc.)	4
Promoter/Contractor: Construction Projects	5	Director (Private/Public Limited Company)	4
Art and Antiquities Dealer	5	High Official of Multinational Company (MNC)	4
Restaurant/Bar/Night Club/Parlour/Hotel	5	Homemaker	4
Export/Import	5	Information Technology (IT) sector employee	4
Manpower export	5	Athlete/Media Celebrity/Producer/Director	4
Firearms	5	Freelance Software Developer	4
RMG/Garments Accessories/Buying House	5	Government service	3
Share/Stocks Investor	5	Landlord/Homeowner	3
Software/Information and Technology Business	5	Private Service: Managerial	3
Travel Agent	4	Teacher (Public/Private/Autonomous Educational Institution)	2
Merchant with over 10 million takas invested in business	4	Private Sector Employee	2
Freight/Shipping/Cargo Agent	4	Self-employed Professional	2
Automobiles business (New or Reconditioned)	4	Student	2
Leather/Leather goods Business	4	Retiree	1
Construction Materials Trader	4	Farmer/Fisherman/Labourer	1
Business Agent	3	Others: **(Please State Below and circle numerical score as needed)**	
Thread/"Jhut" Merchant	3		1..2..3..4..5
Transport Operator	3		
Tobacco and Cigarettes Business	3		
Amusement Park/Entertainment Provider	3		
Motor Parts Trader/Workshop	3		
Small Business (Investment below BDT 5 million)	2		
Computer/Mobile Phone Dealer	2		
Manufacturer (except, weapons)	2		
Others: **(Please State Below and circle numerical score as needed)**			
	1..2..3..4..5		

Chapter-19

AML & CFT Compliance for Mobile Financial Services/Mobile Banking (mCash) of IBBPLC

19.1 : Preamble

Mobile Financial Services shortly known as MFS is a technique of delivering money services that combines banking with mobile wireless networks, enabling customers to conduct banking and other financial transactions using their cell-phones. Accounts can be operated by users by Unstructured Supplementary Service Data, Short Message Service, or particular apps on the smartphone. Agents approved by the bank typically cherishes mobile financial services, allowing account holders to transact outside of bank locations in the place of individual agents. Due to its affordability and safe medium of transaction, it has gained widespread acceptance across the country. Mobile financial services encourage socio-economic development and financial Inclusion of under-privileged rural people through mobile financial services for balanced growth of the economy of Bangladesh.

Considering its rapid expansion and popularity among the mass, it was necessitated to bring MFS under regulatory control and monitoring and hence several regulatory guidelines were issued in this regard and ***Guidelines for Mobile Financial Services (MFS) for the Banks*** and ***Bangladesh Mobile Financial Services* (*MFS*) *Regulations*, 2022"** issued by Bangladesh Bank may be prominently mentioned.

Apart, Mobile Financial Services (MFS), due to its widespread acceptance and use, may usher potential money laundering and terrorist financing risks for Banks as well as MFS service provider institutions which the above mentioned ***Regulations/Guidelines*** also addressed and issued directions to prevent the same.

Bangladesh Financial Intelligence Unit (BFIU) also issued their directives solely to the MFS provider institutions vide Circular No. 20 dated 17.09.2017 to prevent ML & TF risks in their operations and mentioned that the Bank having MFS operations shall not require to completely abide by this circular no.20 because of the enforcement of BFIU Circular 26 dated 16.06.2020 to prevent ML & TF risks through banking channel.

Islami Bank Bangladesh PLC introduces Mobile Financial Services namely **mCash** wherein related Laws, Rules, Regulations-Guidelines of the country shall also be applicable. In order to ensure AML & CFT compliance in mCash operations of IBBPLC, following programs/activities as were laid down vide BFIU Circular 20 dated 17.09.2017 and BFIU Circular 26 dated 16.06.2020 shall be implemented and the same shall be reported by the concerned Division(s) of Head Office to Central Compliance Committee for their next course of actions:

19.2 : AML & CFT Compliance Programs for mCash of IBBPLC

A. Proper selection and acceptance of the mCash Agents/Distributors/Merchants/Clients.
B. On-boarding of the mCash customers by observing all CDD measures including KYC procedures as per BFIU Circular 20 dated 17.09.2017 and BFIU Circular 26 dated 16.06.2020.

C. Ensuring that suspicious transactions/activities can be isolated for subsequent investigation through automated/manual means to identify suspicious activity/transaction report (STR/SAR).

D. Any suspicious, unusual or doubtful transactions likely to be related to money laundering or terrorist financing activities shall be reported immediately and spontaneously to the CAMLCO of Head Office for onward submission of the same to Bangladesh Financial Intelligence Unit (BFIU). Strict confidentiality of the reported STR/SAR shall be maintained.

E. mCash officers, distributors/agents, customers shall be brought under minimum awareness program once every two year on AML & CFT compliance issues by the concerned Division (mCash Division/Department) of Head Office.

F. All sorts of KYC data and transactions records shall be preserved accordingly.

The End