MANAGING CORE RISK IN BANKING

Money Laundering &Terrorist Financing Risk Management Guidelines- 2016 (Amendment 2019)

Approval Note Sheet

Document Name	**ML&TF Risk Management Guidelines- 2016 (Amendment 2019)**
Document Owner	**AML & CFT Department**
Version Number	**2.0**
Developed By	**AML & CFT Department & Enterprise Transformation**

IFIC Tower
61, Purana Paltan, Dhaka-1000

Effective Date: May 2019

Review History Sheet			
Details	**By Whom (Name, Designation, Department)**	**Date**	**Version**
Guided By	**Ms. Sharmilla Manzoor** Head of Enterprise Transformation **Mr. Md. Akbar Ali** Head of AML & CFTD **Mr. M. M. Haikal Hashmi** DMD, CRO & CAMLCO **Mr. Md. Monitur Rahman** DMD & Chief of Operations & IT	17/06/2018 To 16/04/2019	2.0
Developed By	**Mr. Maruf Ashraf** Enterprise Transformation **Mr. Md. Shamim Imtiaz** Enterprise Transformation **Ms. Halima Jahan** AML & CFTD **Mr. William Chowdhury** AML & CFTD	17/06/2018 To 24/06/2018	2.0
Reviewed By	**Md. Mehedi Hasan** Enterprise Transformation **Mr. Md. Akbar Ali** AML & CFTD **Ms. Sharmilla Manzoor** Head of Enterprise Transformation **Mr. Md. Monitur Rahman** DMD & Chief of Operations & IT **Mr. M. M. Haikal Hashmi** DMD, CRO & CAMLCO	24/06/2018 To 16/04/2019	2.0
Finalized By	**Ms. Sharmilla Manzoor** Head of Enterprise Transformation **Md. Akbar Ali** Head of AML & CFTD **M. M. Haikal Hashmi** DMD, CRO & CAMLCO **Mr. Md. Monitur Rahman** DMD & Chief of Operations & IT	17/06/2018 To 16/04/2019	2.0

1. Method of revision/development was in combination of meeting, person to person and group discussions and through email.
2. After the end of reviewing final draft, no further observation/feedback was received from any stakeholder. Hence, this version is considered as 'final version' of **"ML&TF Risk Management Guidelines-2016 (Amendment-2019)".**

Approval Signatory Sheet	
Name & Designation	**Signature with Date**
Ms. Sharmilla Manzoor **Head of Enterprise Transformation**	
Mr. Md. Akbar Ali **Head of AML & CFTD & Deputy CAMLCO**	
Mr. Md. Monitur Rahman **DMD & Chief of Operations & IT**	
Mr. Syed Mansur Mustafa **DMD & Chief Credit Officer**	
Mr. Md. Nurul Hasnat **DMD & Head of Business**	
Mr. Shah Md. Moinuddin **DMD & Head of International Division**	
Mr. M. M. Haikal Hashmi **DMD, CRO & CAMLCO**	
Mr. M. Shah A. Sarwar **Managing Director & CEO**	

Foreword

Money Laundering (ML) and Terrorist Financing (TF) can potentially damage and pose serious threats to the integrity and stability of a financial system. To protect the Banking industry from these threats, IFIC Bank has been working in partnership with financial institutions and BFIU, government departments and other key stakeholders to put in place an effective regime to fight against these crimes.

In response to the growing concern about money laundering and terrorist activities, the international community has acted on many fronts Central Bank in an agreement over the issue with the rest of the world, have been prompt to identify it as one of the Core Risks in our Banking Sector. Consequently, in alignment with the international initiatives and standards, Bangladesh has also enacted Money Laundering Prevention Act, 2012 (Amendment 2015) and Anti-Terrorism Act, 2009 (Amendment 2012 & 2013). The new acts address all the deficiencies identified in the 2nd Mutual Evaluation of Bangladesh conducted by APG in 2008 to determine the extent of its compliance, with the global standards. Both the Acts have empowered Bangladesh Bank (BB) to perform the anchor role in combating ML&TF through issuing guidance and directives for reporting agencies including IFIC Bank (FIs), as defined in section 2(g) of Money Laundering Prevention Act, 2012 (Amendment 2015).

IFIC Bank Limited being an active member of the main stream banking industry of the country, obviously remains obliged to comply with the directives of the BFIU, Bangladesh Bank-Central Bank of the Country towards a cause which has not been identified in isolation but collectively by various international agencies including UN General Assembly. In this regard, over the past few years the Basle Committee on Banking Supervision issued numerous statements of principles and developed a set of Core Principles for Effective Banking Supervision as important guidelines to eliminate the risks related to Money Laundering in Banking Sector. Therefore, In line with the national legislations, BFIU instructions and international standards, IFIC developed its own AML & CFT Policy Guideline and reviewed the same from time to time. With the issuance of new guidelines, circulars and instructions by BFIU, Money Laundering Prevention Act, 2012 (Amendment 2015), Anti-Terrorism Act, 2009 (Amendment 2012 & 2013) and increasing national and international initiatives to minimize money laundering and terrorist financing risk, it has been necessary to revise the Policy Guideline, which, after revision, shall be renamed as IFIC Money Laundering & Terrorist Financing Risk Management Guideline-2016 (Amendment-2018).

The prevention of money laundering and terrorist financing requires collective effort from all relevant government and private organizations. An effective AML/CFT regime can only be implemented if all the major participants of the financial system comply with the country's AML/CFT laws, rules and regulations.

"Money Laundering &Terrorist Financing Risk Management Guidelines-2016(Amendment), 2018" to be used in IFIC Bank Limited is prepared and draft copy placed for kind approval of Board of Directors of the bank.

Contents

Chapter 1: Introduction

1.1 Introduction

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 international initiatives, Bangladesh has also acted on many fronts.

1.1.1 Broad Objective

To ensure that a system is established within which money laundering and terrorist financing control is managed through stringent and appropriate procedures in order to discharge our legal and moral duties.

1.1.2 Specific Objective

Apart from these broad objectives, the specific objectives are:

a) To make staff aware of legal obligations and national policy guideline in terms of AML & CFT;
b) To focus on methods of prevention of money laundering and combating the financing of terrorism;
c) To prevent the bank's products or services from being used as a channel for money laundering and financing of terrorism;
d) To prevent damage to the bank's name and reputation by associating with money launderers or terrorists financiers or proliferation financier of weapons of mass destruction;
e) To ensure that the bank complies with money laundering prevention and anti-terrorism legislation/regulations;
f) To assist regulators/law enforcement agencies in their efforts to investigate and track money launderers & terrorist financiers.

1.1.3 ML & TF RISK ASSESSMENT GUIDELINE

IFIC has developed an ML & TF Risk Assessment Procedure of its own considering the size, range of activities, complexity of operations, customer base, use of technology, diversity of products, delivery channel, external linkage and geographic locations of IFIC. IFIC Central Compliance Unit (CCU) has developed an ML & TF Risk Assessment Guideline, which is attached with this Policy Guideline **(Appendix-I).**

1.4.4 SCOPE & ENFORCEMENT

a) All employees of the bank shall have to comply with the Policy Guideline and all relevant employees must be thoroughly familiar with and make use of the material contained in the Guideline;

b) The Policy Guideline shall be applicable for all the subsidiaries and branches of IFIC located at home and abroad;

c) Copy of this Policy Guideline shall be distributed to all employees of the bank including to those of the subsidiary companies of the bank so that it can be readily available to all relevant employees;

d) Senior Management shall be responsible for ensuring the directives implemented and administered in compliance with the approved Policy Guideline.

e) Changes to this policy guideline shall require approval of the Board of Directors.

1.2 What is Money Laundering

The fundamental concept of money laundering is the process by which proceeds from a criminal activity is disguised to conceal their illicit origins.

As per stipulations contained in Section 2 (V) of the Money Laundering Prevention Act, 2012 (Act No.05 of 2012) in Bangladesh "Money Laundering" means:

(i) Knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:
   a. Concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
   b. Assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;

(ii) Smuggling money or property earned through legal or illegal means to a foreign country;

(iii) Knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or

(iv) Concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;

(v) Converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;

(vi) Acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;

(vii) Performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;

(viii) Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

1.2.1 Why Money Laundering is Done

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

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

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

1.2.2 Stages of Money Laundering

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

(i) **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.

(ii) **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.

(iii) **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.

1.2.3 Reporting Organization

(i) Bank;

(ii) Financial institution;

(iii) Insurer;

(iv) Money changer;

(v) Any company or institution which remits or transfers money or money value;

(vi) Any other institution carrying out its business with the approval of Bangladesh Bank;

(vii) (1) stock dealer and stock broker,

(2) Portfolio manager and merchant banker,

(3) Securities custodian,

(4) Asset manager;

(viii) (1) Non-profit organization,

(2) Non-government organization,

(3) Cooperative society;

(ix) Real estate developer;

(x) Dealer in precious metals or stones;

(xi) Trust and company service provider;

(xii) Lawyer, notary, other legal professional and accountant;

(xiii) Any other institution which Bangladesh Bank may, from time to time, notify with the approval of the Government;

1.2.5 Predicate Offence

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

1. Corruption and bribery;
2. Counterfeiting currency;
3. Counterfeiting deeds and documents;
4. Extortion;
5. Fraud;
6. Forgery;
7. Illegal trade of firearms;
8. Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;
9. Illegal trade in stolen and other goods;
10. Kidnapping, illegal restrain and hostage taking;
11. Murder, grievous physical injury;
12. Trafficking of women and children;
13. Black marketing;
14. Smuggling of domestic and foreign currency;
15. Theft or robbery or dacoity or piracy or hijacking of aircraft;
16. Human trafficking;
17. Dowry;
18. Smuggling and offences related to customs and excise duties;
19. Tax related offences;
20. Infringement of intellectual property rights;
21. Terrorism or financing in terrorist activities;
22. Adulteration or the manufacture of goods through infringement of title;
23. Offences relating to the environment;
24. Sexual exploitation;
25. Insider trading and market manipulation using price sensitive information relating to the capital market in share transactions before it is published for general information to take advantage of the market and attempting to manipulate the market for personal or institutional gain;
26. Organized crime, and participation in organized criminal groups;
27. Racketeering; and
28. Any other offence declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official Gazette, for the purpose of this Act.

1.2.6 Penalties of Money Laundering:

Money laundering is a criminal offence under section 4(1) of MLPA, 2012 (including amendments) and penalties for money laundering offence and non-compliance of the provisions of the law are as follows-

Offence	Reference	Penalties

Committing money laundering, a criminal offence	Sub sections 1, 2, 3, 4 & 5 of Section 4, MLPA, 2012 including amendments)	For person: Imprisonment for a term of at least 4 years but not exceeding 12 years and in addition fine equivalent to the twice of the value of the property involved in the offence or BDT 10 lac, whichever is greater. For entity: A fine of not less than twice of the value of the property or BDT 20 lac, whichever is greater and in addition to this the registration of the said entity shall be liable to be cancelled.
Non-compliance	**Reference**	**Penalties**
Failure to provide with required information on time	Sec 23(3) of MLPA, 2012 (including amendments)	Maximum BDT 5 lac fine at the rate of BDT 10 Thousand per day. Even cancellation of license if fined more than 3 occasions in a year.
Providing wrong & false information by the institution	Sec 23(4) of MLPA, 2012 (including amendments)	Maximum BDT 5 lac fine with a minimum of BDT 20 thousand. Even cancellation of license if fined more than 3 occasions
Failure of reporting institutions to comply with the direction of BFIU.	Sec. 23(5) of MLPA, 2012 (including amendments 2015)	Maximum BDT 5 lac fine at the rate of BDT 10 thousand per day. Even cancellation of license if fined more than 3 occasions in a year.
Failure to comply with the freezing order	Sec. 23(6) of MLPA, 2012 (including amendments)	Not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.
Individual responsible in the entity for non-compliance	Sec 23(8) of MLPA, 2012 (including amendments)	If any reporting organization is imposed fine under sub-sections (3), (4) (5) & (6) BFIU may also impose a fine not less than BDT 10 thousand but not exceeding BDT 5 lac on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.
Failure to comply with the provision of sub-section (1) of section 25 a. Not to maintain complete and correct information of customer (KYC). b. Not to preserve records of transaction at least 5 years after termination of relationship. c. Not to provide with the above Information to BFIU as per their requirement. d. Not to submit suspicious transaction	Sub section (1 & 2) of section 25, MLPA, 2012 (including amendments)	(a) Fine at least BDT 50 thousand but not exceeding BDT 25 lac on the reporting organization. (b) In addition to the above, cancel the license of the organization and branches, service centers, booths or agents or as the case may be.

report spontaneously to BFIU for unusual/ doubtful transaction.		

1.3 What is Terrorist Financing

As per Ant-Terrorism Act, 2009 –

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

(a) to carry out terrorist activity;

(b) by a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.

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

Punishment for the offence of Terrorist Financing under ATA, 2009

If any person is convicted of any of the offences mentioned in sub-section (1) of section 7, the person shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or taka 10(ten) lac, whichever is greater, may be imposed.

☐☐If any entity is convicted of any of the offences mentioned in the sub-section (1) of section 7 –

(a) steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lacs, whichever is greater, may be imposed; and

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

Other offences as per ATA, 2009 Supporting any proscribed entity, criminal conspiracy of committing an offence, attempt of committing an offence, aid and abetment of an offence, participating as an accomplice, organizing or directing others; or contributing, instigating terrorist activities, harbouring an offender are also punishable offence under this Act.

Duties of BFIU and ROs Adequate powers have been assigned to BFIU through section 15 of the Anti-Terrorism Act 2009 to take all necessary actions that the Unit deems fit to combat TF. Duties of the Reporting agency have been delineated in section 16 of the Act.

What is terrorist activity?

As per Anti-Terrorism Act, 2009 Offences are described as under. Terrorist activities. - (1) If any person, entity or foreigner

(a) for the purposes of threatening the unity, integration, public security or sovereignty of Bangladesh by creating panic among the public or a section of the public with a view to compelling the Government or any entity or any person to do any act or preventing them from doing any act,–

(i) Kills, causes grievous hurt to, confines or kidnaps any person or attempts to do the same;

(ii) Conspires, abets or instigates any person to kill, injure seriously, confine or kidnap any person; or

(iii) Damages or tries to damage the property of any other person, entity or the Republic; or

(iv) Conspires or abets or instigates to damage the property of any other person, entity or the Republic; or

(v) Uses or keeps in possession any explosive substance, inflammable substance and arms for the purposes of sub-clauses (i), (ii), (iii) or (iv);

(b) With an intent to disrupt security of or to cause damage to the property of any foreign State, commits or attempts to commit or instigates or conspires or abets to commit an offence similar to the offences mentioned in sub-clauses (i), (ii), (iii), (iv) or (v) of clause (a);

(c) With a view to compelling any international organization to do any act or preventing it from doing any act, commits or attempts to commit or instigates or conspires or abets to commit an offence similar to the offences mentioned in sub-clauses (i), (ii), (iii), (iv) or (v) of clause (a);

(d) KNOWINGLY uses or possesses any terrorist property;

(e) Abets, instigates, conspires to do or commits or attempts to commit an offence described in the United Nations conventions included in the Schedule 1 of this Act;

(f) Commits any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act; the person, entity or foreigner shall be deemed to have committed the offence of "terrorist activities";

Punishment for the offence of Terrorist Activity as mentioned in Anti-Terrorism Act 2009:

If any person or foreigner, (a) commits an offence under sub-clause (i) of clause (a) of sub-section (1) of section 6, the person shall be punished with death or imprisonment for life and in addition to that a fine may also be imposed; (b) commits an offence under sub-clause (ii) of clause (a) of sub-section (1) of section 6, the person shall, if the offence is punishable with death, be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14 (fourteen) years but not less than 4(four) years, and with fine; (c) commits an offence under sub-clause (iii) of clause (a) of sub-section (1) of section 6, the person shall be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14 (fourteen) years but not less than 4(four) years, and with fine; (d) commits an offence under sub-clause (iv) of clause (a) of sub-section (1) of section 6, the person shall be punished with rigorous imprisonment for a term not exceeding 14 (fourteen) years but not less than 4(four) years, and with fine; (e) commits an offence under sub-clause (v) of clause (a) of sub-section (1) of section 6, the person shall be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14 (fourteen) years but not less than 4(four) years, and with fine.

☐☐If any person or foreigner commits an offence under clause (b), (c), (d), (e) or (f) of sub-section (1) of section 6, the person shall be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14 (fourteen) years but not less than 4(four) years, and with fine.

☐☐If any entity commits the offence of terrorist activities, then

(a) steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is greater, may be imposed; and

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

UNSCR Implementation Mechanism:

Measures to implement United Nations Security Council Resolutions as mentioned in section 20(A) of Anti-Terrorism Act, 2009 For the purposes of implementing United Nations Security Council Resolution No. 1267 and its successor resolutions and United Nations Security Council Resolution No. 1373 and United Nations Security Council resolutions related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing, the Government of Bangladesh shall, in addition to the power mentioned in other sections of this Act or in any other law for the time being in force, have power of taking measures-

(a) To freeze, seize or attach, without delay and without issuing any prior notice, the property, funds or other financial assets or economic resources held by, including funds derived or generated from property owned or controlled directly or indirectly by the listed person or entity or by any undertaking owned or controlled by the listed person or entity, or on behalf of a natural person or an entity, if the name of the person or entity is included in the lists, maintained by the committee established under Resolution NO. 1267 of the United Nations Security Council;

(b) To freeze, seize or attach, without delay and without issuing any prior notice, the funds or other financial assets or economic resources of the person who commits, or attempts to commit terrorist acts or participates in or facilitates the commission of terrorist acts; or of entities owned or controlled directly or indirectly by such person; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such person and associated persons and entities listed by the United Nations Security Council or proscribed or listed under Resolution No. 1373 of the United Nations Security Council;

(c) To prohibit any willful provision or collection, directly or indirectly, of funds by any person or entity, whether in or outside Bangladesh, with the intention to use such funds or having the knowledge that they shall be used to carry out any terrorist act;

(d) To prohibit any person or entity from making any funds, financial assets or economic resources of financial or other related services available, directly or indirectly, for the benefit of the persons or entities listed by the United Nations Security Council or proscribed or listed under Resolution No. 1373 or of entities owned or

controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons;

(e) To prevent the entry into or the transit through Bangladesh of the persons listed by the United Nations Security Council through effective border control and immigration measures;

(f) To prevent any direct or indirect supply, sale and transfer, in or outside Bangladesh, of arms and ammunition and other related items, materials, equipment, goods and technologies to the persons or entities listed by the United Nations Security Council;

(g) To deny permission for any aircraft to take off or land in their territory if it is owned, leased or operated by or on behalf of the persons or entities listed by the United Nations Security Council;

(h) To prevent illicit trafficking in nuclear, chemical or biological weapons, their means of delivery and related materials, including through inspection of cargo to and from the persons or entities listed by the United Nations Security Council;

(i) To prohibit and prevent any activity mentioned in the said Resolutions and related with the persons and entities listed by the United Nations Security Council;

(j) To issue directions, from time to time, to the reporting agencies by Bangladesh Financial Intelligence Unit for proper implementation of this section; (k) to determine, by issuing order or notification, the appropriate authority to take required actions as per the power stated in clauses (a) to (i).

Punishment for the offence of violating United Nations Security Council Resolutions as mentioned in Anti-Terrorism Act 2009-

a) If any person or entity violates a freezing or attachment order issued under this section, the person or the concerned person of the entity shall be punished with imprisonment for a term not exceeding 04(four) years or with a fine equivalent to twice the value of the property subject to freeze or attachment, or with both.

b) If any person or entity does any act or fails to do an act in contravention of clauses (c) and (d) of sub-section (1) of 20(A), the said person or entity shall be deemed to have committed an offence of financing of terrorist activities and shall be punished according to the provisions of sub-section (3), (4)(a) or, as the case may be, (4)(b) of section 7.

c) If any person or entity does any act or fails to do an act in contravention of clauses (e) to (h) of sub-section (i), the person or entity shall be deemed to have committed an offence of terrorist activity and shall be punished according to the provisions of sub-section (2), (3)(a) or, as the case may be, (3)(b) of section 6.

d) If any reporting agency fails to comply with the directions issued by Bangladesh Financial Intelligence Unit under this section, or fails to take immediate freezing action required under this section, the said reporting agency shall be liable to pay a fine, determined and directed by Bangladesh Financial Intelligence Unit, not exceeding taka 25 (twenty five) lac but not less than 05 (five) lac or twice the value of the suspected fund, whichever is greater, and Bangladesh Bank may also suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

(e) If any charge of negligence in implementing the provisions of this section is proved against any public servant, administrative actions shall follow in accordance with his respective service rules. Besides Money Laundering Prevention Rules 2013, Circular and Circular Letter issued by BFIU; Statutory Regulatory Order

(SRO) issued by Ministry of Foreign Affairs (MoFA) under The United Nations (Security Council) Act, 1948; Comprehensive Implementation Procedures outlined in Anti Terrorism Rules, 2013; Agency Specific Implementation Guidelines contains detailed guidance on combating TF and PF.

Part iii of MLPR, 2013 provides detailed instructions on Freezing of account or suspension of transaction by BFIU, Penalties imposed by the BFIU, Domestic proscription and enlistment, Requesting other country to take reasonable measures under the authority of UNSCR 1373, Review of proscription or enlistment order, Proposing a name to the 1267 Committee of the United Nations Security Council, Proposing a name to the 1988 Committee of the United Nations Security Council.

Part IV of the MLPR, 2013 provides adequate instructions on Implementation of the provisions of United Nations Security Council Resolutions

Part V of the MLPR, 2013 provides detailed instructions on Freeze, seize, attachment or confiscation of proceeds of terrorism.

Requirements of the Reporting Organizations

A) Sanctions against which ROs should create a compliance program:

☐ UNSCRs 1267 and its successor resolutions including UNSCR 2178;

☐ UNSCRs 1373 and its successors resolutions including UNSCRs 2178

☐ UNSCRs 1540

☐ UNSCRs 1718

☐ UNSCRs 1737 and its successor's resolutions including UNSCRs 2231.

B) Requirements for the Sanction regime

Sanctions regimes narrowly require a specific legal base and/or course of actions for the followings:

☐ Trade embargos;

☐ Travel bans;

☐ Freezing of Assets; and

☐ Economic sanctions.

Trade embargos and freezing of assets are directly related with the reposting organizations. A reporting organization must ensure that they are not maintaining or continuing business relationship with sanctioned/designated person and not engaged in the trade activities with sanctioned individual, entity or territories. Beneficial ownership issues should be consider very carefully and critically while complying with the sanction regime, as money launderer of sanctioned individual or entities always try to hide them from front person or legal entity.

C) Following mechanisms should be established by reporting organizations to comply with the Sanction regime:

☐ Put in place a comprehensive policy approved by the Board of Directors;

☐ Ensure all relevant sanctions lists (updated) are used electronically to detect the existence of the sanctioned individuals, entities, or territories;

☐ Ensure that existing arrangements of customer screening are able to detect the relevant lists of named terrorist and sanctioned entities.

☐ Ensure that existing arrangements of customer screening are able to detect the relevant lists of trade embargos;

☐ Conduct real-time transaction screening on all cross-border payments, SWIFT and other modes of payments in relation to relevant lists of named terrorist and sanctioned entities, or embargos;

☐ Freeze the accounts and the relevant transaction in relation to relevant lists of named terrorist and sanctioned entities, or embargos immediately;

☐ Report to the detected incidents to the BFIU without delay;

☐ Keep records or audit trail for all sorts of monitoring mechanism including the false positives;

☐ Take necessary training and awareness building arrangements; and

☐ Review the existing policies with any additional requirements of sanction regime.

D) As per MLPR ROs should do the followings:

☐☐Maintain and update the listed individuals and entities in electronic form;

☐☐Regularly run a check at the website of United Nations for updated list;

☐☐Run regular check on the given parameters, including transactional review, to verify;

☐☐In case of a match found the ROs shall immediately stop payment or transaction of funds, financial assets or economic resources;

☐☐Report to the BFIU within the next working day with full particulars.

1.4 Link between Money Laundering and Terrorist Financing

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

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

1.5 Why we must combat Money Laundering and Terrorist Financing

Money laundering & Terrorist Financing has potentially devastating economic, security, and social consequences. Money laundering is a vital process to make crime worthwhile. It provides the fuel for drug

dealers, smugglers, terrorists, illegal arms dealers, corrupted public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences resulted from ML & TF.

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

Money laundering distorts assets and commodity prices and leads to misallocation of resources. For financial institutions it can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability and even systemic crisis. The loss of credibility and investor's confidence, that such crisis can bring, has the potential of destabilizing financial systems, particularly in smaller economies.

One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers often use front companies, which co-mingle the proceeds of illicit activity with legitimate funds, to hide the ill-gotten gains. These front companies have access to substantial illicit funds, allowing them to subsidize front company products and services at levels well below market rates. This makes it difficult, if not impossible, for legitimate business to compete against front companies with subsidized funding, a situation that can result in the crowding out of private sector business by criminal organizations.

Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government, and citizens to criminals. Furthermore, the sheer magnitude of the economic power that accrues to criminals from money laundering has a corrupting effect on all elements of society.

The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. Bribing of government officials undermines the moral fabric in society, and, by weakening collective ethical standards, corrupts our democratic institutions. When money laundering goes unchecked, it encourages the underlying criminal activity from which such money is generated.

A nation cannot afford to have its reputation and financial institutions tarnished by involvement with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions (FIs) and the underlying criminal activities like fraud, counterfeiting, narcotics trafficking, and corruption weaken the reputation and standing of any financial institution. Actions taken by FIs to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. A financial institution tainted by money laundering accusations from regulators, law enforcement agencies, may lose their good market reputation and damage the reputation of the country. It is very difficult and requires significant resources to rectify a problem that could be prevented with proper program.

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

have to face legal risk. Finally, the reputation of an FI can also be heavily affected through its involvement with ML & TF activities.

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

1.6 Targeted Financial Sanctions

The term Targeted Financial Sanctions (TFS) means both asset freezing and prohibition to prevent funds on other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. This TFS is a smart solution to combat terrorism, terrorist financing and proliferation financing of weapons of mass destruction (WMD) by state actors or non-state actors from the UN Security Council. In contrast with the economic sanction on a jurisdiction, TFS is imposed on only suspected person or entities while innocent person or entities remain safe.

1.6.1 TFS related to terrorism and terrorist financing-

FATF recommendation 6 requires 'Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)'.

1.6.2 TFS related to Proliferation-

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

1.7 PROPERTY MEANS:

i. any type of tangible, intangible, movable immovable property or

ii. cash, any deed or legal instruments of any form including electronic or digital form giving evidence of title or evidence of interest related to title in the property which is located within or outside the country.

1.8 Bank Perspective

From the viewpoint of banking activities, prevention of money laundering and terrorist financing has three dimensions:

- Ethical- taking part in the prevention of money laundering and terrorist financing;
- Professional- ensuring that the bank is not involved in recycling the proceeds of crime that would call into question its reputation and integrity;

- Legal-complying with laws and regulations that impose a series of specific obligations to banks and their employees.

A bank cannot afford to have its reputation tarnished by involvement with money laundering and terrorist financing. Money Laundering and Terrorist Financing erodes confidence on banks, instigates liquidity crisis and the underlying criminal activities weaken the reputation and standing of the bank. Therefore, bank shall prevent money laundering and terrorist financing not only because it is obligated under legislation but also to protect self-interest.

Chapter 2: International Initiatives on ML and TF

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

2.1 The United Nations (UN)

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

- It is the international organization with the broadest range of membership. The UN, founded in 1945, has 193 members from all across the world.
- The UN actively operates a program to fight money laundering; the Global Program against Money Laundering, headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).
- The UN has the ability to adopt international treaties or conventions that obligate the ratifying countries to reflect those treaties or conventions in their local laws.

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

The Vienna Convention

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

The Palermo Convention

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

- Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;
- Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
- Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyze and disseminate information; and
- Promote international cooperation. This convention has come into force from 29th September 2003, having been signed by 147 countries and ratified by 82 countries.

International Convention for the Suppression of the Financing of Terrorism

The financing of terrorism was an international concern prior to the attacks on the United States on 11 September, 2001. In response to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002 with 132 countries signing the convention and as of February 2018, the treaty has been ratified by 187 states; in terms of universality, it is therefore one of the most successful anti-terrorism treaties in history.

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

Security Council Resolution 1267 and Successors

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

The Committee was initially established pursuant to resolution 1267 (1999), which imposed a limited air embargo and assets freeze on the Taliban. Over time, the regime evolved and the measures became a targeted assets freeze, travel ban and arms embargo against designated individuals and entities. Exemptions to the assets freeze and travel ban were also introduced and the fairness and clarity of the procedures for listing and de-listing was improved, in particular through the establishment of the Office of the Ombudsperson.

On 17 June 2011, the Security Council unanimously adopted resolutions 1988 (2011) and 1989 (2011). With the adoption of these resolutions, the Security Council decided that the list of individuals and entities subject to the measures would be split in two. The Committee was henceforth known as the Al-Qaida Sanctions Committee, mandated to oversee implementation of the measures against individuals and entities associated with Al-Qaida. A separate Committee was established pursuant to resolution 1988 (2011) to oversee implementation of the measures against individuals and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan.

On 17 December 2015, the Security Council unanimously adopted resolution 2253 (2015). With the adoption of this resolution, the Security Council decided to expand the listing criteria to include individuals and entities supporting the Islamic State in Iraq and the Levant (ISIL). The resolution also directs the Monitoring Team to submit reports on the global threat posed by the Islamic State in Iraq and the Levant (ISIL, also known as Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities. Member States are encouraged to (a) designate national focal points on issues related to the implementation of the measures described in the resolution, and (b) report to the Committee on obstacles to the implementation of the

measures described in the resolution; also, calls upon all States to submit an updated report to the Committee no later than 120 days from the adoption of the resolution. The mandates of the Monitoring Team and the Office of the Ombudsperson are extended to December 2019.

On 20 July 2017, Security Council unanimously adopted resolution 2368 (2017). With the adoption of the resolution, the Security Council reaffirmed the assets freeze, travel ban and arms embargo affecting all individuals and entities on the ISIL (Da'esh) & Al-Qaida Sanctions List. The resolution also extended the mandates of the Monitoring Team and the Office of the Ombudsperson to December 2021 and added eight names to the ISIL (Da'esh) and Al-Qaida Sanctions List.

Security Council Resolution 1373

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

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

The UN Office for Disarmament Affairs provides support for activities of the Committee established pursuant to resolution 1540 (2004), which is tasked to report to the Security Council on the implementation of the resolution. Currently, UNODA activities are focusing on the following key areas:

- Facilitation of national implementation activities including through regionally coordinated approaches
- Cooperation between international, regional and sub-regional organizations
- Effective partnerships of key stakeholders including civil society, private sector and academia

Security Council Resolution 1540

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

The Counter-Terrorism Committee

As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take

specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism. Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution's measures and report regularly on progress. In this regard, the CTC asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism in relation to the requirements of Resolution 1373.

The Counter-Terrorism Committee (CTC) was established by Security Council resolution 1373 (2001), which was adopted unanimously on 28 September 2001 in the wake of the 11 September terrorist attacks in the United States.

The Committee, comprising all 15 Security Council members, was tasked with monitoring implementation of resolution 1373 (2001), which requested countries to implement a number of measures intended to enhance their legal and institutional ability to counter terrorist activities at home, in their regions and around the world, including taking steps to:

- Criminalize the financing of terrorism
- Freeze without delay any funds related to persons involved in acts of terrorism
- Deny all forms of financial support for terrorist groups
- Suppress the provision of safe haven, sustenance or support for terrorists
- Share information with other governments on any groups practicing or planning terrorist acts Cooperate with other governments in the investigation, detection, arrest, extradition and prosecution of those involved in such acts; and
- Criminalize active and passive assistance for terrorism in domestic law and bring violators to justice.

The resolution also calls on States to become parties, as soon as possible, to the relevant international counter-terrorism legal instruments.

In September 2005, the Security Council adopted resolution 1624 (2005) on incitement to commit acts of terrorism, calling on UN Member States to prohibit it by law, prevent such conduct and deny safe haven to anyone "with respect to whom there is credible and relevant information giving serious reasons for considering that they have been guilty of such conduct." The resolution also called on States to continue international efforts to enhance dialogue and broaden understanding among civilizations.

The Security Council directed the CTC to include resolution 1624 (2005) in its ongoing dialogue with countries on their efforts to counter terrorism.

Counter-Terrorism Implementation Task Force (CTITF)

The Counter-Terrorism Implementation Task Force (CTITF) was established by the Secretary-General in 2005 and endorsed by the General Assembly through the United Nations Global Counter-Terrorism Strategy, which was adopted by consensus in 2006. The mandate of the CTITF is to enhance coordination and coherence of counter-terrorism efforts of the United Nations system. The Task Force consists of 38 international entities which by virtue of their work have, have a stake in multilateral counter-terrorism efforts. Each entity makes contributions consistent with its own mandate. While the primary responsibility for the implementation of the Global Strategy rests with Member States, CTITF ensures that the UN system is attuned to the needs of

Member States, to provide them with the necessary policy support and spread in-depth knowledge of the Strategy, and wherever necessary, expedite delivery of technical assistance.

Global Program against Money Laundering

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

2.2 The Financial Action Task Force

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. There are currently 38 members of the FATF; 36 jurisdictions and 2 regional organizations (the Gulf Cooperation Council and the European Commission). These 37 Members are at the core of global efforts to combat money laundering and terrorist financing

FATF 40 Recommendations

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

The 40+9 Recommendations, together with their interpretative notes, provide the international standards for combating money laundering (ML) and terrorist financing (TF). The FATF revised the 40 and IX Recommendations. The revision of the FATF Recommendations was adopted and published in February 2012.

FATF New Standards

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

Summary of New FATF 40 Standards

Group	Topic	Recommendations
1.	Policies and Coordination	1-2

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

Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of 40+9 recommendations is facilitated by a two-stage process: self-assessments and mutual evaluations. In the self-assessment stage, each member country responds to a standard questionnaire, on an annual basis, regarding its implementation of 40+9 recommendations. In the mutual evaluation stage, each member country is examined and assessed by experts from other member countries in every five years. The first Mutual Evaluation (ME) of Bangladesh was conducted by a joint team of World Bank and International Monetary Fund in October, 2002 and the report thereof was adopted by the APG in September, 2003. The 2nd & 3rd Mutual Evaluation (ME) of Bangladesh was conducted by an APG team in August, 2008 & October, 2015 and 4th round of ME is going on.

The NCCT List

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

A total of 47 countries or territories were examined in two rounds of reviews (in 2000 and 2001). A total of 23 were listed as NCCTs—15 in 2000 and 8 in 2001. The FATF has not reviewed any new jurisdictions since 2001 in the framework of the NCCT initiative. As of October 2006, there are no Non-Cooperative Countries and Territories in the context of the NCCT initiative.

International Cooperation and Review Group (ICRG)

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

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

FATF Public Statement

Now FATF Identifies jurisdictions that have strategic deficiencies, publishes the list and works with them to address with those deficiencies that pose a risk to the international financial system.

2.3 Asia Pacific Group on Money Laundering (APG)

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

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

The APG has five key roles:

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

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

2.4 The EGMONT Group of Financial Intelligence Units

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

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

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

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

The Egmont Group is a united body of 155 Financial Intelligence Units (FIUs). The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF). This is especially relevant as FIUs are uniquely positioned to cooperate and support national and international efforts to counter terrorist financing and are the trusted gateway for sharing financial information domestically and internationally in accordance with global Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) standards.

The Egmont Group continues to support the efforts of its international partners and other stakeholders to give effect to the resolutions and statements by the United Nations Security Council, the G20 Finance Ministers, and the Financial Action Task Force (FATF). The Egmont Group is able to add value to the work of member FIUs by improving the understanding of ML/TF risks amongst its stakeholders. The organization is able to draw upon operational experience to inform policy considerations; including AML/CFT implementation and AML/CFT reforms. The Egmont Group is the operational arm of the international AML/CFT apparatus.

The Egmont Group recognizes sharing of financial intelligence is of paramount importance and has become the cornerstone of the international efforts to counter ML/TF. Financial Intelligence Units (FIUs) around the world are obliged by international AML/CFT standards to exchange information and engage in international cooperation. As an international financial intelligence forum, the Egmont Group both facilitates and prompts this amongst its member FIUs.

2.5 The BASEL Committee on Banking Supervision

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

Statement of Principles on Money Laundering

In 1988 the Basel Committee issued its Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention). The Statement on Prevention outlines basic

policies and procedures that managements of banks/FIs should undertake to assist in suppressing money laundering. There are essentially four principles contained in the Statement on Prevention:

- proper customer identification
- high ethical standards and compliance with laws
- cooperation with law enforcement authorities and
- policies and procedures to adhere to the statement

Basel Core Principles for Banking

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

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

2.6 Customer Due Diligence

In October, 2001, the Basel Committee issued an extensive paper on KYC principles, entitled Customer Due Diligence for banks/FIs (Customer Due Diligence). This paper was issued in response to noted deficiencies in KYC procedures on a world-wide basis. These KYC standards provide more specific information on the statement on prevention and core principle 15.

Chapter 3: National Initiatives on ML and TF

Major National AML & CFT Initiatives

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

3.1 Founding Member OF APG

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

3.2 Legal Framework

Bangladesh is the first country in the South Asia that has enacted Money Laundering Prevention Act (MLPA) in 2002. To address the shortcomings of the MLPA, 2002 and to meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER), Bangladesh has again enacted Money Laundering Prevention Act in February, 2012 repealing MLPA, 2009. Money Laundering Prevention Rules, 2013 was circulated to promote specific operational procedure to implement the Act. The MLPA was last amended in 2015

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 circulated Mutual Legal Assistance in Criminal Matters Rules, 2013 which mainly emphasize on the process of widest possible range of providing mutual legal assistance in relation to ML & TF and other associated offences.

3.3 Central and Regional Task Forces

The Government of Bangladesh has formed a central and 7 regional taskforces (Chattagram, Rajshahi, Bagura, Sylhet, Rangpur, Khulna and Barishal) on 27 January, 2002 to prevent illegal hundi activities, illicit flow of fund & money laundering in Bangladesh. The Deputy Governor of BB and head of BFIU is the convener of that committee. Both the task force's meeting is held bi-monthly. The meeting minutes of the regional task force are discussed in the central task force meeting. Besides high-profile cases are discussed in the central task force meeting. The central task force set out important decisions that are implemented through banks, financial institutions and Government agencies concerned.

3.4 Anti-Money Laundering Department

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

3.5 Bangladesh Financial Intelligence Unit (BFIU)

As per the provision of Money Laundering Prevention Act, 2012 (Amendment 2015) Bangladesh Financial Intelligence Unit (BFIU) has been established abolishing AMLD as a national central agency to receive, analyze and disseminate STRs/SARs, CTRs and complaints. BFIU has been entrusted with the responsibility of exchanging information related to ML & TF with its foreign counterparts. The main objective of BFIU is to establish an effective system for prevention of money laundering, combating financing of terrorism and proliferation of weapons of mass destruction and it has been bestowed with operational independence. BFIU has also achieved the membership of Egmont Group in July, 2013.

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

3.6 National Coordination Committee (NCC) and Working Committee

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

3.7 National ML & TF Risk Assessment (NRA)

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

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

3.8 National Strategy for Preventing ML and TF

National Strategy for Preventing Money Laundering and Combating Financing of Terrorism, 2011-2013 was adopted by the NCC in April 2011. Bangladesh has completed all the action items under the 12(twelve) strategies during that time. A high-level committee headed by the Head of BFIU and Deputy Governor of

Bangladesh Bank has formulated the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2015-2017 which has been approved by the National Coordination Committee (NCC) on ML/TF. The strategy identifies the particular action plan for all the Ministries, Division and Agency to develop an effective AML/CFT system in Bangladesh. The strategy consists of following 11 (eleven) strategies against 11 (eleven) strategic objectives:

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

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

Separate annual conferences for the Chief Anti-Money Laundering Compliance Officers (CAMLCO) of Banks, Financial Institutions, Insurance Companies and Capital Market Intermediaries has been arranged by BFIU. Fruitful discussions among the participants regarding performance of the previous year, trends and typologies on ML & TF, strategic directions, etc. have taken place in CAMLCO conferences. It also arranges a number of training programs, workshops, seminars and road-shows to create awareness among the staff of reporting organizations, regulatory authorities about related issues.

3.10 EGMONT Group Memberships

BFIU has achieved the membership of Egmont group in the Egmont plenary on July, 2013 in Sun City, South Africa. Through Egmont membership, BFIU has achieved access to a wider global platform and this will help to establish relationship with other FIUs of different countries to get benefit by exchanging views, experiences and information via Egmont Secure Web.

3.11 Anti-Militants and De-Radicalization Committee

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

3.12 Memorandum of Understanding (MOU) between ACC and BFIU

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

3.13 NGO/NPO Sector Review

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

3.14 Implementation of TFS

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

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

3.15 Coordinated Effort on the Implementation of the UNSCR

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

3.16 Risk Based Approach

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

In this regard BFIU has issued a guideline titled 'Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector' in January, 2015 (Circular letter no. 01/2015) for providing the basic ideas of identifying, assessing and mitigating ML & TF risks that banks may encounter in doing businesses. Banks were instructed to assess their own ML & TF risk considering their customers, products, delivery channels and geographical positions. BFIU were also instructed to assess regulatory risk i.e. risk arises from non-compliance of AML & CFT measures.

To comply with the BFIU instruction Bank has submitted ML & TF risk assessment reports. The Bank's risk register has been prepared by comparing with own risk register with the 'Annexure-H'.

3.17 Memorandum of Understanding (MOU) BFIU and Other FIUs

To enhance the cooperation with foreign counterparts, BFIU signed Memorandum of Understanding (MoU) with other FIUs. BFIU has signed 51 (till 2016-2017) MoU so far to exchange the information related to ML & TF with FIU of other countries.

Chapter 4: AML & CFT Compliance Program of the Bank

National ML & TF risk assessment suggests that banking sector is one of the most vulnerable sectors for the ML & TF among the financial sectors due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership. Bank can play a vital role in preventing ML,TF & PF and, in this regard , its role & responsibilities are delineated in MLPA, 2012(including amendments) , ATA , 2009 (including amendment) and rules & instruction issued under the legal framework & BFIU. To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, rules and directives of BFIU, IFIC has revised its AML and CFT compliance program. IFIC Bank has developed and maintains an effective AML and CFT compliance program to prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU. The compliance program covers senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building of employee as well as customer because at present Banking sector is one of the most vulnerable sectors for the ML & TF issues due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership.

4.1 Component of AML & CFT compliance program

To ensure compliance, IFIC Bank shall document & communicate to all levels of Bank after getting approval by the Board of Directors. IFIC Bank shall pay attention on priority basis regarding the size and range of activities, complexity of operations, the nature and the degree of ML & TF risk faced by Bank for developing AML & CFT compliance program.

IFIC Bank AML & CFT program shall include following -

(i) Every year senior management i.e. MD/CEO shall provide a clear message as a commitment to prevent ML, TF & PF issues to all branch as well as all Departments/Divisions of Head office and instruct to ensure the same.

(ii) IFIC Bank internal policies, procedure and controls shall include AML & CFT policy, customer acceptance policy, Know Your Customer (KYC), customer due diligence (CDD), enhance due diligence (EDD), correspondent banking relationship management, transaction monitoring, self-assessment, independent testing procedure, wire transfer, sanction screening, employee screening, recruitment & training, record keeping and reporting to BFIU.

(iii) As per BFIU directives IFIC Bank shall maintain a compliance structure where focus on the establishment of Central Compliance Committee (CCC), appointment of Chief Anti-money Laundering Compliance Officer (CAMLCO) and Deputy CAMLCO at Head Office level as well as Branch Anti-money Laundering Compliance Officer (BAMLCO) at branch level.

(iv) There is an independent audit function at IFIC Bank that includes the role and responsibilities of internal audit on AML & CFT compliance and external audit function.

(v) For creating awareness of employee's IFIC Bank shall arrange training, workshop, seminar on regular basis regarding AML & CFT issues as well as for the member of the Board of Directors & owners. For customers' awareness IFIC Bank shall provide leaflet & posters to the branch in respect to AML/CFT issues.

4.2 Development of IFIC Bank's AML & CFT Compliance Program

IFIC Bank has develop AML & CFT compliance program considering BFIU guidelines. IFIC Bank has consider all relevant laws, regulations, guidelines relating to AML & CFT and also the best practices related to corporate governance. General banking, credit, foreign exchange, information technology, international division, alternative delivery channels, human resource division, internal audit & compliance and central compliance committee department/division are involved in the compliance program. The involvement has been documented or reflected in the compliance program. IFIC Bank shall pay proper attention to the size and range of activities of transaction, complexity of operations, customer base, and use of technology, diversity of product, delivery channel, external linkage, geographic location and the output of ML & TF risk assessment of IFIC Bank.

Central Compliance Committee (CCC) constituted of Human resource division, Credit division, retail & corporate banking division, foreign exchange division, card division & information technology division are involved in the compliance program. The Central Compliance Committee shall devise organizational strategy for AML & CFT and AML & CFT Annual Program and revise the same from time to time. The AML & CFT Division shall implement the annual program under the direct supervision of CCC and the CAMLCO.

4.3 Communication of Compliance program of IFIC Bank

IFIC Bank shall communicate the compliance program after getting approval from the board of directors to all of the employees, member of the board of the directors and other relevant stakeholders at home and abroad by issue circular/circular letters. IFIC Bank shall upload the compliance program in the website for customers or other stakeholders.

4.4 Senior Management Role of IFIC Bank

IFIC Bank senior management play important role for preventing ML, TF & PF. As per BFIU directives senior management means members of the board of directors, the member of highest management committee in absence of the board of directors and the Chief Executive Officer (CEO)/Managing Director (MD).

4.4.1 Obligations under Law Anti-Terrorism Act, 2009 (Amendment 2012 & 2013)

'The Board of Directors, or in the absence of the Board of Directors, the Chief Executive of each reporting organization shall approve and issue directions regarding the duties of its officers and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, which are applicable to the reporting agency, have been complied with or not.'

4.4.2 Obligations under BFIU Circular (Circular -19; Dated - September 17, 2017)

"All banks must have their own policy manual that must conform international standards, laws and regulations in force in Bangladesh and instructions of BFIU on preventing money laundering and terrorist financing, and this policy manual must be approved by their Board of Directors or by the highest management committee, where applicable. This policy manual shall be communicated to all concerned persons. Banks shall conduct review of the policy manual from time to time and shall amend/change where necessary."

"The chief executive of the bank shall announce effective and specific commitment, give the necessary instructions to fulfill the commitments in preventing ML & TF to all the employees of all branches, agent offices,

regional offices and the head office and shall ensure the implementation of the commitments. This statement of commitment shall be issued in every year."

As per Anti-Terrorism Act, 2009 (Amendment 2012 & 2013) & BFIU Circular No. 19, dated 17.09.2017 IFIC Bank senior management (CEO /BOD) shall give due importance for successful AML & CFT program as well as for the development and enforcement of the AML & CFT objectives which can deter criminals from using the bank for ML, TF & PF and ensuring the compliance with the obligations under the laws and regulations.

4.4.3 Role of Senior Management of IFIC Bank

Board of Directors (BoD)

- Will approve every AML & CFT compliance program and will ensure its effective implementation from all the employee.
- Will issue different directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009.
- Will analyze the report of self-assessment and independent testing properly and take necessary steps to prevent AML/TF issues.
- Will be aware about ML & TF risk of the bank and take necessary measures to mitigate those risk.
- CEO/MD will issue a clear message every year to all the employee of Bank to prevent ML, TF & PF.
- Will ensure compliance of AML & CFT program.
- Will allocate enough human resource and other logistics for effective implementation of AML & CFT compliance program.

As part of the AML & CFT policy CEO/MD in his clear message communicates to all the employees on an annual basis indicating the importance of ML, TF & PF and any activity i.e. profits, marketing and customer service which facilitates money laundering or the funding of terrorist or criminal activities considering reputation of the bank. The statement shows the strong commitment of bank and senior management to comply all laws and regulations designed to combat money laundering and terrorist financing.

4.4.4 Statement of Commitment of CEO/MD

Every year CEO/MD of Bank will issue a clear message to all the employees include the following-

- IFIC Bank's policy has been formulated to prevent ML, TF & PF by following rules & regulation in order to comply ML, TF & PF.
- IFIC Bank's AML & CFT compliance program emphasize on an effective implementation of the same.
- IFIC bank clearly indicates the balance between business and compliance, considering risk and mitigating measures to any financial transaction.
- Every year a clear message is circulated regarding the responsibilities of each employee during their normal course of assignment related to compliance and in case of excuse for non-compliance ignorance are not considered.
- In case of any ambiguity arises for clarification the matter is escalated to the top management.
- Positive actions may be taken in respect to non-compliance regarding AML/CFT issues as per IFIC Bank HR policy.

The senior management of IFIC Bank will be accountable to ensure bank's policy, process and procedures towards AML & CFT are appropriately designed and implemented and are effectively operated to minimize the risk of the bank in connection with ML & TF.

Senior management will ensure the adequacy of the human and other resources devoted to AML & CFT. Moreover, they ensure the autonomy of the designated officials related to AML & CFT. Senior management takes the report from the CCC-AML into consideration which assesses 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.

IFIC bank HR policy adopted following issues for non-compliance by the employees of the Bank:

- IFIC Bank Employee (discipline & appeal) Rules-2003 already covers the issue in a broader sense. As per the rule:

  (8) "Misconduct" means conduct prejudicial to good order or service discipline or conduct unbecoming of an officer or gentleman and includes-

  a) Insubordination or disobedience to any lawful or reasonable order of the superior.
  b) Gross negligence of duty.
  c) Flouting of the orders, circular or directives of the Bank without any lawful cause;

For ensuring the compliance of AML & CFT measures by the employees of the Bank, IFIC bank HR policy may adopt the following for proper implementation of AML & CFT measures as per BFIU, Bangladesh Bank directives:

- Gross negligence of duty including non-compliance of Anti-Money Laundering and Combating the Financing of Terrorism issue.
- Weight and marks may be allocated in the annual performance evaluation (APA Form) of employees on AML/CFT issues:

In case of building any business relationship with high-risk it is escalated to the senior management for approval since senior management is responsible for all level of money laundering and terrorist financing risk.

4.5 Institutional Policy and Procedures

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

4.5.1 Establish clear lines of internal accountability, responsibility and reporting. Primary responsibility for the prevention of money laundering & terrorist financing rests with the nature of business which must ensure that appropriate internal controls are in place and operating effectively and that bank Officials are adequately trained. The business is supported in meeting this responsibility by the Legal and Compliance function and by Bank Investigations.

4.5.2 Given its importance in reputational and regulatory terms, the effectiveness of the money laundering Prevention & combating financing of terrorism regime across all businesses should form part of the governance oversight responsibilities of all branch managers.

4.5.3 Document, implement and maintain, procedures and controls which interpret Bank Policy and Bank Standards for each business in the context of applicable laws and regulations and corporate ethical standards. Compliance with such procedures and controls and with Bank Policy and Bank Standards will be effectively monitored.

4.5.4 Establish an effective 'Know Your Customer' Policy for the Branch Manager which will contain a clear statement of management's overall expectation matching local regulations and establishing specific

line of responsibilities. Detailed guideline on Know Your Customer (KYC) procedures are given at chapter #12 of this guideline.

4.5.5 Co-operate with any lawful request for information made by government agencies during their investigations into money laundering and terrorist financing.

4.5.6 Support governments, law enforcement agencies and Bangladesh Bank in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal purposes.

4.5.7 Report money laundering & terrorist financing issues to Head Office Management on a regular basis. The Branch Manager responsible to combat Money Laundering & terrorist financing shall determine and communicate the content, format and frequency for management reporting.

4.6 Customer Acceptance Policy

A concrete Customer Acceptance Policy is very important so that inadequate understanding of a Customer's background and purpose for utilizing a bank account or any other banking products/services may not expose the bank to a number of risks. Therefore, IFIC Bank adopts a Risk-based Approach and Procedures for assessing and effectively managing the Risk of its services being used for ML & TF purposes.

The bank has a Customer Acceptance Policy 2013 (Amendment 2018) approved & updated from time to time by the Board of Directors which specifies the methodology of customer assessment, policy for customer acceptance/rejection, policy regarding the introducer, general principles and responsibilities regarding accounting opening, customer type wise account opening procedure, policy regarding special type of customer, strategy for address verification, policy regarding customers without standard identification document etc.

The primary objectives of the Customer Acceptance Policy are:

a) To manage any money laundering and terrorist financing risk that the services provided by the Bank may be exposed to;
b) To prevent the Bank from being used, intentionally or unintentionally, for ML/TF purposes; and
c) To identify customers who are likely to pose a higher than average risk.

Policies are appended as under:

a) To prevent illegal or criminal elements from using the Bank for Money Laundering activities.
b) To enable the Bank to know/understand the customers and their financial dealings better which, in turn, would help the Bank to manage risks prudently.
c) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws or laid down procedures.
d) To comply with applicable laws and regulatory guidelines.
e) To ensure that the concerned staffs are adequately trained in KYC, AML, CFT procedures.

The customer acceptance policy of Bank should not be used against the less privileged people or the people who have not proper identification document. It should encourage the ultimate goal of transparent, accountable and inclusive financial system in Bangladesh.

This policy is applicable to all domestic/foreign branches/offices/subsidiaries/affiliates/associates of the bank and is to be read in conjunction with related operational guidelines issued from time to time.

The basic principles of the Customer Acceptance Policy of IFIC Bank are:

1. The Bank will accept only those customers who have clear documents to establish identity and physical place of business or residence.
2. The Bank will not open/maintain accounts of black listed individuals/organization/entity by Bangladesh Government or United Nations Security Council Resolutions (UNSCRs) for terrorism or financing terrorism.
3. The Bank will not deal with any shell company. In other words, a company only in name, paper operated by fictitious persons cannot become a customer of the Bank.
4. The Bank will accept only those customers who would be willing to provide information to carry on the Banks due diligence exercise.
5. The Bank will categorize customers on the basis of risk, details of which are attached in the KYC Format.
6. The Bank will ensure that the less privileged customers are not harassed. This will be achieved through acceptable thresholds specially at the rural branches. However, such thresholds will not compromise on criteria number one and two above.
7. It is the duty of the bank officials to ensure confidentiality of customers.
8. The Bank will establish the background of each and every customer before acceptance.
9. The Bank will assess and keep on record details of business activities prior to accept him as a customer. At the same time individual or joint accounts should also be supported by personal and professional details.
10. Although business considerations are foremost in acquiring customers, transparency and legitimacy of the business concern should form the main priority.

Chapter 5: Responsibilities of the Bank in Preventing ML & CFT

According to Section 25 of Money Laundering Act, 2012 (amendment-2015), the responsibilities of IFIC Bank as a reporting organization are:

Quote

For the purpose of preventing and identifying money laundering & terrorist financing reporting organizations shall-

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

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

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

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

Unquote

Chapter 6: The Standards

6.1 Scope and Implementation

The Bank will document, implement and maintain procedures and controls which interpret Bank Policy and Bank Standards for each business in the context of applicable law and regulations. Compliance with such procedures and controls and with Bank Policy and Bank Standards will be monitored effectively.

6.1.1 These Standards are designed to help the business meet its responsibilities in relations to the prevention of money laundering & combating financing of terrorism.

6.1.2 The Standards are based on Banks Policy, the Money Laundering Prevention Act, 2012 (Amendment 2015), Anti-Terrorism Act, 2009 (Amendment 2012 & 2013) and circulars/guidelines issued by BFIU, Bangladesh Bank/IFIC Bank, Head Office from time to time. IFIC Guidelines are approved by the senior management of the bank and are subject to review from time to time. They cover the following areas of money laundering prevention & terrorist financing combating:

a) Internal Controls
b) Reporting Suspicious Transactions/Activities
c) Sanction Screening
d) Training and Awareness

6.1.3 The Standards set out minimum mandatory requirements for all business as required under Banks Policy. Such requirement may be enhanced where applicable law or regulation sets a more demanding requirement for a particular aspect of money laundering prevention. If, in exceptional circumstances, a business is unable to apply a particular standard, the issue should be referred to Head Office for necessary guidance.

6.1.4 The Standards cover all aspects of bank business activities from business relationships and the processing of transactions, through to the provision of advice to customers. Businesses must also consider the application of the Standards in relation to, for example, joint venture activities, subsidiary operations and outsourced services–particularly when cross border issues are involved.

6.2 Retrospective Application:

6.2.1 The Standards apply to both new and existing business relationships. Where necessary, therefore, remedial action on customer identification and due diligence must be undertaken for existing accounts, no matter how long the relationship has been in operation. Remedial work must be done as soon as possible. Where significant numbers of accounts are involved work plans for remedial action should priorities those relationships considered to represent higher risks.

6.2.2 The progress of remedial projects should be reported to Head Office, Senior Management.

6.3 Branch Managers Obligations:

The Branch Managers shall be primarily responsible for the prevention of Money Laundering, Terrorist Financing, Proliferation Financing as well Trade Based Money Laundering. They shall effectively reciprocate for the development, implementation and maintenance and monitoring of procedures and controls that meet the requirements of Money Laundering Prevention Act, 2012(2015) and Anti-Terrorism Act, 2009 (2012 &

2013) , Customer Acceptance Policy, 2013 (amendment-2018), Bank standards of best practice , BFIU, Bangladesh Bank's Circulars/Guidelines and our Head Office Circulars/Instructions issued from time to time.

CHAPTER 7: Compliance Structure of IFIC Bank

IFIC Bank must have its own policy manual that must confirm international standards, laws and regulations in force in Bangladesh and instructions of BFIU on preventing money laundering and terrorist financing, and this policy manual must be approved by the bank's Board of Directors. This policy manual shall be communicated to all concerned persons. Banks shall conduct review of the policy manual from time to time and shall amend/change where necessary.

IFIC Bank's compliance structure is an organizational setup who deals with AML & CFT compliance and the reporting procedure. The compliance structure is given below

- Central Compliance Committee (CCC) is formed by the CEO/MD.
- Chief Anti-Money Laundering Compliance Officer (CAMLCO) is appointed by the CEO/MD.
- Deputy Chief Anti-Money Laundering Compliance Officer (D-CAMLCO) is appointed by the CEO/MD.
- AML & CFT Department
- Branch Anti-Money Laundering Compliance Officer (BAMLCO) is appointed by members of CCC.

Appoint Compliance Officer & others

7.1 Obligations are under BFIU Circular-19, dated September 17, 2017:

'Every Bank will form a Central Compliance Committee at the Head Office under the supervision of a Senior Executive of the bank. The committee shall report directly to the CEO/MD.

To keep the bank free from the risks related to Money Laundering & Terrorist Financing and for the effective and proper compliance of all existing acts, rules and directives of BFIU from time to time, bank shall set up a Central Compliance Committee (CCC) that will be directly monitored by the CEO/MD of the bank.

7.1.1 "Central Compliance Committee (CCC)" will be headed by the senior executive who'll be known as the Chief Anti-Money Laundering Compliance Officer (CAMLCO) of the bank. His rank must not be lower than two steps of the MD & CEO. It must be ensured that his/her existing duties and responsibilities will not hinder his activities as the CAMLCO or the Chairman of CCC. Central Bank must be informed if the CAMLCO is changed.

7.1.2 There shall be an "Anti-Money Laundering & Combating Financial Terrorism (AML & CFT) Department" with sufficient human resources to ensure AML-CFT compliance and to carry out the secretarial jobs of CCC. The Head of AML-CFT Department will be the Deputy Chief Anti-Money Laundering Compliance Officer (D-CAMLCO) of the bank. The rank of D-CAMLCO should not be lower than Senior Vice President.

7.1.3 Central Compliance Committee (CCC) shall formulate bank's own strategies and programs to prevent Money Laundering & to combat Financial Terrorism and update them from time to time. AML-CFT Department will ensure the execution of these programs every year under the supervision of CCC and CAMLCO.

7.1.4 CAMLCO and D-CAMLCO should have adequate knowledge regarding existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML & TF.

7.1.5 Duties and responsibilities of AML-CFT Department, Central Compliance Committee (CCC), CAMLCO and D-CAMLCO must be specified.

7.1.6 The committee shall have at least 7 (seven) members from different departments of the bank such as Human Resources Management Division, Credit Division, Retail & Corporate Banking Division, Foreign Exchange Division, Operation Division, Card Division, IT Division etc. Any officer working at the bank's ICC Division cannot be a member of Central Compliance Committee (CCC).

7.1.7 Central Compliance Committee (CCC) shall arrange at least 4 (four) meetings every year to discuss the overall status of the banks money laundering activities and enforce necessary directives for the bank as

well. The bank shall assess its money laundering risks as per ML/TF Risk Assessment Guidelines for Banking Sector issued by BFIU at regular intervals and take necessary measures to mitigate the risks.

7.2 Central Compliance Committee (CCC) shall report the AML-CFT related initiatives, implementation progress and recommendations semi-annually (Jan-Jun and Jul-Dec) to the MD & CEO of the bank and/or if required to the Board of Directors of the bank for their information and directives. The report should be placed before the Board of Directors with the opinions and recommendations of the MD & CEO. A copy of the report must be sent to BFIU within 2 (two) months of every half-year end.

7.3 Central Compliance Committee (CCC) shall provide necessary directives to the AML & CFT Department including directives regarding customer due diligence, transaction monitoring, internal control system etc. policies and guidelines.

7.4 Central Compliance Committee (CCC) and Internal Control & Compliance (ICC) Division will perform their assigned responsibilities to prevent money laundering and terrorist financing separately and independently to ensure the independent audit function of bank. Though CCC as well as ICC is separated from each other but both should have co-ordination and co-operation to perform the responsibility and information exchange. In this regard every year ICC should examine the performance of CCC and AML & CFT compliance program

7.5 IFIC Bank shall nominate an experienced Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch. The manager, the second man of the branch or a official experienced in general banking/foreign exchange/credit etc. shall be nominated as the BAMLCO. The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and bank's own policies on preventing Money Laundering and Terrorist Financing. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her appointment letter.

Central Compliance Committee shall-

01. Review & update AML (Anti Money Laundering) & CFT (Combating Financing of Terrorism) Policies, Procedures, Guidelines, Circulars and Strategies, implementation & enforcement thereof as well as review and update Customer Acceptance Policy (CAP).
02. Coordinate the Bank's ML (Money Laundering) & TF (Terrorist Financing) and compliance initiatives.
03. Coordinate the ML, TF and MFS risk assessment of the Bank and review thereon.
04. Undertake organizational strategy and program regarding internal control policies and procedures to prevent money laundering and terrorist financing activities and will update the same from time to time.
05. Advise and guide "AML & CFT Department" to issue instruction circulars to the branch regarding the procedure of customer identification, transaction monitoring and internal control mechanism etc. to prevent money laundering and terrorist financing
06. Present the compliance status with recommendations before the Chief Executive Officer or Managing Director on quarterly/half yearly basis on AML & CFT.
07. Forward STR (Suspicious Transaction Report)/ SAR (Suspicious Activity Report) and CTR (Cash Transaction Report) to BFIU in time and in proper manner.
08. Report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner.
09. Impart training, workshop, seminar related to AML & CFT for the employee of the Bank.
10. Take required measures to submit information, report or documents in time.

11. Supervise/Review of internal, external, Bangladesh Bank audit report and BFIU's inspection report on Branches and yearly system check inspection report on Head Office on AML/CFT issues and monitor for regularization of the irregularities detected by them.
12. Conduct inspection, checking of records/papers/documents at Branches and MFS as required under Prevention of Money Laundering & Combating Financing of Terrorism and ensure compliance of the same on regular basis.
13. Implement and update of WLC (Watch List Checking) software in live and ensure screening of WLC software in all levels.
14. Disposal of files related to Correspondent Banks/ Relationship Management Application (RMA) on AML/CFT Issues.
15. Implement screening of all types of remittance (inward and outward) and all Customers, Agents and Distributors related to MFS and foreign exchange business.
16. Ensure Screening Mechanism during recruitment of new employee to avoid AML/CFT risk.

7.2 Chief Anti-Money Laundering Compliance Officer (CAMLCO)

The bank shall appoint a Chief Anti-Money Laundering Compliance Officer (CAMLCO) who's rank must not be lower than two steps of the MD & CEO. The CAMLCO will also act as the Chairman of the Central Compliance Committee (CCC). Before assigning any other duties or responsibilities to the CAMLCO of the bank, it must be ensured that this will not hinder his activities as the CAMLCO or the Chairman of CCC.

Roles and responsibilities of CAMLCO shall include but not restricted to the following:

01 Overall Supervision & Management of the Department.

02 Implementation, enforcement and review of AML/CFT policies, Procedures, Guidelines & Measures.

03 Submit periodical Reports to BFIU & Managing Director of the Bank.

04 Placing of Memo to Board of Directors on different regulatory issues related to AML & CFT.

05 Conduct Seminar/Training of AML & CFT issues at IFIC Bank Training Academy as well as outside of the Dhaka city.

06 Shall remain free from undue influence/intervention from anyone in discharging responsibilities as CAMLCO.

07 Send STR/SAR and any document or information to BFIU without any permission or consultation from MD/CEO as CAMLCO.

08 None shall deny access to any information of the Bank and if any one disregards her/his instructions he/she will face disciplinary action.

09 He is liable to MD for proper functioning of CCC.

10 Ensure to monitor, review and coordinate application and enforcement of the bank's compliance policies including AML/CFT Compliance Policy. This will include – an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity and a written AML/CFT training plan.

11 Ensure to monitor changes of laws/regulations and directives of Bangladesh Bank and revise its internal policies accordingly.

12 Ensure to respond to compliance questions and concerns of the staff and advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk.

13 Ensure to the bank's AML/CFT policy is complete and up-to-date, to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered by the bank.

14 Ensure to develop the compliance knowledge of all staff especially the compliance personnel and conduct training courses in the institution in this regard.

15 Ensure to develop and maintain ongoing relationships with regulatory authorities, external and internal auditors and regional/branch/unit heads and compliance resources to assist in early identification of compliance issues.

16 Ensure to assist in review of control procedures in the bank's, to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses.

17 Ensure to monitor the business through self-testing for AML/CFT compliance and take any required corrective action.

18 Ensure to manage the STR/SAR process and maintain confidentiality.

19 Ensure to review transactions referred by divisional, regional, branch or unit compliance officers as suspicious.

20 Ensure to review the transaction monitoring reports (directly or together with account management personnel).

21 Ensuring that internal Suspicious Activity Reports (SARs):
are prepared when appropriate
reflect the uniform standard for "suspicious activity involving possible money laundering or terrorist financing" established in its policy
are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy
are advised to other branches of the institution who are known to have a relationship with the customer
are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk.

22 Ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager.

23 Ensure to maintain a review and follow up process that planned corrective action, including possible termination of an account, be taken in a timely manner.

24 Ensure to manage the process for reporting suspicious activity to BFIU after appropriate internal consultation.

25 Any other works as & when assigned by the Managing Director.

7.3 Deputy Chief Anti-Money Laundering Compliance Officer (D-CAMLCO)

The bank shall appoint a Deputy Chief Anti-Money Laundering Compliance Officer (D-CAMLCO) who'll work as the Head of the AML & CFT Department of the bank and as the Member Secretary of the Central Compliance

Committee (CCC). The D-CAMLCO reports to the CAMLCO. The rank of D-CAMLCO should not be lower than Senior Vice President.

Roles and responsibilities of D-CAMLCO shall include but not restricted to the following:

1. Act in accordance with the directives of BFIU under guidance of CAMLCO.
2. Act as a Member Secretary of Central Compliance Committee (CCC).
3. Ensure that decisions taken by Central Compliance Committee (CCC) are timely implemented and, if applicable, disseminated to relevant parties.
4. Coordinate & Supervise works of the Department under the guidance of CAMLCO.
5. Ensure activities of the AML & CFT Department are aligned with AML & CFT strategies.
6. Ensure to Implementation, Enforcement and Review of AML/CFT Policies, Procedures, Guideline, Customer Acceptance Policy (CAP) & measures as and when required.
7. Dispose files related to Correspondent Banks/ Relationship Management Application (RMA) on AML/CFT issues.
8. Supervise ICC inspection report on branches and to monitor regularization of the observations raised.
9. Coordinate submission of statements/returns/ reports to BFIU of Bangladesh Bank on time.
10. Placing of Memos to Board of Directors on different regulatory issues related to AML & CFT
11. Ensure implementation of Annual AML & CFT program which includes, but not limited to-
    a) Annual Training/Workshop plan
    b) Annual Inspection Plan
    c) Off-site Monitoring
    d) Timely Review of existing possesses.
12. Any other works as & when assigned by the Management of the Bank.

7.4 AML & CFT Department:

As per instruction of BFIU circular no. 19 dated September 17, 2017, responsibilities of AML & CFT Department shall include to the following:

- Ensure implementation of annual "AML & CFT Compliance Program"
- Implement the bank's policy, procedure and strategies in prevention ML, TF & PF designed by CCC
- Issue circulars/instructions to branches as guided by CCC
- Coordinate the ML, TF and MFS risk assessment of the Bank and review thereon.
- Present the compliance status with recommendations before CCC
- Submit CTR and STR/SAR to BFIU
- Report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner
- Impart training, workshop, seminar related to AML & CFT for the employee of the Bank
- Take required measures to submit information, report or documents to internal and external stakeholders in time.

7.5 Branch Anti-Money Laundering Compliance Officer (BAMLCO)

The bank's CCC shall appoint an experienced officer as the Branch Anti-Money Laundering Compliance Officer (BAMLCO). Roles and responsibilities of BAMLCO shall include but not restricted to the following:

- **Ensure to have enough knowledge about acts, rules, regulations, policies & circulars relating to AML & CFT. Ensure to be updated about AML & CFT regulations, national initiatives and share the same with all members of the branch team.**
- Ensure to implement all the directives contained in "Money Laundering Prevention Act, 2012 (Amendment 2015) & Anti-Terrorism Act, 2009 (Amendment 2012 & 2013), AML/CFT Policy in line with any change/revision, Circulars/Circulars letters and different letters issued by HO & Circulars/Circulars letters and different letters issued by BB & BFIU and MD's clear message at the Branch level comprehensively.
- Ensure the customer's identity and underlying purpose of establishing relationship with the bank and collect adequate information and documentation as per IFIC —Customer Acceptance Policy-2013(amendment-2018).
- Ensure to identify & verify the identity of the customer based on data, information & documents obtained from reliable and independent source.
- Ensure to obtain correct and accurate information of customer in the Uniform AOF, KYC & TP and input all data of KYC & TP in the Misys System on regular basis. All information/documents for opening of Account have been obtained and verified.
- Ensure the screening of different sanction list and domestic sanction list checked properly beforeopening of account and while making any international/foreign transaction.Sanction screening records (False Positive) keep with AOF.
- Ensure to 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/Head Office AML instruction. Confirmation Legacy accounts are marked as Dormant.
- Ensure regular transaction monitoring to find out any unusual transaction in an effective way. The transaction should be examined at the end of day against transaction profile. TP matched with profession & income. Actual Transaction whether verified with Declared TP. Records of all transaction monitoring should be kept in the file.
- Check correctly CTR reporting done on monthly basis. Ensure to review cash transaction to find out any STR/SAR. Preserve CTR copy and check regularly.
- Ensure to review of Structuring to find out any STR/SAR. Check whether system to identify STR/SAR is active. Also check whether all officers have proper knowledge for reporting and identifying STR/SAR.
- Ensure all the employees of branch are well aware and capable to identify any unusual transaction or any attempt of unusual transactionor unusual customer behavior.
- Ensure to perform the self-assessment on AML & CFT compliance position to evaluate the branch on a half yearly basis and arrange meeting with concerned officials before finalizing the evaluation report to solve the problem as identified at branch level without any delay.
- Accumulate training records of all branch officials of your branch and take initiatives including reporting to CCC, HR and training academy. Ensure that all officers have taken 01(one) day training on AML & CFT knowledge and aware of it.
- Ensure all the required information and document i.e. monthly and quarterly are submitted properly to CCC 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 your branch with the involved person if so BAMLCO make an STR/SAR and send the same to AML & CFT department without any delay.

- Ensure branch is maintaining AML & CFT files properly and record keeping is done as per our Money Laundering & Terrorist Financing Risk Management Guideline requirements.
- Ensure that corrective actions have been taken by your branch to address & rectify the deficiency identified by the BFIU or BB or ICC. Whether all audit objections is implemented & complied.
- Take approval from CAMLCO while opening PEP's/IP's account and ensure enhanced due diligence as per BFIU Master Circular No# 19date 17.09.2017. PEPs/IPs accounts are monitored as per BFIU Circular.
- Selection of customer/opening of Account/ services based on AML & CFT Risk Management Guideline. Ensure to risk categorization of the customer as per Uniform AOF, KYC & TP & keep the list of High Risk Customers as well as Enhanced Due Diligence to be applied and monitor transaction of the same customer.
- Ensuring the compliance of AML/CFT issues at Branch level in order to manage and control Money Laundering& Terrorist Financing risks and also develop strong interpersonal relationship with the customers to develop customers' awareness regarding AML/CFT issues.
- Ensure to update and review AOF, KYC & TP from time to time as per BFIU circular and keep the relevant records with AOF. Ensure to retain the records of customer information and transactions at least for five(05) years after termination of relationship with customer
- Ensure to obtain information/documents/short KYC of depositor(s) and withdrawer(s) for walk-in/online customer (other than account holder) as per instructions mentioned in BFIU circular 19 dated 17.09.2017.

- Ensure to obtain Positive Pay instruction in case of all corporate/proprietorship firm customer for Taka-01(one) lac or above and for individual account 05(five) lac or above and keep record of the same as per Bangladesh Bank instruction.
- Ensure to verify the address of the customer by sending thanks letter both account holder & introducer and keep the record of sending receipt with acknowledgement receipt from post office or POD from Courier with AOF.
- Ensure to obtain and verify the required identification documents with photos of customers and nominees.
- Ensure to obtain and verify documents related to profession of the customer.
- Ensure to obtain and verify documents related to source of funds and TP has been matched properly.
- Inward & Outward remittance monitored or not. Details of walk-in/one-off customers in respect of PO/Foreign Remittance, wire transfer and others must be obtained by the branches.
- Ensure that preventive measures have been taken by the branch to prevent Money Laundering & Terrorist Financing for foreign & local trade financing.
- Ensure to identify Beneficiary owner of the account, obtain complete and accurate information of beneficial owner and complete KYC.
- Ensure proper risk grading of customer in line with occupation, income and transaction profile (TP) and consider the risk score in branch risk register and risk rating of beneficial owner during risk grading.

- Ensure to arrange AML & CFT meeting with concern officials of the branch on monthly basis by issuing notice of the meeting and to take effective measures as per BFIU instruction.
- Ensure to monitor the staff of the branch team to check whether any of them are directly or indirectly involved in or is facilitating Money Laundering & Terrorist Financing.

BAMLCO will arrange AML & CFT meeting every month with other concerned important officials of their branch and takes 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,
- Screening sanction list & local banned list,
- Record keeping,
- Training,
- Identify high risk customer,
- Update KYC and TP (as & when required)
- Self-Assessment related activities

BAMLCO will send the minutes of these meetings to AML-CFT Department.

7.6 Responsibilities of Other Branch Officials

- 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;
- 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 AMLCO.

7.7 Internal Control and Compliance (ICC)

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

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

- Understand ML & TF risk of the bank and check the adequacy of the mitigating measures.
- 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 Bank's AML/CFT policies, procedures and processes.
- Examine the AML & CFT compliance activities of the branches during comprehensive audit.
- Examine the special AML & CFT compliance activities of at least 10% of the branches annually and send copies of the reports to AML & CFT Department.
- Send a copy of the report with the rating of the branches inspection /audited by them to AML & CFT Department of the bank.
- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations).
- Assess the adequacy of the FI's processes for identifying and reporting suspicious activity.
- Communicate the findings to the Board and/or Senior Management in a timely manner.
- Recommend corrective action for deficiencies.
- Track previously identified deficiencies and ensures 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 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.
  - Participation of personnel from all applicable areas of the FI.
  - Frequency of training
  - Coverage of FI'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.

7.8 External Auditor

External auditor shall play an essential part in reviewing the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External audit should focus their audit programs on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits, to the financial sector supervisors.

Chapter 8: Identification and Verification of Customers Account

A meaningful anti-money laundering & combating financing of terrorism compliance program of the Bank will include identification and verification of customers at account opening. Accordingly, IFIC Branch will ensure to:

- Verify the identity of any person seeking to open an account to the extent reasonable and practicable;
- Maintain records of the information used to verify a person's identity, including name, address and other identifying information; and
- Consult lists of known or suspected terrorists or terrorist organizations provided to the financial institution by the regulators/government agency to determine whether a person seeking to open an account appears on any such list.

The following options will recommend for bank branch to consider in developing customer identification process:

8.1 Customer Identification

Customer identification is an essential part of CDD measures. A 'Customer' is defined in BFIU Circular No. 19 dated 17.09.2017, as under:

a) The person or entity that maintains an account /have business relationship with the Bank;
b) True Beneficial Owner* of bank account or of business relations, in whose behalf an account is operated/maintained directly or indirectly;
c) Professional intermediaries (such as Lawyer, Law Firm, Chartered Accountants etc.) engaged for conducting/operating accounts of account holder, trusts or actual beneficial owner of transaction under the existing legal infrastructure;
d) Any individual or entity in a single transaction conducted a high value** occasional transaction or any person or entity involved in a financial transaction that may pose significant reputational and other risks to the institution.
e) Any Person or entity defined as "Customer" by BFIU from time to time.

Beneficial Owner would be identified for each and every account. By following process, the actual beneficial owner of the account would be confirmed:

a) If any customer operates accounts on behalf of other person, in that case bank will obtain & retain correct and complete information of that person other than customer.
b) Seemingly if any person controls/influences any customer directly or indirectly, bank will obtain & retain correct and complete information of that person other than account holder.
c) In case of company, controlling shareholder or individual shareholder holding 20% and more shares shall be considered as beneficial owner, bank will obtain & retain correct and complete information of those persons.
d) If it is not possible to identify any natural person in context of above sl.no b & c, in that case bank will obtain & retain correct and complete information of MD/CEO as beneficial owner.

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, the bank will undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially or when there is a material change in the way that the account is operated. However,

the bank will also aware of any time that it lacks sufficient information about an existing customer, they will take steps to ensure that all relevant information is obtained as quickly as possible.

Whenever, at the time of opening of an account or business relationship with the customer, the branch considers One-off transaction or series of linked transactions which is to be undertaken according to standard identification Procedures. Customer Identification is verified in all cases where money laundering & terrorist financing is known or suspected.

Once verification of identity will be satisfactorily completed, no further evidence will be needed when other transactions are subsequently undertaken. Branch will maintain records as per record keeping (Chapter-10) and information will be updated or reviewed as and when required.

8.2 Verification of Source of Funds

IFIC Bank will collect and verify the document supporting source of fund of the person at the time of establishing any business relationship or while conducting CDD. The document includes present employment identity, salary certificate/copy/advice (for salaried person), Proof of employment /income(employment certificate/pay slip/employment contract mentioning annual income/bank statement mentioning monthly salary or last tax return paper), Employed ID & visiting card(for ascertaining level of employment), self-declaration acceptable to the Bank(commensurate with declared occupation), documents in support of beneficial owner's income (source of fund of house wife, students etc.) ,Trade License if the customer declared to be a business person, Documents of property sale(if any), Document of FDR encashment (if any) , Document of foreign remittance (if any fund comes from outside the country), Document of retirement benefit, Bank loan documents (if any), Document of Inheritance/Gift/ Return on Investment , pension book, financial statement, income tax return, business document or any other document that satisfies the branch Official. IFIC Bank will also request customers to provide E-TIN (Electronic Tax Identification No) certificate which declares taxable income.

8.3 Verification of Address

IFIC Bank Official will verify the address of customer at the time of establishing any business relationship or while conducting CDD. This is to be done by physical verification of branch official or through standard mail or by courier service correspondence. The branch will collect any other document i.e. latest utility bill/ utility card (not beyond 03 months old) mentioning the name and address of the customer as per branch Official's satisfaction.

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

8.4 Persons without Standard Identification Documentation

IFIC Bank Officials will apply common sense approaches and some flexibility considering risk profile of prospective customers such as the elderly, the disabled, street children or people, students and minors without compromising sufficiently rigorous anti-money laundering procedures is recommended. In this situation

internal procedure provides appropriate guideline to the officials on how identity can be confirmed in these exceptional circumstances.

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

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

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

8.5 Customer Profiling

(i) Obtaining and document the customer's basic background information.

(ii) Try to use this information to evaluate the appropriateness and reasonableness of the customer's transaction activity.

(iii) Determine the source of the customer's funds.

8.6 KYC Profile should disclose:

(i) The customer's expected transaction trends (monthly or annually),

(ii) The source of wealth and

(iii) Net income

8.7 Update Customer Information, TP & KYC Profile

(i) Update customer profile if there is any change in information;

(ii) Regular reviews of transaction activity & balance fluctuation reports and update Transaction Profile with proper justification if there is any change transaction pattern;

(iii) Update KYC profile form, if there is any change in customer information and/or any change in transaction due to update of TP (as applicable);

(iv) Review and update (as applicable) TP & KYC as per BFIU Circular No. 19 dated September 17, 2017 in every 5 (five) years for Low Risk customers and every 1 (one) year for High Risk Customers;

(v) Newspapers and magazine articles, financial statements, brochures, industry activities relating to the customer;

(vi) Periodical discussions with the client relating to their business activities including future plan of the business for the next 12 months.

8.8 Bank should focus on:

- High risk customers
- Source of significant fund

- Transactions which are inconsistent with the transaction profile.
- Client borrowing should be monitored in the course of business by the responsible Officer of advances department to ascertain repayments or settlement of loans or loan draw down is in line with the client business activities.

8.9 Monitor Funds Transfer activities to track Money Laundering & Terrorist Financing:

- Sending or receiving frequent or large volume of Swift/Telegraphic transfers to and from domestic and offshore institutions.
- Depositing funds into several accounts, usually in amounts below the banks tractable threshold, and then consolidating into a master account and transferring them outside of the country.
- Instructing the bank to transfer funds abroad and to expect an equal incoming Swift/Telegraphic transfer from other sources.
- Regularly depositing or withdrawing large amounts by Swift/Telegraphic transfers to, from, or through countries that are known sources of narcotics or whose bank secrecy laws facilitate the laundering of money & financing of terrorism.
- Receiving Swift/Telegraphic transfers and immediately purchasing monetary instruments prepared for payment to a third party.

8.10 Tracking of Large – Value Funds Transfers:

To curtail money laundering & terrorist financing activities, the branch focuses on the identification and documentation of currency-based transactions. It is recommended to provide complete information about the parties to a funds transfer. The information includes to the extent practical, complete originator and beneficiary information for payment orders sent through all funds transfers systems. Branch includes the following information, to the extent possible, in the text of every payment order:

- Name, address and account number of the applicant;
- The beneficiary's name, address and account number, if available.

8.11 Monitor activity not consistent with the Customer's Business:

- Corporate account(s) where deposits or withdrawals are primarily in cash rather than cheques.
- A customer who operates a retail business and does not make substantial drawings against cheque deposited. This may indicate that the customer has another source of cash.
- Accounts with a large volume of deposits in demand Draft, Pay Order and/or Swift/Telegraphic transfer, when the nature of the account holders business does not justify such activity.
- Accounts that show frequent large cash transactions for a business that generally does not deal in large amounts of cash.
- Retail deposits of numerous cheques but rare withdrawals for daily operations.
- An account that sends and receives Swift/Telegraphic transfer without an apparent business reason or when inconsistent with the customers' business or history.

8.12 Monitor unusual characteristics or activities in the customer's account:

- An account holder or customer that has frequent deposits of large amounts of cash deposit.
- Client or in-house company accounts, such as trust accounts, escrow accounts, etc. that show substantial cash deposits.

- An account opened in the name of a Money Exchanger that receives Swift/Telegraphic transfers and/or structured deposits.
- A customer who purchase a number of Demand Draft, Pay Orders or Travelers Cheques for large amounts just under a specified threshold or without apparent reason.

Chapter 9: Customer Due Diligence

The CDD obligations is a process which compel the banks to understand who customers in order are to guard against the risk of committing offences under MLPA, 2012 (Amendment-2015) including 'Predicate Offences' and the relevant offences under Anti-Terrorism Act, 2009 (Amendment 2012 & 2013).

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources. Considering the risks of money laundering and terrorist financing the bank will demonstrate to the supervisory authority to put in place, implement adequate CDD measures. CDD measures will be based on-

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

IFIC Bank will adopt effective standard KYC from the customer which is an essential part of banks' risk management policies. The Bank officials will be aware regarding inadequate KYC program because of legal and reputational risk.

An adequate KYC Policies and Procedures not only contribute to the bank's overall safety and soundness but also protect the integrity of IFIC banking system by reducing money laundering, terrorist financing and other unlawful activities.

Bank will carry out customer due diligence for two broad reasons:

a) Because it will help the bank to identify customers who 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
b) It will also help the bank to investigate, law enforcement by providing available information about customers in due process.

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

9.1 Legal Obligations of CDD

Obligations under MLPA, 2012:

"The reporting organizations shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to Bangladesh Bank."

Obligations under MLP Rules, 2013:

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

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

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

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

9.2 General Rule of CDD

9.2.1 Completeness and Accuracy

As per AML Act, 2012 (Amendment-2015) & BFIU directives it is an obligation for the bank to maintain complete and accurate information of customer and person acting on behalf of a customer.

'**Complete'** means to combination of all information for verifying the identity of the person or entity. For example: name and detail address of the person, profession, source of funds, Passport/National Identity Card/Birth Registration Certificate/acceptable ID card with photo, phone/ mobile number etc.

'**Accurate'** means to such complete information that has been verified for accuracy.

To comply AML Act 2012(amended-2015) & BFIU directives, while opening an account for the identification purpose of customer, IFIC bank will take sufficient information up to branch official's satisfaction.

'Satisfaction of 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.

'**KYC'** means knowing a customer physically and financially. It also means to conduct an effective KYC, it is essential to accumulate complete and accurate information about the prospective customer.

The verification is generally a cumulative process. To complete this process the bank will verify all the documents of prospective customer before opening an account. The bank will not take any single piece of identification which is not guaranteed as genuine or as being sufficient to establish identity. The overriding principle means bank knows who their customers are and take the necessary documentary evidences to verify this.

If Bank is unable to identify customer and verify 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, in that case Bank will not open the account, commence business relations or performs the transaction or terminates the business relationship and bank will also consider it as a suspicious transaction report in relation to the customer and send report to the CCC. IFIC bank will follow Annexure-C that provides an example of collection of documents has been provided to find it's useful for the purpose.

9.2.2 Ongoing CDD measures (Review and update)

IFIC Bank will take all necessary measures to review and update the KYC of the customer after a certain interval. For Low Risk customers this procedure will be conducted once every 5 (five) years, for High Risk customers, it will be conducted once every 1 (one) year.

If the bank is informed about any change in source of fund of customer, bank must collect latest documents and update the KYC as soon as possible. Besides bank must also update KYC information anytime if there is

any particular necessity realized. Depending on the updated information the risks associated with the accounts will be assessed again without any delay.

If there is any subsequent change of the customer's name, address or employment details the bank will aware to record it 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.

The bank will 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, the bank will again collect the Transaction Profile along with the amendments in it from the customer by reviewing the transactions of the customer within 6 (six) months of establishing business relation and assessing the effectiveness with a logical consideration.

9.3 Obligations under BFIU Circular No- 19, dated September 17, 2017:

Considering the risk associated with the customer, customer due diligence measures has to be undertaken as follows:

(a) While establishing relationship with the customer

(b) During occasional transactions amounting BDT 5(five) lac or above by walk-in customer

(c) When there is sufficient ground to doubt the veracity or adequacy of previously obtained customer identification data

(d) If there is any possibility of tipping off while conducting CDD for any suspicious transactions in terms of ML & TF, then STR/SAR has to be submitted without conducting CDD.

2. The bank shall have 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" means satisfaction of the appropriate authority, that is, necessary due diligence has been conducted considering the risks of the customers. This customer due diligence process should be reviewed on regular basis.

3. The bank shall identify the beneficial owner of each account and take reasonable measures to verify the identity of the beneficial owner using information or data obtained from a reliable source. The identity of the beneficial owner has to be ensured through following manners:

a) If any customer operates accounts on behalf of other person, in that case bank will obtain & retain correct and complete information of that person other than customer.

b) Seemingly if any person controls/influences any customer directly or indirectly, bank will obtain & retain correct and complete information of that person other than account holder.

c) In case of company, controlling shareholder or individual shareholder holding 20% and more shares shall be considered as beneficial owner, bank will obtain & retain correct and complete information of those persons.

d) If it is not possible to identify any natural person in context of above sl.no b & c, in that case bank will obtain & retain correct and complete information of MD/CEO as beneficial owner.

9.4 Simplified Customer Due Diligence

a) For transactions made by walk-in customers the bank shall obtain name and address of sender/applicant and receiver/beneficiary and telephone number of sender/applicant when the transaction is BDT 50,000 or less and preserve the same.

b) The bank shall obtain photo ID along with the above mentioned particulars of sender/applicant or depositor/withdrawer when the transaction is more than BDT 50,000 but less than BDT 5,00,000 and preserve the same .

c) To facilitate financial inclusion program, simplified due diligence may be carried out for low-risk accounts such as accounts of school students, farmers and other no-frill accounts.

9.5 Other Instructions Regarding CDD

1) During opening of a customer account, IFIC Bank will use its approved Account Opening Forms designed according to the Uniform Account Opening Form issued by BFIU. The Bank will preserve all documents after verification of customer identification and proper CDD.
2) If a customer maintains more than one account, Bank must assign only one Unique Customer Identification Code (UCIC) i.e. Customer Number for the customer's accounts. The UCIC will be used to track all services and transactions of the customer with the bank.
3) The bank shall collect the declaration of customer about the Transaction Profile of customer account in the specified form. After reviewing the nature of the customer, occupation and the source of fund in the account and the nature of transaction , the bank shall determine the appropriate transaction profile by making required amendments in the TP after 06(six) months of establishing business relation-
    - ❖ However, if the transactions increase significantly than what the customer estimated during establishing relationship, then the TP has to be amended in consultation with the customer.
    - ❖ Branch has to raise suspicious transaction report (STR) in applicable cases.
4) Updating KYC information is a continuous process. Bank should update KYC information on the basis of Uniform Account Opening Form issued by BFIU every 5 (five) years for Low Risk customers and every 1 (one) year for High Risk customers.
    - ➢ The bank shall update the changes in any information on the KYC as soon as it gets to know about such changes.
    - ➢ The bank shall update KYC information anytime if there is any particular necessity felt.
    - ➢ Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay.
5) Legacy accounts refer to those accounts opened before 30 April, 2002. Accounts of such period, KYC of which have not completed shall be marked as "Dormant"-
    - ❖ No withdrawal shall be permitted in those accounts; however, deposit can be allowed;
    - ❖ These accounts will be made fully functional only after conducting proper CDD measures;
    - ❖ Branches as well as IFIC AML & CFT Department shall preserve data of such accounts at their respective ends.
6) All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied for foreigner and non-resident Bangladeshis.

9.6 In Case Where Conducting CDD Measure is Not Possible

IFIC bank will take the following steps if conducting CDD measures in not possible due of lack of cooperation from the customer or if the collected information seems to be unreliable or bank cannot collect/verify satisfactory information on customer identification:

a) Bank shall not open the account of the customer or carryout transactions or, if necessary, close the account;
b) Send notice to the customer explaining the reason of closer of the account and obtain senior management approval before terminating such account(s);
c) Information related to refusal of opening new account and termination of existing account shall be sent to AML & CFT Department who'll inform the other branches the same;
d) Shall submit STR/SAR of such accounts, if appropriate.

9.7 Timing of CDD

IFIC bank will apply CDD measures when it does any of the following:

a) While establishing a relationship;
b) While carrying out any occasional transaction (including wire transfer) of amount 5 Lacs or above;
c) If suspicion arises regarding the accuracy of documents, data or information previously obtained for the purpose of identification or verification;
d) If suspicion arises regarding Money Laundering /Terrorist Financing activity.

If there is any possibility of information leakage or tipping off, suspected transactions should be reported without conducting CDD.

9.8 Enhanced CDD measures

In addition to normal CDD measures IFIC bank must conduct Enhanced CDD measures if necessary. In this regard the bank will conduct Enhanced Due Diligence (EDD) under the following circumstances:

- Individuals or legal entities scored with high risk;
- Individuals who are identified as Politically Exposed Persons (PEPs), Influential Persons (IPs) and Chief Executives or top-level officials of any international organization;
- Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes;
- While establishing and maintaining business relationship and conducting transaction with a person including legal representative, financial institution or any other institution of the countries and territories that do not meet international standard in combating money laundering and terrorism financing such as the countries and territories enlisted as High –Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force's Public Statement.

Enhanced CDD measures shall include, but not limited to the following:

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

9.9 Walk-In customer/Online transaction (other than account holder)

While serving Walk-in customer (i.e. other than account holder) services like DD. TT. MT. Pay Order and online transaction Bank shall follow instruction of BFIU circular no. 19 dated 17.09.2017 as well as AML & CFT Circular no 04/2018(amended) dated 12.09.2018 regarding this issues.

IFIC bank will collect complete and correct information while serving Walk-in customer i.e. a customer without having an account. The Bank will know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT. A detail provisions are discussed in the paragraph 9.3 & 9.4 of this Guidelines.

IFIC Bank will collect complete and correct information of any person other than customer (bearer information) deposit or withdrawal using on-line facilities. Additionally, in regards to online deposit, bank also identifies sources of funds as well.

9.10 Non Face to Face Customers

The Bank will assess Money Laundering and Terrorist Financing risks while providing service to non face to face customers and develops the policy and techniques to mitigate the risks as well as reviews time to time.

"Non face to face customer' means "the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the bank branch".

9.11 Customer Unique Identification Code

IFIC bank will use unique identification code for any customer maintaining more than one account or availing more than one facilities. Such unique identification system facilitates the branch to avoid redundancy and saves time and resources. This mechanism also enables the bank branch to monitor customer transactions effectively.

9.12 Correspondent Banking Relationship

Correspondent banking relationship sometimes creates risk that the other bank's customers may be using that bank to launder funds. It is not necessarily possible to conduct due diligence on that Bank's customer base and as such, these relationships require additional care and attention to guard against becoming unwilling participants in this activity.

Bank must follow the following instructions to establish and/or continue Cross Border Correspondent Banking relationship:

a) Before providing any Correspondent Banking service, bank must be confirmed about the nature of the correspondent/respondent bank's business by obtaining information as per Appendix-KA of BFIU Circular No- 19, dated September 17, 2017 and take approval from the CAMLCO. Bank may further collect additional information if required from open sources.
b) Before establishing and/or continuing relationship with any correspondent/respondent bank, bank must ensure that the foreign bank is regulated and monitored by relevant regulatory authority.
c) No relationship to be established with Shell Banks that have no physical presence in any country.
d) The Bank will keep sufficient information about a respondent institution to understand fully the nature of their business.
e) The Bank will be satisfied with the respondent institution's anti-money laundering and terrorist financing controls.

f) Before establishment of relationship, the Bank will know whether the respondent institutions have customers who are based in countries classified by FATF as "high risk" and if so, whether they maintain enhanced due diligence on such customer(s).
g) The Bank will not allow third parties to use its Correspondent Bank account(s) i.e. in the form of "payable through account".
h) No relationship to be established with Numbered Account, un-anonymous account, nested account.
i) The Bank may review correspondent banking relationship as and when required.

9.13 Politically Exposed Persons (PEPs) and Influential Persons (IPs)

IFIC bank will assess all the clients regarding to determine whether they are PEPs or Influential Persons or chief executives or top-level officials of any international organization and their linked entities. Because these types of 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 increase the risk to the bank due to the possibility of that individuals holding such positions 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 do not incriminate individuals or entities. It does, however, put a prospective or existing Client into a higher risk category.

9.13.1 Definition of PEPs

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

a) Heads and deputy heads of state or government
b) Senior members of ruling party
c) Ministers, deputy ministers and assistant ministers
d) Members of parliament and/or national legislatures
e) Members of the governing bodies of major political parties
f) Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
g) Heads of the armed forces, other high-ranking members of the armed forces and heads of the intelligence services
h) Heads of state-owned enterprises

9.13.2 CDD Measures for PEPs

IFIC Bank will be conscious whether any of their customers is PEPs. When the bank will identify PEPs, it applies enhanced CDD measures that is set out in 9.2.3 of this guideline. Moreover, the bank will perform the following:

- To adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a PEP;

- Obtain CAMLCO approval before establishing such business relationship
- Take reasonable measures to establish the source of fund of a PEP's account
- Monitor their transactions in a regular basis and
- All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act has to be complied accordingly

9.13.3 Definition of Influential Persons

'Influential persons' means "Individuals who are or have been entrusted with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials." The following individuals must always be classed as Influential persons:

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

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

9.13.4 CDD Measures for Influential Persons (IPs)

IFIC bank will be conscious whether any of their customers is an IPs. When our bank identifies IPs it applies enhanced CDD measures that are set out in 9.2.3 of this guideline. Moreover, the bank will perform the following:

a) Adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is an IP
b) Obtain CAMLCO's approval before establishing such business relationship
c) Take reasonable measures to establish the source of fund of an IP's account
d) Monitor their transactions in a regular basis and

e) All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly

9.13.5 Definition of Chief Executives or Top-Level Officials of Any International Organization

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

9.13.6 CDD Measures for CEO or Top-Level Officials of any International Organization

IFIC bank will be conscious whether any of their customers is a CEO or top-level officials of any international organization. If the bank will identify the same it applies enhanced CDD measures that is set out in 9.2.3 of this guideline. Moreover, the bank will perform the following:

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

9.13.7 Close Family Members and Close Associates of PEPs, IPs and CEO or Top-Level Officials of Any International Organization

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

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

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

A Close Associate of a PEP/Influential Person/Chief executive of any international organization or any top-level official includes:

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

In addition, it includes 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.

9.13.8 CDD Measures for Close Family Members and Close Associates of PEPs, IPs and CEO OR Top-Level Officials of Any International Organization

IFIC Bank will be conscious whether any of their customers is a family member or close associates of a PEP, IP or CEO or top-level officials of any international organization. When our bank identifies the same it applies enhanced CDD measures that is set out in 9.2.3 of this guideline. Moreover, the bank will perform the following-

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

9.14 CDD for New Technology

Now –a-days ATM, Debit Card/Credit Card, POS & Ecommerce purchase have been identified as the most vulnerable to Money Laundering & Financing of Terrorism vehicle and fraudulent activities.

Money Launderers and criminals utilize these facilities to legalize their illicit funds. Therefore,

- ML & TF risk assessment shall have to be performed before launching a new product, channel and technology
- Furthermore, enhanced due diligence shall have to be carried out for non-face to face transactions.

9.15 CDD for International Trade & Trade Based Money Laundering (TBML) and Financing of Terrorism-

According to the International Narcotics Control Strategy Report (INCSR) hundreds of billions of dollars are laundered annually by way of Trade Based Money Laundering (TBML). It is one of the most sophisticated methods of cleaning dirty money and also one of the most difficult one to detect.

By definition Trade Based Money Laundering (TBML) is the process by which criminals use a legitimate trade to disguise their criminal proceeds from their devious sources. The crime involves a number of schemes in order to complicate the documentation of legitimate trade transactions; such actions may include moving illicit goods, falsifying documents, misrepresenting financial transactions and under-or over-invoicing the value of goods.

Misuse of International trade system is one of the main methods by the criminals to integrate their proceeds into the formal economy. As evidence emerges that International trade is becoming haven of dirty money, the basic techniques of Trade Based Money Laundering (TBML) include:

- ✓ Over-and under-invoicing of goods and services;
- ✓ Multiple invoicing of goods and services;
- ✓ Over- and under-shipments of goods and services;
- ✓ Falsely described goods and services;

Customer due diligence shall be performed both at the time of establishing relationship and executing transactions. Bank shall obtain sufficient detail from the customer to enable it to assess the risk and perform risk based assessment to determine the appropriate level of due diligence that shall be undertaken. In this connection, all AD branches and concerned divisions shall follow the ML & TF risk register set out for international trade related customers, products/services and delivery channels.

9.15.1 CDD to Prevent Trade based Money Laundering (TBML):

a) Export check-points may include, but not limited to, the following:

- ❖ Screening of all relevant parties against different sanction list (UN, OFAC, EU & HMT) and domestic sanction lists
- ❖ Line of business Vs. exportable items
- ❖ Volume of export Vs. capacity of the customer
- ❖ Whether destination country is a High-Risk and Non-Cooperative Jurisdiction in the FATF's Public Statement
- ❖ Credit report of the buyer
- ❖ Pricing :
  - ✓ Common commodity basket pricing
  - ✓ Public database through internet for other products
  - ✓ Informal market information from peer banks and correspondent institutions.

b) Import check-points may include, but not limited to, the following:

- ❖ Screening of all relevant parties against different sanction list (UN, OFAC, EU & HMT) and domestic sanction lists
- ❖ Performing Bank's usual due diligence before execution of import
- ❖ Line of business Vs. imported items
- ❖ Check dual use of goods
- ❖ Volume of import Vs. capacity of the customer
- ❖ If the importing country including port of loading is a High-Risk and Non-Cooperative Jurisdiction in the FATF's Public Statement
- ❖ Credit report of the supplier
- ❖ Pricing :
  - ✓ Common commodity basket pricing
  - ✓ Public database through internet for other products
  - ✓ Informal market information from peer banks and correspondent institutions.

9.16 CDD for Preventing Money Laundering through Credit Card:

Credit Cards can be vulnerable to abuse unless effective controls are employed to minimize the risks. Credit Cards, for example, may be used to transfer funds that are the result of criminal activity. Periodic reviews shall be undertaken by the bank to identify risks related to Credit Cards and AML & CFT related controls that are need to address these risks-

- Card Division of IFIC bank shall perform due diligence applying a risk-based approach and follow the ML & TF risk register for IFIC Bank Card Division.
-
- Once the card has been issued, bank shall establish an effective transaction monitoring framework as part of ongoing due diligence.
- IFIC Bank Card Division shall develop and, where appropriate, integrate its AML monitoring scenarios with other systems for example, those used for fraud control.
-
- The monitoring program shall include an appropriate use of technology solutions, and must ensure that all personnel who are evaluating and investigating the transactions are adequately trained to do so.

9.17 Wire Transfer

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

Investigations of major money laundering cases have shown that criminals make extensive use of telegraphic transfers (TT) and electronic payment and message systems because of the complexity of cross-border investigations. Investigations become more difficult if the identity of the original ordering customer (i.e. purchaser) or the ultimate beneficiary is not clearly shown in a TT and electronic payment message instruction. In such a situation, all branches must include accurate and meaningful information of the followings on all outgoing funds transfers:

- The originator (name, account number, and where possible address)
- The beneficiary (account name and/or account number) and
- The related messages that are sent.

All this information should remain with the transfer or related message throughout the payment chain. Records of electronic payments and messages must be kept for at least 5 (Five) years.

9.17.1 Cross-Border Wire Transfer

Cross border correspondent banking means providing banking services to another bank respondent by a bank that is correspondent. This kind of banking services refer to credit, deposit, collection, clearing, payment, cash management, international wire transfer, drawing arrangement for demand draft or other similar services.

IFIC bank will follow-

- Under general or special consideration, for cross-border wire transfers of minimum 1000 (one thousand) or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank.
- Furthermore, for amounts below 1000(one thousand) USD or equivalent foreign currency , full and meaningful information of the originator has to be obtained so as to identify him/her and preserved the same information.
- While providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information of the beneficiary has to be obtained and preserved.
- Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file has to contain required and accurate originator information as well as complete beneficiary information. In addition, the bank shall include the account number of the originator.

9.17.2 Domestic Wire Transfers

In case of threshold domestic wire transfers of at least 25000/- (twenty-five thousand) BDT IFIC bank will obtain correct and accurate information of the originator and preserves the same as well as sends to intermediary/beneficiary bank/institutions. Furthermore, for domestic wire transfers below the threshold full and meaningful originator information has been preserved. For providing money of domestic wire transfers to beneficiary the bank will be obtain full and meaningful beneficiary information and preserves the same. Mobile financial services of the bank will use KYC format and provides to 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, the bank will preserve in the payment related message/instructions.

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

Ordering Bank:

The ordering bank ensures that qualifying wire transfers contain required and accurate originator information and required beneficiary information. This information has to be preserved minimum for 5 (five) years.

Intermediary Bank:

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

An intermediary financial institution has 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 are consistent with straight-through processing.

Beneficiary Bank:

When the bank will work as a beneficiary financial institution it initiates risk-based procedure to identify wire transfers that lack required originator or required beneficiary information. In case of insufficient originator information, the bank collects that information through mutual communication or using any other means. During the payment to receiver/beneficiary the bank also collects full and accurate information of receiver/beneficiary and preserves the information for 5 (five) years.

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

9.18 CDD for Beneficial Owners

IFIC Bank will 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, the bank will put in place appropriate measures to identify beneficial owner. Upon its own satisfaction ensures CDD of beneficial ownership by collecting information and documents from independent and reliable sources that includes publicly available information, information from customer or information from other reliable sources. The Bank will consider following aspects while identifying beneficial ownership:

(a)If any customer operates accounts on behalf of other person, in that case bank will obtain & retain correct and complete information of that person other than customer.

(b) Seemingly if any person controls/influences any customer directly or indirectly, bank will obtain & retain correct and complete information of that person other than account holder.

(c)In case of company, controlling shareholder or individual shareholder holding 20% and more shares shall be considered as beneficial owner, bank will obtain & retain correct and complete information of those persons.

(d)If it is not possible to identify any natural person in context of above sl.no b & c, in that case bank will obtain & retain correct and complete information of MD/CEO as beneficial owner.

As per BFIU instruction, Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

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

9.19 Reliance on Third Party

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

- A third party should immediately obtain necessary information related to (i)–(iii) as mentioned above;

- Without any delay the bank takes all necessary data and documents from third party which are available;
- In compliance with CDD the bank takes appropriate measures after satisfying that the third party is regulated, supervised and monitored for and keep record of the same which is set out in this guideline.

9.20 CDD for Legacy Accounts

As per BFIU instruction all branches of IFIC Bank must update the KYC profiles of the accounts opened before April 30, 2002. The Bank also instructed the branches that these legacy accounts will be treated as Dormant Account & no withdrawal will be permitted from these accounts. However, deposits to these accounts can be permitted. After conducting proper CDD measures these accounts will be made fully functional. AML Department of the bank will preserve data of such accounts at their end.

9.21 Transaction Monitoring

IFIC bank will develop an effective system named Suspicious Activity Module at Head Office, which monitors the transaction of Core Banking System (CBS) and create cases based on different rulebook parameters as well as review the risk by monitoring time interval. Based on review Enhance Due Diligence (EDD) will be maintained for accounts which are high risk category. Transactions related with International Trade and transaction screening with local and different Sanction list (UN, OFAC, EU & HMT) which has been complied by automated screening software named Watch List Checking (WLC).

The bank shall monitor customer transactions carefully as transaction monitoring is important to detect suspicious transaction. While monitoring transactions, the bank should emphasize on focusing on the following issues:

- monitor customer transaction on aregular basis either manually or by automated system.
- Transactions that seem complex, abnormal and doesn't have any apparent financial/legal purpose should be monitored with extra care.
- Bank should be vigilant at all times to identify 'Structuring' i.e. reporting avoidance as per Money Laundering Prevention Act, 2012 (Amendment 2015) clause 2(FA)(EE) is taking place in the branches, and , in applicable cases submit STR to AML& CFT Department.
- Consider all foreign exchange transactions as well as electronic transactions during monitoring activities.
-
- While monitoring, take into consideration UN Security Council Resolutions (UNSCRs) and countries which have failed to fulfill international standards of AML & CFT or have significant lacking.
- Apply Enhanced Due Diligence for accounts that are in high risk category.

Bank shall put in place various transactions monitoring scope that includes but not limited to the followings:

- Transactions in local currency i.e. account value, account volume, account velocity, repeat cash deposit, in/out: a large payment into the account is quickly mirrored by more or less equal payment(s)out of the account (potential cross firing or layering), large cash deposit, repeat deposit transaction and large transactions.
- Transactions in foreign currency
- Transaction above the designated threshold

- Transaction in CTR
- On-line transactions
- Transactions that exceed the transaction profiles
- Transactions with possible structuring attempts
- Rule book parameters of Suspicious Activity Module (SAM) will be defined based on transaction above the designated threshold determined by the branch.
- Transactions related with International Trade and remittance.
- Transaction screening against sanction list
- Also monitor blocked account, high account balance, dormant account receives.

9.22 Transaction Monitoring Process

9.22.1 Appropriate monitoring program for the activities and transactions routed through the customer's account to be instituted. Depending on the type and nature of the account branch may fix/set a specific threshold covering the following account activities to identify the client activities that do not appear commensurate with the client's business activities.

- Large Cash transactions including cash deposits & withdrawals on any particular day.
- Large volume credit turnover or month-end credit balance of the same threshold.
- Remittance monitoring.

9.22.2 The branch is to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for Branch to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the Customer. Possible areas to monitor are:

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

9.22.3 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 depending on the amount. Different "floor levels" or limits may be set for different categories of customers.

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

9.22.5 It may not be feasible for some branch or specific branches of having very large number of customers to track every single account against the TP where a risk-based approach is to be taken for monitoring transactions based on use of "Customer Categories" and "Transaction Limits" (individual and aggregate) established within the branch. 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 to be maintained either in the manual ledgers or in computer systems.

9.22.6 On regular basis the branch prepares an exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer based on Anti-Money Laundering and Terrorist Financing risk assessment exercise.

9.22.7 Branch Manager/ BAMLCO/ Operations Officer or other designated Officer reviews 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 documents their review by initial on the report and where necessary prepare internal Suspicious Activity Reports (SARs) with action plans for approval by the relevant Branch Manager and review with the BAMLCO. A copy of the transaction identified will be attached to the SARs.

9.22.8 BAMLCO reviews the SARs and responses from the Operations Officer or other concerned Officer. If the explanation for the exception does not appear reasonable then the Branch Manager will review the transactions prior to considering submitting them to the CAMLCO.

9.22.9 If the BAMLCO believes the transaction should be reported, then the BAMLCO will supply the relevant details to the CAMLCO.

9.22.10 The CAMLCO will investigate any reported accounts and will send a status report to BFIU, Bangladesh Bank on any of the accounts reported. No further action should be taken on the account until notification is received from BFIU, Bangladesh Bank.

9.22.11 For any change in the TP of a customer the Operations Officer is responsible for documenting the reasons why the transaction profile has been changed and will amend the KYC profile accordingly.

9.23 Exception When Opening a Bank Account

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

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

9.24 Subsidiaries and Off-shore Banking Unit (OBU)

- The bank shall ensure compliance of Money Laundering Prevention Act, 2012(including amendments), Anti-Terrorism Act, 2009(including amendments), related rules and instruction issued by BFIU from time to time by all its subsidiaries and branches outside the country.

- The bank shall immediately notify BFIU in case of failure to comply of the above by any of its subsidiaries and branches outside the country.
- All the relevant instructions of this policy guideline shall be applicable to Off-Shore banking unit of the bank.
- CCC-AML & CFTD shall issue necessary instruction in this regard.

Chapter 10: Record Keeping

Record keeping is an essential component for the audit trail because sometimes the Laws & Regulations seek to establish in order to assist in any financial investigation and to ensure the criminal funds.

To comply the Laws & Regulations directives IFIC Bank must retain records concerning customer identification and transactions as evidence of the work because they are undertaken in complying with legal and regulatory obligations as well as for use as evidence in any investigation conducted by law enforcement.

10.1 Legal Obligations

Obligations under MLPA, 2012:

'The reporting organizations shall have to preserve previous records of transactions of any close account for at least 5(five) years from the date of such closure and provide with the information maintained under the clause to Bangladesh Bank.'

Obligations under MLP Rules, 2013:

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

(1) Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;

(2) The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction;

(3) The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order.'

10.2 Obligations under Circular

Obligations under BFIU Master Circular No. 19/2017, dated 17.09.2017:

(1) After the closure of an account, bank must retain the following information and/or documents for at least 5 (five) years:

a) All necessary information/documents of domestic and foreign transactions
b) All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on the customer.
c) All necessary information/documents of a walk-in Customer's transactions.

(2) All documents related to training, seminar, audit, inspection and special inspections on AML & CFT must be retained by the bank.

(3) Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence. Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU."

10.3 Record Keeping

Record keeping is not only law & Regulatory requirement but also it has an objective to ensure that IFIC Bank shall meet its obligations. If any subsequent investigation will arise than Bank can provide the information to the authorities with its sanction of the audit trail.

In this regard IFIC Bank Branch will keep following record:

- Customer information
- Transactions
- Internal and external suspicious reports
- Report from CCC/CAMLCO
- Training and compliance monitoring
- Information about the effectiveness of training

10.4 Customer Information

In relation to the evidence of a customer's identity IFIC Bank shall keep a copy of or the references during the application of CDD measures. The Bank will retain customers' all information after receiving a confirmation of the identification of the certificate from the customer for the evidence purpose. The Bank will often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

IFIC Bank will keep all records 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.

10.5 Transactions

IFIC Bank shall retain all records of all transaction relating to a customer for a period of five years from the date on which the transaction is completed. Transaction records in support of the accounts i.e. credit/debit slip/cheques form for the satisfaction of the audit trail or establish a financial profile of any suspect account or customer these documents are preserved.

10.6 Internal and External Reports

IFIC Bank shall make and retain:

- To fulfill internal and external reporting requirements.
- If the compliance officer has considered information or other material concerning possible money laundering but does not make a report to the CCC/BFIU that record also considered as other material.

In addition, IFIC Bank shall retain copies of any STRs which sent to the BFIU for five years. All internal and external records will retain for five years from the date the report was made.

10.7 Other Measures

IFIC Bank's shall record following:

Related 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.

Related 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.

10.8 Formats and Retrieval of Records

Record keeping is a vital part to satisfy the requirements of the law and to meet the purpose which is capable of retrieval without due delay. But it is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch. In this regard IFIC Bank shall retain the hard copy at a central archive, holding records in electronic form which can be reproduced and recollected without undue delay.

However, IFIC Bank shall keep the record requirements which are the same regardless of the format or the transaction was undertaken by paper or electronic means. Centrally bank shall hold Documents in core banking system which must be capable of differences between the transactions relating to different customers and of identifying where the transaction takes place and in what form.

Chapter 11: Non-Profit Organizations & NGO Sector

Accounts of Charities, Non-Profit Organizations, Non-Government Organizations to be treated as high risk accounts and Enhanced Due Diligence (EDD) will be performed for opening and operating such accounts to prevent money laundering and combating financing of terrorism.

Chapter 12: Guideline on Know Your Customer (KYC) Procedures

12.1 Know Your Customer (KYC)

To comply BFIU , Bangladesh Bank circular No. 19 dated 17.09.2019 the followings must be ensured during customer identification and verification for preventing ML & TF risk:

1. Know Your Customer (KYC) procedures refer to knowing a customer physically and financially. It is legal obligation for the bank to maintain complete and accurate information of its 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, date of birth, profession, source of funds, passport/national identity card/birth registration certificate/acceptable ID card with photo, phone/ mobile number etc.
- 'Accurate' refers to such complete information that has been verified through issuing authority for accuracy & genuineness.

2. Information of individual and entity customers as indicated in the Uniform Account Opening Form shall have to be collected and accuracy of such information has to be verified.

3. The bank must ensure that the person operating an account on behalf of a customer has due authorization to operate the account. Complete and accurate information of the person, operating the account, has to be collected.

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

5. Bank shall collect complete and correct information while serving walk-in customer for services like DD, TT, MT, Pay Order and online transactions.

12.1.1 A KYC policy tailored to the bank's operation:

- Helps detect suspicious activity in a timely manner
- Promotes compliance with all banking laws
- Promotes safe and sound banking practices
- Minimize the risk that the bank will be used for illicit activities
- Reduces the risk of government seizure and forfeiture of a customer's loan collateral when the customer is involved in criminal activity and
- Protects the bank's reputation.

Generally, a branch should never establish a relationship with a customer until it knows the customers true identity. If a potential customer is unwilling to provide the necessary information, the relationship should be reconsidered. However, the unwilling customer shall be impressed upon by the branch

manager to provide such information. If our bank has established a customer relationship, it should be alert for any unusual business transactions.

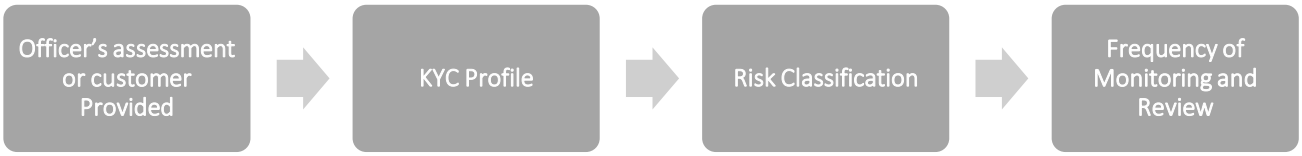
12.1.2 Before opening an account due diligence is required to be performed on all prospective clients. This process should be completed by fulfilling the documentation requirements (Account Application, Bank References, Source of funds and Identification for example) and also a 'Know Your Customer' (KYC) profile which is used to record a client's source of wealth, expected transaction activity at its most basic level.

12.1.3 Once the identification procedures have been completed and the client relationship is established, Branch should monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened. Branch do this firstly by their Officer being diligent, reporting suspicious transactions undertaken by the customer, updating the client's KYC profile for any significant changes in their lifestyle (e.g., change of employment status, increase in net worth) and by monitoring the transaction activity over the client's account on a periodic basis.

12.1.4 KYC profile must contain the basic information about the customer like, Name, Address, phone Numbers, line of business, Annual sales. If the customer is a Public Figure, the account is to be treated as High Risk Account.

12.1.5 The KYC Profile information will also include the observations of the Officer of the Branch when they visit the customer's business place like, the business place is owned or rented, the type of clients visited, by what method is the client paid (cheque or cash). The Officer will record his observations and sign the KYC Profile form.

12.1.6 The KYC Profile leads to Risk Classification of the Account as High/Low Risk.



12.2 Risk Categorization - Based on Activity/KYC Profile:

12.2.1 When opening accounts, the concerned Officer assesses the risk that the accounts may be used for "money laundering" and may classify the accounts as either High Risk or Low Risk. The risk assessment may be made using the KYC Profile Form given in ('Annexure-A') which following seven risk categories are scored:

- Profession/Nature of customer's business
- Monthly Income of the customer
- Mode of opening the account
- Customer's expected monthly transactions (amount)
- Customer's expected monthly transactions (number)
- Customer's expected monthly cash transactions (amount)
- Customer's expected monthly cash transactions (number)

12.2.2 The risk scoring of less than 14 indicates low risk and 14 or more than 14 indicate high risk. The risk assessment scores are to be documented in the KYC Profile Form ('Annexure-A'). However, management may judgmentally override this automatic risk assessment to "Low Risk" if it believes that there are appropriate mitigators to the risk. This override decision must be documented (reasons why) and approved by the Branch Manager, and Branch AML Compliance Officer.

12.2.3 KYC Profiles and Transaction Profiles must be updated ('Annexure-A and B') and re-approved at least annually for "High Risk" accounts as defined above. In case of "Low Risk" transactional account KYC Profiles and Transaction Profiles must be updated ('Annexure-A and B') and re-approved at least once in 5 years. These should, of course, be updated if and when an account is reclassified to "High Risk", or as needed in the event of investigations of suspicious transactions or other concern.

12.2.3 Customer other than Account holder(s): Follow BFIU Circular no. 19 dated 17.09.2017 and IFIC Bank Circular no. 04 dated 10.09.2018 directives meticulously. Walk in Customer Form Annexure-F

Chapter 13: Structuring of Cash Transaction

Structuring is the practice of executing financial transactions such as making bank deposits in a specific pattern, calculated to avoid triggering financial institutions to file reports required by law. Structuring may be done in the context of money laundering, fraud, and other financial crimes. Legal restrictions on structuring are concerned with limiting the size of domestic transactions for individuals.

As per Money Laundering Prevention Act, 2012 (Amendment 2015) clause 2(FA)(EE) & Anti-Terrorism Act, 2009 (Amendment 2012 & 2013) structuring is an offence. If a customer intent to conduct such transaction to avoid reporting requirement is called structuring. Branch officials should be vigilant to detect structuring is taking place in the branches, and in applicable cases, submit STR to AML & CFT Department.

Chapter 14: Quarterly Report to be submitted to The MD's & CEO

As per Bangladesh Bank directives IFIC Bank CAMLCO shall submit report to the MD's & CEO in connection with steps taken by CCC, progress of its implementation and details suggestive report in this regard on Quarterly basis.

Chapter 15: Reporting to BFIU

15.1 Legal Obligations

Obligations under MLPA, 2012

'The reporting organizations shall have to report any suspicious transaction (defined in Section 2(za) of MLPA, 2012 and Section 2(16) of ATA, 2009) to the Bangladesh Bank immediately on its own accord.'

Obligations under MLP Rules, 2013

'Every bank is obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self-assessment, independent testing procedure etc.) to Bangladesh Bank without any delay or in due time. Besides they have to produce any document that is sought by Bangladesh Bank.'

15.2 Suspicious Transaction/Activity Reporting

As per Money Laundering Prevention Act, 2012 (Amendment 2015) 'suspicious transaction' means such transactions –

1) which deviates from usual transactions;
2) of which there is ground to suspect that:
    a. the property is the proceeds of an offence;
    b. it is financing to any terrorist activity, a terrorist group or an individual terrorist;
3) 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.

STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seeming to be usual manner. As STR is a personal & subjective assessment, bank follows the four Stages to identify STR. The stages are given below:

- Identification- of Suspicious transaction/activity
- Investigation- through appropriate questioning investigation
- Evaluation- against previous account transaction/activity
- Disclosure- if doubt/ suspicion, report to BFIU of Bangladesh bank through CCC.

Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is a best tool for mitigating or minimizing the AML & CFT risk because it is the final output of an AML & CFT compliance program. Therefore, it is necessary for the safety and soundness of bank.

15.3 Identification of STR/SAR

Through identifying unusual transaction and activity identification of STR/SAR may be started. STR depends on complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Usually 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(annexure-E)

An unusual transaction in the account of a customer is not necessarily suspicious. As per transaction profile provided by the customer may have unusual periodic transactions. Upon periodic supervising & monitoring transaction the bank determines the qualified STR/SAR and report to the BFIU accordingly. Annexure E provide some red flags indicator identifying STR/SAR related to ML/TF.

All suspicious reported to the AML & CFT Department will be documented or recorded electronically. The report will include full details of the customer and full statements of the information giving rise to the suspicion. All internal enquiries made in relation to the report are to be documented. This information is required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date.

To identify STR/SAR the following chart shows the graphical presentation:

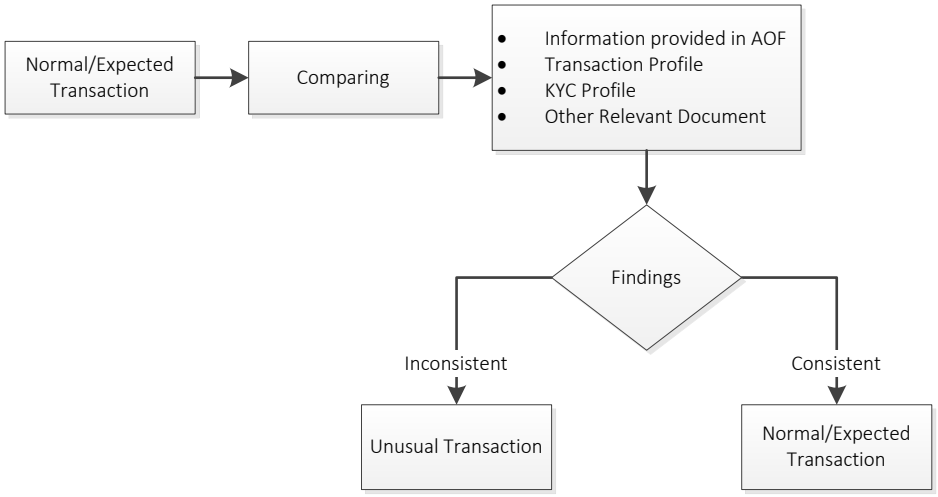


Fig: Identifying STR/SAR

As discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR bank conducts the following 4 stages:

Identification:

The initial stage is identification of STR/SAR which is very vital for reporting. The Bank monitors the unusual transactions which depend on size, need and complexity of the bank manually.

Investigation:

Investigation is the second stage of STR/SAR at branch level, BAMLCO investigates the transaction/activity to identify suspicious by interviewing their customer or through any other means.

Evaluation:

After Investigation of STR/SAR at branch level, BAMLCO evaluates against previous account transaction/activity with the compare of present account transaction/activity to identify suspicious. If BAMLCO is not satisfied, he/she forwards the report to CCC-AML/CFT Department. After receiving report from branch, the CCC-AML& CFT Department checks the sufficiency of the required documents. Every stages of evaluation whether reported to BFIU or not bank keeps records with proper manner.

Disclosure:

This is the final stage and bank submits STR/SAR to BFIU if it still looks suspicious. For simplification, the flow chart given below shows STR/SAR identification and reporting procedures:

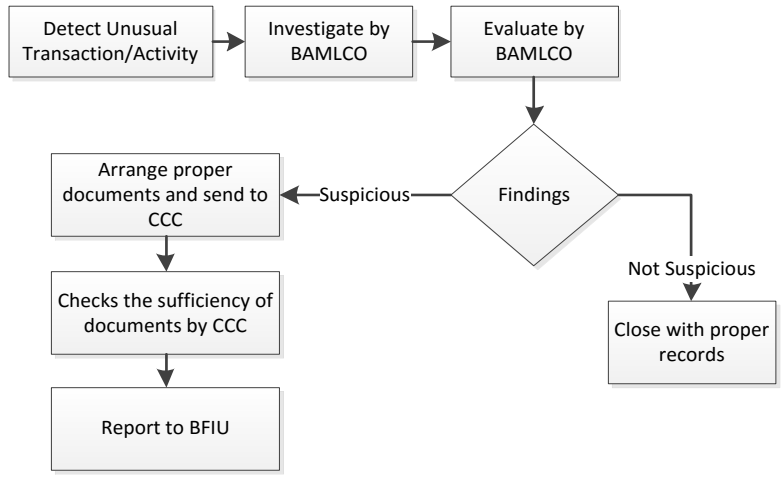


Fig: STR/SAR Reporting

15.4 Tipping Off

- Concerned bank officials must ensure strict confidentiality of the reporting of STR/SAR as soon as they surface or has been reported. Otherwise, this will be considered as a punishable offence under the MLPA, 2012(including amendments).
- Confidentiality of sensitive information sought by BFIU time to time has to be ensured.

IFIC Bank officials will consider the confidentiality of the reporting of STR/SAR. They will make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious.

15.5. Cash Transaction Report (CTR)

Branches will submit monthly Cash Transaction Reporting (CTR) to CCC-AML& CFT Department of Head Office by goAML software.

1. The bank , upon examining the transaction of the earlier month, will report to BFIU through AML & CFT Department , the cash transactions (deposit or withdrawal) of BDT 10 lac or above or equivalent foreign currency; made online ,ATM or any type of cash transactions, on a specific day by one or several transactions.

The following cash transactions are not reportable under CTR:

- ✓ Deposits in accounts maintained by government, semi government, autonomous and government owned entities (however, withdrawals by these entities shall be reportable).
- ✓ Inter-bank and inter branch transactions.

2. The bank shall submit monthly CTR to BFIU within the 21st of the following as per instructions of the goAML manual using the goAML web.

3. If there is no such transaction in branch, the respective branch shall report to AML & CFT Department stating "There is no reportable CTR".
4. While submitting the CTR, the AML & CFT Department shall inform BFIU through goAML message board of such branches by a list.
5. Branch shall generate a report of transactions, reportable under the CTR, and take a print out of the same to examine whether there is/are any suspicious transaction(s) amongst those.
6. If they identify any such suspicious transactions, then the same has to be reported to AML & CFT Department separately as STR/SAR.
7. However, if no suspicious transaction is identified, then the branch shall submit a confirmation letter stating "No suspicious transaction found in reportable CTR".
8. Based on the branch report of suspicious transaction amongst CTR , AML & CFT Department shall submit STR to BFIU separately.
9. However, if certificates stating " No suspicious transaction found in reportable CTR" are received from the branches , then AML & CFT Department shall, while submitting CTR to BFIU, also submit a certificate through goAML message board stating "No suspicious transaction found".

Branch generates monthly Cash Transaction Report (CTR) for threshold amount Tk. 10 lacs & above for goAML Software filing up the mandatory fields within given deadline. CCC-AML & CFT Department on verification & compilation sends XML Cash Transaction Report (CTR) directly to BFIU of Bangladesh Bank using goAML web software as per BFIU Master Circular No. 19/2017, dated 17.09.2017.

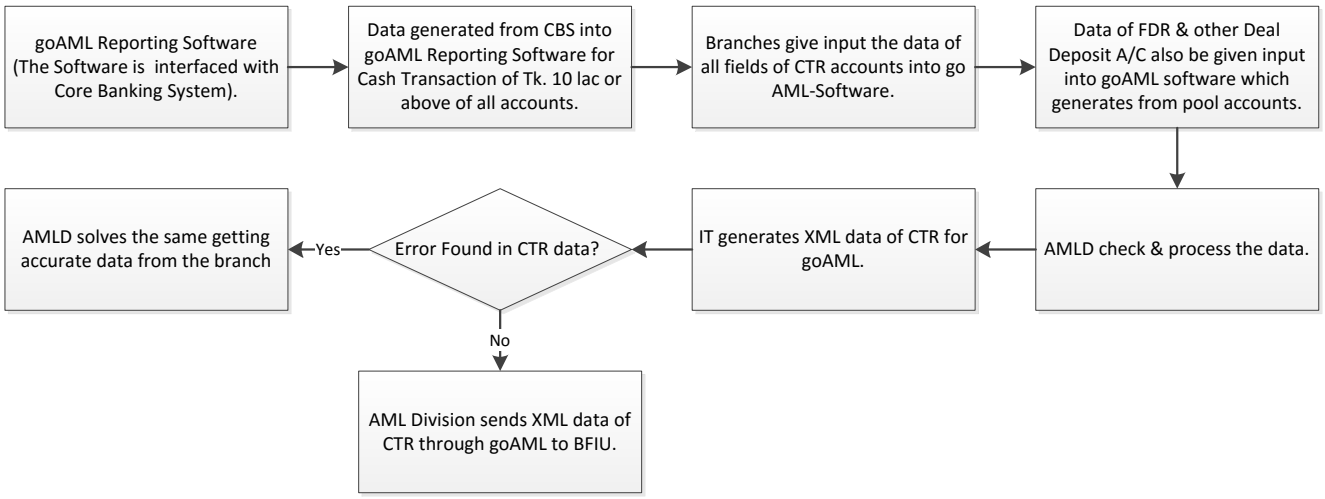


Fig: CTR through goAML Reporting Software

The Bank will ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

15.6 Self-Assessment& Independent Testing

15.6.1 Responsibilities of Branch Regarding Self-Assessment:

All branches should establish self-assessment process that will assess how effectively the branch's anti-money laundering& combating financing of terrorism procedures enable management to identify areas of risk or to assess the need for additional control mechanisms. Branches should follow the following steps to assess itself in a half yearly basis:

- Branches shall assess themselves and prepare a Report on the basis of Self-Assessment Checklist as per BFIU Master Circular No. 19/2017, dated 17.09.2017 issued by BFIU, Bangladesh Bank on a half yearly basis.
- On the basis of such assessment, the branch shall arrange a meeting on monthly basis of all important officials of the branch and to be presided over by the Branch Manager of the branch.
- The meeting shall:
    - Discuss the branch's self-assessment report
    - Identify areas of risk/problem, if any
    - Find out ways or recommendations to mitigate the risk/problem areas and
    - Prepare minutes on self-assessment
- Next meetings shall also discuss:
    - The issues discussed in the previous meeting
    - Assigned responsibilities and
    - Implementation status
- Every branch shall send the following to the CCC-AML& CFT Department and Internal Audit Division of Head Office within the 15th of the next month after completion of each half year:
    - Self-Assessment Report
    - Steps taken by the branch and
    - Recommendations in this regard

15.6.2Responsibilities of ICC'S Regarding Self-Assessment & Independent Testing Procedure

Internal Control & Compliance Division shall perform the following duties:

- The ICC shall analyze the branch Self-Assessment Reports received from the branches and if there is/are any issue(s) that might seem risky to ICC, it shall inspect the branch immediately and inform AML & CFT Department.
- While carrying out inspection/audit activities in various branches according to ICC own yearly inspection/audit schedule, the ICC Division shall examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure (ITP) and prepare reports for each branch after rating those branches.
- In addition to the above, ICCD shall examine the AML & CFT activities of at least 10% of the total branches of the bank using the specified checklists for the Independent Testing Procedure and prepare reports for each branch after rating those branches.
- The ICC shall send a copy of the report with the rating of the branches inspected/audited by them to AML & CFT Department of the Bank.

15.7 Responsibilities of AML & CFT Department regarding Self-Assessment and Independent Testing Procedure:

1) Based on the self-Assessment reports received from branches and inspection/audit report from ICCD, the AML & CFT Department shall prepare, for the half-year period, a checklist based evaluation report on the branches. In that report, among others, the following must be included:

a) Total number of branches and number of self-assessment reports received from branches;

b) The number of branches inspected/audited by ICCD at the time of reporting and the status of branches (branch wise achieved number);

c) Measures taken by AML & CFT Department to prevent similar irregularities that have been observed in maximum number of branches according to the received self-assessment report.

d) The general and special irregularities mentioned in the report submitted by ICC and the measures taken by AML & CFT Department to prevent those irregularities and

e) Measures to improve the rating of the branches that are evaluated as 'Unsatisfactory' or 'Marginal' in the report by ensuring compliance activities.

2) If AML & CFT Department, upon analyzing the branch Self-Assessment Reports received from the branches, identifies any issue(s) that is/are risky, it shall inspect the branch immediately or have the branch inspected by ICCD and will bring this to the notice of the appropriate authority.

AML & CFT Department shall submit the overall Self-Assessment Report of IFIC Bank with comments and recommendations of Managing Director/CEO to the Board of Directors for their perusal.

Finally, CCC-AML& CFT sends the overall Self-Assessment Report of IFIC Bank with comments and recommendations of Board of Directors to BFIU, Bangladesh Bank, Head Office, Dhaka on a half-yearly basis within 60 days after completion of the concerned half- year as per BFIU Master Circular No. 19/2017, dated

17.09.2017.

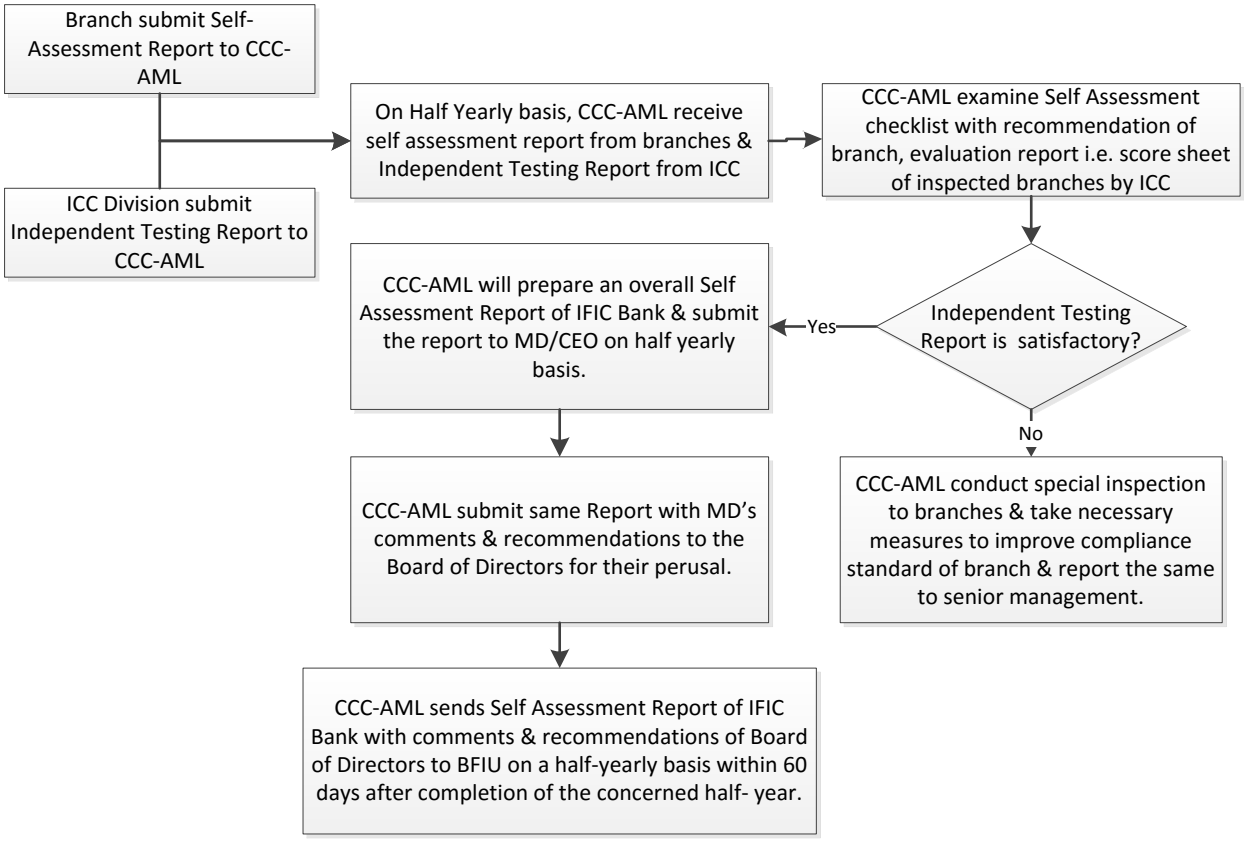


Fig: Self-Assessment Report through CCC-AML

Chapter 16: Responsibilities

IFIC bank establishes clear lines of internal accountability, responsibility and reporting system. The details of the individual responsibilities of the Bank are as under:

Function	Role/ Responsibilities
Account opening Officer	Perform Sanction Screening prior opening any account. Perform due diligence on prospective clients prior to opening any account. Be diligent regarding the identification (s) of account-holder. Ensure all required documentation is completed accordingly. Complete the KYC/CDD Profile for the new customer. Follow BFIU Circular No.19 dated 17.09.2017 instruction regarding PEP/IP account opening & maintaining. Obtain documentary evidence of Identification, profession, source of fund & proof of address. Ensure that all control points are completed prior to allow transactions. Ongoing diligence on transaction trends for clients. Update customer transaction profiles as per BFIU Circular No.19 dated 17.09.2017 instruction. Ensure Update KYC of High & Low Risk Customer as per BFIU Circular No.19 dated 17.09.2017 instruction.
General Banking/Credit Officer/Foreign Trade/Internal Control Unit	Perform AML & CFT risk assessment for the Business. Perform continuous quality assurance on the AML & CFT and Trade Based Money Laundering (TBM) program in the Branch and concerned department/Division.
IT Division of Head Office	Ensure that the required reports and systems are in place to ensure monitoring & maintaining an effective AML & CFT program at Branch and Head Office.
BAMLCO	Ensure to have enough knowledge about acts, rules, regulations, policies & circulars relating to AML & CFT. Ensure to be updated about AML & CFT regulations, national initiatives and share the same with all members of the branch team. Ensure to implement all the directives contained in "Money Laundering Prevention Act, 2012 (Amendment 2015) & Anti-Terrorism Act, 2009 (Amendment 2012 & 2013), AML/CFT Policy in line with any change/revision, Circulars/Circulars letters and different letters issued by HO & Circulars/Circulars letters and different letters issued by BB & BFIU and MD's clear message at the Branch level comprehensively. Ensure the customer's identity and underlying purpose of establishing relationship with the bank and collect adequate information and documentation as per IFIC —Customer Acceptance Policy-2013(amendment-2018). Ensure to identify & verify the identity of the customer based on data, information & documents obtained from reliable and independent source.

	Ensure to obtain correct and accurate information of customer in the Uniform AOF, KYC & TP and input all data of KYC & TP in the Misys System on regular basis. All information/documents for opening of Account have been obtained and verified. Ensure the screening of different sanction list and domestic sanction list checked properly before opening of account and while making any international/foreign transaction. Sanction screening records (False Positive) keep with AOF. Ensure to 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/Head Office AML instruction. Confirmation Legacy accounts are marked as Dormant. Ensure regular transaction monitoring to find out any unusual transaction in an effective way. The transaction should be examined at the end of day against transaction profile. TP matched with profession & income. Actual Transaction whether verified with Declared TP. Records of all transaction monitoring should be kept in the file. Check correctly CTR reporting done on monthly basis. Ensure to review cash transaction to find out any STR/SAR. Preserve CTR copy and check regularly. Ensure to review of Structuring to find out any STR/SAR. Check whether system to identify STR/SAR is active. Also check whether all officers have proper knowledge for reporting and identifying STR/SAR. Ensure all the employees of branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction or unusual customer behavior. Ensure to perform the self-assessment on AML & CFT compliance position to evaluate the branch on a half yearly basis and arrange meeting with concerned officials before finalizing the evaluation report to solve the problem as identified at branch level without any delay. Accumulate training records of all branch officials of your branch and take initiatives including reporting to CCC, HR and training academy. Ensure that all officers have taken 01(one) day training on AML & CFT knowledge and aware of it. Ensure all the required information and document i.e. monthly and quarterly are submitted properly to CCC 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 your branch with the involved person if so BAMLCO make an STR/SAR and send the same to AML & CFT department without any delay. Ensure branch is maintaining AML & CFT files properly and record keeping is done as per our Money Laundering & Terrorist Financing Risk Management Guideline requirements.

	Ensure that corrective actions have been taken by your branch to address &rectify the deficiency identified by the BFIU or BB or ICC. Whether all audit objection are implemented & complied. Take approval from CAMLCO while opening PEP's/IP's account and ensure enhanced due diligence as per BFIU Master Circular No# 19 date 17.09.2017. PEPs/IPs accounts are monitored as per BFIU Circular. Selection of customer/opening of Account/ services based on AML & CFT Risk Management Guideline. Ensure to risk categorization of the customer as per Uniform AOF, KYC & TP & keep the list of High Risk Customers as well as Enhanced Due Diligence to be applied and monitor transaction of the same customer. Ensuring the compliance of AML/CFT issues at Branch level in order to manage and control Money Laundering & Terrorist financing risks and also develop strong interpersonal relationship with the customers to develop customers' awareness regarding AML/CFT issues. Ensure to update and review AOF, KYC & TP from time to time as per BFIU circular and keep the relevant records with AOF. Ensure to retain the records of customer information and transactions at least for five(05) years after termination of relationship with customer Ensure to obtain information/documents/short KYC of depositor(s) and withdrawer(s) for walk-in/online customer (other than account holder) as per instructions mentioned in BFIU circular 19 dated 17.09.2017. Ensure to obtain Positive Pay instruction in case of all corporate/proprietorship firm customer for BDT.1 (one) lac or above and for individual account BDT.5 (five) lac or above and keep record of the same as per Bangladesh Bank instruction. Ensure to verify the address of the customer by sending thanks letter both account holder & introducer and keep the record of sending receipt with acknowledgement receipt from post office or POD from Courier with AOF. Ensure to obtain and verify the required identification documents with photos of customers and nominees. Ensure to obtain and verify documents related to profession of the customer. Ensure to obtain and verify documents related to source of funds and TP has been matched properly. Inward & Outward remittance monitored or not. Details of walk-in/one-off customers in respect of PO/Foreign Remittance, wire transfer and others must be obtained by the branches. Ensure that preventive measures has been taken by the branch to prevent Money Laundering & Terrorist Financing for foreign & local trade financing. Ensure to identify Beneficiary owner of the account, obtain complete and accurate information of beneficial owner and complete KYC. Ensure proper risk grading of customer in line with occupation, income and transaction profile (TP) and consider the risk score in branch risk register and risk rating of beneficial owner during risk grading.

	Ensure to arrange AML & CFT meeting with concern officials of the branch on monthly basis by issuing notice of the meeting and to take effective measures as per BFIU instruction. Ensure to monitor the staff of the branch team to check whether any of them are directly or indirectly involved in or is facilitating Money Laundering & Terrorist Financing.
Branch Manager	Ensure that the AML & CFT program is effective within the Branch. Ensure that BAMLCO is effectively performing his/her duties within the Branch. Overall responsibility to ensure that the Branch has an AML & CFT program in place and that it is working effectively.
Deputy CAMLCO	Ensure that decisions taken by CCC are timely implemented and, if applicable, disseminated to relevant parties. Oversee the day to day activities of the AML & CFT Department. Ensure activities of the AML & CFT Department are aligned with AML & CFT strategies. Ensure implementation of annual AML & CFT program which includes, but not limited to- Annual training/workshop plan Annual inspection plan Off-site monitoring Timely review of existing possesses Ensure that all out support is extended to the CAMLCO to enable him in discharging his duties Extending support to the CCC for smooth functioning of the committee Coordinate with various committees related to AML & CFT issues Ensure compliance of BFIU instructions Ensure timely submission of information sought by regulators/competent authorities Maintain liaison with regulatory authorities Ensure timely submission of statement/report to CCC and/or management.
AML & CFT Department	Ensure implementation of annual "AML & CFT Compliance Program" Implement the bank's policy, procedure and strategies in prevention ML, TF & PF designed by CCC Issue circulars/instructions to branches as guided by CCC Coordinate the ML, TF and MFS risk assessment of the Bank and review thereon. Present the compliance status with recommendations before CCC Submit CTR and STR/SAR to BFIU Report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner Impart training, workshop, seminar related to AML & CFT for the employee of the Bank Take required measures to submit information, report or documents to internal and external stakeholders in time.

Central Compliance Committee(CCC)	Review & update AML (Anti Money Laundering) & CFT (Combating Financing of Terrorism) Policies, Procedures, Guidelines, Circulars and Strategies, implementation & enforcement thereof as well as review and update Customer Acceptance Policy (CAP). Coordinate the Bank's ML (Money Laundering) & TF (Terrorist Financing) and compliance initiatives. Coordinate the ML, TF and MFS risk assessment of the Bank and review thereon. Undertake organizational strategy and program regarding internal control policies and procedures to prevent money laundering and terrorist financing activities and will update the same from time to time. Advise and guide "AML & CFT Department" to issue instruction circulars to the branch regarding the procedure of customer identification, transaction monitoring and internal control mechanism etc. to prevent money laundering and terrorist financing Present the compliance status with recommendations before the Chief Executive Officer or Managing Director on quarterly/half yearly basis on AML & CFT. Forward STR (Suspicious Transaction Report)/ SAR (Suspicious Activity Report) and CTR (Cash Transaction Report) to BFIU in time and in proper manner. Report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner. Impart training, workshop, seminar related to AML & CFT for the employee of the Bank. Take required measures to submit information, report or documents in time. Supervise/Review of internal, external, Bangladesh Bank audit report and BFIU's inspection report on Branches and yearly system check inspection report on Head Office on AML/CFT issues and monitor for regularization of the irregularities detected by them. Conduct inspection, checking of records/papers/documents at Branches and MFS as required under Prevention of Money Laundering & Combating Financing of Terrorism and ensure compliance of the same on regular basis. Implement and update of WLC (Watch List Checking) software in live and ensure screening of WLC software in all levels. Disposal of files related to Correspondent Banks/ Relationship Management Application (RMA) on AML/CFT Issues. Implement screening of all types of remittance (inward and outward) and all Customers, Agents and Distributors related to MFS and foreign exchange business. Ensure Screening Mechanism during recruitment of new employee to avoid AML/CFT risk.
CAMLCO	Overall Supervision & Management of the Department. Implementation, enforcement and review of AML/CFT policies, Procedures, Guidelines & Measures. Submit periodical Reports to BFIU & Managing Director of the Bank.

	Placing of Memo to Board of Directors on different regulatory issues related to AML & CFT. Conduct Seminar/Training of AML & CFT issues at IFIC Bank Training Academy as well as outside of the Dhaka city. Shall remain free from undue influence/intervention from anyone in discharging responsibilities as CAMLCO. Send STR/SAR and any document or information to BFIU without any permission or consultation from MD/CEO as CAMLCO. None shall deny access to any information of the Bank and if any one disregards her/his instructions he/she will face disciplinary action. He is liable to MD for proper functioning of CCC. Ensure to monitor, review and coordinate application and enforcement of the bank's compliance policies including AML/CFT Compliance Policy. This will include – an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity and a written AML/CFT training plan. Ensure to monitor changes of laws/regulations and directives of Bangladesh Bank and revise its internal policies accordingly. Ensure to respond to compliance questions and concerns of the staff and advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk. Ensure to the bank's AML/CFT policy is complete and up-to-date, to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered by the bank. Ensure to develop the compliance knowledge of all staff especially the compliance personnel and conduct training courses in the institution in this regard. Ensure to develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues. Ensure to assist in review of control procedures in the bank's, to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses. Ensure to monitor the business through self-testing for AML/CFT compliance and take any required corrective action. Ensure to manage the STR/SAR process and maintain confidentiality. Ensure to review transactions referred by divisional, regional, branch or unit compliance officers as suspicious. Ensure to review the transaction monitoring reports (directly or together with account management personnel). Ensuring that internal Suspicious Activity Reports (SARs): are prepared when appropriate

	reflect the uniform standard for "suspicious activity involving possible money laundering or terrorist financing" established in its policy are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy are advised to other branches of the institution who are known to have a relationship with the customer are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk. Ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager. Ensure to maintain a review and follow up process that planned corrective action, including possible termination of an account, be taken in a timely manner. Ensure to manage the process for reporting suspicious activity to BFIU after appropriate internal consultation. Any other works as & when assigned by the Managing Director.
Chief Executive Officer (CEO)/ MD	Overall responsibility to ensure that our Bank has an AML & CFT program in place and that it is working effectively.

Non-compliance of the 'Money Laundering & Terrorist Financing Risk Management Guidelines' by the responsible official will be seriously viewed by the Management.

Chapter 17: Internal Control

17.1 Recruitment, Training and Awareness

Obligations under BFIU Master Circular No. 19/2017, dated 17.09.2017

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

17.1.1 Recruitment

With a view to mitigating ML, TF and PF, bank shall consider the following while recruiting employees:

a) Shall follow appropriate screening mechanism prior recruitment.
b) Shall deploy adequate number of skilled employees to the AML & CFT Department

Employee Screening

In absence of proper risk mitigating measures ML & TF risk may arise from customers as well as employees. As per HR policy IFIC bank will follow fair recruitment procedures for minimizing ML & TF risk arise by or through its employees. This fair recruitment procedure not only includes implementation of fairness in judging publicly declared competitive recruitment but also includes the judgment of good character. In this regard, the bank's HR policy will follow background check i.e. each & every educational certificate and other documents of the employee.

IFIC bank will examine the consistency and capability of their employee and ensures their employee that has necessary training on AML & CFT lessons for the particular job or desk before assigning an employee.

17.1.2 Know Your Employee (KYE)

- IFIC bank shall take essential precaution for their customers as well as employees because a lot of incidents occur with the involvement of employees and customers in fraudulent transactions. Therefore, the bank will focus 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.
- Before assigning an employee in a particular job or desk, HR shall examine the consistency and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.
- The bank auditors will be conversant with these and other requirements and follow up that they are constantly and uniformly updated. KYE requirements are included in the HR policy.

17.1.3. Training and Awareness

The senior management of the Bank will raise awareness on Money Laundering & Terrorist Financing and shall train Banks Officials for recognition of suspicious transactions/suspicious activities, the requirement of applicable rules and regulations, Banks Policy and Standards on the prevention of money laundering & terrorist financing and the procedures and control in each jurisdiction. As senior management responsibility, the Bank will pursue a training program consisting of various modules as shown at Annexure G.

- **The Need for Employees Awareness**

All employees of the Bank must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All employees must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities.

It is, therefore, important that the Bank will introduce comprehensive measures to ensure that all employees and contractually appointed agents are fully aware of their responsibilities.

- **Education and Training Programs**

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

- **New Employees**

New employee of the Bank will be provided training on Prevention of Money Laundering, Combating Financing of Terrorism and Regulatory requirement in their foundation course.

- **Refresher Training**

Bank will arrange refresher training for its employees to make them update with Anti- Money Laundering laws, Combating Financing of Terrorism and regulatory requirement.

- **In House Discussion**

Branch will arrange in house discussion on regular basis to update the employees of the Branch on Prevention of Money Laundering laws, Combating Financing of Terrorism, Circulars issued by BFIU, Bangladesh Bank and Head Office from time to time.

- **Training Records**

That the Bank can demonstrate that it has complied with the regulations concerning employees training, it will maintain records which include:

Head Office Level:

(i) Details of the content of the training programs provided
(ii) The names of employees who have received the training
(iii) The date on which the training was delivered
(iv) The results of testing carried out to measure employees understanding of the money laundering requirements and
(v) An on-going training plan.

Branch level:

(i) Details of the content of the training programs provided
(ii) The names of employees who have received the training
(iii) The date on which the training was delivered

The Bank will continue to devote considerable resource to establish and maintain employees' awareness of the risks of money laundering and terrorism financing, and their competence to identify and report relevant suspicions in this area. The Bank is dedicated to a continuous program of increasing awareness and training of employees' at all appropriate levels in relation to their knowledge and understanding of AML/CFT issues, their respective responsibilities and the various controls and procedures introduced by the Bank to deter money laundering and financing of terrorism.

17.1.4 Awareness of Senior Management

The members of the senior management of the bank will be a part of AML, TF & PF training program because without proper concern and awareness of senior management it is difficult to have effective implementation of AML/CFT measures in the bank. IFIC bank shall arrange awareness program at least once a year for all the members of its board of directors and senior management of the bank. The activities of ML & TF of the Bank will be escalated to the senior Management & to the Board of Directors for their perusal and comments.

17.1.5 Customer Awareness

With a view to increasing awareness amongst the customer regarding prevention of ML, TF and PF, bank shall undertake the following:

1. Inform the prospective customers about the logic behind the information and the documents sought at the time of account opening.
2. Continue distributing leaflet to the customers for creating awareness.
3. Display poster at Branch's visible places for creating awareness.

Beside, to create customers' awareness the bank shall take proper actions for broadcasting awareness building advertisement and documentaries regarding prevention of money laundering and terrorist financing through different mass digital & print media.

17.1.6. Awareness of Mass People

Prevention of ML & TF widely depends on awareness at all level. Public or mass people awareness on AML & CFT measures provides synergies to bank in implementing the regulatory requirement. For creating public awareness on AML & CFT issues when BFIU, BB, other regulators as well as the government arrange programs IFIC bank shall participate in the said program. The bank will encourage arranging public awareness programs like advertisements through billboard, poster, festoon and mass digital & print media, distribution of handbills, leaflet and so on.

17.2 Development of Software Profile System

In order to facilitate detection of money laundering & terrorist financing, our Bank has developed equation functions of Core Banking system which is used capturing KYC & TP information. IT Division has introduced an equation function to monitor High Risk Customers of Bank. Bank has implemented Suspicious Activity Module (SAM) Software integrated with our CBS for monitoring suspicious transactions of customers based on different rules. Bank has also developed Structuring Monitoring Report management software to detect suspicious transactions. Moreover, Bank has introduced an automated screening mechanism of UNSCRs & Local banned list named Watch List Check (WLC) Software that is used to detect any listed individuals or entities prior to establish any relationship with the bank. Classifying customers on the basis of the risk matrix provided by BFIU, Bangladesh Bank under new KYC Profile & TP has been incorporated in our CBS and IT

Division will develop the automated systems for detecting & monitoring suspicious transactions with the transaction profile provided by the customers as well as Threshold Based transaction Monitoring system. The Bank is already using goAML software that is used for Cash Transaction Report & Suspicious Transaction/Activity Report. These new systems will improve our ability to detect unusual transactions, screen the customers with listed individuals or entities & help the authorities to identify and respond to new money laundering & terrorist financing techniques.

17.3 Branch Managers Certifications

Each Branch Manager shall certify that he/she maintains customer profiling applying due diligence KYC. The Branch Manager will further certify that all Officers and Members of the Branch are aware of Money Laundering Prevention Act, 2012 (Amendment 2015), Anti-Terrorism Act, 2009 (Amendment 2012 & 2013), Bank standards of best practice, BFIU, Bangladesh Bank Circulars/ Guidelines and Head Office Circulars/ Instructions issued from time to time and necessary care taken for following them meticulously. The Branch Manager will also certify that he/she and his/her members of the Officials have read and understood the 'Money Laundering & Terrorist Financing Risk Management Guideline as well as Customer Acceptance Policy-2013(2018)' issued from Head Office and standards of best practice with 'Know Your Customer' (KYC) procedures.

Chapter 18: Prevention of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction

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.

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

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

Situations indicating possible proliferation financing activities is in Annexure-D.

18.1 Legal Obligations

Obligations under ATA, 2009

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

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

18.2 Obligations Under Circular

Obligations under BFIU Master Circular No. 19/2017, dated 17.09.2017

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

(2) As soon as any news is published in the public media regarding financing of terrorism and financing of proliferation of weapons of mass destruction, banks must send all relevant information in detail to BFIU if any account is being maintained by any individual or entity involved with it.

(3) Every bank must electronically preserve updated information of the individuals and entities listed in the UNSCR and blacklisted by Bangladesh Government suspected to be involved with terrorism, terrorism financing and financing of proliferation of weapons of mass destruction.

(4) Before any international business transaction, bank will review the transaction to identify whether the concerned parties of that transactions are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or proscribed by Bangladesh government. Immediately after the identification of any account of any listed individual or entity concerned bank will stop that transaction and inform BFIU the detail information at the following working day.

18.3 Necessity of Funds by Terrorist

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

18.4 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.

18.5 Movement of Terrorist FUND

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

- The use of the financial system
- The physical movement of money for example through the use of cash couriers and
- The International trade system

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

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.

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.

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.

Use of Alternative Remittance Systems (ARS)

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

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 traveling 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.

18.6 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. Most of the countries agree that better targeting of such measures on the individuals responsible for the policies condemned by the international community and the elites who benefit from and support them would increase the effectiveness of sanctions while minimizing the negative impact on the civilian population. The considerable interest in the development of targeted sanctions regimes has focused primarily on financial sanctions travel and aviation bans and embargoes on specific commodities such as arms or diamonds.

Targeted financial sanctions entail the use of financial instruments and institutions to apply coercive pressure on transgressing parties—senior officials, elites who support them or members of non-governmental entities—

in an effort to change or restrict their behavior. Sanctions are targeted in the sense that they apply only to a subset of the population—usually the leadership, responsible elites or operationally responsible individuals; they are financial in that they involve the use of financial instruments such as asset freezing, blocking of financial transactions or financial services; and they are sanctions in that they are coercive measures applied to effect change or constrain action.

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

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 named Watch List Checking (WLC) has been developed in Anti-terrorism Rules, 2013. Under rule 16 of AT rules, 2013, as a reporting agency our bank has to maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. In case there is any fund or economic resources held by the listed individuals and entities, our bank immediately stops 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.

18.7 An Automated Screening Mechanism of UNSCRs

For effective implementation of TFS relating to TF & PF IFIC bank will develop an automated screening mechanism named 'Watch List Check' Software provided by Misys International Banking Systems Ltd. This enhancement enables bank to set up and manage a 'watch list'. The list enables Bank to check customers when they are added or maintained and also to identify individuals, companies or other entities that on the watch list when they are making or receiving payments in order to comply with International and regional regulations. This software permits intelligent matching of the text of an inward or outward payment message or the name and address of a customer, against a list of proscribed entities provided by a national or international agency. When OFAC-Agent Server (WLC) finds a possible match, a 'case' is created in Equation. After a decision has been made on the case, the transaction in Equation that prompted the case is then either cancelled or released.

In a word, bank will ensure that screening done before-

Customer

- Customer is added, maintained, cancelled/deletion
- Addresses added or maintained
- Account opening
- Add Loans & Making new payments

Deal

- Deals added, maintained, cancelled
- FX/MM Deals added
- Add & Withdraw/Close Retail Deposits
- Deal settlements maintenance
- Deal Authorization

Clean Payment

- Inward Clean payment added/maintained
- Inward Clean payment Reviewed
- Inward clean payment authorized
- Outward Clean payment added/maintained
- Outward Clean payment Reviewed
- Outward Clean payment authorized

For successful implementation of UN sanction list, IFIC bank official shall adequate 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

18.8 Role of IFIC Banks in Preventing Terrorist Financing & Proliferation Finance

- The Bank will establish an effective 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& has issued instructions about the duties of Bank officials, review those instruction time to time and ensure the compliance with the instructions issued by BFIU. Implementation of SAM & Watch List Check in IFIC bank is part of this procedure.
- The Bank will take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions. In this context the bank will implement Suspicious Activity Module (SAM) software by which suspicious transaction is identified, the Bank will send spontaneously reports it to BFIU, Bangladesh Bank without any delay.
- If the Bank will find any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media then bank will always send the details of the accounts of any persons who will engaged in those activities to BFIU without any delay.
- Effective implementation of TFS relating to TF & PF the bank will develop an automated screening mechanism named 'Watch List Check' Software provided by Misys International Banking Systems Ltd. This enhancement enables bank to set up and manage a 'watch list'. The list enables Bank to check customers when they are added or maintained and also to identify individuals, companies or other entities that on the watch list when they are making or receiving payments, in order to comply with

International and regional regulations Bank runs regular check on the given parameters, including transactional review to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.

- The Bank will run a regular check on the given parameters based on transaction review by SAM & WLC software to verify whether individuals or entities listed or scheduled under the ATA, 2009(amended-2012, 2013) individuals or entities owned or controlled directly or indirectly by such persons or entities as well as persons and entities acting on behalf of or at the direction of, individuals or entities listed or scheduled under the Act are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.
- The bank shall preserve the records of false positives.
- The bank shall maintain electronically, and update the list of individuals or entity banned under different resolutions if UNSC and by the government of the country.

Duties of Bank Officials for detection and prevention of Financing of Terrorism and Financing in proliferation of Weapons of Mass Destruction:

Bank shall establish clear lines of internal accountability, responsibility and reporting system. Duties and responsibilities of the bank officials/divisions/departments in detecting and preventing financing of terrorism and financing in proliferation of weapons of mass destruction are detailed as under:

Individuals bank officials/ divisions/departments	Roles/Responsibilities
Account Opening Officer	a) Obtain complete and accurate information of the customer; b) Identify the purpose of opening account; c) Be confirmed regarding the identification of the customer; d) Appraise the customer as per Customer Acceptance Policy, 2013(amendment-2018); e) Perform screening of customer information against different sanction list, adverse media list and entities banned by Bangladesh Govt. before opening account; f) Complete KYC.
Operations Officer	a) Ensure that proper verification of documents is completed prior to allowing transaction in the account; b) Keep transactions of customer under monitoring with the support of available tools in CBS; c) Inquire customer regarding any transaction not consistent with his/her/their profile(s) and preserve the record; d) Review transaction profile(TP) and KYC profile and update the same as required as BFIU instructions.

Teller	a) Obtain document(s) in support of identity of the non-account holder customer while receiving or paying cash including online transaction; b) Complete Short KYC of the customer in applicable case; c) Obtain source of large cash deposits and preserve record of the same; d) Perform call back process; e) Make query to the account holder in case of TP exceeds and record the same.
Credit /Foreign Exchange/SME officials of the Branch	a) Perform risk assessment of customer's business with respect to terrorist financing(TF) and Proliferation Financing(PF) in weapons of mass destructions; b) Appraise the customer based on IFIC ML & TF Risk Management Guideline and take action accordingly;
Credit /Foreign Exchange/SME officials of the Branch	c) Perform screening of customer information against different sanction list, adverse media list and entities banned by Bangladesh Govt.; d) Ensure implementation of instructions issued by BFIU and Head Office to combat TF & PF.
Branch Manager/BAMLCO	a) Be familiar with laws, regulations, policies, guidelines relating to combating TF & PF; b) Ensure screening of customer information against different sanction list, adverse media list and entities banned by Bangladesh Govt.; c) Perform and supervise sanction screening and transaction monitoring process; d) Ensure training to branch employees on combating TF & PF; e) Follow the media report on terrorism, terrorist financing or other offence, and if any relationship of the branch with the involved person is found, make an STR/SAR , as applicable; f) Ensure that branch has an effective program in place to combat TF & PF.
International Business Division	a) Ensure that the applicant and beneficiary of foreign trade are not involved in TF & PF; b) Perform screening of all relevant parties including vessel and port information against different sanction list, adverse media list and entities banned by Bangladesh Govt.; c) Appraise the customer based on IFIC ML & TF Risk Management Guideline and take action accordingly.
Remittance payment officer at Branch	a) Obtain information of remitter/sender; b) Complete Short KYC of the customer; c) Perform screening of remitter/sender information against different sanction list, adverse media list and entities banned by Bangladesh Govt.

IT Division	a) Develop system and monitoring tools so that terrorist financier and party(ies) involved in proliferation financing of weapons of mass destruction can be detected/identified; b) Ensure that the system will generate report required by BFIU and AML & CFT Department from time to time; c) Update the system in line with the internal and regulatory requirements.
IFIC Treasury Department	a) Treasury Department will not release remittance fund suspected to be in the sanction list until receipt of confirmation/clearance from the concerned office/division/department
IFIC Credit Risk Management Division	a) Ensure that the borrowers are not involved in terrorist financing and proliferation financing of weapons of mass destruction; b) Perform screening of borrower information against different sanction list, adverse media list and entities banned by Bangladesh Govt.; c) Perform risk assessment of customer's business with respect to TF & PF in weapons of mass destruction; d) Appraise the customer based on IFIC Money Laundering and Terrorist Financing Risk Management Guideline and take action accordingly.
Card Division	a) Ensure customer due diligence while issuing cards and monitoring transactions; b) Perform screening of customer information against different sanction list, adverse media list and entities banned by Bangladesh Govt.; c) Perform risk assessment of customer's business with respect to Terrorist Financing & Proliferation Financing in weapons of mass destruction; d) Appraise the customer based on IFIC Money Laundering and Terrorist Financing Risk Management Guideline and take action accordingly.

IFIC Internal Control & Compliance Division	a) Be familiar with laws, regulations, policies, guidelines relating to combating TF & PF; b) Check the implementation status of combating TF & PF at branch level as well as Head Office level; c) Comply with the instructions of BFIU.
Central Compliance Committee(CCC)	a) Oversee implementation of BFIU guidelines, circulars, instructions and policy of the Bank.
CAMLCO	a) Ensure that bank has an effective system in place to combat TF & PF; b) Take necessary initiatives to ensure compliance with the policy guideline with respect to combating TF & PF.
AML & CFT Department	a) Implement strategy and annual program to combat TF & PF in the bank; b) Monitor bank activities in line with BFIU guidelines, circulars, instructions and policy of the bank.
MD & CEO	a) Share commitment of senior management towards the fight against TF & PF with all the employees of the bank; b) Extend necessary support and guidance in implementing the policy guideline with respect to combating TF & PF; c) Review the performance of the bank in terms of combating TF & PF and provide suggestions accordingly.

All the employees of the bank shall remain vigilant to ensure that bank is not used by terrorist financer and proliferation financer of weapons of mass destructions.

18.9 Flow-Chart for Implementation of TFS by Banks

Sources of Sanction List
(a) UN, OFAC, EU, HMT etc.
(b)Domestic sanction list from BFIU

Run a regular check including transactional review-
- ✓ Before any foreign/domestic transactions
- ✓ Before opening of any account

If any match found → **Stop proceeding & Report to BFIU**

Flow-Chart for Implementation of TFS by IFIC Bank

- Watch List Check
- OFAC Agent Server
- Rules (False Positive Hits)
- Algorithms
- Sanction Lists
- Equation Data
- Resource File

Sources of Sanction List
(a) UN, OFAC, EU, HMT etc. from website.
(b)Domestic sanction list from BFIU website.

Equation Data
Core Banking System

Filter Process

Run a regular check including transactional review-
- Before any foreign/ domestic transaction
- Before opening of any account

If any match found → **Stop proceeding & Report to BFIU**

If a suspected match is found. The transaction is accepted and placed on the database. But it will not yet be authorized.

An entry will be placed on the Case Manager Queue for the compliance officer to review.

Once reviewed by the compliance officer, the transaction is either authorized or sent for further investigation.

The transaction may be viewed but it cannot be amended. Authorized or cancelled until reviewed by the compliance officer.

The compliance officer must the relevant authorities of positive matches.

A full audit trail is kept of both approved and rejected transactions.

Schedule-1, Schedule-2 & Schedule-3 included in the Anti-Terrorism Act, 2009 to be followed for Combating Financing of Terrorism which is annexed in this policy:

Schedule-1

[See clause (3A) of section 2]

(a) Convention for the suppression of unlawful seizure of Aircraft done at The Hague on 16th December, 1970;

(b) Convention for the suppression of unlawful acts against the safety of civil aviation, done at Montreal on 23rd September, 1971;

(c) Convention on the prevention and punishment of Crimes against internationally protected person, including diplomatic agents, adopted by the General Assembly of the United Nations on 14th December, 1973;

(d) International convention against the taking of hostages adopted by the General Assembly of the United Nations on 17th December, 1979;

(e) Convention on the physical protection of nuclear material, adopted at Vienna on 3rd March, 1980;

(f) Protocol for the suppression of unlawful acts of violence at airports serving International Civil Aviation, supplementary to the convention for the suppression of unlawful acts against the safety Of Civil Aviation, done at Montreal on 24th February, 1988;

(g) Convention for the suppression of unlawful acts against the safety of maritime navigation, done At Rome on 10th March, 1988;

(h) Protocol for the suppression of unlawful acts against the safety of fixed platforms located on the Continental shelf, done at Rome on 10th March, 1988;

(i) International convention for the suppression of terrorist bombings, adopted by the General Assembly of the United Nations on 15th December, 1997.

Schedule-2
(See section 18)

1	2	3	4	5
Serial No.	**Name of the entities**	**Address of the entities**	**Date of proscription**	**Remarks**
01.	Shahadat-e-Al Hikma party Bangladesh	House of Mizanur Rahman, Horogram natunpara bypass road, P.S. Rajpara, RMP, Rajshahi	09-02-2003	
02.	Jagrata Muslim Janata Bangladesh (JMJB)	No specific address	23-02-2005	
03.	Jamatul Mujahedin	No specific address	23-02-2005	
04.	Harkatul Jehad Al Islami	No specific address	17-10-2005	
05.	Hizbut Tahrir Bangladesh	H.M. Siddique Manson, 55/A, Purana Palton, Dhaka and 201/C, Palton Tower (3rd Floor), 27 Purana Palton Lane	22-10-2009	
06.	Ansarullah Bangla Team(ABT)	-	-	
07.	New Ansar Al Islam	-	-	

Schedule-3
(See section 18)

1	2	3	4	5
Serial No.	**Name of the entities**	**Address of the entities**	**Date of proscription**	**Remarks**

Annexure A: Know Your Customer (KYC) Profile Form

IFIC BANK

IFIC 40 years of Matured Dynamism

KYC PROFILE FORM-INDIVIDUAL

To be filled by Bank only

_____ Branch Date d d m m y y y y

1. Name of Account:
2. Type of Account:
3. Customer ID:
4. Account No.: -
5. Profession of customer (details):
6. Monthly probable income:
7. Source of fund(s) in details:
8. i) Document(s) collected against source of fund: a) _____ b) _____ c) _____
   ii) Collected document(s) verified- ☐ Yes ☐ No
9. Has actual Beneficiary owner been selected? ☐ Yes ☐ No ☐ Not applicable
   (If yes, fill up the personal information form for each of Beneficial owner.)
10. Customer Identification:

Sl. No.	KYC Supporting Document Number (Where applicable)	Whether photocopy obtained?		Whether Supporting Document Verified?	
a.	Passport Number:	Yes	No	Yes	No
b.	National ID :	Yes	No	Yes	No
c.	Birth Reg. Certificate :	Yes	No	Yes	No
d.	E-TIN Number :	Yes	No	Yes	No
e.	Driving License Number:	Yes	No	Yes	No
f.	Others				

11. Reasons for opening of Account of Non-residents and Foreigners:
    অনিবাসী (Non-resident) এবং বিদেশীদের ক্ষেত্রে হিসাব খোলার উদ্দেশ্যঃ

    a) Type of Visa (Resident/ Work):_____ Validity: _____

    b) Have Work Permit Letter & Permission Letter from competent authority been obtained in case of account opening of Work Permit Holder? [কর্মানুমতি (Work Permit) প্রাপ্তদের হিসাব খোলার ক্ষেত্রে কর্মানুমতি (Work Permit) পত্র ও ব্যাংক হিসাব খোলার জন্য যথাযথ কর্তৃপক্ষের অনুমোদন রয়েছে কিনা?] ☐ Yes ☐ No

    (অনিবাসি বাংলাদেশীদের ক্ষেত্রে আবশ্যিকভাবে পাসপোর্টের কপি এবং বিদেশীদের ক্ষেত্রে আবশ্যিকভাবে ভিসাসহ পাসপোর্টের কপি সংগ্রহ করতে হবে)

12. Has the address (es) of the account holder been verified? ☐ Yes ☐ No

    If yes, how it is verified? ☐ Thanks Letter ☐ Physically (Please mention by whom)_____

13. The name of customer is listed or related to person or entity under relevant laws, regulations and circulars in the light of different UN security Council Resolutions on suspicion of involvement in the financing of terrorism, terrorism and the spread of weapons of mass destruction and listed under the Government of Bangladesh to the list of persons or entities / organization banned, is found matched (personally or under entity)? ☐ Yes ☐ No

    সংশ্লিষ্ট আইন, বিধিমালা ও সার্কুলারের আলোকে গ্রাহকের নাম জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজল্যুশনের আওতায় সন্ত্রাসী কার্যে, সন্ত্রাসী কার্যে অর্থায়নে ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারের অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকার সাথে যাচাইবাছাইপূর্বক কোনরূপ মিল পাওয়া গিয়েছে কিনা ?

    If the Answer, yes, disclose the details of action taken_____

14. Politically Exposed Persons (PEPs)/ Influential Person (IP): [According to BFIU Circular]
    a) Obtained approval from Senior Management? ☐ Yes ☐ No
    b) Face to Face interview with the Customer: ☐ Yes ☐ No

15. Risk Grading:

Sl. No.	Profession/Nature of Business	Score		Sl. No.	Profession/Nature of Business	Score
01	Jewellary/Gems Trade/Precious Metal Trade	5		24	High Officials of Multinational Co.	4
02	Money Changer/Courier Service/ Mobile Banking Agent	5		25	House Wife	4
03	Real Estate Developer/Agent	5		26	Service in IT Sector	4
04	Construction Project Undertaker/Contractor	5		27	Player/Media Celebrity / Producer/Film-Maker	4
05	Art / Antique Dealers	5		28	Freelance Software Developer	4
06	Restaurant/Bar/Night Club/Hotel & Motel owner/ Parlour Business	5		29	Business - Agent	3
				30	Govt. Services	3
07	Import / Export	5		31	Building / Land Owner	3
08	Manpower Export Business	5		32	Yearn Dealer / Jhoot (Left over) Brokers	3
09	Arms Dealer	5		33	Transport Operator	3
10	Garments Business/Garments Accessories/Buying House	5		34	Tobacco & Cigarette Business	3
11	Pilot / Flight Attendant	5		35	Organization of Entertainment/Park	3
12	Trustee	5		36	Motor Parts/Workshop Business	3
13	Stock /Share Business Investor	5		37	Private Service Managerial	3
14	Software/ICT Business	5		38	Teacher (Govt. / Private / Autonomous)	2
15	Expatriate (Foreign national working in Bangladesh)	5		39	Private Services	2
16	Travel Agent	4		40	Small Enterprise (Turnover less than Tk. 50.0 Lac per annum)	2
17	Business Investing Tk. 1.00 crore & above yearly	4				
18	Freight/Shipping/Cargo Agent	4		41	Self-Employment Professional	2
19	Auto Dealer (New/Re-conditioned Car)	4		42	Dealer of Computer / Mobile Phone	2
20	Business - Leather & Leather products	4		43	Manufacturer (Except Arms)	2
21	Building Construction Materials Business	4		44	Student	2
22	Professional (Journalist/Lawyers/Doctor/Engineer/ Chartered Accountant)	4		45	Retired from Service	1
				46	Farmer/Worker/Fisher Man	1
23	Director (Private/Public Ltd. Co.)	4		47	Others (Bank will fix risk score as per nature of Business)	1-5

(Bank shall consider the details of profession of the customer to assess risk: For Business - type of business and nature of business, transaction volume, area of business, size of business, actual beneficial owner etc. by scoring the customer as 'High Risk' or 'Low Risk'. For Service Holder, the same process shall follow by collecting paper and documents, specially: Service Sector, responsibilities etc. Considering the above facts bank may provide higher scores than the prescribed scores mentioned under serial No. 16-46, for respective customer.)

b. Monthly Income of the Customer

Amount (Tk.) in Lac	Score
Upto 1.00	0
> 1.00 – 3.00	1
above 3.00	3

c. How the Account was opened?

Mode (by/through)	Score
By RM/Branch Official	0
By DST	3
Internet/Non Face to Face	3
Unsolicited/Walk-in	3

d. Customer's Expected Monthly Transaction (Amount)

Transaction in Current Account (Amount in Lac)	Transaction in Savings A/C (Amount in Lac)	Score
0 - 10	0 - 5	0
> 10 – 20	> 5 – 10	1
> 20	> 10	3

e. Customer's Expected Monthly Transaction (Number)

No. of Transaction in Current Account	No. of Transaction in Savings Account	Score
0 – 15	0 – 10	0
16 – 25	11 – 20	1
> 25	> 20	3

f. Customer's Expected Monthly Cash Transaction (Amount)

Transaction in Current Account (Amount in Lac)	Transaction in Savings A/C (Amount in Lac)	Score
0 – 5	0 – 2	0
>5 – 10	> 2 – 5	1
> 10	> 5	3

g. Customer's Expected Monthly Cash Transaction (Number)

No. of Transaction in Current Account	No. of Transaction in Savings Account	Score
0 – 10	0 – 5	0
11 – 20	6 – 10	1
> 20	> 10	3

16. Overall Risk/Risk Rating Assessment (উপরের a হতে g ক্রমিক পর্যন্ত রিস্ক স্কোরের যোগফল)

Total Risk Score	Risk Rating
>=14	High
< 14	Low

IFIC BANK

Matured Dynamism

17. Comments:

* The Beneficial Owner may be graded in the level of High Risk under subjective judgement even if risk rating falls below 14.)

Prepared by: (Account Opening Officer/Branch Manager)	Verifying & Confirming by: (Branch Operation Manager/BAMLCO)
Signature with Date	Signature with Date
Name	Name
Name Seal	Name Seal

When the Account related information is reviewed and updated last?

Name

Designation

Date d d m m y y y y

Signature with Seal

IFIC BANK

Matured Dynamism

KYC PROFILE FORM – INSTITUTION/GOVT.

To be filled by Bank only

_____ Branch Date d d m m y y y y

1. Name of Account:
2. Type of Account:
3. Customer ID:
4. Account No.: -
5. Type of Institution (details):
6. Net Worth of the Institution:
7. Source of fund(s) in details:
8. i) Document(s) collected against source of fund: a) _____ b) _____ c) _____
   ii) Collected document(s) verified- ☐ Yes ☐ No
9. Has the address (es) of the Organigation been verified? ☐ Yes ☐ No
   If yes, how it is verified? ☐ Thanks Letter ☐ Physically (Please mention by whom)_____
10. Has actual Beneficiary owner been selected? ☐ Yes ☐ No ☐ Not applicable

    (If yes, fill up the personal information form for each of Beneficial owner. In case of Company, KYC in details should be completed for shareholder holding 20% or above share singly. Besides that KYC in details of controlling shareholder shall be completed.)

11. Customer Identification:

Sl. No.	KYC Supporting Document Number (Where applicable)	Whether photocopy obtained?		Whether Supporting Document Verified?	
a.	E-TIN Number :	Yes	No	Yes	No
b.	VAT Registration Number.	Yes	No	Yes	No
c.	Registration Number of Organization:	Yes	No	Yes	No
d.	Other documents	Yes	No	Yes	No

12. Reason for opening of Account of Foreign Company/Institution (if applicable)
    বিদেশী কোম্পানি/প্রতিষ্ঠানের হিসাব খোলার উদ্দেশ্য:

    a) Name of controlling authority:
    সংশ্লিষ্ট নিয়ন্ত্রণকারী কর্তৃপক্ষের নাম
    b) Approval details:
    অনুমোদন সংক্রান্ত তথ্য

13. Politically Exposed Persons (PEPs)/ Influential Person (IP): [According to BFIU Circular]
    a) Obtained approval from Senior Management? ☐ Yes ☐ No
    b) Face to Face interview with the Customer: ☐ Yes ☐ No

14. The name of customer is listed or related to person or entity under relevant laws, regulations and circulars in the light of different UN security Council Resolutions on suspicion of involvement in the financing of terrorism, terrorism and the spread of weapons of mass destruction and listed under the Government of Bangladesh to the list of persons or entities / organization banned, is found matched (personally or under entity)? ☐ Yes ☐ No

    সংশ্লিষ্ট আইন, বিধিমালা ও সার্কুলারের আলোকে গ্রাহকের নাম জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজল্যুশনের আওতায় সন্ত্রাসী কার্যে, সন্ত্রাসী কার্যে অর্থায়নে ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারের অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকার সাথে যাচাইবাছাইপূর্বক কোনরূপ মিল পাওয়া গিয়েছে কিনা ?

    If the Answer, yes, disclose the details of action taken_____

15. Risk Grading:

a. What does customer do/ in what kind of profession the customer is engaged?

Sl. No.	Profession/Nature of Business	Score		Sl. No.	Profession/Nature of Business	Score
01	Jewellary/Gems Trade/Precious Metal Trade	5		29	Event Management	4
02	Money Changer /Courier Service/ Mobile Banking Agent	5		30	Chartered Accountant	4
03	Real Estate Developer/Agent	5		31	Corporate Customer	4
04	Construction Project Undertaker / Contractor	5		32	Law Firm / Engineering Firm /Consultancy Firm	4
05	Offshore / Non Resident Corporation	5		33	Fuel & Electricity Production Company	4
06	Restaurant/Bar/Night Club/Residential Hotel / Parlour Business	5		34	Print / Electronic Media	4
				35	Travel Agent/Tourism Company	4
07	Import / Export & Import / Export Agent	5		36	Auto Dealer (Reconditioned Car)	4
08	Garments/Garments Accessories /Packaging/ Buying House	5		37	Freight/Shipping/Cargo/C&F Agent	4
				38	Auto Primary (New Car) Business	4
09	Share/Stock Dealer, Broker, Portfolio Manager, Merchant Banker	5		39	Building Construction Materials Business	4
				40	Business - Leather & Leader Products	4
10	NGO / NPO	5		41	Telecommunication Company	4
11	Manpower Export Business	5		42	Chain Store / Shopping Mall	4
12	Film Production/Distribution agency	5		43	Textile / Spinning	3
13	Arms Dealer	5		44	Organization of Entertainment/Park	3
14	Mobile Phone/Internet/Cable TV Operator	5		45	Motor Parts/Workshop Business	3
15	Brokerage agency of Land/Real Estate Selling & Buying	5		46	Agent Business	3
16	Bank/Leasing/Finance Company	5		47	Business (Manufacturing Pharmaceutical & Marketing)	3
17	Transport Operator	5		48	Business (Cold Storage)	3
18	Insurance/Brokerage Agency	5		49	Business (Frozen Foods)	3
19	Religious & Educational Institution	5		50	Business (Hardware)	3
20	Trustee	5		51	Business (Advertisement)	3
21	Business (Petrol Pump/CNG Station)	5		52	Service Provider	3
22	Business (Tobacco & Cigarette)	5		53	Computer/Mobile Phone Dealer	2
23	Software/ICT Business	5		54	Poultry/Dairy/Fishing Firm	2
24	Ship Breaking Business	5		55	Agro/Rice Mill/Beverage Business	2
25	Business - Clearing & Forwarding Agent	4		56	Manufacturer (Except Weapons/Arms)	2
26	Business – Dealer / Distributor / Agent	4		57	Shop (Retail Traders)	2
27	Indenting Agent	4		58	Others (Bank will fix risk score as per nature of Business)	1-5
28	Outsourcing Business	4				

(Bank shall consider the details of profession of the customer to assess risk: For Business - type of business and nature of business, transaction volume, area of business, size of business, actual beneficial owner etc. by scoring the customer as 'High Risk' or 'Low Risk'. Considering the above facts Bank may provide higher scores than the prescribed scores mentioned under serial no. 25-57, for respective customer.)

b. Customer's Net Worth

Amount (Tk.) in Crore	Score
0 - 1.00 Crore	0
> 1.00 – 3.00 Crore	1
>3.00 Crore	3

c. How the Account was opened?

Mode (by/through)	Score
By RM/Branch Official	0
By DST	3
Internet/Non Face to Face	3
Unsolicited/Walk-in	3

d. Customer's Expected Monthly Transaction (Amount)

Transaction in Current Account (Amount in Lac)	Transaction in Savings A/C (Amount in Lac)	Score
0 – 10	0 - 5	0
> 10 – 50	> 5 – 20	1
> 50	> 20	3

e. Customer's Expected Monthly Transaction (Number)

No. of Transaction in Current Account	No. of Transaction in Savings Account	Score
0 – 100	0 – 20	0
101 – 250	21 – 50	1
> 250	>50	3

f. Customer's Expected Monthly Cash Transaction (Amount)

Transaction in Current Account (Amount in Lac)	Transaction in Savings A/C (Amount in Lac)	Score
0 – 10	0 – 2	0
>10 – 25	> 2 – 7	1
> 25	> 7	3

g. Customer's Expected Monthly Cash Transaction (Number)

No. of Transaction in Current Account	No. of Transaction in Savings Account	Score
0 – 15	0 – 5	0
16 – 30	6 – 10	1
>30	> 10	3

IFIC BANK Matured Dynamism

16. Overall Risk/Risk Rating Assessment (উপরের a হতে g ক্রমিক পর্যন্ত রিস্ক স্কোরের যোগফল)

Total Risk Score	Risk Rating
>=14	High
< 14	Low

17. Comments:

* The Beneficial Owner may be graded in the level of High Risk under subjective judgement even if risk rating falls below 14.)

Prepared by: (Account Opening Officer/Branch Manager)	Verifying & Confirming by: (Branch Operation Manager/BAMLCO)
Signature with Date	Signature with Date
Name	Name
Name Seal	Name Seal
Name	

When the Account related information is reviewed and updated last?

Name

Designation

Date d d m m y y y y

Signature with Seal

Annexure B: Transaction Profile

IFIC BANK

IFIC 40 YEARS OF Matured Dynamism

TREANSACTION PROFILE

Date d d m m y y y y

Customer ID _____ For Bank use Only

Account No. _____ - ___

1. Name of Account / হিসাবের নাম _____

Type of Account _____ Account Number _____ - ___

Monthly probable income (for individual) _____ Monthly probable turnover (for institution) _____

Purpose of Account Opening ☐ Personal Account Transaction ☐ Salary ☐ Savings ☐ Loan/Deposit Scheme Repayment ☐ Investment ☐ Foreign Remittance ☐ Others (Please Specify)

Sources of Fund for Transaction ☐ Salary ☐ Own Business ☐ Commission ☐ Inheritance/Gift/Return on Investment ☐ Foreign Remittance ☐ Others (Please Specify)

Nature and Volume of Monthly Transaction _____

DEPOSITS	Numbers of Deposit (Monthly)	Total Amount (Monthly)	Maximum Amount (Per Transaction)
Cash Deposit (including online & ATM)			
Deposit by Transfer/Instrument			
Deposit Through Foreign inward remittance			
Deposit of Income from Export			
Receive/Transfer from BO(Capital Market) Account			
Others (Please Specify)			
Total Probable Deposit			

WITHDRAWAL	Numbers of Withdrawal (Monthly)	Total Amount (Monthly)	Maximum Amount (Per Transaction)
Cash Withdrawal (including online & ATM)			
Payment by Transfer/Instrument			
Payment for Foreign outward remittance			
Payment against Import			
Deposit / Transfer to BO (Capital Market) Account			
Others (Please Specify)			
Total Probable Withdrawal			

I/we, the undersigned, hereby confirm that this transaction profile truly represents the expected transactional activities in my/our/organization account. I/we further confirm that the transaction profile will be revised/ updated, if necessary, from time to time.

Account Holder(s)/Account Operator(s)	Account Holder(s)/Account Operator(s)	Account Holder(s)/Account Operator(s)
Name :	Name :	Name :
Designation :	Designation :	Designation :
Date :	Date :	Date :

Bank Use Only

Transaction Profile (TP) of customer has been scrutinize as per instruction of BFIU.

Reason behind the Changing/Not Changing of Customer's Probable Transaction Profile:	

Signature of verifying Officer:_____ Date: _____ Seal with Name: _____

Annexure C: KYC Requirements for High Net Worth Customers

KYC Requirements for High Net Worth Customers		
A. Source of Fund		
Type of Source of Fund		
☐ Business Ownership	☐ Top executive	☐ Inheritance
☐ Profession*	☐ Investments**	☐ Other
*Profession **Investments	Physician, lawyer, engineer, accountants and sports professional etc. Someone who buys and sells assets of any type: real estate, securities, companies, royalties and patents etc.	
Instructions: Please refer to the list of questions to be used when obtaining source of wealth, you may need to choose more than one category for a business owner with inherited wealth.		
B. Notes of Face-to-Face Meeting with Customers		
C. Annual Review of Customer Profile		
Prepared By (TSO/TSI/TSM)		**Reviewed By (BOM/BM)**
Signature with Date		Signature with Date
Name:		Name:

Annexure D: Source of Fund Verification

List of Questions to be used when obtaining source of wealth:
A. Wealth Generated from Business Ownership
▪ Description and nature of the business and its operations ▪ Ownership type: private or public? ▪ What kind of company? ▪ Percent of ownership? ▪ Estimated sales volume? ▪ Estimated net income? ▪ Estimated net worth? ▪ How long in business? ▪ How was the business established? ▪ Other owners or partners (yes/no)? ▪ Names of other owners or partners? ▪ Percent owned by other owners or partners? ▪ Number of employees ▪ Number of locations? ▪ Geographic trade areas of business ▪ Other family members in business? ▪ Significant revenues from government contract or licenses?
B. Wealth Derived from Being a Top Executive
▪ Estimate of compensation? ▪ What does the company do? (for example, manufacture, service etc.) ▪ Position held (for example, President, CFO) ▪ Length of time with company? ▪ Area of expertise (for example, finance, production, etc.) ▪ Publicly or privately owned? ▪ Client's past experience (for example, CFO at another company)
C. Primary Source of Wealth was Through Inheritance
▪ In what business was the wealth generated? ▪ Inherited from whom? ▪ Type of asset inherited (For example: land, securities, company trusts…) ▪ When were the assets inherited? ▪ How much was inherited? ▪ Percent ownership for a business that is inherited
D. Wealth Generated from a Profession (Physician, dentist, lawyer, engineer, entertainer etc.)
▪ What is the profession, including area of specialty (e.g. arts – singer, construction – engineer) ▪ Source of wealth (Example: lawyer who derived wealth form real estate, Dr. running a client.) ▪ Estimate of income
E. Wealth Generated from Investments
▪ Where did the source of wealth come from? (example, invested in shares, bonds, etc.) ▪ What do they currently invest in? (for example, real estate, stock market etc.) ▪ What is the size of the investment? ▪ Cite notable public transactions if any ▪ What is the client's role in transaction (e.g. takes positions, buy companies, middle man)? ▪ Estimated annual income/capital appreciation? ▪ How long has the client been an investor?

Note: This form must be renewed every year.

Annexure- E: Red Flags pointing to ML & TF

Red Flags pointing to Money Laundering

- ✓ The client cannot provide satisfactory evidence of identity.
- ✓ Situations where it is very difficult to verify customer information.
- ✓ Situations where the source of funds cannot be easily verified.
- ✓ Transactions in countries in which the parties are non-residents and their only purpose is a capital investment (they are not interested in living at the property they are buying).
- ✓ Frequent change of ownership of same property in unusually short time periods with no apparent business, economic or other legitimate reason and between related persons.
- ✓ Client wants to re-sell Property shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.
- ✓ Client wishes to form or purchase a company whose corporate objective is irrelevant to the client's normal profession or activities, without a reasonable explanation.
- ✓ The client sets up shell companies with nominee shareholders and/or directors.
- ✓ Client repeatedly changes Attorneys within a short period of time without any reasonable explanation.
- ✓ Client purchases property in names of other persons or uses different names on offers to purchase, closing documents and deposit receipts.
- ✓ Client deposits a large amount of cash with you to make payments which are outside of the client's profile.
- ✓ Client negotiates a purchase but wants to record a lower value on documents, paying the difference "under the table", (inadequate consideration).
- ✓ Client's documents such as identification, statement of income or employment details are
- ✓ provided by an intermediary who has no apparent reason to be involved, (the intermediary may be the real client).
- ✓ Transaction involves legal entities and there is no relationship seen between the transaction and the business activity of the buying company, or the company has no business activity.
- ✓ Client requests the firm to act as his agent in obtaining high sum bankers' drafts, cashiers' cheques and other cash equivalent or near cash monetary instruments or in making wire transfers to and from other banks or financial institutions, (anonymity).
- ✓ Divergence from the type, volume or frequency of transactions expected in the course of the business relationship.
- ✓ Client gives power of attorney to a non-relative to conduct large transactions (same as above).

- ✓ Use of letters of credit to move money between those countries, where such trade would not normally occur and / or is not consistent with the customer's usual business activity. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.
- ✓ The method of payment requested by the client appears inconsistent with the risk characteristics of the transaction. For example, receipt of an advance payment for a shipment from a new seller in a high-risk jurisdiction.
- ✓ The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or that includes changes in regard to the beneficiary or location of payment without any apparent reason.
- ✓ Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction of same business entity are indicators for TBML. In this regard the study of foreign exchange remittances may help detect the offence.
- ✓ The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities or sensitive / non-co-operative jurisdictions.
- ✓ The commodity is transshipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
- ✓ Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense.
- ✓ Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- ✓ Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.
- ✓ Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management.

Red Flags pointing to Financing of Terrorism

Behavioral Indicators

- ✓ The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- ✓ Use of false corporations, including shell-companies.
- ✓ Inclusion of the individual or entity in the United Nations 1267 Sanctions list.
- ✓ Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.

- ✓ Beneficial owner of the account not properly identified.
- ✓ Use of nominees, trusts, family members or third-party accounts.
- ✓ Use of false identification.
- ✓ Abuse of non-profit organization.

Indicators linked to the financial transactions:

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

Annexure-F: KYC for Walk-In Customers

AvB Gd AvB wm e¨vsK wjwg‡UW
Walk-in Customer/Online Customer
Rgv`vbKvixi/ D‡ËvjbKvixi (wnmveavix e¨ZxZ)
Short KYC

ZvwiL	
Rgv`vbKvix / D‡ËvjbKvixi bvg(wnmveavix e¨ZxZ)	
wnmveavixi wnmve b¤^i	
UvKvi cwigvb	
UvKvi Drm	
wnmveavixi mv‡_ m¤úK©	
‡jb‡`‡bi D‡Ïk¨	
wcZvi bvg	
gvZvi bvg	
RvZxqZv	
Rgv`vbKvix / D‡ËvjbKvixi †ckv (wnmveavix e¨ZxZ)	
Rgv`vbKvix/ D‡ËvjbKvixi (wnmveavix e¨ZxZ) wVKvbv	
‡gvevBj/†dvb b¤^i	
‡h‡Kvb Qwehy³ AvBwW(RvZxq cwiPq cÎ/cm‡cvU©/Rb¥ wbeÜb bs/Ab¨vb¨	

Rgv`vbKvixi/ D‡ËvjbKvixi (wnmveavix e¨ZxZ)
¯^v¶i:

Kg©KZ©vi ¯^v¶i **ev‡gj‡Kv/ g¨v‡bRvi Ac‡ikb/kvLv e¨e¯’vc‡Ki ¯^v¶i**

bvgt **bvgt**
ZvwiL I mxj **ZvwiL I mxj**

Annexure-G: Training on "Money Laundering, Terrorist Financing & Trade Based Money Laundering and it's Prevention"

Considering the devastating economic, security and social consequences of Money Laundering & Terrorist Financing through Banking channel and having due regard to the importance of Anti-Money Laundering steps; IFIC Bank Ltd. will pursue a training program consisting of four modules as follows:

1. Module – I : Trainers training on "Money Laundering & Terrorist Financing".
2. Module – II : Course on Money Laundering & Terrorist Financing.
3. Module – III : Workshops/Seminar on Prevention of ML & CFT.
4. Module – IV : Off the Desk Steps on Prevention of ML & CFT.

Module – I: Trainers Training on "Money Laundering, Terrorist Financing & its Prevention"

Objectives: The main objectives of the program will be to:

- make the participants (designated Officers of the branches/In-charge of branches) aware about the Money Laundering Prevention Act, 2012 & Anti-Terrorist Act, 2009.
- help them realize the importance of the Act and the duties and responsibilities vested on the bankers by the Act.
- enable them to acquire required skill to act as trainers at Branch/ Head Office level.

Outline: Money Laundering Prevention Act, 2012(amendment-2015), Anti-Terrorist Act, 2009 (amendment-2012-2013) and its importance. Bank's obligation to implement Money Laundering Prevention Act, 2012 (amendment-2015) & Anti-Terrorist Act, 2009(amendment-2012-2013). Duties and responsibilities of the Officers to strictly follow the various provisions of the Act. Bangladesh Bank and Bank's guidelines on Prevention of Money Laundering & Combating Financing of Terrorism. Procedure to Know Your Customers (KYC) and Business Associates. Internal controls to prevent Money Laundering & Terrorist Financing Communication skill.

Duration: 02 (two) days

Level of participants: Manager/ In-charge of Branches/ Designated Officers of all branches/ Head Office.

Faculty: Executives/ Officers from Head Office & Branches, Guest speaker(s) from BFIU, BB/ BIBM etc.

Methods: Lecture/ Discussion/ Case study etc.

Module – II: Short Course on "Money Laundering, Terrorist Financing & its Prevention"

Objectives: The main objectives of the course will be to:

- help the participants understand and appreciate the various provisions of Money Laundering Prevention Act, 2012 (amendment-2015) & Anti-Terrorist Act, 2009 (amendment-2012-2013).
- help them in appreciating the role, duties and responsibilities given to them by the Acts.
- make them understand the various steps, circulars, etc. issued by Bangladesh Bank, the Bank from time to time.
- enable them to acquire the skill to understand the Know Your Customers (KYC)

Outline: Money Laundering Prevention Act, 2012(amendment-2015) & Anti-Terrorist Act, 2009(amendment-2012-2013) and its importance. Bank's obligation to implement Money Laundering Prevention Act & Anti-Terrorist Act. Duties and responsibilities of the Officers to follow the various provisions of the Acts. Bank's Guidelines, procedure

	to Know Your Customer (KYC), Business Associates and Internal controls to prevent Money Laundering & combating financing of terrorism.
Duration:	02 (two) days.
Level of participants:	Officers of all branches/Head Office.
Faculty:	Executives/Officers from Head Office & Branches, Guest speakers from BB/BIBM etc.
Methods:	Lecture/ Discussion/ Case study etc.

Module – III: Workshop/Seminar on "Prevention of Money Laundering & Combating Financing of Terrorism"

Objectives:	The main objective of the Workshop/ Seminar will be to exchange opinion about the problems of implementation of the various provisions of the Prevention of Money Laundering Act, 2012 (amendment-2015), Anti-Terrorist Act, 2009 (amendment-2012-2013) and to find out solutions thereof.
Outline:	General discussion on the problems faced by the branches and Head Office in the implementation of the Act. Cases of Money Laundering & Terrorist Financing so far detected by the Bank and lesson therefrom, recommendations and future course of action.
Duration:	01 (one) day
Level of participants:	Manager/ In-charge of Branches/Designated Officers of all branches/ Head Office.
Faculty:	Executives/Officers from Head Office & Branches, Guest speakers from BB/BIBM etc.
Methods:	Discussion/ Case study etc.

Module – IV: Off the Desk Steps on 'Prevention of Money Laundering & Combating Financing of Terrorism'

Objectives:	The objective of this program will be to educate all Officers about the consequences of Money Laundering and steps undertaken to stop such activities.
Outline:	Circulation of Bangladesh Bank circulars, Bank circulars, paper cuttings, write-ups, articles, research papers etc. on the subject.
Duration:	01(one) day
Level:	All Officers
Faculty:	As above
Methods:	Discussion/Case study.

Annexure H: Risk Register

1. ML & TF Risk Register for Customers

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
Walk-in customer (beneficiary is government/ semi government/ autonomous body/ bank & NBFI)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Walk-in customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBFI)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Non-resident customer (Bangladeshi)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
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)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
A customer making series of transactions to the same individual or entity	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer involved in outsourcing business	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer appears to do structuring to avoid reporting threshold	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer appears to have accounts with several banks in the same area	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Negative news about the customers' activities/ business in media or from other reliable sources	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Customer is secretive and reluctant to meet in person	Very likely	Moderate	=3(High)	Risk likely to happen and/or to have serious consequences.

				Response: Do not allow until risk reduced.
Customer is a mandate who is operating account on behalf of another person/ company.	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Large deposits in the account of customer with low income	Very likely	Moderate	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customers about whom BFIU seeks information (individual)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
A customer whose identification is difficult to check	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Significant and unexplained geographic distance between the bank and the location of the customer	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Customer is a foreigner	Very likely	Moderate	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer is a minor	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Customer is Housewife	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Customers that are politically exposed persons (PEPs) or influential persons (IPs) or chief/senior officials of international organizations and their family members and close associates	Very likely	Moderate	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Very likely	Moderate	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customers doing significant volume of transactions with higher-risk geographic locations.	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
A customer who brings in large amounts of used notes and/or small denominations	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers,	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.

art and antique dealers and auction houses, estate agents and real estate brokers)				
Customer is a money changer/ courier service agent / travel agent	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customer is involved in Manpower Export Business	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Customer has been refused to provide banking facilities by another bank	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Accounts opened before 30 April, 2002	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Customers with complex accounting and huge transaction	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Receipt of donor fund, fund from foreign source by micro finance institute (MFI)	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Wholesale Banking Customer				
Entity customer having operations in multiple locations	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Customers about whom BFIU seeks information (large corporate)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Owner of the entity that are IPs and their family members and close associates	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Very likely	Moderate	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
A customer whose identification is difficult to check.	Very likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level

Owner of the entity that are PEPs or chief / senior officials of International Organizations and their family members and close associates	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Charities or NPOs (especially operating in less privileged areas).	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Credit Card Customer				
Customer who changes static data frequently	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Credit Card customer	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
International Trade Customer				
A new customer (Outward remittance-through SWIFT)	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
A new customer (Import/ Export)	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
A new customer (Inward remittance-through SWIFT)	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
A new customer who wants to carry out a large transaction (Import/ Export)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
A new customer who wants to carry out a large transaction (Inward/ outward remittance)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
A customer wants to conduct business beyond its line of business (import/ export/ remittance) Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level

A new customer who wants to carry out a large transaction (Import/ Export)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Correspondent Banks	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk

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

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Locker Service	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Foreign currency endorsement in Passport	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Large transaction in the account of under privileged people	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
FDR (less than 2 million)	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
FDR (2 million and above)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Special scheme deposit accounts opened with big installment and small tenure	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Multiple deposit scheme accounts opened by same customer in a branch	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Multiple deposit scheme accounts opened by same customer from different location	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Open DPS in the name of family member Or Installments paid from the account other than the customer's account	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Early encashment of FDR, special scheme etc.	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence

				Response: go ahead but preferable reduce risk
Non face to face business/transaction	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Retail Privilege Facilities				
Pre- Approved Credit Card with BDT 300K limit	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Enhanced ATM cash withdrawal Limit BDT 100K	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
SME Banking Product				
Early encashment of FDR	Unlikely	Moderate	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Repayment of loan EMI from source that is not clear	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Repayment of full loan amount before maturity	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
Loan amount utilized in sector other than the sector specified during availing the loan	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Source of fund used as security not clear at the time of availing loan	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Wholesale Banking Product				
Development of new product & service of bank	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level.
Payment received from unrelated third parties	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
High Value FDR	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
Term loan, SOD(FO), SOD(G-work order), SOD(Garment),SOD(PO), Loan General, Lease	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence

finance, Packing Credit, BTB L/C				Response: go ahead but preferable reduce risk.
BG(bid bond), BG(PG), BG(APG)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
L/C subsequent term loan, DP L/C	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
C.C(H), SOD(G-Business), STL	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
OBU	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
Syndication Financing	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
Credit Card				
Supplementary Credit Card Issue	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Credit card issuance against ERQ and RFCD accounts	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
International Trade				
Line of business mismatch (import/export/remittance)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Under/ Over invoicing (import/export/remittance)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Retirement of import bills in cash (import/export/remittance)	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Wire transfer	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.

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

Risk	Likelihood	Impact	Risk Score	Treatment/Action

Online (multiple small transaction through different branch)	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
BEFTN	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
BACH	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk.
IDBP	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Mobile Banking	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Credit Card				
New Merchant sign up	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
High volume transaction through POS	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Alternate Delivery Channel				
Large amount withdrawn from ATMs	Likely	Major	=3(High)	Risk likely to happen and/or to have serious consequences. Response: Do not allow until risk reduced.
Larger amount transaction from different location and different time(mid night) through ATM	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Unlikely	Minor	=1(low)	Unlikely to happen and/or have minor or negligible consequence Response: Ok to go ahead.
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103) .	Likely	Moderate	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk

4. Risk Register for Country/jurisdiction

Risk	Likelihood	Impact	Risk score	Treatment/Action
Import and export form/to sanction country	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level

Trans-shipments, container, flag vessel etc. under global sanction	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Establishing correspondent relationship with sanction bank and/or country	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Establishing correspondent relationship with poor AML&CFT practice country	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Customer belongs to countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Customer belongs to High Risk ranking countries of the Basel AML index.	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Customer belongs to the countries identified by the bank as higher-risk because of its prior experiences or other factors.	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Any country identified by FATF or FSRBs-(FATF style Regional Body) as not having adequate AML&CFT systems	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Any bank that provide service to 'Shell Bank'	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Any bank that allow payable through account	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences.

				Response: Do not allow transaction to occur or reduce the risk to acceptable level
Any country identified as destination of illicit financial flow	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Branches in a Border Area	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Area identified as high risk in the NRA	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level
Countries subject to UN embargo/sanctions	Very Likely	Major	=4(Extreme)	Risk almost sure to happen and/or have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level

5. Register for Regulatory Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML/CFT guideline	Unlikely	Major	=2(Medium)	a)Develop bank's own ML & TF Risk Management Guideline; b) Update the guideline from time to time.
Not forming a Central Compliance Unit (CCU)	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Not having an AML&CFT Compliance Officer	Unlikely likely	Major Major	=2(Medium) =3(High)	Nominate AML & CFT Compliance Officer as per the instruction of BFIU
Not having Branch Anti Money Laundering Compliance Officer	Unlikely likely	Major moderate	=2(Medium) =2	Nominate BAMLCO as per BFIU instruction and updated the AML & CFT Deptt. regarding the nomination.
Not having an AML&CFT program	Unlikely Likely	Major Major	=2(Medium) =3(High)	Develop AML & CFT program and review the same from time to time ,at least annually
No senior management commitment to comply with MLP and AT Act	Unlikely	Major	=2(Medium)	a)Provision of commitment of senior management to be included in the ML & TF Risk Management Guideline; b)Share the commitment of senior management in the form of yearly message will all employees of IFIC Bank
Failure to follow the AML & CFTD/BFIU circular, circular letter, instructions etc.	Unlikely Likely	Major Major	=2(Medium) =3(High)	Follow the AML & CFTD/BFIU circular, circular letter, instructions issued from time to time

Unique account opening form not followed while opening account	Unlikely Likely	Major Moderate	=2(Medium) =2(Medium)	a)Revise account opening form of the bank in line with the Unique account opening form and KYC profile form prescribed by BFIU; b)Ensure use of Unique account opening form and KYC profile form prescribed by BFIU
Non-compliance regarding screening of new and existing customers against different Sanction lists, adverse media list and entities banned list by Bangladesh Govt.	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Comply with screening requirements of BFIU; b) Ensure proper application of sanction screening software; c) Update the software /process from time to time(as applicable).
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Complete and accurate information of customer not obtained	Unlikely Likely	Major Moderate	=2(Medium) =2(Medium)	a)Obtain complete and accurate information of customer; b) Develop control mechanism to check whether business units are collecting complete and accurate information of customer and reviewing and updating the same from time to time; c)If fails, close the account with prior notice to customer on approval of CAMLCO
Failure to verify the identity proof document and address of the customer	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Verify the identity proof document and address of the customer; b) Develop control mechanism to check whether business are- -verifying the identity proof document with the support of database from concerned authority; -verifying address by procedure prescribed in IFIC CAP, 2013(2018.
Beneficial owner identification and verification not done properly	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Identify Beneficial owner and obtain complete and accurate information; b)Check whether business units -identify beneficial owner(s) of the account(s) and obtain complete and accurate information of them; -complete KYC of beneficial owner(s).
Customer Due Diligence (CDD) not practiced properly	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk

Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPS and influential person and senior official of international organization.)	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Perform EDD for High Risk customers; b) Check whether business units are obtaining CAMLCO's approval before opening/maintaining such account(s); c) Check whether business units are conducting both CDD & EDD for high risk customer as per BFIU instruction.
Failure to complete KYC of customer including walk in customer	Unlikely Likely	Major Major	=2(Medium) =3(High)	Complete KYC of customer including walk-in customer as per BFIU instructions.
Failure to update TP and KYC of customer	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Update TP & KYC as per BFIU instruction; b)Develop control mechanism to check whether business units are updating TP & KYC as per the instruction of BFIU.
Keep the legacy accounts operative without completing KYC	Unlikely	Major	=2(Medium)	a)Update KYC of legacy account, else keep those as dormant; b) Ensure off-site monitoring of legacy account from AML & CFT Deptt.
Failure to assess the ML & TF risk of a product or service before launching	Unlikely Likely	Major Major	=2(Medium) =3(High)	Assess the ML & TF risk of a product or service, devise action plan to manage the risk before launching the same.
Failure to complete the KYC of Correspondent Bank	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Complete the KYC of Correspondent Bank; b) Obtain updated KYC of Correspondent Bank from time to time.
Senior Management approval not obtained before entering into a Correspondent Banking relationship	Unlikely	Major	=2(Medium)	Obtain Senior Management approval before entering into a Correspondent Banking relationship
Failure to comply with the instruction of BFIU by bank Foreign subsidiary	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Monitor the AML & CFT activity of foreign subsidiary; b) Obtain confirmation from the subsidiary on AML & CFT compliance.
Failure to keep record properly	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Keep records as per BFIU instruction; b) Check compliance status periodically.
Failure to report complete and accurate CTR on time	Unlikely	Major	=2(Medium)	a)Rectify the limitation of information in goAML; b) Ensure uniformity in the number and amount of CTR data submitted through goAML web and ISS report; c)Submit complete and accurate CTR to BFIU on time.

Failure to review CTR	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Generate a statement of CTR data from CBS b)Monitor the CTR data on a monthly basis and identify whether there is any suspicious transaction; c) AML & CFT Deptt. to monitor the CTR data on a random basis and identify whether there is any suspicious transaction.
Failure to identify and monitor structuring	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Generate a statement of structuring report from CBS b)Monitor the report on a monthly basis and identify whether there is any suspicious transaction;
Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Failure to conduct quarterly meeting properly	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Failure to report suspicious transactions (STR)	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Monitor account transaction and customer activity and report when found suspicious; b) Generate unusual transaction reports from the system, analyze the same and identify whether there is any suspicious transaction.
Failure to conduct self-assessment properly	Unlikely Likely	Major Major	=2(Medium) =3(High)	a)Conduct self-assessment on half yearly basis; b) Portray the actual strength, weakness and position of the branch in self-assessment; c)AML & CFT Deptt. to check the self-assessment report submitted by branch; d)AML & CFT Deptt. to cross-check the self-assessment report with ITP and inspection report and take appropriate action.
Failure to submit statement/ report to BFIU on time	Unlikely	Major	=2(Medium)	a)Submit statement /report to BFIU timely; b) Check statement submission status during audit/inspection.
Submit erroneous statement/ report to BFIU	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Not submitting accurate information or	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence

statement sought by BFIU or BB.				Response: go ahead but preferable reduce risk
Not submitting required report to senior management regularly	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Failure to rectify the objections raised by BFIU or bank inspection teams on time	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Failure to obtain information during wire transfer	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Failure to scrutinize staff properly	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Failure to circulate BFIU guidelines and circulars to branches	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
Inadequate training/ workshop arranged on AML & CFT	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk
No independent audit function to test the AML program	Unlikely	Major	=2(Medium)	Possible this could happen and /or have moderate consequence Response: go ahead but preferable reduce risk

To calculate the above Risk Register our Bank use following Risk Assessment Score:

Calculation of Risk Score

Measure the size & importance of risk:

- Likelihood – chance of the risk happening
- Impact – the amount of loss or damage if the risk happened

likelihood X impact = level of risk (risk score)

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

Therefore, each risk element can be rated by:

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

To help assess the risks identified in the first stage of this process, we can apply the risk rating scales for likelihood (Table 2 and impact (Table 3) and from these get a level of risk or risk score using the risk matrix (Figure 2).

What is Likelihood scale?

A likelihood scale refers to the potential of an ML & TF risk occurring in the business for the particular risk being assessed. Three levels of risk are shown in Table 2:

Table 2: Likelihood scale

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

What is Impact scale?

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

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

Three levels of impact are shown in Table 3, but the bank can have as many as they believe are necessary.

Table 3: Impact scale

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.

Risk matrix and risk score

Use the risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk. How the risk score is derived can be seen from the risk matrix (Figure 2) and risk score table (Table 4) shown below. Four levels of risk score are shown in Figure 2 and Table 4.

Figure 2: Risk matrix

Threat level for ML/TF risk

		IMPACT		
		Minor	**Moderate**	**Major**
LIKELIHOOD	**Very Likely**	Medium (2)	High (3)	Extreme (4)
	Likely	Low (1)	Medium (2)	High (3)
	Unlikely	Low (1)	Low (1)	Medium (3)

Table 4: Risk score table

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

Use the above risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk:

Very Likely

Likelihood- **chance of the risk happening**	Impact- **the amount of loss or damage if the risk happened**	Risk Score
Very Likely- **Almost certain: it will probably occur several times a year**	Major- **Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**	=4 (extreme)
Very Likely	Moderate- **Moderate level of money laundering or terrorism financing impact.**	=3 (high)
Very Likely	Minor- **Minor or negligible consequences or effects.**	=2(medium)

Likely

Likelihood	Impact	Risk Score
Likely- **High probability it will happen once a year**	Major **Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**	=3 (high)
Likely	Moderate- **Moderate level of money laundering or terrorism financing impact.**	=2(medium)
Likely	Minor- **Minor or negligible consequences or effects.**	=1(low)

Unlikely

Likelihood	Impact	Risk Score
Unlikely- **Minor or negligible consequences or effects**	Major- **Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**	=2(medium)
Unlikely	Moderate- **Moderate level of money laundering or terrorism financing impact.**	=1(low)
Unlikely	Minor- **Minor or negligible consequences or effects.**	=1(low)

Table 4: Risk score table

Rating	Impact – of an ML&TF risk

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

Use the above risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk:

Very Likely

Likelihood- **chance of the risk happening**	Impact- **the amount of loss or damage if the risk happened**	Risk Score
Very Likely- **Almost certain: it will probably occur several times a year**	Major- **Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**	=4 (extreme)
Very Likely	Moderate- **Moderate level of money laundering or terrorism financing impact.**	=3 (high)
Very Likely	Minor- **Minor or negligible consequences or effects.**	=2(medium)

Likely

Likelihood	Impact	Risk Score
Likely- **High probability it will happen once a year**	Major **Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**	=3 (high)
Likely	Moderate- **Moderate level of money laundering or terrorism financing impact.**	=2(medium)
Likely	Minor- **Minor or negligible consequences or effects.**	=1(low)

Unlikely

Likelihood	Impact	Risk Score
Unlikely- **Minor or negligible consequences or effects**	Major- **Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**	=2(medium)
Unlikely	Moderate- **Moderate level of money laundering or terrorism financing impact.**	=1(low)
Unlikely	Minor- **Minor or negligible consequences or effects.**	=1(low)

Annexure I: KYC Documentation

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Individuals	➢ Passport ➢ National Id Card ➢ Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) ➢ Valid driving license (if any) ➢ Credit Card (if any) ➢ Any other documents that satisfy to the bank. NB: But in case of submitting the birth registration certificate, any other photo id (issued by a Government department or agency) of the person has to be supplied with it. If he does not have a photo id, then a certificate of identity by any renowned people has to be submitted according to the bank's requirement. That certificate must include a photo which is duly attested by the signing renowned person. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.	➢ Salary Certificate (for salaried person). ➢ Employed ID (For ascertaining level of employment). ➢ Self-declaration acceptable to the bank. (commensurate with declared occupation) ➢ Documents in support of beneficial owner's income (income of house wife, students etc.) ➢ Trade License if the customer declared to be a business person ➢ TIN (if any) ➢ Documents of property sale. (if any) ➢ Other Bank statement (if any) ➢ Document of FDR encashment (if any) ➢ Document of foreign remittance (if any fund comes from outside the country) ➢ Document of retirement benefit. ➢ Bank loan.	➢ Acknowledgement receipt of thanks letter through postal department. ➢ Proof of delivery of thanks letter through courier. ➢ Third party verification report. ➢ Physical verification report of bank official ➢ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. ➢ Residential address appearing on an official document prepared by a Government Agency
Joint Accounts	➢ Passport ➢ National Id Card ➢ Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) ➢ Valid driving license (if any) ➢ Credit Card (if any) ➢ Any other documents (photo) that satisfy to the bank.	➢ Salary Certificate (for salaried person). ➢ Employed ID (For ascertaining level of employment). ➢ Self-declaration acceptable to the bank. (commensurate with declared occupation) ➢ Documents in support of beneficial owner's income (income of house wife, students etc.) ➢ Trade License if the customer declared to be a business person ➢ TIN (if any) ➢ Documents of property sale. (if any)	➢ Acknowledgement receipt of thanks letter through postal department. ➢ Proof of delivery of thanks letter through courier. ➢ Third party verification report. ➢ Physical verification report of bank official ➢ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. ➢ Residential address appearing on an official

		➢ Other Bank statement (if any) ➢ Document of FDR encashment (if any) ➢ Document of foreign remittance (if any fund comes from outside the country) ➢ Document of retirement benefit. ➢ Bank loan.	document prepared by a Government Agency
Sole Proprietorships or Individuals doing business	➢ Passport ➢ National Id Card ➢ Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) ➢ Valid driving license (if any) ➢ Credit Card (if any) ➢ Rent receipt of the shop (if the shop is rental) ➢ Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents) ➢ Membership certificate of any association. (Chamber of comers, market association,	➢ Trade License ➢ TIN ➢ Self-declaration acceptable to the bank. (commensurate with nature and volume of business) ➢ Documents of property sale. (if injected any fund by selling personal property) ➢ Other Bank statement (if any)	➢ Acknowledgement receipt of thanks letter through postal department. ➢ Proof of delivery of thanks letter through courier. ➢ Third party verification report. ➢ Physical verification report of bank official ➢ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. ➢ Residential address appearing on an official document prepared by a Government Agency
Partnerships	➢ Partnership deed/ partnership letter ➢ Registered partnership deed (if registered) ➢ Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. ➢ Passport of partners ➢ National Id Card of partners ➢ Birth Registration Certificate of partners (Printed copy, with seal & signature from the Registrar) ➢ Valid driving license of partners (if any) ➢ Credit Card of partners (if any) ➢ Rent receipt of the shop (if the shop is rental) ➢ Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents)	➢ Trade License ➢ TIN ➢ Documents of property sale. (if injected any fund by selling personal property of a partner) ➢ Other Bank statement (if any) ➢ Document of FDR encashment (if any partner injected capital by enchasing Personal FDR) ➢ Document of foreign remittance (if any fund comes from outside the country) ➢ Personal Borrowing (if any)	➢ Acknowledgement receipt of thanks letter through postal department ➢ Proof of delivery of thanks letter through courier. ➢ Third party verification report. ➢ Physical verification report of bank official ➢ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. ➢ Residential address appearing on an official document prepared by a Government Agency

	➢ Membership certificate of any association. (Chamber of comers, market association, trade association i.e.; Hardware association, cloth merchant association, hawker's association etc. ➢ Any other documents that satisfy to the bank.		
Private Limited Companies	➢ Passport of all the directors ➢ National Id Card of all the directors ➢ Certificate of incorporation ➢ Memorandum and Articles of Association ➢ List of directors ➢ Resolution of the board of directors to open an account and identification of those who have authority to operate the account. ➢ Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. ➢ Nature of the company's business ➢ Expected monthly turnover ➢ Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full-time employee, officer or director of the company.	➢ A copy of last available financial statements duly authenticated by competent authority ➢ Other Bank statement ➢ Trade License ➢ TIN ➢ VAT registration ➢ Bank loan	

Public Limited Companies	➢ Passport of all the directors ➢ National Id Card of all the directors ➢ Certificate of incorporation ➢ Memorandum and Articles of Association ➢ Certificate of commencement of business ➢ List of directors in form -XII ➢ Resolution of the board of directors to open an account and identification of those who have authority to operate the account. ➢ Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. ➢ Nature of the company's business ➢ Expected monthly turnover ➢ Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full-time employee, officer or director of the company.	➢ A copy of last available financial statements duly certified by a professional accountant ➢ Other Bank statement (if any) ➢ Trade License ➢ TIN ➢ Cash flow statement ➢ VAT registration ➢ Bank loan ➢ Any other genuine source	
Government-Owned entities	➢ Statue of formation of the entity ➢ Resolution of the board to open an account and identification of those who have authority to operate the account. ➢ Passport of the operator (s) ➢ National Id Card of the operator (s)	N/A	N/A
NGO	➢ National Id Card of the operator (s) ➢ Passport of the operator (s) ➢ Resolution of the board of directors to open an account and identification of those who have authority to operate the account.	➢ A copy of last available financial statements duly certified by a professional accountant. ➢ Other Bank statement ➢ TIN ➢ Certificate of Grand / Aid	

	➢ Documents of nature of the NGO ➢ Certificate of registration issued by competent authority ➢ Bye-laws (certified) ➢ List of Management Committee/ Directors		
Charities or Religious Organizations	➢ National Id Card of the operator (s) ➢ Passport of the operator (s) ➢ Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. ➢ Documents of nature of the Organizations ➢ Certificate of registration issued by competent authority (if any) ➢ Bye-laws (certified) ➢ List of Management Committee/ Directors	➢ A copy of last available financial statements duly certified by a professional accountant ➢ Other Bank statement ➢ Certificate of Grant / Aid/ donation ➢ Any other legal source	
Clubs or Societies	➢ National Id Card of the operator (s) ➢ Passport of the operator (s) ➢ Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. ➢ Documents of nature of the Organizations ➢ Certificate of registration issued by competent authority (if any) ➢ Bye-laws (certified) ➢ List of Management Committee/ Directors	➢ A copy of last available financial statements duly certified by a professional (if registered) ➢ Other Bank statement ➢ Certificate of Grant / Aid ➢ Subscription ➢ If unregistered declaration of authorized person/ body	
Trusts, Foundations or similar entities	➢ National Id Card of the trustee (s) ➢ Passport of the trustee (s) ➢ Resolution of the Managing body of the Trusts, Foundation, or similar entities for opening of the account and identification of those who have authority to operate the account. ➢ Certified true copy of the Trust Deed ➢ Bye-laws (certified)	➢ A copy of last available financial statements duly certified by a professional (if registered) ➢ Other Bank statement ➢ Donation	

	➢ Power of attorney allowing transaction in the account.		
Non-Banking Financial Institutions (NBFI)	➢ Passport of all the directors ➢ National Id Card of all the directors ➢ Certificate of incorporation☐ ➢ Memorandum and Articles of Association ➢ Certificate of commencement of business ➢ List of directors in form -XII ➢ Resolution of the board of directors to open an account and identification of those who have authority to operate the account. ➢ Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. ➢ Nature of the company's business ➢ Expected monthly turnover ➢ Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee, officer or director of the company.	➢ A copy of last available financial statements duly certified by a professional accountant. ➢ Other Bank statement ➢ Trade License ➢ TIN ➢ VAT registration ➢ Cash flow statement	
Embassies	➢ Valid Passport with visa of the authorized official ➢ Clearance of the foreign ministry ➢ Other relevant documents in support of opening account	N/A	