Guideline for Prevention of Money Laundering & Terrorist Financing

2023

Bank Asia

Focus Group

Coordinator:

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

Members:

Mr. Md. Arshad Mahmud Khan
EVP, DCAMLCO & Head of AML & CFT Division
Bank Asia Ltd, Corporate Office, Dhaka

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

Md. Abdus Sabur Khan
AVP, AML & CFT Division
Bank Asia Ltd, Corporate Office, Dhaka

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

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

Preface

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

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

To comply with the requirement of Bangladesh Financial Intelligence Unit (BFIU) under the international initiatives, Bank Asia has prepared "Guidelines for Prevention of Money Laundering and Terrorist Financing-2023". Bank Asia instructs the Branches/Divisions/Departments/SME Service Centers/Islamic Wings/Agent Banking to follow the guideline in order to mitigate Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks.

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

Table of Contents

CHAPTER I: BACKGROUND

1.1 Preamble:

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

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

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

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

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

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

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

1.2 Definition of Money Laundering

Money laundering can be defined in a number of ways. But the fundamental concept of Money Laundering refers to the methods criminals use to hide and disguise money constructing from crime or illegitimate source. If it is successful, then the identity of money can be disguised and ultimately appears to legitimate.

The term "laundering" is used when criminals turn their "dirty" criminal money into 'clean' funds without arousing suspicion. Getting it into the financial system means that it becomes harder to trace and confiscate. Drug traffickers, terrorists, armed robbers, burglars and fraudsters all tend to launder the proceeds of their crimes through banking channels.

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

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

Most countries subscribe to the following definition which was adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

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

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

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

"Money Laundering" means -

i) knowingly move, convert, or transfer property involved in an offence for the following purposes:-
   1) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
   2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
ii) smuggling money or property earned through legal or illegal means to a foreign country;
iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or
iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;

v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
viii) participating in, associating with conspiring, attempting, abetting, instigate or counsel to commit any offence(s) mentioned above;

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

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

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

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

01.	Corruption and bribery;	15.	Theft or robbery or dacoity or piracy or hijacking of aircraft;
02.	Counterfeiting currency;	16.	Human Trafficking or obtaining money or trying to obtain money or valuable goods giving someone false assurances of employment abroad;
03.	Counterfeiting deeds and documents;	17.	Dowry;
04.	Extortion;	18.	Smuggling and offences related to customs and excise duties;
05.	Fraud;	19.	Tax related offences;
06.	Forgery;	20.	Infringement of intellectual property rights;
07.	Illegal trade of firearms;	21.	Terrorism or financing in terrorist activities;
08.	Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;	22.	Adulteration or the manufacture of goods through infringement of title;
09.	Illegal trade in stolen and other goods;	23.	Offences relating to the environment;
10.	Kidnapping, illegal restrain and hostage taking;	24.	Sexual exploitation;
11.	Murder, grievous physical injury;	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;
12.	Trafficking of women and children;	26.	Organized crime, and participation in organized criminal groups;
13.	Black marketing ;	27.	Racketeering; and
14.	Smuggling of domestic and foreign currency;	28.	Any other offence(s) declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official (Bangladesh) Gazette, for the purpose of this Act.

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

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

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

i) Bank;
ii) Financial institution;
iii) Insurer;
iv) Money changer;
v) Any company or institution which remits or transfers money or money value;
vi) Any other institution carrying out its business with the approval of Bangladesh Bank;
vii) (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-Governmental Organization
(3) Cooperative Society
ix) Real estate developer;
x) Dealer in precious metals and/or stones;
xi) Trust and Company Service Provider;
xii) Lawyer, notary, other legal professionals and accountant;
xiii) Any other institution which Bangladesh Financial Intelligence Unit (BFIU) may notify from time to time with the approval of the Government.

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

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

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

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

"Bank" has been defined in section 2(t) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as – "Bank" means a bank company defined under section 5 (o) of the Bank Companies Act, 1991 (Act No. XIV of 1991) and it shall also include any other institution designated as a bank under any other law.

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

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

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

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

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

"Stock Dealer and Stock Broker" has been defined in section 2 (ee) (1) of the Money Laundering Prevention Act, 2012 (Amendment 2015) as – **"**Stock Dealer and Stock Broker" means an institution defined under rule 2(i) and (j) of the Securities and Exchange Commission (Stock Dealer, Stock Broker and Authorized Representative) Rules 2000.
"Portfolio Manager and Merchant Banker" has been defined in section 2 (ee) (2) of the Money Laundering Prevention Act 2012 (Amendment 2015) as – "Portfolio Manager and Merchant Banker" means institution defined under rule 2(f) and 2 (j) of the Securities and Exchange Commission (Merchant Banker and Portfolio Manager) Rules 1996.

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

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

1.3 The Economic and Social Consequences of Money Laundering

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

The potential macroeconomic consequences of unchecked money laundering include:

- **Increased Exposure to Organized Crime and Corruption:** Successful money laundering enhances the profitable aspects of criminal activity. When a country is seen as a haven for money laundering, it will

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

- **Undermining the Legitimate Private Sector:** One of the most serious microeconomic effects of money laundering is felt in the private sector.
  Money launderers are known to use front companies businesses that appear legitimate and engage in legitimate business but are in fact controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to hide the ill-gotten gains.
  By using front companies and other investments in legitimate companies, money laundering proceeds can be used to control whole industries or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxes, thus depriving the country of revenue.
- **Weakening Financial Institutions:** ML, TF and PF can harm the soundness of a country's financial sector. They can negatively affect the stability of individual banks or other financial institutions, such as securities firms and insurance companies. The establishment and maintenance of an effective AML, CFT & CPF program is usually part of a financial institution's charter to operate; non-compliance can result not only in significant civil money penalties, but also in the loss of its charter.

- **Dampening Effect on Foreign Investments:** Although developing economies cannot afford to be too selective about the sources of capital they attract, there is a dampening effect on foreign direct investment when a country's commercial and financial sectors are perceived to be compromised and subject to the influence of organized crime. To maintain a business-friendly environment these impedances have to be weeded out.
- **Loss of Control of, or Mistakes in, Decisions Regarding Economic Policy:** Due to the large amounts of money involved in the money laundering process, in some emerging market countries these illicit proceeds may dwarf government budgets. This can result in the loss of control of economic policy by governments or in policy mistakes due to measurement errors in macroeconomic statistics.
  Money laundering can adversely affect currencies and interest rates as launderers reinvest funds where their schemes are less likely to be detected, rather than where rates of return are higher. ML can increase the threat of monetary instability due to the misallocation of resources from artificial distortions in asset and commodity prices.

- **Economic Distortion and Instability:** Money launderers are not primarily interested in profit generation from their investments, but rather, in protecting their proceeds and hiding the illegal origin of the funds. Thus, they "invest" their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, to the extent that money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin, economic growth may suffer.

- **Loss of Tax Revenue:** ML diminishes government tax revenue and, therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case.

A government revenue deficit is at the center of economic difficulties in many countries, and correcting it is the primary focus of most economic stabilization programs.

- **Risks to Privatization Efforts:** ML threatens the efforts of many states trying to introduce reforms into their economies through the privatization of state-owned properties such as land, resources, or enterprises. Sometimes linked with corruption or inside deals, a government may award a state privatization tender to a criminal organization potentially at an economic loss to the public. Moreover, while privatization initiatives are often economically beneficial, they can also serve as a vehicle to launder funds.
- **Reputation Risk for the Country:** A reputation as a ML, TF & PF haven can harm development and economic growth in a country. It diminishes legitimate global opportunities because foreign financial institutions find the extra scrutiny involved in working with institutions in money laundering havens is too expensive.

  Once a country's financial reputation is damaged, reviving it is very difficult and requires significant resources to rectify a problem that could have been prevented with proper anti money laundering controls. Other effects include specific counter-measures that can be taken by international organizations and other countries, and reduced eligibility for governmental assistance.

- **Risk of International Sanctions:** In order to protect the financial system from ML, TF and PF the United States, the United Nations, the European Union, and other governing bodies may impose sanctions against foreign countries, entities or individuals, terrorists and terrorist groups, drug traffickers, and other security threats.

  FATF also maintains a list of jurisdictions identified as high-risk and non-cooperative, whose AML, CFT & CPF regimes have strategic deficiencies and are not at international standards. As a result, FATF calls on its members to implement counter-measures against the jurisdiction such as financial institutions applying enhanced due diligence to business relationships and transactions with natural and legal persons from the identified jurisdiction in an attempt to persuade the jurisdiction to improve its AML, CFT & CPF regime.

- **Social Costs:** Significant social costs and risks are associated with money laundering. It also enables drug traffickers, smugglers and other criminals to expand their operations. This drives up the cost of government expenses and budgets due to the need for increased law enforcement and other expenditures (for example, increased healthcare costs for treating drug addicts) to combat the serious consequences that result. Financial institutions that rely on the proceeds of crime face great challenges in adequately managing their assets, liabilities and operations, attracting legitimate clients.

1.4 Stages of Money Laundering

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

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

- **Placement**: The physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international. Examples of placement transactions include:
    - Blending of funds: Comingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned restaurant.
    - Foreign exchange: Purchasing of foreign exchange with illegal funds.
    - Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements.
    - Currency smuggling: Cross-border physical movement of cash or monetary instruments.
    - Loans: Repayment of legitimate loans using laundered cash.
    - Purchasing monetary instruments i.e. travelers' checks, payment orders.
    - Using cash to purchase expensive items that can be resold.
- **Layering**: The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds. This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds. Examples of layering transactions include:
    - Electronically moving funds from one country to another and dividing them into advanced financial options and or markets.
    - Moving funds from one financial institution to another or within accounts at the same institution.
    - Converting the cash placed into monetary instruments.
    - Reselling high value goods and prepaid access/stored value products.
    - Investing in real estate and other legitimate businesses.
    - Placing money in stocks, bonds or life insurance products.
    - Using shell companies to obscure the ultimate beneficial owner and assets.
    - Early surrender of an annuity without regard to penalties.
    - L/Cs with false invoices/bills of lading etc.
- **Integration**: Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth.

  This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets. Examples of integration transactions include:
    - Purchasing luxury assets like property, artwork, jewelry or high end automobiles.
    - Getting into financial arrangements or other ventures where investments can be made in business Enterprises.

1.5 Definition of Terrorist Financing

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

Financing of Terrorism includes:

- providing or collecting property for carrying out an act of terrorism;
- providing services for terrorism purposes;
- arranging for retention or control of terrorist property; or
- Dealing with terrorist property.

The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

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

2) For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b).

According to the article 6 of the Anti-Terrorism Act, 2009 (Amendment 2012 & 2013) of Bangladesh, terrorist activities means:

(1) If any person, entity or foreigner-

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

i) kills, causes grievous hurt to, confines or kidnaps any person or attempts to do the same;
ii) conspires, abets or instigates any person to kill, injure seriously, confine or kidnap any person; or
iii) damages or tries to damage the property of any other person ,entity or the Republic ; or
iv) conspires or abets or instigates to damage the property of any other person, entity or the Republic; or
v) uses or keeps in possession any explosive substance, inflammable substance and arms for the purposes of sub-clauses (i),(ii), (iii) or (iv);

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

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

(d) knowingly uses or possesses any terrorist property;

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

(f) commits any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature

or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act; the person, entity or foreigner shall be deemed to have committed the offence of "terrorist activities";

(2) If any person or foreigner,-

(a) commits an offence under sub-clause (i) of clause(a) of sub- section(1), the person shall be punished with death or imprisonment for life and in addition to that a fine may also be imposed;

(b) commits an offence under sub-clause (ii) of clause (a) of sub-section (1),the person shall, if the offence is punishable with death, be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14(fourteen) years but not less than 4(four) years, and with fine;

(c) commits an offence under sub-clause (iii) of clause (a) of sub-section (1), the person shall be punished with imprisonment for life or rigorous imprisonment for a term not exceeding 14(fourteen) years but not less than 4(four) years, and with fine;

(d) commits an offence under sub-clause (iv) of clause (a) of sub-section(1), the person shall be punished with rigorous imprisonment for a term not exceeding 14(fourteen) years but not less than 4(four) years, and with fine;

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

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

(4) If any entity commits the offence of terrorist activities,

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

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

Offence of Terrorist Financing: -

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

(a) to carry out terrorist activity;

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

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

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

1.6 The Link between Money Laundering and Terrorist Financing

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or of illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.
As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

1.7 Why We Must Combat Money Laundering and Terrorist Financing

According to Mr. Min Zhu, former Deputy Managing Director of the IMF --
"Effective AML and CFT regimes are essential to protect the integrity of markets and of the global financial Framework as they help mitigate the factors that facilitate financial abuse."
Actions taken by Bank 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.

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 & PF activities, and it did not take proper action against that ML, TF & PF 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 & PF 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.

1.8 How Financial Institutions can Combat Money Laundering

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

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

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

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

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

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

7. Bank Asia shall maintain and update the listed individuals and entities in electronic form to run on regular basis a system checking at the website of United Nations for updated list. Bank Asia shall run regular check on the given parameters, including transactional review, to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.

CHAPTER II: INTERNATIONAL INITIATIVES

2.1 International Initiatives

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

2.2 The United Nations

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

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

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

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

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

2.3 The Vienna Convention

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

2.4 The Palermo Convention

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

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

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

2.5 International Convention for the Suppression of the Financing of Terrorism

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

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

2.6 Security Council Resolution 1267 and Successors

The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the "Sanctions Committee" (now called the 1267 Committee). The initial Resolution 1267 of October 15, 1999, dealt with the Taliban and was followed by 1333 of December 19, 2000, on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002), provided some exclusions (1452 of December 20, 2002), and measures to improve implementation (1455 of January 17, 2003).

The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States. The most recent list is available on the website of the 1267 Committee.

2.7 Security Council Resolution 1373

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

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

2.8 Security Council Resolution 1540

UNSCR 1540 (2004) imposes binding obligations on all States to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery, and establish appropriate domestic controls over related materials to prevent their illicit trafficking. It also encourages enhanced international cooperation on such efforts. The resolution affirms support for the multilateral treaties whose aim is to eliminate or prevent the proliferation of WMDs (weapons of mass destructions) and the importance for all States to implement them fully; it reiterates that none of the obligations in resolution 1540 (2004) shall conflict with or alter the rights and obligations of

States Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, the Chemical Weapons Convention, or the Biological Weapons Convention or alter the responsibilities of the International Atomic Energy Agency (IAEA) and Organization for the Prohibition of Chemical Weapons (OPCW).

2.9 The Counter-Terrorism Committee

As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism.

Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution‘s measures and report regularly on progress. In this regard, the CTC has asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism in relation to the requirements of Resolution 1373.

2.10 Counter-Terrorism Implementation Task Force (CTITF)

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

2.11 Global Program against Money Laundering

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

2.12 The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 35 countries and territories and two regional organizations. There are also 31 associate members or observers of FATF (mostly international and regional organizations) that participate in its work.

2.13 FATF 40 Recommendations

FATF adopted a set of 40 recommendations to prevent money laundering. These Forty Recommendations constituted a comprehensive framework for AML and were designed for universal application by countries

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

2.14 FATF New Standards

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

Table 1: Summary of new FATF 40 Standards

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

2.14.1 The FATF Recommendations

A. AML & CFT Policies and Coordination

1. Assessing risks and applying a risk-based approach

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

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

2. National cooperation and coordination

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

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

B. Money Laundering and Confiscation

3. Money laundering offence

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

4. Confiscation and provisional measures

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of *bona fide* third parties:
(a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations, or (d) property of corresponding value.

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

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

C. Terrorist Financing And Financing of Proliferation

5. Terrorist financing offence

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

6. Targeted financial sanctions related to terrorism and terrorist financing

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The

resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) Designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and it's financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organizations

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

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

D. Preventive Measures

9. Financial institution secrecy laws

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

Customer Due Diligence and Record-Keeping

10. Customer due diligence

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

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

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

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

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

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

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

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

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

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

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

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

12. Politically exposed persons

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

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

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

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

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

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

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(b) assess the respondent institution's AML & CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships;

(d) clearly understand the respective responsibilities of each institution; and

(e) With respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

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

14. Money or value transfer services

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take

action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

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

15. New technologies

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

16. Wire transfers

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

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

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

Reliance, Controls and Financial Groups

17. Reliance on third parties

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

The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with

Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

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

18. Internal controls and foreign branches and subsidiaries

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

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

19. Higher-risk countries

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

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

Reporting of Suspicious Transactions

20. Reporting of suspicious transactions

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

21. Tipping-off and confidentiality

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

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

Designated Non-Financial Businesses and Professions

22. DNFBPs: Customer Due Diligence

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

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) Lawyers, notaries, other independent legal professionals and accountants - when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers - when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures

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

(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities

of accountants, including auditing.

(b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

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

E. Transparency and Beneficial Ownership of Legal Persons and Arrangements

24. Transparency and beneficial ownership of legal persons

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

25. Transparency and beneficial ownership of legal arrangements

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

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

26. Regulation and supervision of financial institutions

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

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML & CFT purposes. This should include applying consolidated group supervision for AML & CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML & CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML & CFT requirements.

27. Powers of supervisors

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

28. Regulation and supervision of DNFBPs

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

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML & CFT measures. At a minimum:

- Casinos should be licensed;
- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
- Competent authorities should ensure that casinos are effectively supervised for compliance with AML & CFT requirements.

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML & CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

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

Operational and Law Enforcement

29. Financial intelligence units

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing and for the dissemination of the results of that analysis.

The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities

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

31. Powers of law enforcement and investigative authorities

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

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

32. Cash couriers

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

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

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

General Requirements

33. Statistics

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

34. Guidance and feedback

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

Sanctions

35. Sanctions

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

G. International Cooperation

36. International instruments

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

37. Mutual legal assistance

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

(a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.

(b) Ensure that they have clear and efficient processes for the timely prioritization and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

(c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

(d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

(e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

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

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

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

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

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

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

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

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

38. Mutual legal assistance: freezing and confiscation

Countries should ensure that they have the authority to take expeditious action in response to , with requests to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is

inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

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

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

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

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

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

40. Other forms of international cooperation

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

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

2.15 Monitoring Members Progress

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

2.16 The NCCT List

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

2.17 International Cooperation Review Group (ICRG)

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

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

2.18 The Basel Committee on Banking Supervision

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

2.18.1 Statement of Principles on Money Laundering

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

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

2.18.2 Basel Core Principles for Banking

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

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

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

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

2.18.3 Customer Due Diligence

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

2.19 International Organization of Securities Commissioners

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

2.20 The Egmont Group of Financial Intelligence Units

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

of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs worldwide.

The mission of the Egmont Group has been expanded in 2004 to include specifically financial intelligence on terrorist financing. To be a member of the Egmont Group, a country's FIU must first meet the Egmont FIU definition, which is "a central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national regulation, in order to counter money laundering and terrorist financing."

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

2.21 Asia Pacific Group on Money Laundering (APG)

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

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

The APG has five key roles:

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

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

CHAPTER III: NATIONAL INITIATIVES

3.1 National Initiatives

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

3.2 Founding Member of APG:

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

3.3 Legal Framework:

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

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

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

3.4 Central and Regional Taskforces

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

3.5 Anti-Money Laundering Department

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

3.6 Bangladesh Financial Intelligence Unit

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

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

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

3.7 National ML & TF Risk Assessment (NRA)

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

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

3.8 National Strategy for Preventing ML, TF & PF

National Strategy for Preventing Money Laundering and Combating Financing of Terrorism, 2011-2013 was adopted by the NCC in April 2011. Bangladesh has completed all the action items under the 12(twelve) strategies during that time. A high level committee headed by the Head of BFIU and Deputy Governor of Bangladesh Bank has formulated the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2015-2017 which has been approved by the National Coordination Committee (NCC) on ML & TF. The strategy identifies the particular action plan for all the Ministries, Division and Agency to develop an effective AML & CFT system in Bangladesh. The strategy consists of following 11 (eleven) strategies against 11 (eleven) strategic objectives:

- Updating National ML & TF Risk Assessment Report regularly and introducing Risk Based Approach of monitoring and supervision of all reporting organizations.
- Deterring corruption induced money laundering considering corruption as a high risk.

- Modernization of Border Control Mechanism and depriving perpetrators from use of proceeds of crime to prevent smuggling of gold and drugs, human trafficking, other transnational organized crimes considering the risk thereon.
- Tackling illicit financial flows (IFF) by preventing the creation of proceeds of crime, curbing domestic and cross-border tax evasion and addressing trade based money laundering.
- Discouraging illicit fund transfer by increasing pace of stolen assets recovery initiatives and 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 were arranged by BFIU. It also has arranged a number of training programs, workshops, seminars and road-shows to create awareness among the staff of reporting organizations, regulatory authorities about related issues.

3.10 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 intelligence agencies. The committee tried to find out more sensitive and sophisticated ways to create awareness among the general people about the negative impact of terrorism.

3.12 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 & PF risk associated with the NGO/NPO sector in 2008. As the sector was mainly depending on foreign donation, the report identified strategic deficiencies of supervision and control of the

regulator. According to the requirement of FATF Recommendation 8, BFIU has conducted NGO/NPO sector review with the help from NGO Affairs Bureau, Microcredit Regulatory Authority, Department of Social Services and Research Department of Bangladesh Bank. The review report is a very comprehensive one that covers legal & institutional aspects, supervision mechanism, compliance requirements and risk & vulnerabilities relating to ML &TF.

3.14 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 and Bangladesh Bank.

3.16 Risk Based Approach

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

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

3.17 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 79 (till June 22) MoU so far to exchange the information related to ML & TF with FIU of other countries.**

CHAPTER IV: VULNERABILITIES OF FINANCIAL INSTITUTIONS

4.1 Vulnerability of the Financial System to Money Laundering

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

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

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

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

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

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

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

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

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

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

to fund the business activity. Banks and non-banking financial institutions offering international trade services should be on their guard for laundering by these means.

4.2 Vulnerabilities of Products and Services

4.2.1 Lease/Term Loan Finance

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

4.2.2 Factoring

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

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

(a) Direct Export Factoring: The direct export factoring is mostly used when handling exports to countries where the corresponding factoring network does not reach. This form of direct export factoring is often provided in combination with outside credit insurance scheme and the traditional services offered by a banking network.

1) The exporter ships the goods to his importer/ debtor.
2) The exporter assigns his invoices to the export factor.
3) The export factor pays the seller the agreed advance.
4) The export factor handles the accounts receivable in accordance with the sale contract between the exporter and the importer.
5) The importer pays on the due date to export factor.
6) The export factor settles the advance with the funds received and forwards the balance to the seller.

(b) Direct import factoring: Factors in an exporter's country are not sometimes perceived very active in marketing international factoring services. In that case, factors in importers' country offer their services directly to foreign suppliers. The exporter may also establish direct contact with factors in the importing country. The resultant arrangement will be of direct import factoring.

1. The exporter ships the goods to his importer.
2. The exporter assigns his invoices to the import factor, who assumes the credit risk, provided this has been agreed to beforehand.

3. The import factor handles the accounts receivable in accordance with the sales contract between the exporter and the importer.
4. The importer pays the import factor on the due date.
5. The import factor forwards the payment to the exporter, possibly deducting the agent's commission.

(c) Back to back factoring:

This is a highly specialized form of international factoring. It is used when the supplier sells his goods through his subsidiary to the importers/ debtors in the import factors' country. This is done to avoid large volumes of sales to a few importers/ debtors for whom it is difficult for the import factor to cover the credit risk. In such a case, import factor can sign a domestic factoring agreement with the importer/ debtor. This agreement will facilitate to get debtors' receivables as security for the credit line as it has been asked to establish in favor of export factor.

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

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

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

4.2.3 Private Placement of Equity/Securitization of Assets

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

4.2.4 Personal Loan/Car Loan/Home Loan

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

4.2.5 SME/Women Entrepreneur Loan

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

4.2.6 Deposit Scheme

FIs can sell deposit products with at least a six months maturity period. However, the depositor can encash their deposit money prior to the maturity date with prior approval from Bangladesh Bank, foregoing interest income. This

Deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong measures.

4.2.7 Loan Backed Money Laundering

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

4.2.8 Electronic Transfers of Funds

An electronic transfer of funds is any transfer of funds that is initiated by electronic means, such as an Automated Clearing House (ACH) computer, an automated teller machine (ATM), electronic terminals, mobile telephones, telephones or magnetic tapes. It can happen within a country or across borders, and trillions of dollars are transferred in millions of transactions each day as it is one of the fastest ways to move money. As such, illicit fund transfers can be easily hidden among the millions of legitimate transfers that occur each day.

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

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

4.2.9 Correspondent Banking

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

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

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

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

4.2.10 Payable through Accounts

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

PTAs differ from normal correspondent accounts in that the foreign bank's customers have the ability to directly control funds at the correspondent bank. PTAs can have a virtually unlimited number of sub-account holders, including individuals, commercial businesses, finance companies, exchange houses or casas de cambio, and even other foreign banks. The services offered to subaccount holders and the terms of the PTAs are specified in the agreement signed by the correspondent and the respondent banks. PTAs held in the names of respondent banks often involve checks encoded with the bank's account number and a numeric code to identify the sub-account, which is the account of the respondent bank's customer. Sometimes, however, the sub-account holders are not identified to the correspondent bank.

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

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

4.2.11 Crypto-Currencies:

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

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

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

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

Ensuring price stability is likely to remain the pre-eminent monetary policy objective for central banks, an objective unchanged by the growth of crypto-currencies. As the 'licensed distributors' of fiat currency, central banks should remain able to set interest rates in their domestic fiat currency units. The introduction of crypto-currencies should not fundamentally disrupt central banks' use of interest rates to stabilize the inflation rates of their own fiat currencies.
Crypto-currencies also raise consumer protection, anti-money laundering, and counter-terrorism financing concerns. As niche payment systems, crypto-currencies do not currently pose material financial stability concerns, but risks could increase in materiality if crypto-currencies become more popular and/or more integrated with the activities of traditional financial institutions. Crypto-currencies are extremely volatile, and there are significant risks associated with holding such assets. There is no certainty that specific crypto-currencies, such as Bitcoin, will continue to function and be valued by Trans actors, and there are non-trivial risks of loss and theft.

4.3 Structural Vulnerabilities

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

CHAPTER V: COMPLIANCE REQUIREMENTS UNDER THE LAW & CIRCULAR

5.1 Compliance Requirements under the Laws

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

5.1.1 Money Laundering Prevention Act 2012 (Amendment 2015)

Under the Section -

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

(1) For the purposes of this Act, money laundering shall be deemed to be an offence.

(2) Any person who commits or abets or conspires to commit the offence of money laundering shall be punished with imprisonment for a term of 4(four) years but not exceeding 12(twelve) years and in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10(ten) lacs, whichever is greater. However, in case of failure of the payment of the fine in due time, the court may issue an order of extra imprisonment considering the amount of the unpaid fine.

(3) In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved or related with money laundering or any predicate offence.

(4) Any entity which commits or abets, assists or conspires to commit the offence of money laundering under this section, subject to the provisions of section 27, measures shall be taken as per sub-section (2) and punished with a fine of not less than twice the value of the property related to the money laundering or taka 20(twenty) lacs, whichever is higher and in addition to this the registration of the said entity shall be liable to be cancelled. However, in case of failure in payment of the fine by the entity in due time, the court may, considering the amount of unpaid fine, issue an order of imprisonment to the entity's owner, chairman or director or by whatever name he is regarded.

(5) It shall not be a prerequisite to charge or punish for money laundering to be convicted or sentenced for any predicate offence.

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

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

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

(1) No person shall, with an ill motive, divulge any information relating to the investigation or any other related information, to any person, organization or news media.

(2) Any person, institution or agent empowered under this Act shall refrain from using or divulging any information collected, received, retrieved or known by the person, institution or agent during the course of

employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purpose of this Act.

(3) Any person who contravenes the provisions contained in sub-sections (1) and (2) shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine, not exceeding Tk. 50 (fifty) thousand or with both.

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

(1) Any person who, under this Act ---

(a) Obstructs or declines to cooperate with any investigation officer for carrying out the investigation; or

(b) Declines to supply information or submit a report being requested without any reasonable ground;

shall be deemed to have committed an offence under this Act.

(2) Any person who is convicted under sub-section (1) shall be punished with imprisonment for a term not exceeding 1 (one) year or with a fine not exceeding Tk. 25 (twenty five) thousand or with both.

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

(1) No person shall knowingly provide false information in any manner regarding the source of fund or self-identity or the identity of an account holder or the beneficiary or nominee of an account.

(2) Any person who violates the provisions of sub-section (1) shall be punished with imprisonment for a term not exceeding (three) years or a fine not exceeding Tk. 50 (fifty) thousand or both.

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

(1) For the purposes of this Act Bangladesh Financial Intelligence Unit (BFIU) shall have the following powers and responsibilities:

(a) To analyze or review information related to cash transactions and suspicious transactions received from any reporting organizations and information obtained through any other sources and to collect necessary additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data and information on the same and, and investigating agency or the relevant law enforcement agencies for taking the necessary actions;

(b) Notwithstanding anything contained in any other law, obtain necessary information or report from reporting organizations.

(c) Issue an order to any reporting organization to suspend or freeze transactions of any account for maximum of 7(seven) times by 30 (thirty) days each if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing an offence or money of an account has been or might be used to commit a crime/an offence:
Provided that such order may be extended for additional period of a maximum of 6 (six) months by of 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account;

(d) Issue from time to time, any directions necessary for the prevention of money laundering to the reporting organizations;

(e) Conduct on-site inspections on the reporting organizations, if necessary.

(f) Arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by Bangladesh Financial Intelligence Unit (BFIU);

(g) Carry out any other functions including monitoring activities of the reporting organizations necessary for the purpose of this Act.

(2) If any investigation agency makes a request to provide it with any information in any investigation relating to money laundering or suspicious transaction, then Bangladesh Financial Intelligence Unit (BFIU) shall provide with such information where no obligation for it is under any existing law or for any other reason.

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

(4) If any reporting organization provides false information or statement requested under this Section, BFIU may impose a fine on such organization not less than taka 20 (twenty) thousand but not exceeding taka 5 (five) lacs and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Financial Intelligence Unit (BFIU) may suspend the registration or license of the organization or any of its branches/service centers/booths/agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.

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

(6) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Financial Intelligence Unit (BFIU) under clause (c) of sub-section (1), BFIU may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.

(7) If any person or entity or reporting organization fails to pay any fine imposed by BFIU under sections 23 and 25 of this Act, Bangladesh Financial Intelligence Unit (BFIU) shall inform Bangladesh Bank and BFIU may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh and in this regard if any amount of the fine remains unrealized Bangladesh Financial Intelligence

Unit (BFIU) may, if necessary, make an application before the court for recovery and the court may pass such order which it deems fit.

(7a) while conducting enquiry and investigation of the offences under this Act an investigation agency may obtain documents and information related to the customer of a bank or financial institution through an order by the competent court or through Bangladesh Financial Intelligence Unit.

(8) If any reporting organization is imposed fine under sub-section (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit (BFIU) may also impose a fine not less than taka 10(ten) thousand but not exceeding taka 5(five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

7. Responsibilities of Reporting Organizations in Preventing the Offence of Money Laundering

– (as per section 25 of MLP Act 2012 (Amendment 2015)

(1) Reporting Organizations shall have the following duties and responsibilities including other duties and responsibilities specified by rules in the prevention of money laundering:

(a) maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;

(b) in case of closed account of any customer, keep previous records of transactions of such account and its transactions for at least 5(five) years from the date of closure;

(c) provide the information maintained under sub-sections (a) and (b) to Bangladesh Financial Intelligence Unit (BFIU) from time to time, as requested;

(d) if any doubtful transaction or attempt of such transaction as defined under 2(n) is observed by reporting organization, it shall be reported as Suspicious Transaction Report (STR) to the Bangladesh Financial Intelligence Unit (BFIU) proactively and immediately.

(2) If any reporting organization violates the provisions contained in sub-section (1), Bangladesh Financial Intelligence Unit (BFIU) or regulatory/controlling authority of the reporting organization**:**

(a) Impose a fine on the said reporting organization of a minimum of Tk. 50 (fifty) thousand and up to a maximum of Tk. 25 (twenty-five) lacs; and

(b) Cancel the license or the authorization for carrying out commercial activities of the said Organization or any of its branches/service centers/booths/agents, in addition to the fine mentioned in clause (a), and where appropriate, shall inform the registration or licensing or authority about the subject matter so that the relevant authority may take appropriate action against the said Organization.

(3) Bangladesh Bank shall collect the sum of fine received under sub-section (2) under manner determined by it and the sum received shall be deposited into the State Treasury.

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

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

Explanation – In this section

"Director" means any partner or the Board of Directors, by whatever name it is called; it also means its member.

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

Under the Section-

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

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

(a) to carry out terrorist activity;

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

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

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

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

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

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

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

(a) to call for a report relating to any suspicious transaction from any reporting agency, analyze or review the same and to collect additional information relating thereto for the purpose of analyzing or reviewing the same and maintain record or database of them and, as the case may be, provide with the said information or report to the police or other concerned law enforcement agencies for taking necessary actions;

(b) if there is reasonable ground to suspect that a transaction is connected to terrorist activities, to issue a written order to the respective reporting agency to suspend or freeze transactions of that relevant account for a period not exceeding 30 (thirty) days and, if it appears necessary to reveal correct information relating to transactions of the said account, such suspension or freezing order may be extended for an additional term not exceeding 6 (six) months by 30 (thirty) days at a time;

(c) to monitor and supervise the activities of the reporting agencies;

(d) to give directions to the reporting agencies to take preventive steps to prevent financing of terrorist activities and proliferation of weapons of mass destructions (WMD);
(e) to monitor the compliance of the reporting agencies and to carry out on-site inspection of the reporting agencies for carrying out any purpose of this Act; and
(f) to provide training to the officers and employees of the reporting agencies for the purpose of identification of suspicious transactions and prevention of financing of terrorist activities. BFIU, on identification of a reporting agency or any of its customers as being involved in a suspicious transaction connected to financing of terrorist activities, shall inform the same to the police or the appropriate law enforcement agency and provide all necessary cooperation to facilitate their inquiries and investigations into the matter.

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

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

(4)The fund seized under sub-section (3) shall be subject to disposal by the concerned court or pursuant to the concerned agreements, conventions or resolutions adopted by the United Nations Security Council.

(5)The power and responsibilities of BFIU under the provisions of this Act shall be exercised by BFIU, and if BFIU requests to provide with any information under this Act, all the governmental, semi-governmental or autonomous bodies, or any other relevant institutions or organizations shall, on such request or, as the case may be, spontaneously provide it with such information.

(6)Bangladesh Financial Intelligence Unit shall, on request or, as the cases may be, spontaneously provide the financial intelligence units of other countries or any other similar foreign counterparts with any information relating to terrorist activities or financing of terrorist activities.

(7) For the interest of investigation relating to financing of terrorist activities, the law enforcement agencies shall have the right to access any document or file of any bank under the following conditions, namely:-
(a) according to an order passed by a competent court or special tribunal; or
(b) with the approval of the BFIU.

(8) If any reporting agency fails to comply with the directions issued by BFIU under this section or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine, determined and directed by BFIU, not exceeding taka 25 (twenty five) lac, and BFIU may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.
(9) If any reporting agency fails to pay or does not pay any fine imposed by BFIU according to sub-section (8), BFIU may recover the amount from the reporting agency by debiting its accounts maintained in any other bank or financial

Institution or in BFIU and in case of any unrealized or unpaid amount, BFIU may, if necessary, apply before the concerned court for recovery.

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

(1) Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through it which is connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to BFIU without any delay.

(2) The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by BFIU under section 15, which are applicable to the reporting agency, have been complied with or not.

2[(3) If any reporting agency fails to comply with the provision under sub-section (1), the said reporting agency shall be liable to pay a fine, determined and directed by BFIU, not exceeding taka 25 (twenty five) lac and BFIU may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

(4) If the Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of any reporting organization fails to comply with the provision of sub-section (2), the Chairman of the Board of Directors, or the Chief Executive Officer, as the case may be, shall be liable to pay a fine, determined and directed by Bangladesh Bank, not exceeding taka 25 (twenty five) lac, and BFIU may remove the said person from his office or, as the case may be, shall inform the competent authority about the subject matter to take appropriate action against the person.

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

5.2 Compliance Requirements under Circulars

5.2.1 Policies for Prevention of Money Laundering and Terrorist Financing

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

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

5.2.2 Appointment and Training

Employee Screening: One of the major purposes of combating ML, TF and PF related activities is to protect Bank Asia from risks arising out of money laundering, terrorist financing. To meet this objective, **Bank Asia shall has maintained** proper screening mechanism in their different appointment procedures so that they do not face ML,TF and PF risks by any of their staff. ML & TF risks arose by or through its employees can be minimized if the bank follows fair recruitment procedure. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, Bank Asia should follow the following measures (at least two or three from the undermentioned points):

- reference check
- background check
- screening through or clearance from Law Enforcement Agency
- personal interviewing
- personal guarantee
- Personal profile check etc.

Before assigning an employee in a particular job or desk, Human Resources Division of the Bank shall examine the consistency and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

Training for the officials: To ensure proper compliance of ML, TF and PF related activities Bank Asia has been arranging AML & CFT training for their all officials.

Every employee of the bank shall have at least basic AML, CFT & CPF training that should cover all the aspects of AML, CFT & CPF measures in Bangladesh. Basic AML, CFT & CPF training should be at least day long model having evaluation module of the trainees. History & background of money laundering, relevant provision of Acts, rules and circulars, guidelines, regulatory requirements, overview of international & local initiatives regarding AML, CFT & CPF, cash transaction report, suspicious transaction or activity reporting, account opening procedure and its documentation, trade based money laundering, ongoing monitoring & UN sanction screening mechanism etc. should be covered in basic AML, CFT & CPF training course. To keep the employees updated about AML & CFT measures, Bank Asia has been arranging refresher training programs of its employees on a regular basis.

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

Awareness of Senior Management

Without awareness & proper involvement of senior management of a bank, it is difficult to have effective implementation of AML & CFT measures in the bank. Banks are required to arrange, at least once in a year, an awareness program for all the members of its board of directors or in absence of board of directors, members of the highest policy making committee and people engaged with policy making of the bank.

Education and training for customers:

Bank Asia has been responding to customers on different matters including KYC. Bank Asia has also been distributed leaflets among customers time to time to make them aware about ML, TF and PF and also arranged to stick posters in every branch/SME service centers at a visible place.

5.2.3 Suspicious Transaction Reporting (STR)

According to the provision of section 25 (1) (d) of MLPA, 2012 (amendment 2015) Bank Asia have to report Bangladesh Financial Intelligence Unit (BFIU) proactively and immediately, facts on suspicious, unusual or

doubtful transactions likely to be related to money laundering. Bangladesh Bank has the power to call STR from FIs related to financing of terrorism according to section 15 of Anti-terrorism Act 2009, (Amendment 2012 & 2013).

5.3 Targeted Financial Sanctions

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

Automated Screening Mechanism of UNSCRs

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

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

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

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

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

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

5.4 Self-Assessment

Banking system in Bangladesh is mainly based on branch banking. The branches of the banks are in every corner of the country and they have an active role in stimulating the economic growth of the country. It is very difficult for

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

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

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

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

- The percentage of officers/employees that received official training on AML & CFT;
- Training, experiences and activities of BAMLCO;
- The awareness of the officers/employees about the internal AML & CFT policies, procedures and programs, and Bangladesh Bank's instructions and guidelines;
- The arrangement of AML & CFT related meeting on regular interval;
- The effectiveness of the customer identification & source of fund verification during opening an account;
- The risk categorization of customers by the branch;
- Regular update of KYC profile as per BFIU circular;
- KYC procedure for walk-in-customer, online customer etc.
- The monitoring of customers' transactions with their declared TP after categorizing the customers based on risk or transactions over specific limit;
- UN sanction screening mechanism;
- Identification of Suspicious Transaction Reports (STRs);
- Identification of Structuring;
- Cash transaction reporting;
- The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees;
- The measures taken by the branch during opening of account of PEPs, Influential person, High Official of International Organization;
- Mobile financial services or wire transfer;
- Compliance related to Head Office, BFIU and Bangladesh Bank audit;
- Transaction monitoring related to inward and outward remittance;

5.5 Independent Testing Procedure

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

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

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

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

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

While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the ICCD should examine the AML & CFT activities of the concerned branch using the specified checklists (attached with instruction circular 08/20 dated 22.06.2020) for the Independent Testing Procedure. The ICCD should send a copy of the report with the rating of the branches inspected/audited by the ICCD to the AML & CFT Division of the bank. Besides these ICCD should audit additional 10% (ten percent) of branches as per section **8.2 (2) of BFIU circular no. 26 dated June 16, 2020**. The audit team of ICCD should examine the AML & CFT related activities & determine the score of the branch and send a copy of the report to the AML & CFT Division.

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

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

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

CHAPTER VI: TRADE BASED MONEY LAUNDERING

6.1 Definition & Process

FATF defined trade-based money laundering (TBML) as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

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

6.2 Methods of Trade Based Money Laundering

TBML represents an important channel of criminal activity and, given the growth of world trade, an increasingly important money laundering and terrorist financing vulnerability. Moreover, as the standards applied to other money laundering techniques become increasingly effective, the use of trade-based money laundering can be expected to become increasingly attractive. Trade-based money laundering involves using of the following techniques to disguise the illicit origin of money:

6.2.1 Over-invoicing and Under-invoicing:

Money laundering through the over- and under-invoicing of goods and services, which is one of the oldest methods of fraudulently transferring value across borders, remains a common practice today. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

• **Over-invoicing:** By invoicing the goods or service at a price above the fair market price, the seller is able to receive value from the buyer (i.e., the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market).

• **Under-invoicing**: By invoicing the goods or service at a price below the fair market price, the seller is able to transfer value to the buyer (i.e., the payment for the goods or service is lower than the value that the buyer will receive when it is sold on the open market).

The over- and under-invoicing of exports and imports can have significant tax implications. An exporter who over-invoices the value of the goods that he ships may be able to significantly increase the value of the export tax credit (or valued-added tax (VAT) rebate) that he receives. Similarly, an importer who is under-invoiced for the value of the goods that he receives may be able to significantly reduce the value of the import duties (or customs taxes) that he pays. Both of these cases illustrate the link between trade-based money laundering and abuse of the tax system.

6.2.2. Over-shipping or Short-shipping:

The difference in the invoiced quantity of goods and the quantity of goods that are shipped whereby the buyer or seller gains excess value based on the payment made.

6.2.3 Ghost-shipping:

Fictitious trades where a buyer and seller collude to prepare all the documentation indicating goods were sold, shipped and payments were made, but no goods were actually shipped.

6.2.4 Shell companies:
Used to reduce the transparency of ownership in the transaction.

6.2.5 Multiple Invoicing:
Another technique used to launder funds involves issuing more than one invoice for the same international trade transaction. By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions.

In addition, even if a case of multiple payments relating to the same shipment of goods or delivery of services is detected, there are a number of legitimate explanations for such situations including the amendment of payment terms, corrections to previous payment instructions or the payment of late fees. Unlike over- and under-invoicing, it should be noted that there is no need for the exporter or importer to misrepresent the price of the good or service on the commercial invoice.

6.2.6 Falsely Described Goods and Services
In addition to manipulating export and import prices, a money launderer can misrepresent the quality, identity or type of a good or service. For example, an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs documents and what is actually shipped. The use of false descriptions can also be used in the trade in services, such as financial advice, consulting services and market research. In practice, the fair market value of these services can present additional valuation difficulties.

6.2.7 Black market trades:
Commonly referred to as the Black Market Peso Exchange whereby a domestic transfer of funds is used to pay for goods by a foreign importer. Letters of credit are another vehicle for money laundering. Letters of credit are a credit instrument issued by a bank that guarantees payments on behalf of its customer to a third party when certain conditions are met. Letters of credit are commonly used to finance export because exporters want assurance that the ultimate buyer of its goods will make payment and this is given by the buyer's purchase of a bank letter of credit. The letter of credit is then forwarded to a correspondent bank in the jurisdiction in which the payment is to be made. The letter of credit is drawn on when the goods are loaded for shipping, received at the importation point, clear customs and are delivered. Letters of credit can be used to facilitate money laundering by transferring money from a country with lax exchange controls, thus assisting in creating the illusion that an import transaction is involved. Moreover, letters of credit can also serve as a façade when laundering money through the manipulation of import and export prices. Another method of using letters of credits illicitly is in conjunction with wire transfers to bolster the legitimate appearance of non- existent trade transactions.

6.3 Trade Based Money Laundering "Red flag" Indicators
Although Trade Based Money Laundering is extremely difficult to monitor, track and identify, there are common Situational or behavioral indicators, or "Red Flags", that Banks should be aware of:

Customers→ Is the nature of each trade consistent with the customer's business?
Countries→ is the buyer, seller, vessel or bank involved in the trade on a sanctions list?
Transactions and Goods→ Is there potential for tax avoidance or money laundering?

Documentation and Products→ Is there complete, accurate and precise documentation for each trade?

Red flags may be present in every step of the Trade finance process and should be promptly examined. Although it is not necessarily an indicator of criminal activity, the presence of a Red flag requires thorough investigation, in order to properly determine if unlawful acts were committed.

Sl. No	Category	Red Flag Indicators
1.	Customer	• The transaction involves the receipt of cash (or by other payment methods) from third party entities that have no apparent connection with the transaction or which involve front or shell companies or wire instructions/ payment from parties which were not identified in the original letter of credit or other documentation. The transactions that involve payments for goods through cheques, bank drafts or money orders not drawn on the account of the entity that purchased the items also need further verification.
		• A client uses unusual or suspicious identification documents that cannot be readily verified.
		• A business is reluctant, when establishing a new trade relationship, to provide complete information about the nature and purpose of its business, anticipated trade activity, prior banking relationship, the names of its officers and directors or information on its business location.
		• A client's home or business telephone is disconnected.
		• The client's background differs from that which would be expected on the basis of his or her business activities.
		• A party to a transaction is a shell company.
		• Transacting businesses share the same address, provide only registered agent's Address or have other address inconsistencies.
		• Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
		• A client who significantly deviates from their historical pattern of trade activity (i.e. in terms of value, frequency or merchandise).
		• The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business strategy (e.g. a steel company that starts dealing in paper products or an information technology company that starts dealing in bulk pharmaceuticals).
		• Customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions(e.g. equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems or certain natural resources such as metals, ore and crude oil).
		• The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations.
		• The customer exhibits a lack of concern regarding risks, commissions or other transaction costs.
		• The customer has little experience in the product in which they are dealing or does not seem to appreciate the risks associated.
		• The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.
		• Excessive insistence of the customer to complete the transaction quickly.
		• Transactions which are between parties controlled by the same business entity.

2.	Countries	• Use of letter of credit to move money between those countries, where such trade would not normally occur and or is not consistent with 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.
		• Shipment locations of the goods, shipping terms or descriptions of the goods are inconsistent with letter of credit. This may include changes in shipment locations to high risk countries or changes in the quality of the goods shipped.
		• Customers are conducting business in higher-risk jurisdictions or geographic locations, particularly when shipping items through higher- risk or non- cooperative countries as defined in the AML Risk Drivers. However, this attribute in isolation would not necessarily deem a transaction as high risk.
		• Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties also should prompt additional UN/OFAC/EU review.
3.	Transactions and Goods	• Unusual deposits i.e. use of cash or negotiable instruments(such as traveler's cheques, cashier's cheques and money orders) in round denominations(to keep below reporting threshold limit) to fund bank accounts and pay for goods and services. The negotiable instruments may sequentially numbered or purchased at multiple locations and may frequently lack payee information. Further, cash payments for high –value orders are also indication of TBML activity.
		• 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.
		• In the case of merchant's trade, the trade finance mechanism should be in place for both export leg as well as import leg of transaction. If the trade finance mechanism, for example, Letters of Credit, have been provided for only the import leg of the transaction and not for export leg, it also indicates the possibility of TBML.
		• Goods or services purchased by the business do not match the customer's stated line of business.
		• The size of shipment appears inconsistent with the scale of the exporter or importer's regular business activities.
		• The goods are shipped through one or more jurisdictions or unconnected subsidiaries for no apparent economic reason.
		• The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with transaction.
		• Transport documents do not match letter of credit documents and evidence an over-shipment or under shipment not covered by the letter of credit agreement.
		• Significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped.
		• Sudden and unexplained increases in a customer's normal trade transactions.
		• Obvious misrepresentation of quantity or type of goods imported or exported.
		• Obvious over or under pricing of goods and services (as per information received from our regulators, we are not expected to be pricing experts on the many products that could be involved in trade transactions. However, staff completing trade transactions should generally know that over or under pricing can be an indicator of money laundering and or fraud and any instances that come to their attention should be investigated and if suspicious reported).

		• Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
		• The method of payment appears inconsistent with the risk characteristics of the transaction. For example, the use of an advance payment for a shipment from a new supplier in a high risk country.
		• The shipment does not make economic sense. For example, the use of a forty foot container to transport a small amount of relatively low value goods.
		• Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
		• Additionally the shipment of any high value items (such as electronics, autos, auto parts, gems and precious metals) in conjunction with other indicators may be reason for further review.
		• Other in consistencies to be considered; • (a)Routine installation, training or maintenance services are declined by the customer. • (b)Delivery dates are vague or deliveries are planned for out of the way destinations. • (c) A freight forwarding firm is listed as the product's final destination. • (d) Packaging is consistent with the stated method of shipment or destination.
4.	Documentation and Products	• The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or that incudes changes in regard to the beneficiary or location of payment without any apparent reason.
		• "Unnecessarily complex" and confusing transaction structures. These structures potentially aim to obscure a transaction's true purpose and nature.
		• A payment method that does not match the risk characteristics of the transaction.
		• Requests by exporters to take back and replace trade and shipping documents, notably if the new documents provided have been altered or issued by a different entity.
		• Abnormal markings on monetary instruments.
		• Modifications to third party documents, such as customs forms.

6.4 Preventive Measures to Combat Trade Based Money Laundering

6.4.1Risk Assessment

The Bank shall conduct a comprehensive risk assessment of its trade finance business, taking into account the customer base, geographical locations, products offered and emerging risks if any, in determining the financial crime risks they are exposed to. The Bank shall also assess the adequacy of its risk management framework and internal controls to mitigate such risks.

The trade finance-specific risk assessment could be part of the broader risk assessment performed by the Bank at the enterprise-wide level. Such an assessment allows the bank to identify the risk areas in its trade finance activities and determine whether the controls in place are robust. The enterprise-wide risk assessment is intended to enable the bank to better understand its vulnerability to ML & TF risks, including the financial crime risks presented by its trade finance business and forms the basis for the bank's overall risk-based approach.

6.4.2 Due Diligence

The level of financial crime risks posed by customers and trade finance transactions differs based on their business, geographical locations and risk profiles. A typical trade finance transaction involves a number of different parties. The parties range from buyer and seller, to their respective agents, bankers and intermediaries. In general, the bank shall treat an instructing party in a trade finance transaction as their customer and conduct appropriate due diligence measures in accordance with a risk- based approach.

Additional Information to be obtained for Trade Finance Transactions

In addition to the customer due diligence requirements set out in the Bank, the Bank should ensure the followings:

- The Bank should obtain further information to assess the financial crime risks specific to a trade finance transaction.
- The Bank should obtain additional information on other relevant parties to a trade finance transaction, taking into account the bank's role in the transaction. The Bank should develop clear procedures on the additional information required under various circumstances for all the relevant parties, including beneficiaries of L/Cs and documentary collections, agents and third parties identified.
- The type and timing of the additional information obtained depend on the bank's role in the transaction and should be in line with a risk- based approach. This also applies to cases where the bank provides credit lines for, or facilities open account trades (e.g. invoice financing, pre-shipment financing, inventory financing) of its customers. Examples of such additional information are -
    - ♣ Trading partners or counterparties of the customer (including buyers, sellers, shippers, consignees, notifying parties, shipping agents etc.)
    - ♣ nature of the goods traded;
    - ♣ Country or countries of origin of the goods (including whether the goods originate from any sanctioned country);
    - ♣ trade cycle;
    - ♣ flag of vessel, flag history and name history(to check whether it is related to any country in the list of sanctioned countries);
    - ♣ name and unique identification number {e.g. International Maritime Organization (IMO) number} of any vessel proposed to be used (e.g. to better identify if it is ultimately owned by a sanctioned party);
    - ♣ Beneficial owner, commercial operator and registered owner of the vessel involve in the transaction to trace the history of former ship owners with focus on country of residence;
    - ♣ port of loading, port-of-call and port of discharge (including whether the goods originate from or are sold to any sanctioned country) and the trade routes proposed to be used; and
    - ♣ Market prices of goods such as commodities to assess if further information should be obtained where the contract price differs significantly from the market price to mitigate financial crime risk.

- The Bank should verify information obtained on a trade finance transaction (e.g. against commercial documents, transport documents and on a risk-sensitive basis, from independent or public sources) to authenticate the details of the transaction. This should also apply to cases where the bank provide credit lines for or otherwise facilitate, open account trades (e.g. invoice financing, pre-shipment financing, inventory financing) of its customers.

Additional Information to be obtained for Trade Finance Transactions that present higher financial crime risks:

If, at the initial stage or during the course of any trade finance transaction, the bank becomes aware that the transaction presents higher financial crime risks, the bank is expected to obtain information, to assess-

(a) the transaction structure;
(b) the ports of call, including the route of the shipment, ensuring that it appears to be logical with regard to transshipment points and the final destination;
(c) the legitimacy of the payment flows;

(d) the transaction against public sources of specialized data, documents or information (e.g. the International Maritime Bureau) in relation to sea transportation to verify the authenticity of the bills of lading and to confirm that the shipment has taken place; and

(e) Whether they are dual –use goods.

In addition, the bank should conduct site visits and meetings with the instructing party, where appropriate.

6.4.3 Sanctions Controls

- ♣ Sanction screening is a major component of transactional due diligence to ensure that the Bank is not Dealing with sanctioned individuals or entities. The Bank should perform name screening on key parties to each transaction. Besides screening the parties to the transaction, such as the seller of the goods, bank should also screen the vessel used to transport the underlying goods, the shipping company, any agents or third parties present in the transaction and know the ports of call of the vessel for the particular transaction flow (origin port, destination port) where possible.
- ♣ The Bank should be aware of any adverse developments pertaining to some parties (e.g. addition to list of designated individuals/entities) present in the trade finance transaction, between the inception of the trade finance transaction and submission of trade documents since there could be significant time difference during this period. Furthermore, the Bank is expected to perform sanctions screening both at the inception of the trade finance transaction and at the point of submission of the trade finance documents as some of the transactional details e.g. vessel used to transport the cargo, ports of call, may not be known at trade inception and hence would not have been screened at that stage.

6.4.4 Trade Based Money Laundering Controls

Assessment of Deviations from Market Prices

- Checks on the reasonableness of invoice prices of goods/commodities against prevailing market prices (referred to as "price checks") are not only useful to mitigate credit risks; they also serve to identify potential fraud and ML & TF activities arising from over invoicing or under invoicing of transactions.
- Bank should perform price checks, particularly where market prices are available, minimally on a sampling basis. Policies and procedures should be clearly set up to guide staff in performing such checks, including establishing the level of acceptable price variance and escalation procedures when significant differences in prices are identified.
- **AD Branches, CTSU's and CTPCs are advised to adhere to regulatory parameters for verification of import prices and price competitiveness. As usual, AD Branches, CTSU's and CTPCs shall comply with extended due diligence in import transactions and relevant regulations without limiting to provisions of Import Policy Order in force, credit reports of suppliers, KYC and AML/CFT standards, and so on**.
- Bank could consider setting different thresholds for different types of underlying goods/commodities. There should also be periodic assessments of whether the thresholds continue to be reasonable based on prevailing market prices for the goods/commodities.
- Price checks should be performed by functions independent of front office so as to enhance the effectiveness of the checks and minimize conflicts of interest.
- There should be guidelines in place for the selection of reference prices for the purpose of performing price checks.

Related Party Transactions

- There are inherently higher risks of fraud and financial crime associated with the financing of transactions between a customer and its related parties.
- The Bank could consider implementing additional safeguards to mitigate the risks arising from related party transactions e.g. requiring documentary evidence to verify the authenticity of these related party transactions.

- Bank's front office would obtain information about a customer's business and its present and future trading profile, including information on the customer's related parties and where applicable, the typical related party transactions that occur in the course of the customer's business. However, such information may not be made available to the middle or back offices for additional due diligence, such as checks on the rationale for the trade flows and pricing, to be performed on the individual transactions.
- The middle office or back office staff processing the trade finance transactions would be better informed when identifying related party transactions if there is effective sharing of information between the front office, which would have collected information on their customer's related entities as part of the customer on-boarding and regular review process and the control or operations units processing the trade transactions.

Underlying Goods Financed

- Bank should formalize process to identify unusual transaction patterns that are inconsistent with the customers' profiles for further reviews and investigations. In addition to checking for inconsistencies in customers' trading patterns, bank is encouraged to check the descriptions of goods stated in the trade documents, particularly for descriptions which are unclear or worded in a foreign language. Bank should, on a best effort basis, determine whether the underlying goods financed are embargoed goods and there should be special attention paid to dual use goods.
- Bank should ensure that there are effective channels for information obtained by the front office during the customer on-boarding and ongoing review processes, which should include information on typical goods the customer deals in, to be shared with the middle and back office staff. This is to facilitate checks on the underlying goods by the middle and back office staff in their day-to-day processing of transactions.
- The front office should also regularly review customer transactions for inconsistencies with the customers' Profiles.

Controls over Multiple Financing of Invoices

- When invoice financing facilities are granted, banks should ensure that there are proper processes and controls in place to detect if customers have submitted the same invoice for financing more than once.

Screening of underlying import and export shipments through vessel/container tracking:

To ensure onboard of import of goods Authorized Dealers (ADs) shall conduct the tracking of shipments for relevant import transactions and To ensure safeguards of export transactions ADs shall conduct the tracking of shipments in all cases through tracking system recognized by competent authority for relevant trade transactions. (FE Circular No. 07, April 20, 2022 and FE Circular No. 09, May 17, 2022)

6.4.5 Transaction Monitoring & Filing of Suspicious Transaction Reports

- Bank should ensure its transaction monitoring processes and systems are robust to enable suspicious transactions to be fluffed, investigated and escalated. Regular compliance checks, especially on transactions that were not escalated, should be performed for quality assurance purposes.
- Bank should ensure that transactions suspected of being used for ML purposes are duly investigated and promptly escalated to the compliance function or senior management. If there are grounds to suspect that a customer is using trade finance to launder money, finance terrorism or facilitate proliferation financing (PF), STRs must be promptly filed. The bank should also minimally subject the customer account to enhanced monitoring and consider rejecting the transaction.

  Internal Escalation Procedures

  Trade controls should provide clear guidance on a good transaction review process. For example, a sample review process is outlined as follows:

  (a) "Level 1" review by trade processors with a good knowledge of international trade, customers' expected activity and a sound understanding of trade-based money laundering risks, who are responsible for assessing ML or TF or PF risks in each transaction and escalating potentially

Suspicious transactions. "Level 1" should be reviewed by the foreign trade in-charge of AD branch, Bank Asia.

(b) "Level 2" review by official with specialist expertise able to further assess the merits of an escalation from a "Level 1" processor and the relevant suspicion itself. This official is likely to require extensive knowledge of trade-based money laundering risk and make appropriate use of third party data sources to verify key information. "Level 2" should be reviewed by foreign trade specialized official in International Division, Bank Asia.

(c) A "Level 3" compliance or investigation takes referrals from "Level 2" processors. This stage may conduct a further investigation to determine additional measures which may be required to mitigate a risk and whether the obligation to make a suspicious transaction report arises. Where there are unacceptable ML or TF or PF risks, Bank should not process the transaction. "Level 3" should be reviewed by the Head of International Division or Head of International Banking, Bank Asia.

Bank should tailor their own review process to their particular needs. Smaller operations are likely to require fewer stages of review due to the volumes of transactions involved and the nature of their businesses.

6.4.6 Policies and Procedures & Training

The Bank should regularly review the need to allocate more resources toward training to raise the awareness of official to the financial crime risks associated with trade finance and the measures to mitigate such risks. Case Studies and relevant industry publications could be included in the training to highlight high risk areas that require more attention from officials or common typologies. Bank Asia is well-aware of trade based money laundering. Continuous training courses are arranged on "Trade Based Money Laundering" for the concerned officers working in the Foreign Exchange Desks.

6.5 Branches and Subsidiaries Situated/Located in Foreign Jurisdiction

1. Bank would confirm the implementation of Money Laundering Prevention Act-2012(amendment 2015) and Anti-Terrorism Act -2009 (Amendment 2012 & 2013) on subsidiaries and foreign branches of the bank.
2. If branch or a subsidiary located abroad, for any reason fails to comply with the instructions of Money Laundering Prevention Act-2012 (amendment 2015) and Anti-Terrorism Act-2009 (Amendment- 2012 & 2013) it shall without any delay report to such cases to AML & CFT Division mentioning the reason of the failure.
3. In Bank Asia, AML & CFT Division/Central Compliance Committee shall supervise the subsidiaries for proper implementation of Money Laundering Prevention Act-2012 (amendment 2015) and Anti-Terrorism Act-2009 (Amendment- 2012 & 2013). **AML & CFT Division shall conduct audit & inspection of subsidiaries and foreign branches of the bank in order to comply under the BFIU circular # 26 dated 16.06.2020 & Money Laundering** Prevention Act 2012(Amendment 2015) and Anti-Terrorism Act 2009 (Amendment 2012 & 2013).

CHAPTER VII: AML & CFT COMPLIANCE PROGRAM IN BANK ASIA

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

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

7.1 Bank Asia AML, CFT & CPF Compliance Program

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

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

7.2 Roles and Responsibilities of Board of Directors

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

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

- assess the implementation of the approved AML, CFT & CPF policies through regular reporting and updates by the Senior Management and Audit Committee; and

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

7.3 Senior Management Role & Responsibilities

The Senior Management have the following roles and responsibilities:

- be aware of and understand the ML, TF & PF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;
- introduce proper mechanisms and formulate procedures to effectively implement AML, CFT & CPF policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;
- formulate AML, CFT & CPF policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the bank and its geographical coverage;
- provide periodic reporting on time to the Board on the level of ML, TF & PF risks facing the bank, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML, CFT & CPF which may have an impact on the bank;
- convey a clear signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service;
- Communicate clearly to all employees on an annual basis by a statement from the CEO or Managing Director that clearly sets forth its policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement should evidence the strong commitment of the bank to comply with all laws and regulations designed to combat money laundering, terrorist financing and proliferation financing;
- assign adequate resources to effectively implement and administer AML, CFT & CPF compliance programs that are reflective of the size and complexity of the bank's operations and risk profiles;
- appoint a chief anti-money laundering compliance officer (CAMLCO) at management level at Head Office/Corporate Office and designate a compliance officer at management level at each branch or subsidiary;
- provide appropriate level of AML, CFT & CPF training for employees at all levels throughout the bank;
- **Senior management of Bank Asia shall advice Human Resources Division (HRD) for inclusion of AML, CFT & CPF compliance in their manual as well as employee screening process and punishment regarding involvement of ML, TF & PF activities so that it helps to adopt HR or Human Resources Policy for ensuring the compliance of AML, CFT & CPF measures by the employees of the bank.**

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

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

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

7.4 Statement of Commitment of President & Managing Director (MD)

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

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

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

7.5 Customer Acceptance Policy.

Bank Asia has developed a clear Customer Acceptance Policy which was approved at **the 399th Board meeting dated January 23,2019 with effect from January 21,2019. This customer acceptance policy integrated with Know Your Customer (KYC) policy. This policy is available at our web site *(http://www.bankasia- bd.com/home/anti_money_laundering)*.**

This customer acceptance policies and procedures have to be implemented to identify the types of customer that are likely to pose a higher risk of ML and TF pursuant to the Bank's risk assessment. When assessing risk, Branch should consider the factors relevant to the situation, such as a customer's background, occupation (including public or high profile position), source of income and wealth, country of origin and residence (when different), product/service used, nature and purpose of accounts, linked accounts, business activities and other customer oriented risk indicators in determining what is the level of overall risk and the appropriate measures to be applied to manage those risks. Such policies and procedures should require basis due diligence for all customers and

Commensurate due diligence as the level of risk associated with the customer varies. For the lower risk customer, basic due diligence should be followed as per regulatory circulars and laws and for the higher risk customer, Branch should take enhanced measures to mitigate and manage those risks. Enhanced due diligence may be essential for an individual planning to maintain higher risk customer.

7.6 Policy for rejection of customer

a) No account shall be opened in anonymous or fictitious name.
b) Bank Asia will not establish any kind of correspondence relationship with shell Bank.
c) No account should be opened or operated in the name of any person or entity listed under UNSCRs or their close alliance on suspicion of involvement in terrorist and terrorist financing activities and prescribed or enlisted by Bangladesh Government.
d) The legal basis for closing an account.
e) Correspondence with applicable law enforcement and request from the law enforcement to either cancel or maintain the account.

7.7 ML & TF Risk Assessment

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

CHAPTER VIII: COMPLIANCE STRUCTURE OF BANK ASIA

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

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

8.1 Central Compliance Committee

Under the obligation of **BFIU Circular No. 26 dated June 16, 2020, "**To keep the banking sector free from the risks related to Money Laundering & Terrorist Financing and for the effective/proper compliance of all existing acts, rules and issued instructions time to time by BFIU, every bank must set up a **Central Compliance Committee (CCC) will report directly to the Managing Director or the Chief Executive Officer of the bank." [Para 1.3,1 (ka) of BFIU Circular No. 26]**

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

As per guideline of BFIU, Bank can also nominate one or more Deputy of the CAMLCO, who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO). The DCAMLCO will be not below the rank of 'Deputy General Manager' or 'Senior Vice President' or 'Equivalent' of the bank. In line with the BFIU guideline, Bank Asia has designated both the CAMLCO and DCAMLCO who have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML, TF & PF.

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

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

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

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

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

8.3 Responsibilities and Authorities of the CCC:

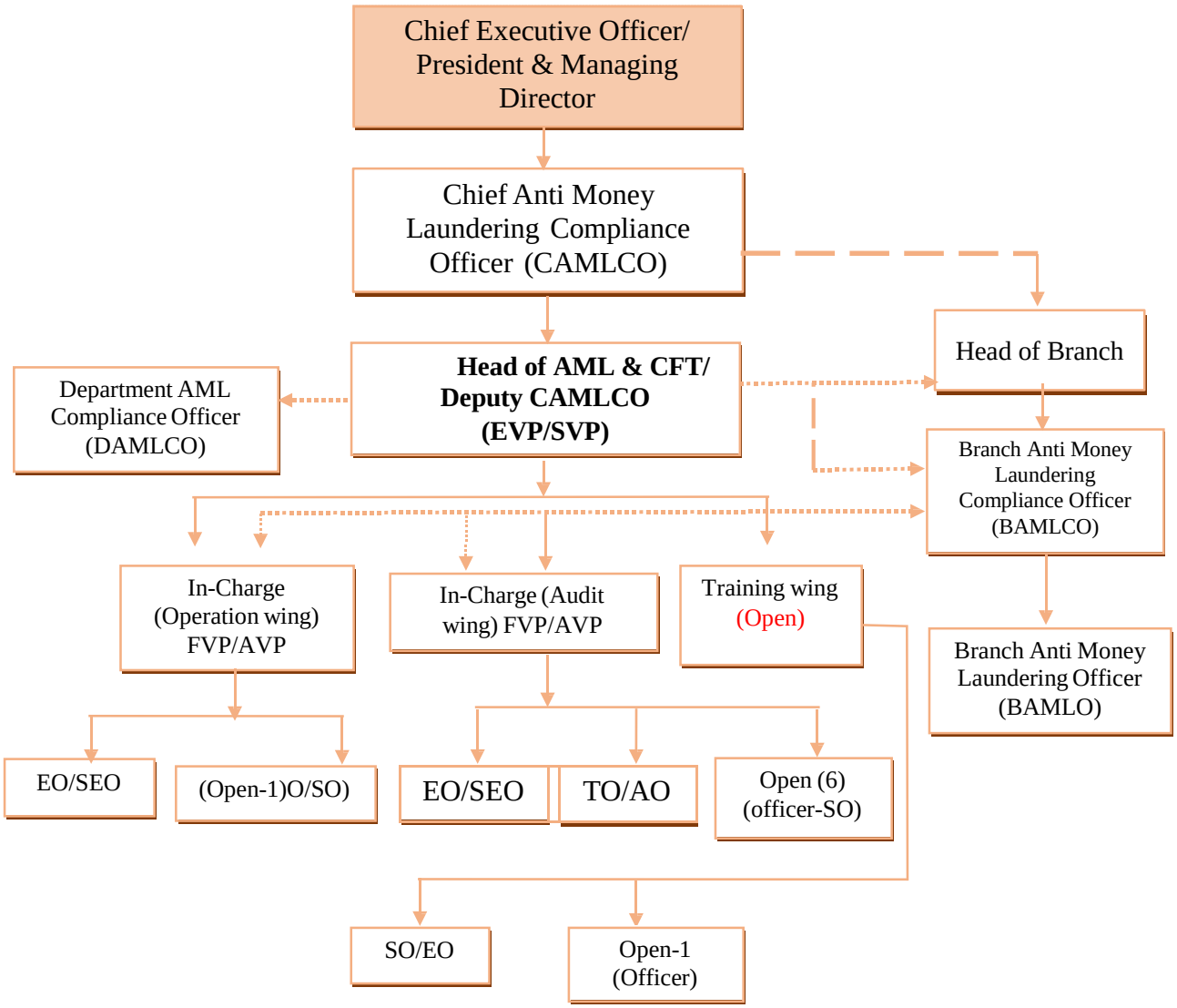
CCC is the prime mover of the Bank Asia for ensuring the compliance of AML, CFT & CPF measures. Its main responsibilities are to--

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

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

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

Organogram of the AML & CFT Division:



8.4 Chief Anti Money Laundering Compliance Officer (CAMLCO)

Bank Asia has designated Chief Anti Money Laundering Compliance Officer (CAMLCO) at its Corporate Office with sufficient authority to implement and enforce corporate wide AML, CFT & CPF policies, procedures and measures

and who will report directly to President & Managing Director. This provides evidence of senior management's commitment to efforts to combat money laundering and terrorist financing and, more importantly, provides added assurance that the officer will have sufficient influence to enquire about potentially suspicious activities. The CAMLCO is responsible for oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering and terrorist financing.

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

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

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

8.5 Authorities and Responsibilities of CAMLCO

Authorities-

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

Responsibilities-

- CAMLCO must ensure overall AML, CFT & CPF compliance of the bank;
- oversee the submission of STR/SAR or any document or information to BFIU in time;
- maintain the day-to-day operation of the bank's AML, CFT & CPF compliance;
- CAMLCO will inform to President & Managing Director or Board of Director for proper functioning of CCC/AML & CFT Division ;
- CAMLCO shall review and update ML, TF & PF risk assessment of the bank;
-
- Corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.

8.6 Branch Anti Money Laundering Compliance Officer (BAMLCO)

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

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

Both BAMLCO and BAMLO have to have sufficient knowledge in the existing acts, rules and regulations, BFIU's instructions (circulars, circular letters, etc.) and our own policies on preventing Money Laundering, Terrorist Financing and Proliferation Financing.
BAMLO will assist BAMLCO to do the job successful and effective regarding AML, CFT & CPF issues. In absence of BAMLCO, BAMLO will act as BAMLCO to mitigate the AML, CFT & CPF matters.

8.7 Responsibilities and Authorities of BAMLCO

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

Responsibilities of BAMLCO

BAMLCO will perform the following responsibilities:

Knowledge on AML, CFT & CPF issues:

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

Branch Compliance Program:

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

Sanctions Screening:

1. Ensure sanction list screening like UN Sanction list, OFAC and EU list and list of organization banned by Bangladesh Government before opening of account and while making any transaction.
2. Reviews suspected matches and reports valid matches to the AML & CFT Division/CCC, Corporate Office for onward submission to regulatory authority

Customer Due Diligence:

1. Identify and verify the identity of the customer information and documents obtained from the reliable source.
2. Ensure the KYC of all customers have done properly.
3. Ensure the update of KYC of the customer have done timely.
4. Ensure due diligence while establishing relationship with the new customer and also while conducting financial transaction with the existing customer.

5. Ensure due diligence when there is a suspicion of ML, TF & PF.
6. Ensure due diligence of walk-in customer, online customers and depositor or withdrawer other than account holder.
7. Identify the beneficial owner of the account and conduct due diligence of the beneficial owners.
8. Keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;

Enhance Due Diligence (EDD):

1. **Obtain CAMLCO approval where necessary of for establishing or continuing existing business relationship with PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates as per circular no. 26 dated June 16, 2020.**
2. Confirm EDD of PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates.
3. Comply Enhance Due Diligence (EDD) for the high risk customer and obtain additional information/documents.
4. Ensure EDD while establishing and maintaining business relationship and conducting financial transaction with a person or entity of the countries and territories that do not meet international (FATF) standard in combating money laundering.

Transaction Monitoring:

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

Risk Grading of Customer:

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

Update Customer Information and TP & KYC:

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

Arrangement of AML & CFT Meeting:

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

Report Submission to AML & CFT Division:

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

STR/SAR Identification and Reporting:

1. Report STR/SAR by monitoring and analyzing transaction.
2. Review the CTR of each month and find out STR/SAR and send it to AML & CFT Division.
3. Ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
4. Analyze the Cash Transactions immediate below the CTR threshold limit to identify structuring.
5. Monitor customer unusual behavior and unusual transaction pattern.
6. Considering all the information of the account holder, investigate the purpose of transaction and source of fund with relevant documents, if found any suspicious transactions then report to AML & CFT Division.

Record Keeping:

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

Training of employees:

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

Others responsibilities:

1. Ensure all the required information and document are submitted properly to CCC/AML & CFT Division and any freeze order or stop payment order are implemented properly and without delay;
2. Follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
3. Create awareness regarding AML, CFT & CPF among the customer of the branch.
4. Ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.
5. Monitor the staff of the branch to check whether any of them are directly or indirectly involved in or is facilitating Money Laundering and Terrorist Financing.
6. Any other responsibility assigned by the CCC/ AML & CFT Division.

Authorities of BAMLCO

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

BAMLCO:

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

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

DAMLCO: In addition, Bank Asia has assigned a Departmental/**Divisional AML Compliance Officer (DAMLCO**) under the Instruction of Bangladesh Bank Money Laundering & Risk Management Guideline 2015 para 4.3 to perform the departmental/divisional AML, CFT & CPF related compliance program smoothly.

DAMLCO will perform the following responsibilities:

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

8.8 Internal Control and Compliance:-

Under the obligation of BFIU Circular No. 26 dated June 16,2020, "with a goal of establishing an effective AML and CFT regime, it shall have to be ensured that the Internal Audit Department of the bank is equipped with enough manpower who have enough knowledge on the existing acts, rules and regulations, BFIU's instructions on preventing money laundering & terrorist financing and bank's own policies in this matter to review the Self-Assessment Report received from the branches and to execute the Independent Testing Procedure appropriately."

Internal Control & Compliance Department (ICCD) of Bank Asia shall have an important role for ensuring proper implementation of bank's AML, CFT & CPF Compliance Program. ICCD of Bank Asia is equipped with enough manpower and autonomy to look after the prevention of ML, TF & PF. The ICCD has to oversee the implementation of the AML, CFT & CPF compliance program of the bank and has to review the 'Self-Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.
To ensure the effectiveness of the AML, CFT & CPF compliance program, bank should assess the program regularly and look for new risk factors. FATF recommendation 18 suggests that-

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

An institution's internal auditors should be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable. The internal audit must-

- understand ML, TF & PF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML, CFT & CPF Compliance Program;

- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML, CFT & CPF Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
    - the importance of the board and the senior management place on ongoing education, training and compliance,
    - employee accountability for ensuring AML, CFT & CPF compliance,
    - comprehensiveness of training, in view of specific risks of individual business lines,
    - training of personnel from all applicable areas of the bank,
    - frequency of training,
    - coverage of bank policies, procedures, processes and new rules and regulations,
    - coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
    - Penalties for noncompliance and regulatory requirements.

8.9 Employee Training and Awareness Program

A formal AML, CFT & CPF compliance program should include an ongoing employee training program. The importance of a successful training and awareness program cannot be overstated. Employees in different business functions need to understand how the financial institution's policy, procedures, and controls affect them in their day to day activities which has been narrated under FATF recommendation 18. As per AML circular, each financial institution shall arrange suitable training for their officials to ensure proper compliance of ML and TF prevention activities.

The Need for Staff Awareness

The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institution appreciates the seriousness of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities.

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

Education and Training Programs

All relevant staff should be educated in the process of the "Know Your Customer" requirements for ML and TF prevention purposes. The training in this respect should cover not only the need to know the true identity

Of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the institution itself. Some sorts of high-level general awareness raising training are, therefore, also suggested.

General Training

A general training program should include the following:

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

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

Job Specific Training

The nature of responsibilities/activities performed by the staff of a financial institution is different from one another. So their training on AML, CFT & CPF issues should also be different for each category. Job specific AML, CFT & CPF trainings are as under:

i) New Employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so. The new or fresh employee may be trained up within a year.

ii) Customer Service/Relationship Managers

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

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

iii) Processing (Back Office) Staff

The staffs, who receive completed Account Opening, FDR application forms and cheques for deposit into customer‘s account or other investments must receive appropriate training in the processing and verification procedures. The staffs, who are in a position to deal with account opening, or to accept new customers, must receive the training given to relationship managers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the organization's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML & CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

iv) Credit Officers

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

v) Audit and compliance staff

These are the people charged with overseeing, monitoring and testing AML, CFT & CPF controls, and they should be trained about changes in regulation, ML, TF and PF methods and enforcement, and their impact on the institution.

vi) Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of ML, TF and PF prevention procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the laws for non-reporting and for assisting money launderers and terrorist financers; internal reporting procedures and the requirements for verification of identity and the retention of records.

vii) Senior Management and Board of Directors

ML, TF and PF issues and dangers should be regularly and thoroughly communicated to the board. It is important that the Compliance Division has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering and terrorist financing poses to the institution. Major AML, CFT & CPF compliance related circulars/circular letters issued by BFIU should be placed to the board to bring it to the notice of the Board members.

viii) AML & CFT Compliance Officer

The CAMLCO, DCAMLCO, and AML & CFT Compliance Officer should receive in depth training on all aspects of the ML, TF & PF Prevention Legislation, BFIU directives and internal policies and standards.

In addition, the CAMLCO, DCAMLCO and AML & CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

ix) Training Procedures

The trainers can take the following steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick "why are they here" assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.
- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file.

ix) Refresher Training

In addition to the above compliance requirements, training may have to be tailored to the needs of specialized areas of the institution's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Some FIs may wish to provide such training on an annual basis; others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction/juxtaposition with compliance monitoring.

Training should be conducted ongoing basis, incorporating trends and developments in an institution's business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions/unusual activity.

8.10 External Auditor

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

External auditor of Bank Asia will review the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report.

CHAPTER IX: CUSTOMER DUE DILIGENCE

A sound Customer Due Diligence (CDD) program is one of the best ways to prevent money laundering and other financial crime. The more you know about its customers, the greater chance of preventing money laundering abuses. Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources.
The CDD obligations on banks under legislation and regulation are designed to make it more difficult to abuse the banking industry for money laundering or terrorist financing or proliferation financing. The CDD obligations compel banks to understand who their customers are to guard against the risk of committing offences under MLP Act, 2012 (amendment 2015) including 'Predicate Offences' and the relevant offences under ATA, 2009 (amendment 2012 & 2013).
Therefore, Bank Asia demonstrate supervisory authority to put in place, implement adequate CDD measures considering the risks of ML, TF & PF. Such risk sensitive CDD measures should be based on-

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

The adoption of effective Know Your Customer (KYC) program is an essential part of financial institutions' risk management policies. Having sufficiently verified/corrected information about customers - "Knowing Your Customer" (KYC) - and making use of that information underpins all AML, CFT & CPF efforts, and is the most effective defense against being used to launder the proceeds of crime.

Bank with inadequate KYC program may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the Bank's overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences.

Bank Asia therefore, need to carry out customer due diligence for two broad reasons:

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

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

9.1 Legal Obligations of CDD

Under the obligation of MLPA, 2012(amendment 2015), "The branch shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to Bangladesh Bank"

Under the MLP Act, 2012, SRO No. 357-Law/2013 dated 21.11.2013, Part –vi, section 17, *(3) 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.

(4) 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.

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

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

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

9.2 Know Your Customer Program

The adoption of effective Know Your Customer (KYC) program is an essential part of financial institutions' risk management policies. Having sufficiently verified/corrected information about customers - "Knowing Your Customer" (KYC) - and making use of that information underpins all AML, CFT & CPF efforts, and is the most effective defense against being used to launder the proceeds of crime.

Financial institutions with inadequate KYC program may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the financial institution's overall safety and soundness, they also protect the integrity of its system by reducing AML, CFT & CPF related offences.

9.3 Know Your Customer (KYC) Procedure

Money Laundering Prevention Act, 2012(Amendment 2015) requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. FATF recommendation 10 states that where the financial institution is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, and to identify the beneficial owner, and to take reasonable measures to verify the identity of the beneficial owner and unable to obtaining information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

(a) Nature of Customer's Business

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

(b) Identifying Real Person

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

(c) Document is not enough

The best identification documents possible should be obtained from the prospective/forthcoming customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process. The overriding principle is that every Bank must know who their customers are, and have the necessary documentary evidence to verify this. Collection of document is not enough for KYC, identification is very important.

9.4 Components of KYC Program

Financial institutions in the process of designing the KYC program should include certain key elements. Such essential elements should start from the financial institutions 'risk management and control procedures and should include -

(i) Customer acceptance policy,
(ii) Customer identification,
(iii) Risk Categorization-Based on Activity and KYC Profile and
(iv) Transaction Monitoring Process.

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

I. Customer Acceptance Policy

Bank Asia has been developing a clear customer acceptance policy and procedures, laying down explicit criteria for acceptance of customers including a description of the types of customer that are likely to pose a higher than average risk to a financial institution. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered.

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

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

1) No account should be opened in anonymous or fictitious name. Branch will collect accurate & full name of clients and preserve documents in conformity with it. Branch will prepare proper KYC of the clients.
2) Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grades.
3) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.
4) Not to open an account or close an account where the financial institution is unable to apply appropriate customer due diligence measures i.e. Financial institution is unable to verify the identity and/or obtain documents required as per the risk categorization due to noncooperation of the customer or non-reliability of the data/information furnished to the financial institution. Decision by a financial institution to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
5) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.
6) Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
7) The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer‘s account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer‘s activities throughout the business relation.

II. Customer Identification

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

Once verification of identity has been satisfactorily completed, no further evidence is needed to undertake subsequent transactions. However, information should be updated or reviewed as appropriate and records must be maintained.

(a) What Constitutes a Customer’s Identity?

Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person‘s identity, remembering that a person may be any one of a range of legal

Persons (an individual, corporate body, partnership, etc). For the purposes of this guidance, the two elements are:

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

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

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

Once account relationship has been established, reasonable steps should be taken by the institution to ensure that descriptive information is kept up-to-date as opportunities arise. It is important to emphasize that the customer identification process does not end at the point of application. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector.

(b) Account of Individual Customers:

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

- full and accurate name;
- parent's names in full;
- spouse's name;
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of fund;
- contact information, such as - mobile/telephone number;
- nominee's information with signature;
- Photograph of both Account Holder and Nominee duly signed by the introducer and a/c holder respectively.

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

- Valid passport; or
- National ID card; or
- Birth Certificate (in case of Birth Certificate, Branch must obtain any other photo ID. In absence of photo ID branch can obtain other identification document or certificate attached with photo duly attested by the reputed person of the society as per **BFIU Circular Letter No. 01/2017 dated January 16, 2017 and 03/2017 dated January 30, 2017);**

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

- provision of a recent utility bill, tax assessment or Bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- checking the telephone directory;
- visiting home/office;
- Sending thanks letter to account holder and Introducer.

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

(c) Account of Proprietorship Concern

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

- Proof of the name, address and activity of the concern
- Valid and updated Trade License /Certificate / license issued by the Municipal authorities
- E-TIN certificate
- Photos of the A/C holder duly signed by the introducer
- Personal information of the Proprietor

(d) Account of Limited Company

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

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

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

- Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified copy of the Memorandum and Articles of Association, or by-laws of the client.

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

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

- All of the directors who will be responsible for the operation of the account / transaction.
- All the authorized signatories for the account/transaction.
- All holders of powers of attorney to operate the account/transaction.
- The beneficial owner(s) of the company.
- Collect Personal Information of at least 5 numbers of shareholder/director and if the company has less than 5 numbers of shareholder/director then collect personal information of all the shareholder/director.

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

(e) Account of Partnership Firms

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

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

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

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

- Two copies of photo of the each partner duly signed by the introducer.
- Registration certificate, if registered / Partnership deed (Notarized)
- Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf.
- Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses.

- E-TIN certificate of the firm and E-TIN certificate of the partners.
- Personal Information and Photos of all the partners.
- Personal Information of the beneficial owner of the firm.

(f) Accounts of other organizations:

Following information must be obtained by the Branch/Bank while opening account or establishing other relationships with Societies, Associations NGOs, Clubs, Trust, and other organizations:

- Certificate of Registration, if registered,
- Bye laws/ Trust deed
- Telephone/Utility Bill in the name of the organization
- List of Managing Committee Members and their bio-data
- Resolution of the Managing Committee of the Organization/trust for opening of the account and delegating powers to operate the accounts of the organization.
- Photos of authorized Managing committee Members duly signed by the introducer.
- Details information of KYC documentation is mentioned in Annexure-A

(g) Joint Accounts

In respect of joint accounts the full name and accurate name and address of the account holders should be in accordance with valid documents under SL no. (b).

(h) No face-to-face contact

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

(i) Walk-in/one off Customers

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

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

(j) Appropriateness of documents

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

(k) Change in address or other details

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

(k) Record keeping

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

Records.

(l) Introducer

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

(m) Persons without Standard Identification Documentation

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

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

In these cases it may be possible for the institution to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc) who knows the person. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person‘s address. A Manager or Head of Branch 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 the customer‘s file, and must also retain this information in the same manner and for the same period of time as other identification records.

(n) Minor

For minor, Bank shall obtain following information while opening accounts relationship:

- Full and accurate name;
- Parent‘s names in full;
- Date of Birth;
- Current and Permanent Address;
- Birth Certificate
- Contact information, such as - mobile/telephone no.
- Full information of the Guardian like Photos, Passport/NID and Personal Information.

Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s). Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

(o) Powers of Attorney/ Mandates to Operate Accounts

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

(p) Timing and Duration of Verification

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

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

This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing.

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

(q) Card/Internet Banking/Mobile Banking

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

Branches should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that if at any point of time Bank appoints/engages agents for marketing of these cards / products are also subjected to KYC measures. It is mentionable that without screening of sanction list i.e. UN sanction, OFAC, EU etc through AML solution software any account cannot be opened in Bank Asia.

(r) Know Your Customer's Customer (KYCC)

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

A Bank should -

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

(s) Know Your Employee (KYE)

Institutions and businesses learn at great expense that an insider can pose the same ML & TF threat as a customer. It has become clear in the field that having co-equal programs to know your customer and to know your employee is essential/vital. In an effort to identify and anticipate trouble before it costs time, money and reputational damage/risk. Financial Institutions should develop program to look closely at the people inside their own organizations.

A Know Your Employee (KYE) program means that the institution has a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job description, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, dual control, and other deterrents/restrictions should be firmly in place.

Background screening of prospective and current employees, especially for criminal history, is essential to keep out unwanted employees and identifying those to be removed. It can be an effective risk management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. It can be used effectively, the pre-employment background checks/examines may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. An institution should verify that contractors are subject to screening procedures similar to its own.

The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications. The extent of the screening depends on the circumstances, with reasonableness the standard as well as source of income.

(iii) Risk Categorization-Based on Activity and KYC Profile

When opening accounts, the concerned officer must assess the risk that the accounts may be used for "Money Laundering & Terrorist Financing" and must be classify the accounts as either High Risk or Low Risk. The risk assessment must be complete using separate KYC Profile Form. in which following risk categories are scored using a scale of 1 to 5 where scale 4-5 denotes High Risk, 3 denotes Medium and 1-2 denotes Low Risk:

1. Occupation or nature of customer's business
2. Type of Onboarding :Mode of opening the account
3. Transactional Risk :Average value of yearly transactions
4. Geographical Risk: Resident/Non Resident/Foreigner
5. Peps /IPS Expected value of monthly cash transactions
6. Credible information of Source of Fund.

The risk scoring of less than 15 indicates low risk but 15 and above 15 would indicate high risk. The risk assessment scores are to be documented in the KYC profile form. Moreover, Branch may change the risk category of the customer subject to qualitative judgment.

(iv) Transaction Monitoring

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

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

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

9.5 General Rule of CDD

Completeness and Accuracy

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

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

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

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

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

If the Branch is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, unable to identify the beneficial owner taking reasonable measures, unable to

Obtain information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer. **Annexure-A** provides an example of collection of documents and verification process of customer before opening account or conducting any transaction.

9.6 Ongoing CDD measures (Review and update)

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

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

9.7 EDD measures for high risk customer

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

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

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

- Source of funds and wealth
- Identifying information on individuals with control over the account, such as signatories or guarantors
- Occupation or type of business
- Financial statements
- Reference checking
- Domicile
- Proximity of the customer's primary trade area and whether international transactions are expected to be routine
- Description of the customer's primary trade area and whether international transactions are expected to be

routine

- Description of the business operations, the anticipated volume of currency and total sales, and list of major customers and suppliers
- Explanation of changes of account activity.

9.8 Exception when opening a bank account with Bank Asia

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

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

9.9 In case where conducting the CDD measure is not possible

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

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

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

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

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

9.10 Customer Unique Identification Code

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

9.11 Corresponding Banking

'Cross Border Correspondent banking' shall refer to "providing banking services to another bank (respondent) by a bank (correspondent). These kinds of banking services shall refer to credit, deposit, collection,

clearing, payment, cash management, international wire transfer, drawing arrangement for demand draft or other similar services.

Bank should establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank through collection of information as per BFIU circular-26 dated June 16, 2020. The Bank should also obtain approval from Chief Anti Money Laundering Compliance Officer before establishing and continuing any correspondent relationship. The Bank must be sure about the effective supervision of that foreign bank by the relevant regulatory authority. Bank should not establish or maintain any correspondent relationship with any shell bank and not to establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank.

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

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

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

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

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

Definition of PEPs:

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

i) heads and deputy heads of state or government;
ii) senior members of ruling party;
iii) ministers, deputy ministers and assistant ministers;
iv) members of parliament and/or national legislatures;
v) members of the governing bodies of major political parties;
vi) members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
vii) heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
viii) Heads of state-owned enterprises.

EDD measures of PEPs

Branch need to identify whether any of their customer is a PEPs. Once identified branch need to apply enhanced EDD measures. Moreover, they need to perform the following-

a) Branch have to adopt the Risk Based Approach to determine whether a customer or the beneficial owner of an account is a PEP;
b) Identifying the customer and verifying that customer's identity using reliable, Independent source documents, data or information.
c) Obtain senior managements' approval before establishing such business relationship;
c) Purpose of account opening, take reasonable measures to establish the source of wealth & source of funds of a PEP's account;
d) Monitor their transactions in a regular basis; and
e) All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

Definition of Influential Persons

'**Influential persons'** refers to, "Individuals who are or have been entrusted domestically 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

j) intelligence services;
k) heads of state-owned enterprises;
l) members of the governing bodies of local political parties;
m) ambassadors, *chargés d'affaires* or other senior diplomats;
n) city mayors or heads of municipalities who exercise genuine political or economic power;
o) 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.

EDD Measures for influential persons
Branch need to identify whether any of their customer is an Influential Person (IP). Once identified branch need to apply enhanced Due Diligence (EDD) measures. Moreover, they need to perform the following-

a) Branch have to adopt the Risk Based Approach to determine whether a customer or the beneficial owner of an account is a PEP;
b) Identifying the customer and verifying that customer's identity using reliable, Independent source documents, data or information.
c) Obtain senior managements' approval before establishing such business relationship;
c) Purpose of account opening, take reasonable measures to establish the source of wealth & source of funds of a PEP's account;
d) Monitor their transactions in a regular basis; and

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

EDD measures for Chief Executives or Top Level Officials of any International Organization
Branch need to identify whether any of their customer is a CEO or top level officials of any international organization. Once identified branch need to **apply EDD measures. Moreover,** they need to perform the following-

a) Branch have to adopt the Risk Based Approach to determine whether a customer or the beneficial owner of an account is a PEP;
b) Identifying the customer and verifying that customer's identity using reliable, Independent source documents, data or information.
c) Obtain senior managements' approval before establishing such business relationship;
c) Purpose of account opening, take reasonable measures to establish the source of wealth & source of funds of a PEP's account;
d) Monitor their transactions in a regular basis; and

Close Family Members and Close Associates of PEPs, Influential Persons and Chief Executives or Top Level Officials of any International Organization.

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

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

There may be exceptional circumstances where the individual should not be classified as a 'Close Family Member' of the 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 should include any person publicly or widely known to be a close business colleague of the PEP, including personal advisors, consultants, lawyers, accountants, colleagues or the PEP's fellow shareholders and any person(s) that could potentially benefit significantly from close business associations with the PEP.

EDD measures for Close Family Members and Close Associates of PEPs, Influential Persons and Chief Executives or Top Level Officials of any International Organization

Branch need to identify whether any of their customer is a family member or close associates of a PEPs, IP or CEO or top level officials of any international organization. Once identified branch need to apply EDD measures. Moreover, they need to perform the following-

a) Branch has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a family member or close associates of a PEPs, IP or CEO or top level officials of any international organization;
b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
c) take reasonable measures to establish the source of fund of the account of a family member or close associates of a PEP, IP or CEO or top level officials of any international organization;
d) monitor their transactions in a regular basis; and
e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

9.13 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.

Cross-Border Wire Transfers

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

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

Domestic Wire Transfers

In case of domestic wire transfers, full and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank/institutions as per BFIU circular no 26 dated 16.06.2020 For providing money of domestic wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved. In case of wire transfer by using debit or credit card (except buying goods and services), similar information as above has to be preserved in the payment related message/instructions. In case of wire transfer for Government, Semi-Government and Autonomous body a minimum KYC should be done by the Branch.

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

Ordering Bank

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

Intermediary Bank

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

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

Beneficiary Bank

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

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

9.15 CDD for Beneficial Owner

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

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

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

9.16 Agent Banking

Agent banking means providing limited scale banking and financial services to the underserved/unbanked population through engaged agents under a valid agency agreement, rather than a teller/cashier. It is the owner of an outlet who conducts banking transactions on behalf of a bank. Agent banking is a most important distribution channel for financial inclusion. Bank Asia has decided to promote this complimentary channel to reach to the poor segment of the society as well as existing bank customer with a range of financial services especially to geographically dispersed locations.

A bank agent is supposed to be equipped with Biometric device, PIN input pad or EMV certified P.O.S. terminal with which they can process withdrawals and deposits of the customer. These P.O.S. devices connect to the core banking system via internet connectivity.

The Bank agency model has been a hub and spoke model, with agents being associated with a nearby bank branch from which their liquidity is managed by the bank. The agent banking outlet must have at least 2 (two) persons (a manager and a teller) with required managerial and financial expertise for this purpose and 1 (one) counter for cash transaction.

For Agent Banking activities, agent outlets and tagged branch must follow the guidelines issued by the Agent Banking Division. Agent outlets and Branches shall also follow the respective agent banking guidelines, circulars issued by Bangladesh Bank, BFIU and ensure its implementation of AML & CFT related instruction contained therein.

For *Agent Banking activities, Bank Asia follow the guidance mentioned in the BFIU Circular No. 26 dated June 16, 2020*. In addition following measures have to be taken

1. UAOF should be used for opening account of agent and customers of the Bank.
2. Bank should be conscious regarding detecting & reporting of suspicious transactions or activity of agent and customer.
3. Activities of prevention of money laundering and terrorist financing shall be included in the compliance program of Agent Banking, and
4. Proper training of Agent on prevention of money laundering and terrorist financing.

Selection criteria of Bank Asia Agent:

- Agent must have a permanent resident (As per as NID/Passport).
- Agent must have enough infrastructures for conducting Agent banking.
- Agent should be financially solvent & have ability to hard cash transaction.
- Agent should have ability to meet commitment with customer under adverse situation.
- Agent should have knowledge and ability to handle Technology based financial services.
- All deeds/transaction's record should be preserved for internal audit with enough securities.
- Agent cannot be engaged with any subversive activities.
- Agent should have ability to perform his/her responsibility properly.
- Agent must be concerned about the reputation of the institution.
- Agent should not be a loan defaulter and not penalized by any civil or criminal court
- For cash transaction, Agent have to maintain an account in Agent Banking system, which is fetched for cash deposit and withdrawal transaction by customers and system automatically debit or credit agent account and customer account simultaneously.
- Agent has to maintain sufficient balance to accommodate customer transaction value. The Agent account balance is determined on the volume of transaction and Agent account have to maintain sufficient balance and Cash in hand balance for uninterrupted transaction of customers.

Risk Grading of Agent: To ensure Risk Based supervision Bank should do the risk grading of the agent as High, Medium and Low based on certain criteria.

- **Net Worth (Asset liability) status of the agent.**
- **Volume & number of transaction per month.**
- **Geographical location of the Agent.**
- **Nature of business and ownership structure of the agent.**
- **Type of onboarding of the agents.**
- **Whether agent is/are politically exposed persons (PEPS) / influential person / chief or high officials of multi-national company & their close associate**
- **Resident/Nonresident status of the agent.**
- **Criminal background check (Police verification).**
- **Credible information of Source of fund.**
- **Educational Back Ground.**

High risk agent to be reviewed on each year where the low and medium risk agent to be reviewed on regular basis to monitor the agent activities.

Agent Responsibilities :

- Agent must be honest, professional & ethical to his / her duties;
- Agent must have proper knowledge about his duties & serve customer Agent Banking facilities;
- Maintenance of electronic device (Computer, POS Printer, Finger print machine etc.) and ensures enough security;
- Agent preserves all sorts of transaction record, evidence & deeds;
- Agent displays fixed charge of agent banking services in his/her booth;
- After a certain period of Agent submit regular/daily activities to respective officer;
- Agent must be bound to maintain internal rules & regulation of Bank Asia;
- Agent is cordially cooperating to all sort of audit;
- Beside these other facilities directed by Bank Asia Limited;
- Collection & preservation of A/C opening Form & others receipts copy;
- Facilitating small value loan disbursement and recovery of loan installments;
- Cheque receive for clearing;
- Provide salary, pension scheme & other gratuity services;
- Collection & preservation of necessary banking E-mail & letters.

As per BFIU Circular No. 26 dated June 16, 2020 Bank shall follow the following steps for appointment of Agent and monitoring their activities:

a) Bank shall follow the proper screening mechanism for selecting agent and confirm the full and accurate information

of the agent.

b) Risk grading of the agent on the basis of (i) transaction number and amount, (ii) geographical location, (iii) business & nature of ownership and (iv) other reasonable subject and monitoring of the transactions & activities of the agent.
c) Ongoing assessment of the risk (high, medium & low) of the agent by the institution.
d) Verification of the AML & CFT compliance level of the agent.
e) Conducting audit and inspection related to AML & CFT of the high risk graded agent annually by the ICCD and the report will send to AML & CFT Division.
f) Conducting audit and inspection related to AML & CFT of medium & low risk graded agent at regular interval.
g) Updated list of Agent based on January to June should be disclosed in the website.
h) List of terminated Agent due to different irregularities or non-compliance should be disclosed in the website.

9.17 Mobile Banking

Mobile Banking is the new era of banking to carry the banking facility to the door step of the customer under financial inclusion. Rapid growth of mobile phone users and wider range of the coverage of Mobile Network Operators (MNOs) has made their delivery channel an important tool-of-the-trade for extending banking services to the unbanked/banked population. In order to ensure the access of unbanked people by taking advantage of countrywide mobile network coverage, Mobile Banking services is introduced by the commercial banks of Bangladesh as per Bangladesh Bank guideline.

Mobile Financial Services:

Bangladesh Bank may allow the following Mobile Financial Services (in broad categories) -

i. Disbursement of inward foreign remittances,
ii. Cash in /out using mobile account through agents/Bank branches/ ATMs/Mobile Operator's outlets.
iii. Person to Business Payments - e.g. a. utility bill payments, b. merchant payments
iv. Business to Person Payments e.g. salary disbursement, dividend and refund warrant payments, vendor payments etc.
v. Government to Person Payments e.g. elderly allowances. Freedom-fighter allowances, subsidies, etc.
vi. Person to Government Payments e.g. tax, levy payments.
vii. Person to Person Payments (One registered mobile Account to another registered mobile account).
viii. Other payments like microfinance, overdrawn facility, insurance premium, DPS, etc.

Permissible Models

Depending on the operation, responsibility and relationship(s) among banks, MNOs, Solution Providers and customers mainly two types of mobile financial services (Bank led and Non-Bank led) are followed worldwide. From legal and regulatory perspective, only the bank-led model will be allowed to operate. The bank-led model shall offer an alternative to conventional branch-based banking to unbanked population through appointed agents facilitated by the MNOs/Solution Providers. Customer account, termed "Mobile Account" will rest with the bank and will be accessible through customers' mobile device. Mobile Account will be a non-chequing limited purpose account.

Opening of Mobile Accounts

Banks must ensure that a 'Mobile Account' has been opened for each customer seeking to avail Mobile Financial Services with all the required documents and accurate KYC as per Bangladesh Bank Guideline.

Anti-Money Laundering Compliance

1. Banks and its partners shall have to comply with the prevailing Anti Money Laundering (AML) & combating the Financing of Terrorism (CFT) related laws, regulations and guidelines issued by BFIU, Bangladesh Bank from time to time.
2. Banks shall have to use a new 'Know Your Customer (KYC)' format as given in the guideline of Mobile Financial Services provided by Bangladesh Bank. The Bank will be responsible for authenticity of the KYC of all the customers.
3. Banks shall have to follow full KYC format issued by Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank for the cash points/agents/partners.
4. Banks shall ensure that suspect transactions can be isolated for subsequent investigation. Banks shall develop an IT based automated system to identify suspicious activity/transaction report (STR/SAR) before introducing the services.
5. Banks shall immediately report to BFIU, Bangladesh Bank regarding any suspicious, unusual or doubtful transactions likely to be related to money laundering or terrorist financing activities.

Record Retention:

MFS transaction-records must be retained for **Six (06)** years from the origination date of the entry. The Participating Bank(s) must, if requested by its customer, or the Receiving Bank(s), provide the requester with a printout or reproduction of the information relating to the transaction. Banks should also be capable of reproducing the MFS transaction-records for later reference, whether by transmission, printing, or otherwise.

Security Issues

1. Banks shall have to follow the Guidelines on ICT Security for Scheduled Banks and Financial Institutions, 2010 issued by the Bangladesh Bank and ICT Act, 2006 to address the security issues of Mobile Financial Services.
2. The following properties need to be addressed to offer a secure infrastructure for financial transactions using mobile technology:
   a. **Confidentiality:** Property that ensures transaction information cannot be viewed by unauthorized persons.
   b. **Integrity:** Property that the transaction information remains intact during transmission and cannot be altered.
   c. **Authorization:** Property that the authentic user has proper permission to perform the particular Transaction. It ensures how the system decides what the user can do.
   d. **Nonrepudiation:** Property that the particular transaction initiated by a user cannot be denied by him/her later.
3. All the transactions must be authenticated by the account holders using their respective Personal Identification Number (PIN) or similar other secured mechanism. To facilitate the mobile financial services, the said PIN may be issued and authenticated by the bank maintaining proper protection and security features.
4. The banks should ensure that a proper process is put in place to identify the customer when the service is being enabled.
5. A second factor of authentication should be built-in for additional security as chosen by the bank.

9.18 Management of Legacy Accounts

Legacy accounts refers those accounts opened before 30 April, 2002 and yet to update KYC procedures. These legacy accounts should be treated as "Dormant". No withdrawal should be permitted in those accounts; however, deposit can be permitted. **These accounts will be fully functional only after conducting proper CDD measures as per BFIU circular no. 26 dated 16.06.2020. Central Compliance Committee should preserve data of such accounts at their end.**

CHAPTER X: RECORD KEEPING

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

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

10.1 Statutory Requirement

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

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

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

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

Records relating to verification of identity will generally comprise:

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

Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. pertaining to:
  (1) the customer;
  (2) the beneficial owner of the account or product;
  (3) the non-account holder conducting any significant one-off transaction;
  (4) any counter-party;
- Details of transaction including:
  1) nature of such transactions;
  2) volume of transactions customer's instruction(s) and authority(ies);

3) source(s) of funds;
4) destination(s) of funds;
5) book entries;
6) custody of documentation;
7) date of the transaction;
8) form in which funds are offered and paid out;
9) parties to the transaction;
10) Identity of the person who conducted the transaction on behalf of the customer.

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

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

Under the obligation of MLP Rules, 2013, *the bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners:*

1) *Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;*
2) *The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction;*
3) *The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order.*

10.2 Obligations under Circulars

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

(1) All necessary information/ documents of customer's domestic and foreign transactions has to be preserved for at least 5(five) years after closing the account.

(2) All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved for at least 5(five) years after closing the account.

(3) All necessary information/documents of a walk-in Customer's transactions has to be preserved for at least 5 (five) years from the date of transaction.

(4) Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence.

(5) Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU.

10.3 Records to be kept

The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that a bank meets its obligations and that, in so far as is practicable, in any subsequent investigation the

bank can provide the authorities with its section of the audit trail.
The records shall cover:

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

10.4 Customer Information

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

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

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

10.5 Transactions

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

10.6 STR/SAR and Investigation

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

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

10.7 Training Records

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

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

10.8 Internal and External Reports

A branch should make and retain:

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

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

10.9 Other Measures

Bank's records should include:

(a) in relation to training:

- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

(b) in relation to compliance monitoring

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

10.10 Formats and Retrieval of Records

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

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

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

CHAPTER XI: SUSPICIOUS TRANSACTION REPORT

The final output of all compliance programs is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the risk for financial institutions. So it is necessary/essential for the safety and soundness of the institution.

11.1 Definition of STR/SAR

Generally STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be usual manner. Such report is to be submitted by financial institutions to the competent authorities.

In the section (2)(z) of MLP Act 2012 (amendment 2015) "suspicious transaction" means such transactions which deviates from usual transactions; of which there is ground to suspect that,

1. the property is the proceeds of an offence,
2. 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 BFIU from time to time.

In Anti-Terrorism Act, 2009 (amendment 2012 & 2013), STR/SAR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. One important thing is that financial institutions need not to establish any proof of occurrence of a predicate offence; it is a must to submit STR/SAR only on the basis of suspicion.

11.2 Obligations of Such Report

As per the Money Laundering Prevention Act 2012 (amendment 2015) FIs are obligated to submit STR/SAR to BFIU. Such obligation also prevails for the FIs in the Anti-Terrorism Act, 2009 (amendment 2012 & 2013). Other than the legislation, BFIU has also instructed the FIs to submit STR/SAR through AML/BFIU Circulars issued by AMLD, Bangladesh Bank and BFIU time to time.

11.3 Reasons for Reporting Of STR/SAR

As discussed above, STR/SAR is very crucial for the safety and soundness of the financial institutions. The Bank should submit STR/SAR considering the followings:

- It is a legal requirement in Bangladesh;
- It helps protect the reputation of Bank(s) ;
- It helps to protect Bank(s) from unfounded allegations of assisting criminals, including terrorists;
- It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

11.4 Identification and Evaluation STR/SAR

Identification of STR/SAR is very crucial for financial institutions to mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place by the financial institutions. Such suspicion may not only at the time of transaction but also at the time of doing KYC and attempt to transaction.

Identification of STR/SAR

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

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

Simply, if any transaction/activity is consistent with the provided information by the customer can be treated as normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.

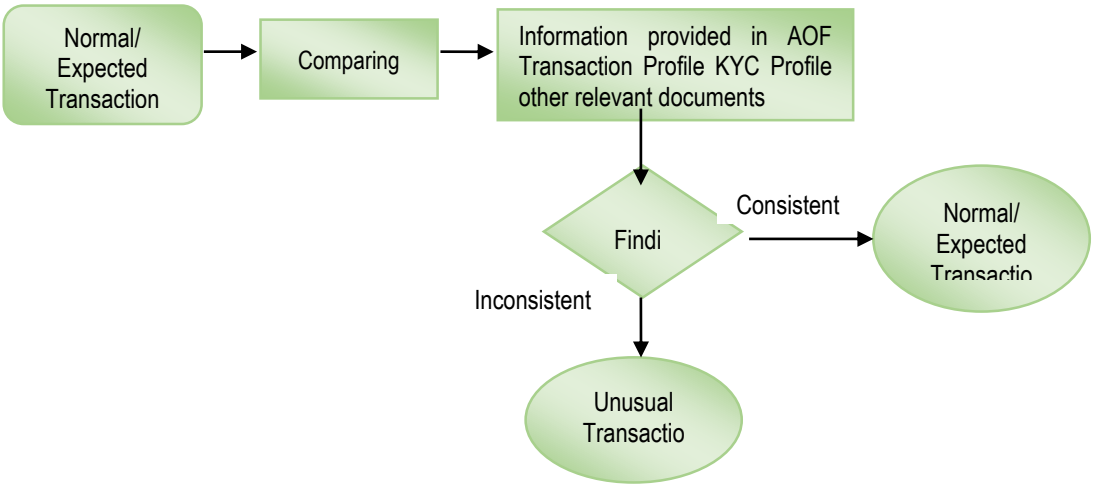


Figure: Identification of STR/SAR

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

a) Identification

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

b) Evaluation

These problems must be in place at Branch level and AML & CFT Division. After identification of STR/SAR, at Branch level BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage concerned BAMLCO must be tactful considering

the tipping off provision of the acts. If BAMLCO is not satisfied, he should forward the report to AML & CFT Division. After receiving report from Branch, AML & CFT Division should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stages of evaluation (whether reported to BFIU or not) financial institutions should keep records with proper manner.

c) Disclosure.

This is the final stage and Bank(s) should submit STR/SAR to BFIU, Bangladesh Bank if it is still suspicious. For simplification the flow chart given in following page shows STR/SAR identification and reporting procedures:

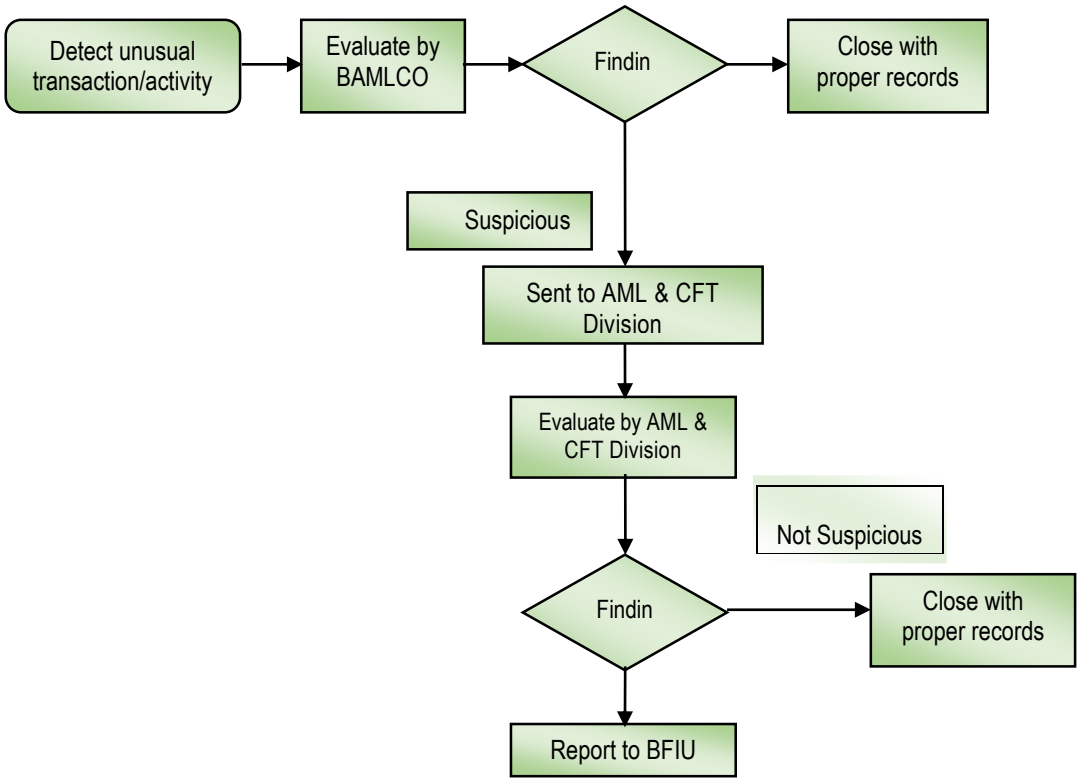


Figure: STR/SAR identification and reporting procedures

11.5 Reporting of STR/SAR

Institutions enlisted as per MLP Act, 2012 (amendment 2015) and ATA, 2009 (as amended in 2012 & 2013) are obligated to submit STR/SAR to BFIU. Such report must come to the BFIU from AML & CFT Division of the respective institutions by using specified format/instruction given by the BFIU.

Tipping Off

Section 6 of MLP Act, 2012(amendment 2015) and FATF Recommendation 21 prohibits financial institution, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the bank is seeking to perform its CDD obligation in those circumstances. The customer's awareness of a possible STR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation.

Penalties of Tipping Off

Under section 6 of MLP Act, 2012 (amendment 2015) if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

11.6 "Safe Harbor" Provisions for Reporting

Safe harbor laws encourage financial institutions to report all suspicious transactions by protecting financial institutions and employees from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. In section (28) of MLP Act, 2012(amendment 2015) provides the safe harbor for reporting.

11.7 Red Flags or Indicators of STR

Moving Customers

A customers who moves every month, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal, could be suspicious.

Out of market windfalls

If customer service officer think a customer who just appeared at our institution sounds too good to be true, he/she might be right. Pay attention to one whose address is far from your institution, especially if there is no special reason why he/she was given the business. Aren't there institutions closer to home that could provide the service? If the customer is a business, the distance to its operations may be an attempt to prevent from verifying there is no business after all. Don't be bullied by your sales personnel who follow the —"no question asked" philosophy of taking in new business.

Suspicious Customer Behavior

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses the institution's record-keeping or reporting duties with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be recorded.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.
- Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.
- Customer who is a student uncharacteristically transacts large sums of money.
- Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

Suspicious Customer Identification Circumstances

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information when opening an account.
- Customer's permanent address is outside the bank's service area.
- Customer asks many questions about how the financial institution disseminates information about the

Identification of a customer.

- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

Suspicious Cash Transactions

- Customer opens several accounts in or more names, then makes several cash deposits under the reporting threshold.
- Customer conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf.
- Corporate account has deposits and withdrawals primarily in cash than cheques.

Suspicious Non-Cash Deposits

- Customer deposits large numbers of consecutively numbered money orders or round figure amounts.
- Customer deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business.
- Funds out of the accounts are not consistent with normal business or personal items of the account holder.
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

Suspicious Activity in Credit Transactions

- A customer‘s financial statement makes representations that do not conform to accounting principles.
- Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.

Suspicious Commercial Account Activity

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.

Suspicious Employee Activity

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires.
- Employee frequently is involved in unresolved exceptions or recurring exceptions on exception reports.
- Employee lives a lavish lifestyle that could not be supported by his/her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.

Suspicious Activity in an FI Setting

- Request of early encashment.
- A DPS (or whatever) calling for the periodic payments in large amounts.
- Lack of concern for significant tax or other penalties assessed when cancelling a deposit.

List of Abbreviations

AML, CFT & CPF: Anti Money Laundering, Combating Financing on Terrorism & Combating Proliferation Financing.

APG	: Asia Pacific Group on Money Laundering
ATA	: Anti-Terrorism Act
BAMLCO	: Branch Anti Money Laundering Compliance Officer
BAMLO	: Branch Anti Money Laundering Officer
BB	: Bangladesh Bank
BDT	: Bangladesh Taka
BFIU	: Bangladesh Financial Intelligence Unit
CAMLCO	: Chief Anti Money Laundering Compliance Officer
DCAMLCO	: Deputy Chief Anti Money Laundering Compliance Officer
CCC	: Central Compliance Committee
CDD	: Customer Due Diligence
CTC	: Counter Terrorism Committee
CTR	: Cash Transaction Report
EU	: European Union
FATF	: Financial Actions Task Force
FI	: Financial Institution
FIU	: Financial Intelligence Unit
FSRB	: FATF Style Regional Body
GPML	: Global program against Money Laundering
ICRG	: International Cooperation and Review Group
IOSCO	: International Organization of Securities Commissions
IAIS	: International Association of Insurance Supervisors
IP	: Influential Person
KYC	: Know Your Customer
KYCC	: Know Your Customer's Customer
KYE	: Know Your Employee
ML	: Money Laundering
MLPA	: Money Laundering Prevention Act
NCC	: National Coordination Committee
NCCT	: Non-cooperating Countries and Territories
OECD	: Organization for Economic Co-operation and Development
OFAC	: Office of Foreign Assets Control
PEP	: Politically Exposed Persons
SAR	: Suspicious Activity Report
STR	: Suspicious Transaction Report
TF	: Terrorist Financing
TP	: Transaction Profile
TFS	: Targeted Financial Sanction
UN	: United Nations
UNODC	: UN Office of Drugs and Crime
UNSCR	: United Nations Security Council Resolution
TBML	: Trade Based Money Laundering