Money Laundering [ML] & Terrorist Financing [TF] Risk Management Policy

Shimanto Bank Limited
Head Office, Dhaka

April - 2019
Version-2.0

DOCUMENT CONTROL

Document Title	**ML & TF Risk Management Policy**
Version	Version 2.0
Date	21st April, 2019
Author	CAMLCO and D-CAMLCO
Document Owner	AML & CFT Department

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document

Version	Date	Changes	Author	Approve by
1.00	August, 2016	1st initiation of the policy	CAMLCO and D-CAMLCO	6th Board Meeting dt.13/08/2016
2.00	April, 2019	1st review of the policy		Board Meeting dt. / /2019

Table of Contents	
Chapter-1: An overview of ML & TF	Page#

CHAPTER – 1: AN OVERVIEW OF MONEY LAUNDERING [ML] AND TERRORIST FINANCING [TF]

1.1: Introduction

Money Laundering is not an isolated issue in our country; rather it has become global and affects almost all countries. In the last decade, crime has become more organized, more sophisticated and has spread out internationally. It is therefore important that the management of banks and other financial institutions view Money Laundering and Terrorist Financing Prevention as a part of their risk management strategy.

This Policy of Shimanto Bank Limited has been prepared in accordance with the guidance of Bangladesh Bank on 'Money Laundering and Terrorist Financing Risk Management Guidelines'. This guideline will assess the adequacy of the internal control, policies and procedures to counter money laundering [ML] and Terrorist financing [TF] of the bank subject to its supervision. It will be reviewed regularly and updated based on any legal/regulatory or business/operational changes, such as additions or amendments to existing Anti-money Laundering rules and regulations, as and when necessary. Besides, the circulars/circular letters issued by Bangladesh Bank, the internal circulars and the forthcoming circulars/guidelines relating to Anti-Money Laundering & Terrorist Financing are and will be the integral part of this guideline.

1.2: The Concept of Money Laundering [ML]

Money Laundering is any transaction or series of transactions undertaken to conceal or disguise the nature and source of funds that have been obtained from illegal activities. It is the process by which 'dirty' money is made to look legitimate or 'clean' so that the funds may be used freely. Examples of illegal activities that often involve money laundering are: illegal arms dealing, drugs trafficking, fraud, terrorism, smuggling, etc.

1.3: Stages of Money Laundering

There are no definitive stages of Money Laundering; however, generally money laundering can have the following 3 stages:

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

1.4: Reasons for Money Laundering

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

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

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

1.5: Terrorist Financing [TF]

Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full of partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

1.6: The Link between Money Laundering [ML] and Terrorist Financing [TF]

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

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

1.7: Necessity to Combat Money Laundering & Terrorist Financing

Money Laundering has devastating economic, security and social consequences. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials and others to operate and expand their criminal enterprises. This drives up the cost of government for increased law enforcement and health care expenditures (for example, for treatment of drug addicts).

Money Laundering diminishes government tax revenue. It also makes government tax collection more difficult. This results in higher tax rates.

Money laundering distorts asset and commodity prices and leads to misallocation of resources. It can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability for banks.

One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers often use front companies, for co-mingling their illicit proceeds with legitimate funds, to hide the ill-gotten gains. Because of substantial illicit funds, these front companies can subsidize their products and services at levels well below market rates. This makes it difficult for legitimate businesses to compete against front companies. This situation can result in the crowding out of legitimate private sector businesses by criminal organizations.

Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government and citizens to criminals.

The social and political costs of laundered money are also serious as laundered money may be used to corrupt

national institutions. Bribing of officials and governments undermines the moral fabric in society, weakens collective ethical standards and corrupts our democratic institutions.

Nations cannot afford to have their reputation and banks cannot have their image tarnished by an association with money laundering, especially in today's global economy.

1.8: Trade Based Money Laundering [TBML]

TBML is "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins."Like money laundering through the financial system, TBML may occur in three stages. At the placement stage, the offender transforms illicit proceeds into a transferable asset (e.g., by purchasing goods); at the layering stage, the offender attempts to obscure the link between the illicit proceeds and their criminal source (e.g., by trading the goods across borders); and at the integration stage, the offender re-introduces the illicit proceeds into the legitimate economy (e.g., through resale of the goods). **There are four basic TBML methods:** (1) **over- and under-invoicing**; (2) **over- and under-shipments**; (3) **falsely describing goods or services**; and (4) **multiple invoicing of goods or services**.

1.9: TBML Red Flags

There are several red flags indicating potential TBML, according to the U.S. Immigration and Customs Enforcement (ICE):

- Payments to a vendor by unrelated third parties
- False reporting, such as commodity misclassification, commodity over- or under-valuation
- Repeated importation and exportation of the same high-value commodity, known as carousel transactions
- **Commodities being traded that do not match the business involved**
- Unusual shipping routes or transshipment points
- Packaging inconsistent with the commodity or shipping method
- **Double-invoicing**

1.10: TARGETED FINANCIAL SANCTIONS

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

1.11: TFS related to terrorism and terrorist financing-

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

1.12: TFS related to Proliferation

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

These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations'.

Chapter-2: Legal & Regulatory Obligations

2.1: Money laundering

Money Laundering is defined in the Money Laundering Prevention Act 2012 as follows:

"Money Laundering" means –

(i) knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:-

(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;

Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above.

2.2: Predicate Offence

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

(1) corruption and bribery;
(2) counterfeiting currency;
(3) counterfeiting deeds and documents;
(4) extortion;
(5) fraud;
(6) forgery;
(7) illegal trade of firearms;
(8) illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;
(9) illegal trade in stolen and other goods;
(10) kidnapping, illegal restrain and hostage taking;
(11) murder, grievous physical injury;
(12) trafficking of women and children;

(13) black marketing;
(14) smuggling of domestic and foreign currency;
(15) theft or robbery or dacoit or piracy or hijacking of aircraft;
(16) human trafficking;
(17) dowry;
(18) smuggling and offences related to customs and excise duties;
(19) tax related offences;
(20) infringement of intellectual property rights;
(21) terrorism or financing in terrorist activities;
(22) adulteration or the manufacture of goods through infringement of title;
(23) offences relating to the environment;
(24) sexual exploitation;
(25) insider trading and market manipulation using price sensitive information relating to the capital market in share transactions before it is published for general information to take advantage of the market and attempting to manipulate the market for personal or institutional gain;
(26) organized crime, and participation in organized criminal groups;
(27) racketeering; and

Any other offence declared as predicate offence by Bangladesh Financial Intelligence Unit, with the approval of the Government, by notification in the official Gazette, for the purpose of this Act.

2.3: Reporting Agency

As per Money Laundering Prevention Act 2012 and Anti Terrorism Act-2009(as Amended), the following are the reporting agencies –

(1) Bank;
(2) Financial institution;
(3) Insurer;
(4) Money changer;
(5) Any company or institution which remits or transfers money or money value;
(6) Any other institution carrying out its business with the approval of Bangladesh Bank;
(7) Stock dealer and stock broker,
(8) Portfolio manager and merchant banker,
(9) Securities custodian,
(10) Asset manager;
(11) Non-profit organization,
(12) Non-government organization,
(13) Cooperative society;
(14) Real estate developer;
(15) Dealer of precious metals or stones;
(16) Trust and company service provider;
(17) Lawyer, notary, other legal professional and accountant;
(18) Any other institution which Bangladesh Bank may, from time to time, notify with the approval of the Government;

2.4 Property Means

"Property" means- (i) any kind of assets, whether tangible or intangible, movable or immovable, however acquired; or

(ii) Cash, legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets

2.5 Suspicious or Unusual Transaction

As per Money Laundering Prevention Act 2012, "suspicious transaction" means such transactions –

(i) which deviates from usual transactions;

(ii) 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;

(iii) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh bank from time to time;

2.6 Power and Responsibility Bangladesh Financial Intelligence Unit

(1) As per Money Laundering Prevention Act 2012, Section 23, (1) for the purposes of this Act, Bangladesh Financial Intelligence Unit shall have the following powers and responsibilities, namely:-

(a) To analyze or review information related to cash transactions and suspicious transactions received from any reporting organization and to collect additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data on the same and, as the case may be, provided with the said information to the relevant investigating concern or law enforcement agencies for taking necessary actions;

(b) Irrespective of any provision in any other law, obtain required information or report from reporting organizations;

(c) issue an order to any reporting organization to suspend or freeze transactions of any account for a period not exceeding 30 (thirty) days if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing any offence or money kept in any account is used or may be used for committing any offence:

Provided that such order may be served up to maximum 7 (seven) times for period of 30 (thirty) days in each order, 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) In require case, carry out on-site inspections of the reporting organizations;

(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;

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

(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 shall provide with such information where there is no obligation for it 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, Bangladesh Financial Intelligence Unit 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 and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization. de

(4) If any reporting organization provides with false information or statement requested under this section, Bangladesh Financial Intelligence Unit 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 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.

(5) If any reporting organization fails to comply with any instruction given by Bangladesh Financial Intelligence Unit under this Act, Bangladesh Bank 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 non compliance and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Financial Intelligence Unit 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 under clause (c) of sub-section (1), Bangladesh Bank may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.

(7) If any person or entity or reporting organization fails to pay any fine imposed by Bangladesh Financial Intelligence Unit under sections 23 and 25 of this Act, Bangladesh Financial Intelligence Unit will inform Bangladesh bank and Bangladesh Bank may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank, and in this regard if any amount of the fine remains unrealized, Bangladesh Financial Intelligence Unit may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.

(8) If any reporting organization is imposed fine under sub-sections (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit 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.

2.7 Responsibility of Reporting Agencies

Responsibilities of the reporting organizations in prevention of money laundering–

(1) the reporting organizations shall have the following responsibilities and any other responsibilities set by the law in the prevention of money laundering, namely:-

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

(b) if any account of a customer is closed, to preserve previous records of the account and transactions of such account for at least 5(five) years from the date of such closure;

(c) to provide with the information maintained under clauses (a) and (b) to Bangladesh Financial Intelligence Unit from time to time, on its demand;

(d) if any doubtful transaction or attempt of such transaction as defined under clause (n) of section 2 is observed, to report the matter as 'suspicious transaction report' to the Bangladesh Financial Intelligence Unit immediately on its own accord.

(2) If any reporting organization violates the provisions of sub-section (1), Bangladesh Financial Intelligence Unit or controlling authority of the reporting organization may-

(a) impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty-five) lacs on the reporting organization; and

(b) in addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities of the said organization or any of its branches, service centers, booths or agents, or as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

(3) The sum of fine imposed under sub-section (2) shall be deposited into treasury of the State

(4) Controlling authority of the reporting organization through their regular monitoring activities shall ensure their specific responsibilities fixed by the sub-clause (1) and the controlling authority will also responsible for any failure of reporting organization to comply with the responsibility fixed by the sub-clause (1) and the Act.

(5) Controlling authority of the reporting organization can take necessary action as per sub-clause (2), if any reporting organization breach any provision of sub-clause (1) any provision fixed by the Act. Information of such action need to be informed Bangladesh Financial Intelligence Unit immediately.

(6) Controlling authority of the reporting organization will inform Bangladesh Financial Intelligence Unit immediately if the authority is informed about any offence is occurs under Money Laundering Prevention Act, 2012 or the authority identifies such offence through their monitoring activities.

3.1 The United Nations

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

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

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

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

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

3.2: The Vienna Convention

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

3.3: 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.

3.4: 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.

3.5: Security Council Resolution 1267 and Successors

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

3.6: Security Council Resolution 1373

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

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

3.7: Security Council Resolution 1540

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

Weapons Convention, or the Biological Weapons Convention or alter the responsibilities of the International Atomic Energy Agency (IAEA) and Organization for the Prohibition of Chemical Weapons (OPCW).

3.8: 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.

3.9: 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.

3.10: 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.

3.11: The Financial Action Task Force [FATF]

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 34 countries and territories and two regional organizations.

3.12: FATF 40+9 Recommendations

FATF adopted a set of 40 recommendations to prevent money laundering. These Forty Recommendations constituted a comprehensive framework for AML and were designed for universal application by countries throughout the world. Although not binding as law upon a country, the Forty Recommendations was widely endorsed by the international community including World Bank and IMF and relevant organizations as the international standard for AML. The Forty Recommendations were initially issued in 1990 and revised in 1996

and 2003 to take account of new developments in money laundering and to reflect developing best practices internationally. To accomplish its expanded mission of combating financing of terrorism FATF adopted nine Special Recommendations in 2001.

3.13: 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.

3.14: Monitoring Members Progress

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

3.15: The NCCT List

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

3.16: International Cooperation and Review Group (ICRG)

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

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

3.17: Asia Pacific Group on Money Laundering (APG)

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

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

The APG has five key roles:

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

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

3.18: The Egmont Group of Financial Intelligence Units

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

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

3.19: The BASEL Committee on Banking Supervision

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

3.20: 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.

3.21: BASEL Core Principles for Banking

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

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

3.22: Customer Due Diligence

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

Chapter- 4: Major National AML & CFT Initiatives

4.1: Founding Member of APG

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

4.2: Legal Framework

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

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

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

Currently Bangladesh prevents Money Laundering and Terrorist Financing with the following laws and rules:

- Money Laundering Prevention Act 2012,
- Money Laundering Prevention Rules 2013 and
- Anti-terrorism Act 2009.
- Anti-Terrorism Rules 2013
- National Risk Assessment Report
- Circulars and Circular letter issued by BFIU
- Issuance of SRO by Ministry of Foreign Affairs November 2012 under the UNSCR (Screening of Al-Quada/Taleban)
- Ordinance on Money Laundering Prevention (Amendment) Act 2015

Besides, AML/CFT legal framework is also supported by many other laws and Rules prevailing in the country like

- Code of Criminal Procedures 1898,
- Penal code 1860
- Anti-Corruption Commission Act 2004
- Foreign Exchange Regulations Act 1947
- Customs Act 1969
- Banker's Book Evidence Act 1891.

4.3: Central and Regional Taskforces

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

4.4: Anti-Money Laundering Department

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

4.5: Bangladesh Financial Intelligence Unit [BFIU]

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

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

4.6: National Coordination Committee [NCC] and Working Committee

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

4.7: 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 considers the output of institutional, sectorial, geographical risk assessment. It covers all the sectors of the economy, legal and institutional framework. The report identifies some high risk areas for Bangladesh that are corruption, fraud-forgery, drug trafficking, gold smuggling and human trafficking. Banks, non-banks financial institutions, real estate developers and jewelers were identified as most vulnerable sectors for ML & TF. The foreign donation receiving NGO/NPO working in the coastal or border area was identified as vulnerable for TF incidence.

4.8: National Strategy for Preventing ML and TF

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

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

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

- Boosting national and international coordination both at policy and operational levels.
- Developing a transparent, accountable and inclusive financial system in Bangladesh.

4.9: 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.

4.10: 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.

4.11: 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.

4.12: 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.

4.13: NGO/NPO Sector Review

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

4.14: 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

4.15: 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.

4.16: Risk Based Approach

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on anti-money laundering (AML) and combating financing of terrorism (CFT) requires financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks. This requirement is reflected in the Money Laundering Prevention Rules (MLPR) 2013. Rule 21 of MLPR 2013 states that every Reporting Organization-Financial Institution (RO-FI) 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.

4.17: 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 36 (till date) MoU so far to exchange the information related to ML&TF with FIU of other countries.

Chapter – 5: AML & CFT Compliance Program

5.1: Introduction

National ML & TF risk assessment suggests that banking sector is one of the most vulnerable sectors for the ML & TF among the financial sectors due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership. Banks can play a vital role in preventing ML, TF & PF and in this regard their roles and responsibilities are delineated in MLPA, 2012, ATA, 2009 and rules and instructions issued under this legal framework by BFIU. To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU, every bank should develop and maintain an effective AML and CFT compliance program. This should cover at least senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

5.2: Component of AML & CFT Compliance Program

The compliance program of a bank should be documented and communicated to all levels of the organization after getting approval by its Board of Directors or the highest management committee (as applicable). In developing an AML&CFT compliance program, attention should be paid to the size and range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by the bank. The program must include-

1. Senior management role including their commitment to prevent ML, TF & PF;

2. Internal policies, procedure and controls- it should 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);

4. Independent audit function- it includes the role and responsibilities of internal audit on AML & CFT compliance and external audit function;

5. Awareness building program includes training, workshop, seminar for banks employees, member of the board of directors, owners and above all for the customers on AML & CFT issues.

5.3: Development of Bank's AML & CFT Compliance Program

In developing its own AML & CFT compliance program, bank may consider any relevant document including this guidelines as a basis for it. The bank should also consider all relevant laws, regulations, guidelines relating to AML & CFT and also the practices related to corporate governance. In drafting the compliance program, a bank should involve all its relevant departments or divisions like branches, Operations, credit, foreign exchange, information technology, international division, alternative delivery channels, internal audit and compliance and above all central compliance Committee. Their involvement should be documented or reflected in the compliance program. Proper attention should be given to the size and range of activities, complexity of operations, customer base, use of technology, diversity of product, delivery channel, external linkage, geographic location and the output of ML & TF risk assessment of every bank.

5.4: Communication of Compliance Program

Bank should communicate their compliance program immediately after the approval from the board of directors or from the highest authority to all of its employees, member of the board of the directors and other relevant stakeholders at home and abroad. The individual bank should select the proper channel that is the best suited to them to communicate with the compliance program. The bank also should upload the compliance program in their website for their customers or other stakeholders.

5.5: Senior Management Role

For the purposes of preventing ML, TF & PF, senior management includes members of the board of directors of the bank, or the member of the highest management committee in absence of the board of directors and the Chief Executive Officer (CEO) or the Managing Director (MD) of the bank.

Obligations under Law (ATA, 2009)	The Board of Directors, or in the absence of the Board of Directors, the Chief Executive of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, which are applicable to the reporting agency, have been complied with or not.
Obligations under BFIU Circular (Circular-19; dated-17 Sep, 2017)	All banks must have their own policy manual that must conform international standards, laws and regulations in force in Bangladesh and instructions of BFIU on preventing money laundering and terrorist financing, and this policy manual must be approved by their Board of Directors or by the highest management committee, where applicable. This policy manual shall be communicated to all concerned persons. Banks shall conduct review of the policy manual from time to time and shall amend/change where necessary. The chief executive of the bank shall announce effective and specific commitment, give the necessary instructions to fulfill the commitments in preventing ML & TF to all the employees of all branches, agent offices, regional offices and the head office and shall ensure the implementation of the commitments. This statement of commitment shall be issued in every year.

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

Role of Senior Management

Board of Directors (BoD) or Highest Management committee (in absence of BoD) shall-

- approve AML & CFT compliance program and ensure its implementation;
- issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- take reasonable measures through analyzing self-assessment report and independent testing report summary;
- understand ML & TF risk of the bank, take measures to mitigate those risk;
- CEO or/and MD shall issue statement of commitment to prevent ML, TF & PF in the bank;
- Ensure compliance of AML & CFT program;
- Allocate enough human resource and other logistics to effective implementation of AML & CFT compliance program.

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

STATEMENT OF COMMITMENT OF CEO OR MD

Statement of commitment of CEO or MD of a bank should include the followings-

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

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

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

Senior management of a bank should adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the bank.

Bank's HR Policy should include at least following issues for proper implementation of AML &CFT measures:

- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- Proper weight should be given in the annual performance evaluation of employees for extra ordinary preventive action vis a vis for non-compliance;
- Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;
- Other measures that shall be taken in case of non-compliance by the bank.

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

5.6: Policies and Procedures

An AML & CFT policy usually includes the 4 (four) key elements; they are -

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

5.7: Policies of SMBL:

In order to lessen the risks, SMBL has the policies and procedures in place to open/operate all types of accounts such as follows:

- SMBL AML & CFT Risk Management Policy – 2016 (amended through this revised policy)
- SMBL AML & CFT Risk Assessment Guidelines-2016
- KYC Policy-2019
- Customer Acceptance Policy-2018
- SMBL Audit Policy-2016
- Uniform AOF (Account Opening Form), Bangladesh Bank
- Circulars and Circular letters, BFIU, Bangladesh Bank

5.8: Customer Acceptance Policy

The Bank encourages making customer relationships with low/average risk clients. But, quite extensive due diligence will be essential for an individual with a high net worth whose source of fund is unclear. The Decision to enter into the business relationships with higher risk customers, such as public figures or politically exposed persons, should be taken exclusively from senior management of the Bank.

The primary objectives of a Customer Acceptance Policy are –

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

Chapter – 6: Compliance Structure

6.1 Introduction

SMBL has designated a Chief Anti-Money Laundering Compliance Officer (CAMLCO) at the Head Office who has sufficient authority to implement and enforce anti-money laundering policies, procedures and measures and who will report through Central Compliance Committee [CCC] to the Senior Management/CEO and the Board of Directors.

6.2.1 The Essential Features of Central Compliance Committee [CCC]

- It will be at head office chaired by CAMLCO or one of the senior executives of Bank;
- It will establish internal control and review by appointing BAMLCO at every Branch.
- It will conduct AML & CFT training regularly.
- It will determine its strategies and programs for achieving its objectives.

6.2.2 Authorities and Responsibilities of the CCC

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

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

6.2.3 Separation of CCC from Internal Control & Compliance (ICC)

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

6.3 The Essential Features of CAMLCO/Deputy CAMLCO

- Position title: Chief Anti-Money Laundering Compliance Officer [CAMLCO]/Deputy CAMLCO
- Should be sufficiently senior in order to command the necessary authority.
- A senior member of the bank on compliance, internal audit or inspection departments.
- Proven leadership and organizational skills and the ability to exert managerial control;
- Have excellent communication skills, with an ability to clearly and diplomatically articulate issues, solutions and rationale; an effective trainer to raise the level of awareness of the control and compliance culture regarding AML;

- Have a solid understanding of AML regulatory issues and product knowledge associated with a broad range of relevant financial services and banking activities;
- Have a fair degree of judgment, good problem solving skills and result- oriented to ensure sound implementation of control and compliance processes and procedures;
- High personal standards of ethics, integrity and commitment to fulfilling the objectives of the position and protecting the interests of the Bank.
- Must be familiar with the ways in which any of the Bank's products and services may be abused by money launderers;
- Must be able to assist the Bank in developing effective AML policies, including programs to provide AML training to all personnel;
- Must be able to assist the Bank in assessing the ways in which products under development may be abused by money launderers in order to establish appropriate AML controls before product is rolled out into the marketplace.
- Must be capable of assisting the Bank to evaluate whether any questionable activity is suspicious under the standards set forth in the AML Policy as well as under any applicable law and regulations ;
- Must attend each year at least one formal AML training program each year, either internal or external;
- The CAMLCO/Deputy CAMLCO may affect his or her responsibilities through the Central Compliance Committee [CCC].
- CAMLCO/Deputy CAMLCO must ensure that a senior level officer is appointed as Branch Anti Money Laundering Compliance Officer (BAMLCO) to ensure that each branch is carrying out policies and procedures as required.
- CAMLCO/Deputy CAMLCO through Central Compliance Committee will communicate with the regulatory agencies.
- All staff engaged in the bank at all levels must be made aware of the identity of the CAMLCO, his Deputy and the branch level BAMLCO, and the procedures to follow when making a suspicious activity report. All relevant staff must be aware of the chain through which suspicious activity reports should be passed to the CAMLCO/Deputy CAMLCO.

6.4 Functions of CAMLCO/Deputy CAMLCO

The Chief Anti-Money Laundering Compliance Officer (CAMLCO)/Deputy CAMLCO, who will report to the Chief Executive Officer for this responsibility, coordinates and monitors day to day compliance with: applicable money laundering laws, rules and regulations; the bank's AML Policy (the "Policy"); and the practices, procedures and controls implemented by the Bank.

The CAMLCO/Deputy CAMLCO must:

1) Monitor, review and coordinate the application and enforcement of the Bank's compliance policies including Anti-Money Laundering Compliance Policy. This will include: an AML risk assessment; practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transactions/account activities and a written AML training plan;

2) Monitor the changes of laws/regulations and directives of Bangladesh Bank that may require revisions to this Policy;
3) Respond to compliance questions and concerns of the staff and advise branches and assist in providing solutions to potential issues involving compliance and money laundering risks;
4) Ensure the Bank's AML Policy is complete and up-to-date and maintain ongoing awareness of new and changing business activities and products and identify potential compliance issues that should be considered by the Bank;
5) Actively develop the compliance knowledge of all staff, especially the compliance personnel. Develop and conduct training courses in the Bank to raise the level of awareness of compliance;
6) Develop and maintain ongoing relationship with regulatory authorities, external and internal auditors, Branch/Unit Heads and Compliance personnel to assist in the early identification of compliance issues;
7) Assist in reviewing the control procedures in the Bank to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
8) Monitor the Bank's self-testing procedure of AML compliance and take any necessary action;
9) Manage the Suspicious Activity Reporting Process;
10) Review the transactions referred by branch compliance officers as suspicious;
11) Review the transactions Monitoring reports (directly or together with account management personnel);
12) Ensure that internal Suspicious Activity Reports ("internal SARs"):
    - are prepared when appropriate;
    - reflect the uniform standard for "suspicious activity involving possible money laundering" established in the Policy;
    - are accompanied by documentation of the branch's decision to retain or terminate the account as required under the Policy;
    - are advised to other branches of the bank who are known to have a relationship with the customer;
    - are reported to the Chief Executive Officer, and the Board of Directors of the Bank when the suspicious activity is judged to represent significant risk to the Bank, including risk of reputation.
13) Ensure that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity is prepared and approved by the Branch Manager;
14) Maintain a review and follow up process to ensure that planned corrective actions, including possible termination of accounts, can be taken in a timely manner;
15) Manage the process for reporting suspicious activity to Bangladesh Bank authorities after appropriate internal consultation;

6.5 Staff Role and Responsibilities

Whilst complying with the rules and regulations, it is the responsibility of each individual in the Bank in the normal course of their assignments, so that they all play a vital role in the effectiveness of the bank AML program:

- Account Officer/Relationship Manager
- Anti Money Laundering Compliance Officer (AMLCO)/BAMLCO
- Branch Manager (BM)
- Operations & Technology Manager
- Chief Anti- Money Laundering Compliance Officer (CAMLCO)
- Chief Executive Officer (CEO)

The Grid below details the individual responsibilities of the above functions:-

Function	**Role / Responsibilities**
Account Officer/ Relationship Manager/ Staff Responsible for account opening	▪ Perform due diligence on prospective clients prior to opening an account ▪ Be diligent regarding the identification(s) of account holders and the transactions relating to the accounts ▪ Ensure all required documentation is completed satisfactorily ▪ Complete the KYC Profile for the new customer ▪ Ongoing monitoring of customer's KYC profile and transaction activities ▪ Obtain documentary evidence of large cash deposits ▪ Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO
BAMLCO	▪ Manage the transaction monitoring process ▪ Report any suspicious activity to BM/CAMLCO ▪ Provide AML training to Branch staff ▪ Update policy with local AML regulations and communicate these to all staff ▪ Submit Branch returns to CAMLCO regularly
Branch Manager (BM)	▪ Ensure that the AML program is effective within the branch ▪ Be the first point of contact for any AML issues
Operations & Technology Manager	▪ Ensure that the required reports and systems are in place to maintain an effective AML program
CAMLCO/Deputy CAMLCO	▪ Implement and enforce bank's Anti-money laundering policies ▪ Report suspicious clients to Bangladesh Bank Instruct BAMLCO' s of the required actions (if any)
Chief Executive Officer (CEO)	▪ Overall responsibility to ensure that the bank has an AML policy & program in place and that it is working effectively

6.6 Internal Control

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

6.7 EXTERNAL AUDITOR

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

Chapter-7: Customer Due-Diligence Procedure

7.0 Customer Due-Diligence:

Effective KYC [Know Your Customer] policy helps to obtain the necessary documents /information of the customers and protects our Bank. This is an essential part of sound risk management. Inadequate control can subject our bank to fraudulent customers and counterparty risks, especially:

- Repetitious risk
- Operational risk
- Legal risk.
- Concentration risk
- Business risk

7.1 Customer Identification

It is mandatory to collect and verify the correct and complete identification information of customers to prevent money laundering and terrorist financing and to keep the financial sector free from risks. KYC (Know Your Customer) procedure shall apply to both individuals and institutions where Customer is defined as follows:

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

To protect banks and financial institutions from risks of money laundering and/or terrorist financing by customers willfully or unwillingly, the Money Laundering Prevention Policy Manual as described in part one of this circular, shall clearly state how to conduct Customer Due Diligence at different stages such as:

- Whilst establishing relationship with the customer;
- Whilst conducting financial transaction with the existing customer;
- Whilst remitting money and providing other services at the request of non-account holders; and

Where there is reasonable ground to suspect the adequacy or veracity of previously obtained customer identification data. To be sure about the customer’s identity and underlying purpose of establishing relationship with the institution, each institution shall collect adequate information up to its satisfaction.

Explanation: “Satisfaction of the institution” means satisfaction of the appropriate authority that the necessary due diligence process has been conducted considering the risks of the customers in the light of existing directions. In case, if a person operates an account on behalf of the customer, the concerned

bank/financial institution must satisfy itself that the person has due authorization to operate the account. Correct and complete information of the person operating the account are to be collected.

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

While establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) from countries and territories that do not meet international standard in combating money laundering (such as the countries and territories enlisted in Financial Action Task Force's Non-cooperating Countries and Territories list), enhanced due diligence shall have to be ensured.

7.2 When CDD is required:

Considering the risk of customer CDD must be ensure in the following stages:

- At the beginning of the establishment of the relationship
- During execution of financial transaction with the existing customer.
- In case of doubt, on the existing information and documents of the customer are not enough or proper.
- If there is any doubt, any transaction is involved with money laundering or financing terrorist activities.

7.3. If Customer Due Diligence is not possible from Bank's end

If due to non-cooperation of the customer or due to non-reliability of the data and information from the end of the customer, CDD is not possible to be ensured; Bank will follow the following steps

- Bank will not open the account or will close the existing account
- In case of closing the existing account, approval of the higher authority of the bank is essential. Before close the account, bank will notify the customer the reasons with proper explanation of closing the account.
- If it may require bank need to submit STR against the account/customer.

7.4 KYC Procedure of Asset Accounts

The KYC procedures cover the following Asset products:

- Unsecured Lending (Consumer Product)- Credit Cards, Clean Loans and overdraft products
- Secured Lending (Consumer product) - Mortgage, Auto and secured overdraft.
- Lending to Business entities

The bank has adopted a risk-based approach to carry out the KYC checks for the customers. KYC procedures including name, address verification etc. are built into process for credit verification of Loan accounts and Credit Card customers.

Although it is the responsibility of credit cycle to ensure that the required documents are obtained for the customer. However, as a minimum, certain documents must be retained on the customer file/ together with the application form:

- Clear and legible photocopy of:
  - Acceptable Identity Card or photocopy of relevant pages of passport or
  - Utility Bills or Banks Statements or
  - Any other documents acceptable for name and address verification approved jointly by Head of Internal Control & Compliance and Head of Business Units
- The Officer/ DST (Direct Sales Team members) collecting the photocopy of the documents must mention/mark on the copies of all pages- "Original seen and verified" and put his/ her full signature and endorsed by the authorized officer (as per PPG) together with the notation.

7.5 Verification of Source of Funds

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

For the customer having low level income, bank may accept self-declaration of the customer if the transaction of the account is aligned with declared profession and other document or information.

7.6 Persons without Standard Identification Documentation

- Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address.
- A manager may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.
- For students or other young people, the normal identification procedures set out as above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant's educational institution.
- Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned 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.

7.7 Address Verification Procedure

To ensure a genuine relationship Bank will assure a proper Address Verification. The possible process of Address Verification could be:

- Address matched with NID
- CPV
- Utility Bills
- Relationship Manager's Visit Report
- Letter of Thanks
- Any other process decided by Senior Management.

7.8. Sanction Screening

Bank's Core Banking System (CBS) enables sanction screening for the 1) Existing Customer and 2) New Customer as per policy recommendation of BFIU or Bangladesh Bank.

- Before opening account, Account opening officer must ensure this screening through CBS.
- CBS will generate alert while it found any match with any existing customer or sanction names.
- SMBL will not open any account with any names which do present in sanction list such as UN, OFAC list etc. As well as, SMBL will not open accounts with new CIF with existing customer to avoid duplication
- Based on the severity, Relationship Manager is advised to accelerate the issue to the senior management.
- For High Risk customer Enhance Due-diligence must be ensued in every one year.
- For Low Risk Customer Due-Diligence needed to be ensured in every five years.

7.9. SMBL Money Laundering and Terrorist Financing Risk Assessment Guidelines

SMBL has its own "SMBL Money Laundering and Terrorist Financing Risk Assessment Guidelines" to protect bank from Money Laundering and Terrorist Financing activities.

- Here we majorly deal with two types of Risks. They are: 1. Business Risk 2. Regulatory Risk.
- In Business Risk, we have to identify Risk of the i) Customers ii)Products & services iii) Business practices/delivery methods or channels iv) Country/jurisdiction
- In Regulatory Risk, we relevant issues are i) Failure to report STRs/SARs ii) Inappropriate customer verification iii) Inappropriate record keeping iv) Lack of AML/CFT program
- After identifying the Risk Bank have to ensure Risk Assessment. In the "SMBL Money Laundering and Terrorist Financing Risk Assessment Guidelines" a proper assessment has already been done by the senior Management of the Bank.
- Lastly Bank will ensure proper Risk Treatment, Risk Monitoring, Record and Review as per the "SMBL Money Laundering and Terrorist Financing Risk Assessment Guidelines"

7.10. KYC Procedure of Beneficial Owner

After identify the actual Beneficial Owner, the identity of the customer needed to be confirmed as per the level of satisfaction of Bank in the following cases:

- If any customer operates any account on behalf of any other person; on that case, the bank needs to collect and preserve the information of that person along with the customer.
- If any person controls any customer, on that note, the proper information of that person needed to be collected and preserved.
- In case of Company the proper information share needed to be collected and preserved of the controlling shareholders or individual shareholders who hold 20% or more share.

7.11 KYC Procedure of the Walk-in Customer

Other than account holders, when money transferred through TT/MT with the request of Walk-in-customer, detailed (like, Name, Present/Permanent Addresses, Photo-ID/Passport/NID/Birth-certificate, Cell phone number & so on) and accurate (correctness of the given particulars are verified) particulars of both the sender and receiver, purpose of sending money, source of funds are to be recorded / preserved. The said due-diligence also applies while issuing of DD and Pay Order by the request of Walk-in-customers.

7.12. KYC Procedure of the Non face-to-face contact

When customer can't directly approach bank & through his agent or professional representative open account & operate the same. In such cases, photographic identification would clearly be inappropriate procedures to identify and authenticate the customer. Bank should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID card where there is no face-to-face contact, then a certified true copy should be obtained. The Power of Attorney or Authority documents are to be properly checked for appropriate authentication. Bank should not allow non-face to face contact to a resident in establishing relationship.

7.13 KYC Procedure of the Agent Banking/ Mobile Banking

Agent-Banking which intends to provide limited scale banking to the underserved population as per direction from Bangladesh Bank through engaging agents under a valid agency agreement. Along with said agreement, bank is also needed to ensure that the KYC, CPV, AML & Terrorists Financing & other associated Customer Due Diligence (CDD) issues as included in line with Bangladesh Bank guidelines for the same are properly addressed while selecting such Agents in order to ensure inclusive banking services through this emerging channel.

7.14 KYC Procedure of the Money Service Business

In case of Money Service Business we have to ensure a short KYC for the beneficiary of the remittance. For remittance those have been sent via MoneyGram and Western Union, the prescribed KYC forms needed to be filled.

7.15 Enhanced Due-Diligence (EDD) Procedure: When, How and for Whom?

Enhanced Due Diligence (EDD) is an important tool, where the risks of money laundering or terrorist financing are higher, banks should be required to conduct Enhanced Due Diligence (EDD) measures for higher-risk business relationships include:

- Obtaining and verifying additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner
- Obtaining and verifying additional information on the intended nature of the business relationship
- Obtaining and verifying information on the source of funds or source of wealth of the customer
- Obtaining and verifying information on the reasons for intended or performed transactions
- Obtaining and verifying the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

7.16 KYC Procedures of PEPs/ Influential Persons (IP)/ Head of International Organization Etc.

7.16.1 Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEPs) means & includes, ''Individuals who are or have been entrusted with prominent public functions by a foreign country, e.g. ***Head of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials,*** etc.''

- The above mentioned instructions will be applicable even in case of family members & close associates of PEP's.
- No individual of middle ranking or more junior individuals would be considered as PEP's as described in the above mentioned article.

Broader 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:

In case of opening & operating an account of PEPs, Branch will ensure the following:

- Branch will ensure Customer's Due Diligence [CDD] as per KYC Policy.
- Bank has to take Risk Management Procedure to ascertain whether their customer or Beneficial Owner of accounts is **PEP's** or not.
- Bank has to establish business relationship with PEP's by obtaining permission of appropriate higher authority.
- Appropriate measures have to be taken to know the source of Fund/Assets of any PEP's account.
- Account transactions of PEP's have to be monitored regularly.
- Rules & regulations regarding account opening of Non Residents imposed by Foreign Exchange Regulation Act, 1947 & under its surveillance by Bangladesh Bank to be complied with accordingly.

7.16.2 Influential Individual/Person

Influential Persons means & includes, ''Individuals who are or have been entrusted domestically with prominent public functions, for example ***Head of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials,*** etc''.

Instructions will be applicable in case of Influential Individual/Person would also be applicable in case of family members & close associates of Influential Persons.

No individual of middle ranking or more junior individuals would be considered as Influential Individual/Person as described in the above mentioned article.

Bank/Branch will ascertain whether the customer or Beneficial Owner of accounts is Influential Individual/Person or not.

Broader Definition:

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

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

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

CDD Measures

- If the banking relation with Influential Individual/Person is seemed Risky, then Bank/Branch will ensure the following:
- Bank has to establish business relationship with PEP's by obtaining permission of appropriate higher authority.
- Appropriate measures have to be taken to know the source of Fund/Assets of any PEP's account.
- Account transactions of PEP's have to be monitored regularly.

7.16.3. Chief of International Organizations or High Officials

Chief of International Organizations or High Officials means & includes, 'Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions, etc'.

Instructions applicable in case of Chief of International Organizations or High Officials would also be applicable in case of family their members & close associates.

No individual of middle ranking or more junior individuals would be considered as Chief of International Organizations or High Officials as described in the above mentioned article.

Bank/Branch will ascertain whether the customer or Beneficial Owner of accounts is Chief of International Organizations or High Officials or not.

- If the banking relation with Chief of International Organizations or High Officials is seemed Risky, then Bank/Branch will ensure the following:
- Bank has to establish business relationship with PEP's by obtaining permission of appropriate higher authority.
- Appropriate measures have to be taken to know the source of Fund/Assets of any PEP's account.
- Account transactions of PEP's have to be monitored regularly.
- Rules & regulations regarding account opening of Non Residents imposed by Foreign Exchange Regulation Act, 1947 & under its surveillance by Bangladesh Bank to be complied with accordingly ***[If applicable].***

7.17 Correspondent Banking

Correspondent banking shall mean providing services which are approved by the Bangladesh Bank like credit, deposit, collection, clearing, payment or other similar services by one bank (correspondent) to another bank (respondent).

Whilst establishing and continuing correspondent banking relationship the following drills should be observed so that the banking system can not be abused for the purposes of money laundering:

- ❖ Before providing correspondent banking service, Senior Management must approve and be satisfied about the nature of the business of the respondent bank through collection of information as per **annex - ka** of BFIU Circular-19 of 2017**.**
- ❖ Banks should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the foreign bank is effectively supervised by the relevant authority.
- ❖ Banks should not establish or continue a correspondent banking relationship with any Shell bank.
- ❖ Banks should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the Countries and Territories enlisted in Financial Action Task Force's Non-cooperating countries and territories list). Enhanced due diligence will generally be required in such cases. Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.
- ❖ Enhanced Due Diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customers to transact business on their behalf (i.e. payable through account)

7.18 Shell Bank

According to BFIU circular no. 19 dated 17th September 2017 2(3) Shell Bank refers to such a bank that is incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with any regulated financial group.

7.19 Internet or Online Banking

Initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied in accordance with the account opening procedures.

7.20 Lockers and Safety Deposit Boxes

Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that the Bank will follow the identification procedures set out in this Manual. In addition such facilities should only be made available to account holders.

7.21. Authority of Risk Approval

A) High Risk Account: BM/RM jointly with Area Head (except PEP/ Influential Person/ Head of International Organization)

B) Low Risk Account: RM jointly with BM/BOM

7.22. Approval of Complex/sensitive type account from ICCD

For the following accounts, Bank Branch may need to take approval of the competent authority as fix by the management:

1) Association
2) Co-operative
3) Club & Society
4) Trust
5) Politically Exposed Persons (PEP)
6) Philanthropic organization like Masjid, Madrasa, Temple, Church, Orphanage
7) Non-government Organization (NGO).

7.23. Periodical Review of Customer Profile

KYC Profiles along with Transaction Profiles must be updated and re-approved (if demanded) at least once annually for “High Risk” accounts (as defined above) under scanner of Enhanced Due Diligence (EDD). There will be required periodic updating of profiles for “Low Risk” transactional accounts under Standard Due Diligence (SDD) every after 5 (five) years. As an outcome of such reviews, SDD (Low Risk) customers may become EDD (High Risk) as well as EDD (High Risk) customers may become SDD (Low Risk).

7.24. Transaction Monitoring

Ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce the risk only if bank has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

7.25 Transaction Monitoring Process

1. Banks are expected to have systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for banks to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the Customer. Possible areas to monitor could be:-

   a. transaction type
   b. frequency
   c. unusually large amounts
   d. geographical origin/destination
   e. changes in account signatories

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

3. Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. This will be declared in a Transaction Profile (TP) at the time of opening account from the customer. Ideally any deviation from the normally expected TP should be reviewed with human judgment and interaction with customer. Such reviews may result in changing the expected profile or closing the customer account. Within six months upon opening of every new account, TP for the same will be monitored in order to verify whether the transactions in the account are in line with the customers’ declared profession or nature of business, source of fund & type of transactions. By doing so, where needed, new TP will have to be collected from certain customers as advised by Bangladesh Bank or BFIU (Circular # 19 of BFIU).

4. On a monthly basis Branch / Unit of the bank must prepare an exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the “transaction limit” established for that category of customer based on Anti Money Laundering risk assessment exercise.

5. Account Officers/Relationship Managers or other designated staff will review and sign - off on such exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer. The concerned staff will document their review by initial on the report, and where necessary will prepare internal Suspicious Activity Reports (SARs) with action plans for approval by the relevant Branch Manager and review with the Branch AMLCO. A copy of the transaction identified will be attached to the SARs.
6. BAMLCO will review the SARs and responses from the Account Officers /Relationship Managers or other concerned staff. If the explanation for the exception does not appear reasonable then the Branch/Unit Head should review the transactions prior to considering submitting them to the CAMLCO.
7. If the Branch/Unit Head and / or BAMLCO believe the transaction should be reported then the BAMLCO will supply the relevant details to the CAMLCO.
8. The CAMLCO will investigate any reported accounts and will send a status report on any of the accounts reported. No further action should be taken on the account until notification has been received.
9. If, after confirming with the client, the transaction trend is to continue the Account Officer is responsible for documenting the reasons why the transaction profile has changed and should amend the KYC profile accordingly.

7.26 Self-Assessment Process

Each BM with the support of BAMLCO will perform an annual self-assessment process that will assess how effectively the branch's anti-money laundering procedures enable management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment should advise management whether the internal procedures and statutory obligations of the bank have been properly discharged. The report should provide conclusions to three key questions:

- Are anti-money laundering procedures in place?
- Are anti-money laundering procedures being adhered to?
- Do anti-money laundering procedures comply with all policies, controls and statutory requirements?

BM and BAMLCO should follow the checklist as mentioned in the Annex- Kha of BFIU Circular no. 19 dated 17th September 2017.

7.27 System of Independent Testing Procedures

Testing is to be conducted at least annually by the bank's internal audit personnel or the compliance department, and by an outside party such as the bank's external auditors. The tests include:

- interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the bank's anti-money laundering procedures;

- a sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- a test of the validity and reasonableness of any exemptions granted by the bank; and
- a test of the record keeping system according to the provisions of the *Act.*

Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline. Internal Auditor should follow the checklist as mentioned in the Annex-Ga of BFIU Circular no. 19 dated 17th September 2017

Chapter – 8: Record Keeping

8.1 Statutory Requirements

The requirement contained in Section 25 of the Anti Money Laundering Act 2012 to retain correct and full records of customers' identification and transactions at least for five years after termination of relationship with the customers is an essential constituent of the audit trail. Where there has been a report of a suspicious activity or the bank is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client should be retained until confirmation is received that the matter has been concluded.

8.2 Record Retention and Disposal Policy

Documents and other related papers/ information are to be kept as per MLPA and ATA-2012 as well as SMBL Record Retention and Disposal Policy.

8.3 Formats and Retrieval of Records

To satisfy the requirements of the law, it is important that records are capable of retrieval without undue delay. It is not necessary to retain documents in their original hard copy form, holding records in microfiche or electronic form is also acceptable since we are operating under fully automated system, and that these can be reproduced without undue delay. In addition, bank may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on the bank itself and the onus is thus on the business to ensure that the third party is willing and able to retain and, if asked to, produce copies of the required records.

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.

8.4 Wire Transfer Transactions

In order to make investigation meaningful identity of the original ordering customer or ultimate beneficiary clearly shown in TT and electronic payment message instruction are required to include accurate originator (name, account number, and where possible address) and beneficiary information (account name and/or account number) on all outgoing fund transfers and related messages that are sent, and this information should remain with the transfer or related message throughout the payment chain. Bank should conduct enhanced scrutiny of and monitor for suspicious incoming funds transfer which do not contain meaningful originator information. The records of electronic payments and messages must be treated in the same way as any other record in support of entries in the account and have to be kept for a minimum of five years.

8.5 Investigations

Where the Bank has submitted a report of suspicious activity to Bangladesh Bank or where it knows that a client or transaction is under investigation, it should not destroy any relevant records without the agreement of the Bangladesh Bank even though the five-year limit may have been reached.

BM should maintain a register or tabular records of all investigations made to it by the Bangladesh Bank and all disclosures to the Bangladesh Bank. The register should be kept separate from other records and contain as a minimum the following details:

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

8.6 Internal and External Reports

A bank 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.

8.7 Other Measures

A bank's records should include:

(a) in relation to training:

- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

(b) in relation to compliance monitoring

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

9.1 Recognition of Suspicious Transactions

At the time of opening an account, Bank should obtain a declaration about probable Transaction Profile [TP] and KYC of that account in order to identify the abnormal/suspicious transaction. Transactions beyond the declared amount shall be treated as abnormal/suspicious if the concerned client fails to give proper clarification regarding the transactions. Transactions of the customers are suspicious or not, one can get an understanding by reviewing Annex-A.

9.1.1 Reporting of Suspicious Transactions

All officers of Branch should remain vigilant and alert in identifying the abnormal/suspicious transactions in any account.

- In the event of detection of such transactions they will submit report in writing immediately to BAMLCO of Branch as per standard format
- The BAMLCO will then scrutinize the relevant transactions in line with Bangladesh Bank guidelines and record his observations regarding the said transactions. If the reported matters are found related with money laundering, the BAMLCO will forward the report with details of occurrence to the Central Compliance Committee [CCC] immediately along with the necessary papers/documents.
- The CCC will also examine the said report and record their observations and if it is deemed suspicious, they shall then forward the report to the Money Laundering Prevention Department of Bangladesh Bank for their consideration. Records of suspicions which are raised internally with the CAMLCO but not disclosed to Bangladesh Bank should be retained for five years from the date of the transaction. Records of suspicions which Bangladesh Bank has advised and which are of no interest should be retained for a similar period. Records of suspicions that assist with investigations should be retained until the bank is informed by the Bangladesh Bank that they are no longer needed.

Following the submission of a suspicious activity report, the Bank is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal commercial reasons. It must not alert the customer to the fact of the disclosure as to do so, would constitute a "tipping-off" offence. Close liaison with Anti Money Laundering Department of Bangladesh Bank and the investigating officer is encouraged in such circumstances so that the interests of all parties may be fully considered.

The National reception point for reporting of suspicions by the CAMLCO/Deputy CAMLCO is:

The General Manager
Bangladesh Financial Intelligence Unit
Bangladesh Bank
Head Office
Dhaka

9.2 Submission of Cash Transaction Report (CTR)

The Bank will analyze the transaction of its branches and submit Cash Transaction Report (CTR) to Bangladesh Bank for the cash deposits or cash withdrawals of any amount set by Bangladesh Bank. If the cash deposit in an account is more than one entry in a day and total exceeds the amount set by Bangladesh Bank, it has to be

reported separately. Besides it has to be reported to Bangladesh Bank if one or more than one cash remittance or online deposit totaling the mentioned amount is transacted in any single account.

This report has to be submitted on a monthly basis. Accordingly, report of cash transactions for each month must be reported to Bangladesh Bank within the 21st of the following month.

Transactions have to be examined properly and if any kind of suspicious transaction/information is noticed while submitting the CTR by branches to the CAMLCO/Deputy CAMLCO, that has to be reported to him with all details mentioning the reason of suspicion.

9.3 Self-Assessment [SA]

- Branch will prepare its self-evaluation on half yearly basis depending on the checklist as per annexure-"Uma".
- Before finalization of the Branch Evaluation Report, Branch Manager will arrange a meeting and presided over there; discussion in the meeting will be held on evaluation report; identify the problem and if the identified problem can be resolved at Branch level, then resolved the same and finalize the Branch Evaluation Report with Recommendations.
- Discuss about the progress of the identified problems and Recommendations in the next quarterly AML & CFT meeting of the Branch;
- After end of every half year [i.e. June & December], Branch will send its Evaluation Report incorporating Branch activities/ activities will be taken and Recommendations for AML & CFT issues to Audit Unit as well as CCC by 15th of next month.

9.4 Independent Testing Procedures [ITP]

- Internal Audit Team will conduct AML audit as per standard format on each Branch as a part of their regular annual audit and submit the copy of Audit Report to the concerned Branch and CCC accordingly.
- Internal Audit Team, in addition to its regular annual audit, will conduct AML audit on at least 10% Branches more and submit the copy of Audit Report to the concerned Branch and CCC accordingly.
- Internal Audit Team will conduct audit on AML & CFT at least 10% it's Cash Point/Agent [if bank engages in Mobile servicing & agent banking] and send the report to CCC.
- Internal Audit will review the Self-Assessment Report received from Branches; if any risky issues identified, then immediate steps need to be taken to inspect the Branch. Besides, Audit unit will inform the issue to CCC.

9.5 ICC's Obligations Regarding Self-Assessment or Independent Testing Procedure

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

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

9.6 CCC's Obligations Regarding Self-Assessment or Independent Testing Procedure

Based on the received branch evaluation reports from the branches and submitted inspection/audit reports by the Internal Audit Department or ICC, the 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 Internal Audit Department at the time of reporting and the status of the branches (branch wise achieved number);

(c) Same kinds of irregularities that have been seen in maximum number of branches according to the received self-assessment report and measures taken by the CCC to prevent those irregularities.

(d) The general and special irregularities mentioned in the report submitted by the Internal Audit Department and the measures taken by the CCC to prevent those irregularities; and

(e) Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as 'unsatisfactory' and 'marginal' in the received report.

Chapter – 10: Training and Awareness

10.1 Statutory Requirements

It is the responsibility of Human Resource Department and Internal Control & Compliance Department of Shimanto Bank Limited to ensure that staff is adequately trained to discharge their responsibilities as per Act requirements.

It is therefore imperative to take appropriate measures to make employees aware of:

- policies and procedures to prevent money laundering and for identification, record keeping and internal reporting;
- the legal requirements; and
- to provide with relevant employees with training in the recognition and handling of suspicious transactions.

10.2 The Need for Staff Awareness

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

10.3 Know Your Employee (KYE)

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

10.4 Education and Training Programs

All relevant staff should be educated in the process of the “know your customer” requirements for money laundering 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 so as 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.

10.5 New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting any suspicious transactions to the Anti Money Laundering Compliance Officer (AMLCO) 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.

10.6 Customer Service/Relationship Managers/Tellers/Foreign Exchange Dealers

Members of staff/employees who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are vital to the bank's strategy in the fight against money laundering. They must be made aware of their legal responsibilities and should be made aware of the bank'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' staff are made aware of the bank'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.

10.7 Processing (Back Office) Staff

Those members of staff who receive completed Account Opening, Payment Order/FDR application forms and cheque for deposit into customer's account or other investments must receive appropriate training in the processing and verification procedures. Those members of staff, who are in a position to deal with account opening, or to accept new customers, must receive the training given to cashiers and the other front office staff as above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the bank'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 Anti Money Laundering 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.

10.8 Refresher Training

It is necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least once in a year to ensure that employees do not forget their responsibilities.

10.9 Awareness of Senior Management

Without proper concern and awareness of senior management of a bank, it is difficult to have effective implementation of AML & CFT measures in the bank. SMBL must 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.

10.10 Customer Awareness

SMBL must take proper actions for broadcasting awareness building advertisement and documentaries regarding prevention of money laundering and terrorist financing through different mass media under Corporate Social Responsibility (CSR) fund.

10.11 Awareness of Mass People

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

Chapter –11: Reservation and Punishment

11.1 Offences and Punishment Regarding Money Laundering

I. **Offence of money laundering and punishment –** As per Money Laundering Prevention Act, 2012 money laundering shall be deemed to be an offence. Following can be the punishment as per the said Act

- Any person who commits or abets or conspires to commit the offence of money laundering, shall be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to that, a monitory fine equivalent to the twice of the value of the property involved in the offence or taka 10(ten) lacks, whichever is greater:

  With a condition that If the person fails to pay monitory fine fixed by the court within the time line, the court may pass an order for additional imprisonment considering unpaid monitory fine amount.

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

- Any entity which commits or abets or conspires to commit the offence of money laundering under Money Laundering Act, 2012, action can be taken as per section 27 of the act and in line with sub-clause 2 of section 5 of the act and shall be punished with a fine of not less than twice of the value of the property involved with the offence or taka 20(twenty) lacks, whichever is greater and in addition to this the registration of the said entity shall be considered as cancelled:

  With a condition that If the entity fails to pay monitory fine fixed by the court within the time line, the court may pass an order for additional imprisonment against the owner, chairman or director at which name is known, considering unpaid monitory fine amount.

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

II. **Punishment for violation of an order for freezing or attachment**.**–** 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.

III. **Punishment for divulging information**.**–** 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

Any person who violates the provision, of section 6, sub-clause (1) of the 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.

IV. **Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information**.**-** 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.

Any person who is convicted with above offence under section- 7, sub-section (1) of the act, shall be punished with imprisonment for a term not exceeding 1 (one) year or with a fine not exceeding taka 25 (twenty five) thousand or with both.

V. Punishment for providing false information. –

(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 provision of above sub-section (1) shall be punished with imprisonment for a term not exceeding 3 (three) years or a fine not exceeding taka 50 (fifty) thousand or with both.

11.2 **Duties of Reporting Agency as per Anti Terrorism Act 2009 (as Amended)**

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

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

(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 Bangladesh Bank not exceeding taka 25 (twenty five) lac and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

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

11.3 Reservation of the Work Done in Good Faith

As per section-28 of the Money Laundering Prevention Act 2012, If any person is affected or there is a chance that he might be affected for the task done in good faith under this Act and rules, then any criminal or civil or any other legal proceedings may not be adopted against the reporting agency.

Chapter-12: Terrorist Financing

12.1 Necessity of Funds by Terrorist

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

12.2 Sources of Fund/Raising of Fund

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

12.3.1 Movement of Terrorist Fund

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

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

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

12.3.2 Formal Financial Sector

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

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

12.3.3 Trade Sector

The international trade system is subject to a wide range of risks and vulnerabilities which provide terrorist organizations the opportunity to transfer value and goods through seemingly legitimate trade flows. To exploit the trade system for terrorist financing purposes could assist in the development of measures to identify and combat such activity.

12.3.4 Cash Couriers

The physical movement of cash is one way terrorists can move funds without encountering the AML/CFT safeguards established in financial institutions. It has been suggested that some groups have converted cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside

of the financial system. The movement of cash across the borders is prevalent in the cash based economy and where the electronic banking system remains embryonic or is little used by the populace.

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

12.3.5 Use of Alternative Remittance Systems (ARS)

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

12.3.6 Use of Charities and Non-Profit Organizations

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

12.4 Targeted Financial Sanctions

In recent years, the concept and strategy of targeted sanctions imposed by the United Nations Security Council, have been receiving increased attention. Most of the countries agree that better targeting of such measures on the individuals responsible for the policies condemned by the international community, and the elites who benefit from and support them, would increase the effectiveness of sanctions, while minimizing the negative impact on the civilian population. The considerable interest in the development of targeted sanctions regimes has focused primarily on financial sanctions, travel and aviation bans, and embargoes on specific commodities such as arms or diamonds.

Targeted financial sanctions entail the use of financial instruments and institutions to apply coercive pressure on transgressing parties—senior officials, elites who support them, or members of non-governmental entities—in an effort to change or restrict their behavior. Sanctions are targeted in the sense that they apply only to a subset of the population—usually the leadership, responsible elites, or operationally responsible individuals; they are financial in that they involve the use of financial instruments, such as asset freezing, blocking of financial transactions, or financial services; and they are sanctions in that they are coercive measures applied to effect change or constrain action.

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

To implement TFS in Bangladesh, the Government has issued Statutory Regulatory Order (SRO) under section 2 of the United Nations (Security Council) Act, 1948 (29 November, 2012) and amended the SRO to make it more comprehensive (June, 2013). To make the process enforceable, a separate section has been included in ATA, 2009 through amendment of ATA in 2013. Section 20(A) of ATA, 2009 covers all the requirements under UNSCR's tool were taken and will be taken under chapter VII of the charter of UN. Before that BFIU used to issue circular letters for reporting organizations to implement UNSCR resolutions.

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

12.5 Role of Shimanto Bank combating Terrorist Financing

12.5.1 Automated Screening Mechanism of UNSCRs

For effective implementation of Terrorist Financing Security relating to TF & PF SMBL has automated Sanction Screening activities with the Bank's core banking system (CBS) that can prohibit any listed individuals or entities to enter into the banking channel. CBS checks to detect any listed individuals or entities prior to establish any relationship with them.

For Trade transaction, SMBL enrolled with Accuity online compliance system for sanction screening purpose. Through this system, SMBL prevents any trade or F.Ex transaction with the listed individual or entity.

In particular, SMBL put emphasize on account opening and Trade transaction for sanction screening mechanism so that any listed individuals or entities could not use the formal financial channel. In short, Shimanto Bank ensure that screening has done before-

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

In line with business model and increased diversification of business, SMBL will consider implementation of separate AML system for more dimensional screening and monitoring through complex processes.

12.5.2 Other Activities of Shimanto Bank in Preventing TF & PF

- If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, Shimanto Bank send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to BFIU immediately.
- SMBL maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list along with some other International and National lists.

SMBL 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.

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

Annexure A: Examples of Potentially Suspicious Transactions

Bank may wish to make additional enquiries in the following circumstances

Banking Transactions

Cash Transactions

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

Accounts

- Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominee names.
- Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
- Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).
- Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.
- Customer's reluctance or refusal to disclose other banking relationships.
- Home address or business location is far removed from the Branch where the account is being opened and the purpose of maintaining an account at your Branch cannot be adequately explained.

- Reluctance or refusal to provide business financial statements.
- Information provided by the customer in the Transaction Profile does not make sense for the customer's business.
- A visit to the place of business does not result in a comfortable feeling that the business is in the business they claim to be in.
- Customers who appear to have accounts with several financial institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.
- Matching of payments out with credits paid in by cash on the same or previous day.
- Paying in large third party cheques endorsed in favor of the customer.
- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
- Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.
- Companies' representatives avoiding contact with the branch.
- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
- Customers who show an apparent disregard for accounts offering more favorable terms
- Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.
- Insufficient use of normal banking facilities, e.g. avoidance of high interest rate facilities for large balances.
- Large number of individuals making payments into the same account without an adequate explanation.

International Banking/Trade Finance

- Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.
- Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from: countries which are commonly associated with the production, processing or marketing of drugs; proscribed terrorist organizations; [tax haven countries].
- Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held in other locations.
- Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.
- Frequent requests for TCs, foreign currency drafts or other negotiable instruments to be issued.

- Frequent paying in of TCs or foreign currency drafts, particularly if originating from overseas.
- Customers who show apparent disregard for arrangements offering more favorable terms.

Institution Employees and Agents

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

Secured and Unsecured Lending

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

Merchant Banking Business

New Business

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

Dealing Patterns and Abnormal Transactions

Dealing Patterns

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

Abnormal Transactions

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

Settlements

Payment

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

Delivery

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

Disposition

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

ANNEXURE B: Abbreviations

Act	Money Laundering Prevention Act, 2012
AML	Anti Money Laundering
MLPA	Money Laundering Prevention Act
ATA	Anti Terrorism Act
BM	Branch Manager
BOM	Branch Operation Manager
CAMLCO	Chief Anti Money Laundering Compliance Officer
BAMLCO	Branch Anti Money Laundering Compliance Officer
TBML	Trade Based Money Laundering
CEO	Chief Executive Officer
SSC	Sales & Service Center
CCC	Central Compliance Committee
KYC	Know Your customer
TP	Transaction Profile
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
CTR	Cash Transaction Report
STR	Suspicious Transaction Report
ICE	Immigration and Customers Enforcement

Annexure-C: References

1. Money Laundering Prevention Act, 2012
2. Anti Terrorism Act, 2009
3. Managing Core Risks: Guideline Notes on Prevention of Money Laundering
4. BFIU Circular no- 19 of 2017
5. SMBL Policy on Prevention of Money Laundering & Terrorist Financing, 2012
6. http://www.bangladeshbank.com.org
7. Different Website on TBML, CFT and AML