AMENDMENT OF GUIDANCE NOTES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

FAS Finance & Investment Ltd.

11 October, 2015

Central Compliance Unit

Pran Gourango Dey
Senior Executive Vice President, CAMLCO

Md. Zahangir Alam Bhuiyan
Sr. Vice President, Deputy CAMLCO

Md. Maniruzzaman Akan
Vice President & CFO, Deputy CAMLCO

Md. Azimul Haque
Vice President, Deputy CAMLCO

Md. Munir Hossain
SAVP, Deputy CAMLCO

Muhammad Motiur Rahman
Deputy Manager Deputy CAMLCO & Member Secretary

Abu Mirja Md. Sayem
Manager & Member

Maximum Money Laundering can be prevented if the KYC is filled up properly

In every case the main guideline issued by Bangladesh Bank shall be the main route

Objective:

As,
-FAS Finance is yet to develop sufficient capacity to verify the identity and source of funds of their clients.
-The human resources are not skilled and trained enough to trace money laundering and terrorist financing activities.

-In pursuance of section 16(2) of Anti terrorism (Amendment) Act, 2012, and Anti-Money Laundering Department's of Bangladesh Bank letter dated 04.07.2006, all FIs must have their own policy manual approved by their Board of Directors/topmost committee to prevent money laundering and terrorist financing. This policy manual must be in conformity with international standard and laws and regulations in force in Bangladesh. FIs shall from time to time review and confirm the meticulous compliance of the circulars issued by Bangladesh Bank and

-To implement the policy manual and compliance of instructions of BB, every FI must have to designate one high level officer as Chief Anti-Money Laundering Compliance Officer (CAMLCO) in the Central Compliance Unit (CCU) and one officer as Branch Anti-Money Laundering Compliance Officer (BAMALCO) 7 in the branch level.

The objectives of the guidance are:

Circulate the way of Prevention of Money laundering & terrorist financing to every employee of FAS Finance & Investment Ltd and ensure to ***make them understand*** the entire dilemma of the act & guidance of Government & Central Bank in this regard, So that they can assure to comply with the whole mechanism of Anti Money Laundering in their day to day operational activities.

Preamble

In response to the growing concern about money laundering and terrorist activities, the international community has acted on many fronts. The United Nations (UN) was the first international organization to undertake significant actions to fight against money laundering through adopting several conventions and resolutions. Following UN action, the Financial Action Task Force on Money Laundering (FATF) was formed by G-7 countries in 1989 as the first intergovernmental body which has recommended forty recommendations to combat money laundering in 1990.
In line with the international initiatives and standards, Bangladesh has also enacted Money Laundering Prevention Act (MLPA), 2012 (repealing the MLPA, 2009) and Anti Terrorism Act (ATA), 2009 (amended in 2012 & 2013). The new acts address all the deficiencies identified in the 2nd Mutual Evaluation of Bangladesh conducted by APG in 2008 to determine the extent of its compliance, with the global standards. Both the Acts have empowered Bangladesh Bank (BB) to perform the anchor role in combating ML & TF through issuing guidance and directives for reporting agencies including Financial Institutions (FIs), as defined in section 2(g) of MLPA, 2012.

Accordingly, this amendment Guidance Notes are designed as per the BFIU circular No. 4 dated 16/09/2012 and rules/ regulation of the 'Anti money laundering law-2012 and Shartrash Birodhi Ain-2009 (Ammended-2013) and BFIU circular No. 12 dated 29/06/2015. This is not constitute a legal interpretation of the said acts but to pay due regard in developing responsible programs suitable for FAS Finance & Investment Ltd.

INTRODUCTION

Money Laundering is being employed by launderers worldwide to conceal the proceeds earned from criminal activities. It happens in almost every country in the world, and a single scheme typically involves transferring money through several countries in order to obscure its origins. And the rise of global financial markets makes money laundering easier than ever, making it possible to anonymously deposit "dirty" money in one country and then have it transferred to any other country for use. Money laundering has a major impact on a country's economy as a whole, impeding the social, economic, political, and cultural development of societies worldwide. Both money laundering and terrorist financing can weaken individual financial institution, and they are also a threat to a country's overall financial sector reputation. Combating money laundering and terrorist financing is, therefore, a key element in promoting a strong, sound and stable financial sector. The process of money laundering and terrorist financing (ML/TF) is very dynamic and ever evolving. The money launderers and terrorist financers are inventing more and more complicated and sophisticated procedures and using new technology for money laundering and terrorist financing. To address these emerging challenges, the global community has taken various initiatives against ML/TF. In accordance with international initiatives, Bangladesh has also acted on many fronts.

1. What is Money Laundering?

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

- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of

assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

- The concealing or disguising the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

- The Financial Action Task Force (FATF) which is recognized as the international standard setter for anti-money laundering (AML) efforts defines the term money laundering succinctly as the processing of criminal proceeds to disguise their illegal origin, in order to legitimize the ill-gotten gains of crime. Money Laundering is defined in Section 2 (v) of the Money Laundering Prevention Act 2012 as follows:

More we can say:

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

a) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
b) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;

c) Smuggling money or property earned through legal or illegal means to a foreign country;
d) 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
e) Concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided
f) Converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
g) Acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
h) Performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised
i) Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above

1.1. Why money laundering is done.

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

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

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

1.2. Why we must combat money laundering

Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a vital process to making crime worthwhile. 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 due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences that result. Crime has become increasingly international in scope and the financial aspects of crime have become more complex due to rapid advances in technology and the globalization of the financial services industry.

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

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

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

No one knows exactly how much "dirty" money flows through the world's financial system every year, but the amounts involved are undoubtedly huge.

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

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

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

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

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

1.3 Stages of money laundering

There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewelries) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). There are a number of crimes where the initial proceeds usually take the form of cash that needs to enter the financial system by some means. Bribery, extortion, robbery and street level purchases of drugs are almost always made with cash. These proceeds of crime have to enter the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated.
Despite the variety of methods employed, money laundering is not a single act but a process accomplished in 3 basic stages which are as follows:

Placement - the physical disposal of the initial proceeds derived from illegal activity.
Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
Integration - the provision of apparent legitimacy to 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.

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

1.4 Defining terrorist financing

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

If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used in full or in part in order to carry out:
An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or
Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such

act by its nature or context is to intimidate a population or to compel a government or an international organization to do or to abstain from doing an act.

For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b)'2.
According to the article 7 of the Anti Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means:

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

a) 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.

b)International Convention for the Suppression of the Financing of Terrorism (1999), Article 2, Web Link to be included.

c) If any person or entity knowingly makes arrangement for money, services, material support or any other property for another person or entity where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any 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.

d) If any person or entity knowingly instigates another person or entity to provide or receive or make arrangement for money, services, material support or any other property in such a manner where there are reasonable grounds to believe that the same have been used or may be used in full or partially by a terrorist person or entity or group or organization for any purpose, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

2. THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

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

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

3. What is risk?

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

3.1 What is risk management?

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

3.2 Which risks does FAS Finance & Investment Limited need to consider

For the AML & CTF aspects, FFIL will take into account two main sources of ML & TF risks i.e., ML & TF risk arises from or through doing their business and non-compliance of regulatory requirements.
ML & TF risk that arises or generated in doing business is the risk that business may be used for ML & TF. The FFIL will at least take into consideration the following segment of their business in assessing ML & TF risk:

- customer risks, i.e. ML&TF risk arisen from or generated through customers
- products or services risks
- business practices and/or delivery method risks
- country or jurisdictional risks

Regulatory risk is associated with not meeting all obligations under the Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two Acts and instructions issued by BFIU. Examples of regulatory obligations are failure to report STR/SAR, unable or inappropriately verification of customers and lacking of AML&CFT program (how a business identifies and manages the ML&TF risk it may face) etc.
It is unrealistic that FFIL would operate in a completely ML&TF risk-free environment. Therefore, it is suggested that FFIL shall identifies the ML&TF risk it faces, and then works out the best ways to reduce and manage that risk.

Part 2: INTERNATIONAL INITIATIVES

INTRODUCTION

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

2.1 THE UNITED NATIONS

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

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

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

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

2.1.2 The Vienna Convention

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

2.1.3The Palermo Convention

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

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

2.1.4 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 oppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002, with 132 countries signing the convention and 112 countries ratifying it.

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

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

2.1.6 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 passed in response to a threat to international peace and security under Chapter VII of the UN Charter, is binding upon all UN member countries. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to,

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

2.1.7 The Counter-Terrorism Committee

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

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

2.1.8 Global Program against Money Laundering

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

2.1.9 THE FINANCIAL ACTION TASK FORCE

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

2.1.10 FATF Recommendations

Recommendation 1 of Financial Action Task Force (FATF), to identify, assess and take effective action to mitigate money laundering and terrorist financing risks. Rule 21 of MLP Rules 2013 contains 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.

The obligation of FATF Recommendation-1 may be shown as follows:

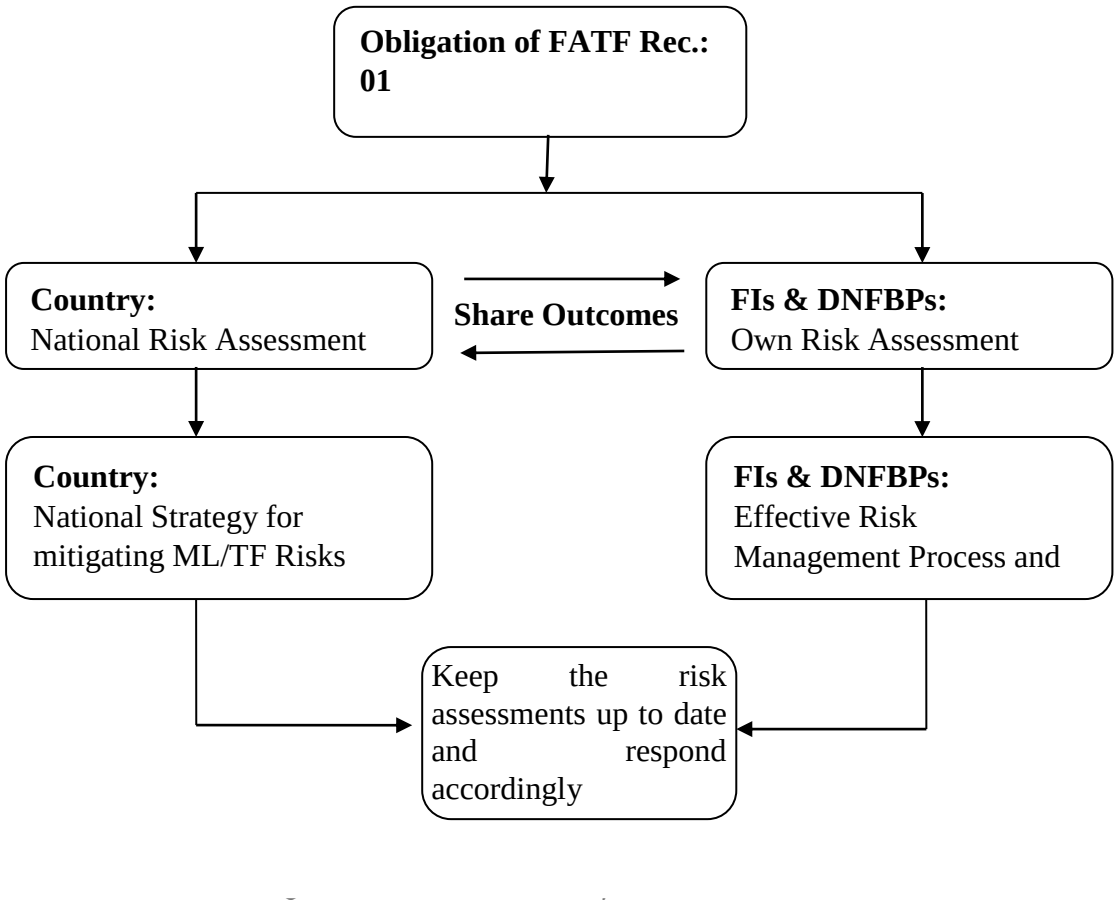


Table 1: Summery of new FATF 40 Standards

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

2.2 THE BASEL COMMITTEE ON BANKING SUPERVISION

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

2.2.1 Statement of Principles on Money Laundering

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

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

2.2.2 Basel Core Principles for Banking

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

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

These"know your customer" or "KYC" policies and procedures are a crucial part of an effective institutional frame work for every country. In addition, the Basel Committee issued a Core Principles Methodology. In 1999, this contains 11 specific criteria and five additional criteria to help assess the adequacy of KYC policies and procedures. These additional criteria include specific reference to compliance with The Forty Recommendations.

2.2.3 Customer Due Diligence

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

2.3 INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONERS

The International Organization of Securities Commissioners (IOSCO) is an organization of securities commissioners and administrators that have day-to-day responsibilities for securities regulation and the administration of securities laws in their respective countries. The current membership of IOSCO is comprised of regulatory bodies from 105 countries. With regard to money laundering, IOSCO

passed a Resolution on Money Laundering in 1992. Like other international organizations of this type, IOSCO does not have law-making authority. Similar to the Basel Committee and IAIS, it relies on its members to implement its recommendations within their respective countries.

2.4 THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

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

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

2.5 ASIA PACIFIC GROUP ON MONEY LAUNDERING (APG)

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

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

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.

CHAPTER 3: NATIONAL INITIATIVES

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

  Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40 recommendations. Subsequently, Bangladesh, as the first South Asian country, promulgated Money Laundering Prevention Act MLPA), 2002 which came into force on 30 April, 2002. For exercising the power and shouldering the responsibilities, as stated in the MLPA, a separate department named Anti-Money Laundering Department (AMLD) was established at Bangladesh Bank.

- To address the shortcomings of the MLPA, 2002 and to meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER), Bangladesh has again enacted Money Laundering Prevention Act in February, 2012 repealing MLPA, 2009.

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

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

- In the process of responding to international concern, Bangladesh Government formed a central and several regional taskforces on 27 January, 2002 to combat money laundering and illegal Hundi activities in Bangladesh.

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

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

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

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

- A rigorous Customer Enhanced Due Diligence (EDD) procedure has been introduced to protect identity theft by customer through issuance of Uniform Account Opening Form for all banks. It includes standardized Know Your Customer (KYC), Transaction Profile (TP) and Risk Grading of Customer. information of client’s profession, net wealth, explanation of transaction and regular interval will be required up dated information and recorded,

- To facilitate exchange of information and intelligence among FIUs, Bangladesh FIU has already signed 13 (thirteen) MoUs with other FIUs.

- To provide guidance for effective implementation of regime, a National Coordination Committee headed by the Honorable Finance Minister and a Working Committee headed by the secretary of Bank and Financial Institutions Division of Finance Ministry were formed consisting representatives from all regulatory authorities.
- Bangladesh Government has developed the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2011-2013. The strategy consists of following 12 (Twelve)strategies against 12 (twelve) strategic objectives:

  1. Strengthening the legal framework
  2. Enhancing effectiveness of the FIU
  3. Enforcing compliance of all reporting agencies
  4. Structural improvement and capacity building in tracing out methods, techniques and channels of money laundering and terrorist financing
  5. Improving transparency in financial reporting on AML/CFT issues
  6. Ensuring transparency in the ownership of legal entities
  7. Enhancing financial inclusion
  8. Maintaining a comprehensive AML/CFT database
  9. Boosting national coordination both at policy and operational levels
  10. Developing and maintaining international and regional cooperation on AML/CFT
  11. Heightening public awareness
  12. Stemming the illicit outflows and inflows of fund

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

1. Definition of Customer for KYC purpose
2. Process and timing of Customer Due Diligence (CDD)
3. Defining and identifying Beneficial Owner
4. Politically Exposed Persons related issues
5. Correspondent Banking
6. Employee screening mechanism
7. Awareness program for the customer

- BFIU in cooperation with Anti Corruption Commission has assessed ML/TF risk and vulnerabilities in Bangladesh and drafted the National ML/TF Risk and Vulnerability Assessment Report.
- Bangladesh has continued its pursuance to get membership of the Egmont Group, the global forum for cooperation. In this regard, the off-site evaluation has already been conducted by Malaysia and Thailand as sponsor and cosponsor respectively.
- Separate annual conferences for the Chief Anti-Money Laundering Compliance Officer (CAMLCO) of Banks, Insurance Companies and Financial Institutions were organized.
- The Bank and Financial Institutions Division, Ministry of Finance has issued a circular instructing all the related agencies to provide relevant information to Bangladesh Bank.

- BFIU has continued its effort to develop its IT infrastructure which is necessary for efficient and effective functioning of the unit. In this regard, it has finalized the procurement process of goAML'software for online reporting and software based analysis of CTRs and STRs.
- BFIU has instructed to FIs for submission of Cash Transaction Report-CTR within 21 days of following month if account cash deposit/cash withdrawn transaction through single or more transactions compounding amount is on or above 10.00 lac each day.
- BFIU has instructed to Central Compliance Unit (CCU) of every FI to verifying the cash transaction report for identification of suspicious transaction. If Central Compliance Unit deemed suspicious transaction has been occurred by the client or any third party on behalf of client through cash transaction, a separate STR report along with CTR must be required to submit BFIU. On the other hand, if CCU deemed that suspicious transaction not occurred through cash transaction then a declaration letter certified by CAMLCO will be required to submit BFIU through goAML Web's Message Board regarding no suspicious transaction occurred in the relevant month CTR.
- If Reportable CTR transaction has not been occurred any month then a declaration letter will be required to submit to BFIU regarding "No transaction occurred eligible for CTR" through goAML Web's Message Board.
- CTR not required to submit for cash deposit to government account (different ministry including department), government organization, semi government/autonomous organization except cash withdrawal.
- Each branch of FI's will be preserved CTR monthly.
- All documents of CTR will be required to preserve minimum 05(five) years from the date of submission of report to BFIU.
- BFIU has established MIS to preserve and update all the information and to generate necessary reports using the MIS.
- BFIU has arranged a number of training programs, workshops, seminars and road-shows to create awareness among the staff of reporting organizations, regulatory authorities about related issues.

CHAPTER 4:
VULNERABILITIES OF FINANCIAL INSTITUTIONS

4.1 VULNERABILITIES OF PRODUCTS AND SERVICES

4.1.1 Lease/Term Loan Finance

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

4.1.2 Factoring:

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

4.1.3 Private Placement of Equity/Securitization of Assets

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

4.1.4 Personal Loan/Car Loan/Home Loan

Any person can take personal loan (FFIL does not provide personal loan) from FIs and repay it by illegally earned money; thus he/she can launder money and bring it in the formal channel. After taking home loan or car loan, money launderers can repay those with their illegally earned money, and later by selling that home/car, they can show the proceeds as legal money.

4.1.5 SME/Women Entrepreneur Loan

Small, medium and women entrepreneurs can take loan facilities from FIs and repay that (in some cases before maturity) with illegally earned money. They even do so only to validate their money by even not utilizing the loan. This way they can bring the illegal money in the financial system.

4.1.6 Deposit Scheme

FIs can sell deposit products with at least a three months maturity period. However, the depositor can encash their deposit money prior to the maturity date with prior approval from Bangladesh Bank, foregoing interest income. This deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong measures.

4.1.7 Loan Backed Money Laundering

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

Chapter: Five
Risk Management Framework

5.1 Introduction

FFIL will have flexibility to construct and tailor risk management framework for the purpose of developing risk-based systems and controls and mitigation strategies in a manner that is most appropriate to business structure (including financial resources and staff), products and/or the services they provide. Such risk-based systems and controls should be proportionate to the ML&TF risk(s) a financial institution reasonably faces.

The risk management framework assists FI's to develop and implement AML&CFT programs in compliance with the existing legal and regulatory requirements and international standards and best practices.

For effective risk management, FFIL will at all levels follow the principles below:

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

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

- Different deposit schemes: where FFIL offer products and services directly to persons, business customers, Corporate bodies, Government offices, NGOs, Clubs, societies such as term deposit schemes;
- Corporate finance and investment services: where FFIL provide corporate finance products such as lease finance, term loan, project finance, factoring finance, working capital finance, short-term finance and investment services to corporations, large and medium size enterprises.
- Consumer finance: where FFIL finance their customers to purchase different consumer products and services.

5.2 Risk Management Framework

A risk management framework would consist of:

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

-the types of customers;

-the nature, scale, diversity and complexity of our business;

-our target markets;

-the number of customers identified as high risk;

-the jurisdictions the FFIL is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML & CFT controls and listed by FATF;

-the distribution channels, including the extent to which the FFIL deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;

-the internal audit and regulatory findings;

-the volume and size of its transactions, considering the usual activity of the FFIL and the profile of its customers.

b) Risk identification;

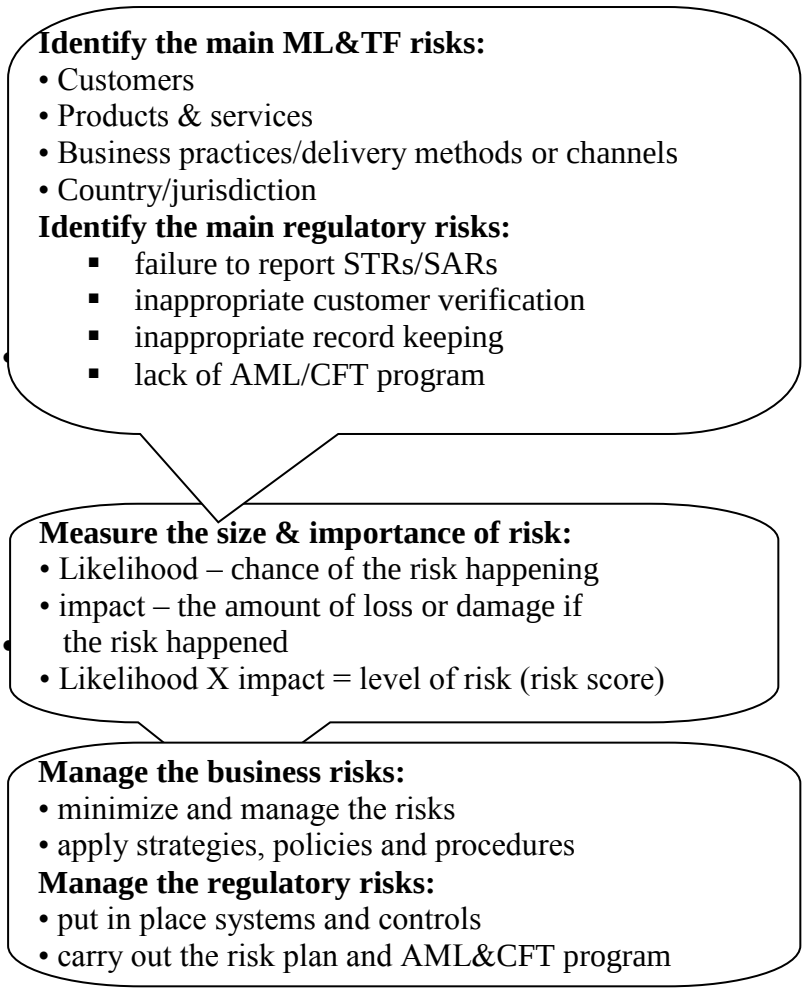
c) Risk assessment or evaluation; and

d) Risk treatment (mitigating, managing, control, monitoring and periodic reviews).

In identifying and assessing the ML & TF risk to which we are exposed, FFIL will consider a range of factors which may include:

Figure 1: The risk management framework at a glance

- **Risk identification:**



- **Risk monitoring and review**

Monitor and review the risk plan:
• develop and carry out monitoring process
• keep necessary records
• review risk plan and AML&CFT program
• do internal audit or assessment
• do AML&CFT compliance report

5.3 The risk management process:

5.3.1 Risk identification

The FFIL will identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The FFIL will apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. Personnel with appropriate knowledge should be involved in identifying risks.

In identification of ML & TF risk FFIL must consider at least risk arisen doing its business i.e. its customers, products or services, delivery channels or methods and jurisdiction and risk of non-compliance.

ML & TF risk arises from business:
FFIL must consider the risk posed by any element or any combination of the elements listed below:

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

Under these four groups, individual risks to a FI can be determined. While not an exhaustive list, some of these individual risks may include:

- **Customers:** followings are some indicators (but not limited to) to identify ML & TF risk arises from customers of a FI.
- a new customer
- a new customer who wants to carry out a large transaction
- a customer or a group of customers making lot of transactions to the same individual or group
- a customer who has a business which involves large amounts of cash
- a customer whose identification is difficult to check
- a customer who brings in large amounts of used notes and/or small denominations.

- customers conducting their business relationship or transactions in unusual circumstances, such as:

- Significant and unexplained geographic distance between the institution and the location of the customer
- Frequent and unexplained movement of accounts to different institutions
- Frequent and unexplained movement of funds between institutions in various geographic locations.

- a non- resident customer
- a corporate customer whose ownership structure is unusual and excessively complex
- customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates
- customers submits account documentation showing an unclear ownership structure
- customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income
- a customer comes with premature encashment of fixed deposit
- a customer generally tries to convince for cash deposit but insists for financial instrument while withdrawing the deposit
- government employee having several large amounts of fixed deposit accounts

Deposit product and services:

- Semi Annul Profit Scheme
- Annual Profit Scheme
- Cumulative Profit Scheme
- Monthly Profit Earner Scheme
- Quarterly Profit Earner Scheme
- Half Yearly Profit Earner Scheme
- Double Money Program
- Triple Money program
- Any new product & service developed.
- Service to walk- in customers

Loans & Advance product and services:

- Lease finance
- Term finance (Home loan, ship manufacturing Industry, Transport, Iron & Steel,)
- Term loan under Project Finance of manufacturing company & R/E developer)
- Working Capital Finance (Trade & commerce, Garment & Knitwear)
- Short term (revolving) finance
- Factoring finance
- Term loan to Brokerage & Securities
- Loans against Term Deposit account.
- Personal loan
- SME finance
- SME Re- finance

Business practice/delivery methods or channels:

- direct to the customer
- Through contractual employee
- phone
- fax
- email

Country/jurisdiction/list of geographical presence:

- Branch in Dhaka, Chittagong, Sylhet and Narsingdi.

Regulatory risk

This risk is associated with not meeting the requirements of the Money laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments) and instructions issued by BFIU. Examples of some of these risks are:

- customer/beneficial owner identification and verification not done properly
- failure to keep record properly
- failure to scrutinize staffs properly
- failure to train staff adequately
- not having an AML&CFT program
- failure to report suspicious transactions or activities
- not submitting required report to BFIU regularly
- not having an AML&CFT Compliance Officer
- failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, IPs)
- not complying with any order for freezing or suspension of transaction issued by BFIU
- not submitting accurate information or statement requested by BFIU or BB.

5.3.2. Risk assessment:

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

Table 1: Risk Management Worksheet – risk

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

A table similar to *Table 1* shown above - Risk management worksheet - could be used for each risk group in preparation for assessing and managing those risks: customers, products and services, business practices/delivery methods, country/jurisdiction and the regulatory risks. Compilation of all risk groups by following table-1 will be treated as risk register of FFIL.

5.3.3. Calculation of Risk Score

- Measure the size & importance of risk:
- Likelihood-chance of the risk happening
- Impact-the amount of loss or damage if the risk happened
- Likelihood X impact= Level of risk(risk score)

Having identified the risks involved, we need to be assessed or measured in terms of the chance (likelihood) we will occur and the severity or amount of loss or damage (impact) which may result if we do occur. The risk associated with an event is a combination of the chance (likelihood) that the event will occur and the seriousness of the damage (impact) it may do.

Therefore each risk element can be rated by:

- the chance of the risk happening – **'likelihood'**
- the amount of loss or damage if the risk happened – **'impact' (consequence)**.

To help assess the risks identified in the first stage of this process, we can apply the risk rating scales for likelihood *(Table 2) on page 15* and impact *(Table 3) on page 16* and from these get a level of risk or risk score using the risk matrix *(Figure 2) on page 16*.

Likelihood X Impact = Risk level/Score

- **Likelihood scale**

A likelihood scale refers to the potential of an ML&TF risk occurring in the business for the particular risk being assessed. Three levels of risk are shown in Table 2, This likelihood can be ascertained based on the available information, group consultation or by applying subjective judgment. FFIL will engage all concerned and competent personnel in ML & TF risk management process including ascertaining the likelihood scale.

Table 2: Likelihood scale

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

- **Impact scale**

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen.

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

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

All these impacts should be considered during measurement of impact scale.

Table 3: Impact scale

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

- **Risk matrix and risk score**

Use the risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to be taken in view of the overall risk. How the risk score is derived can be seen from the risk matrix *(Figure 2)* and risk score table *(Table 4)* shown below. Four levels of risk score are shown in Figure 2 and Table 4, but the FI can have as many as they believe are necessary.

Figure 2: Risk matrix

Threat level for ML/TF risk

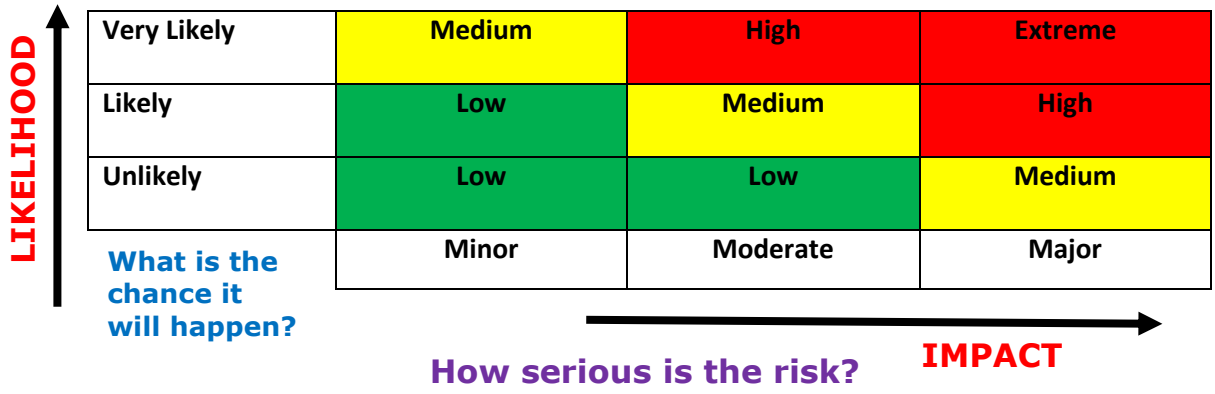


Table 4: Risk score table

Rating	Description
Extreme	Risk almost sure to happen and /or to have very serious consequence. Response: Do not allow transaction to occur without reducing the risk to acceptable level -follow EDD.
High	Risk likely happening and/or having major consequence. Response: Do not allow transaction until risk is reduced-follow EDD
Medium	Possible this could happen and/or have moderate consequence. Response: May go ahead but preferably reduce risk –follow standard CDD.
Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

- **Risk Assessment and Management Exercise:**

FFIL will calculate risk score by blending likelihood and impact, the risk matrix and risk score and can assess the risks of individual customer, product/service, delivery channel and risks related to geographic region by using the simplified risk management worksheet (Table-01). It can also fix up its necessary actions against the particulars outcomes of risks. All the exercises done by the FFIL would be called together **"Risk Registrar"**.

Once threat levels and risk scores have been allocated FFIL can be entered in the risk management worksheet *(Table 5)* next to the risk.

Table 5: Risk management worksheet – threat level and risk score

Risk Group	**Customers**			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
New customer who brings in deposit cash/cheque with matching source of income.	Unlikely	Minor	Low	Okay to go ahead & Standard ID Check
New customer who brings in deposit cash/cheque without declare legitimate source of income.	Likely	minor	Medium	Standard CDD Check
New customer who brings in deposit cash/cheque without matching declared source of income.	Likely	Moderate	High	Do not allow transaction until risk is reduced – follow EDD
Customer who brings in large amounts of used notes and/or small denominations	Likely	moderate	Medium	Standard CDD Check
Customer whose business address and registered office are in different geographic location	Very likely	Major	Extreme	Do not accept as customer.
Customer whose business relationship or transaction unexplained geographic distance between the institution and the location of the customer	Very likely	Major	Extreme	Do not allow transaction
Customer who frequent and unexplained movement of accounts to different institutions	Likely	Moderate	High	Do not allow transaction until risk is reduced – follow EDD
Customer who frequent and unexplained movement of funds between institutions in various geographic locations	Likely	Moderate	High	Do not allow transaction until risk is reduced – follow EDD
A non- resident customer	likely	Moderate	High	Do not allow transaction until risk is reduces – Follow EDD
A corporate customer whose ownership structure is unusual and excessively complex	Likely	Moderate	High	Do not allow transaction until risk is reduces – Follow EDD
Customer of PEPs/IPS/Head of Int'l organization and family members and close associate	Likely	Moderate	High	Do not allow transaction until risk is reduces – Follow EDD
Customers opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known source of legitimate family income	Very likely	Major	Extreme	Do not allow transaction
Customer comes with premature encashment of fixed deposit.	Likely	Moderate	Medium	EDD & STR reporting if deem to be required as per guideline.

Risk Group	Customers			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
Customer generally tries to convince for cash deposit but insists for financial instrument while withdrawing the deposit	likely	Major	High	Standard + Additional ID Check and STR reporting
Government employee having several large amounts of fixed deposit accounts.	Likely	Moderate	High	Standard + Additional ID Check and STR reporting if deem to be required as per guideline.
Private Service holder having several large amounts of fixed deposit accounts.	Likely	Moderate	High	Standard + Additional ID Check and STR reporting if deem to be required as per guideline.
Customer / Group of customers having sanction/embargos or similar measures	Very Likely	Major	Extreme	Do not allow transaction
A loans and advance customer whose business capacity, business related other documents showing in true and fair view.	Unlikely	Minor	Low	Okay to go ahead Standard ID Check
Loans & Advance Customer who adjusted his facility after immense before of expiry date.	Likely	Moderate	High	Standard + Additional ID Check & STR reporting if deemed fit.
A loans and advance customer whose business capacity; business related other documents were shown in ambiguity.	Very Likely	Major	Extreme	Do not allow transaction
Customer's payment received from unknown or un-associated third parties	Very Likely	Major	Extreme	Do not allow transaction
Non –face-to-face business relationships or transactions	Likely	Moderate	High	Standard + Additional ID Check & STR reporting if deemed fit.

Risk Group	Product/Service			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
Prioritized or privileged financial services (in loan or deposit products)	Likely	Moderate	Medium	Standard documentation plus extra precaution.
Factoring products (Fake invoice submission, receivable company might be associated in terrorist financing in collaboration with a fictitious supplier)	Very likely	Major	Extreme	Rigorous documentation plus enhanced due diligence
Service to walk-in customers (Both TDR/Loan products)	Likely	Moderate	Medium	EDD=Extra care and effort to know about the client and their source of fund

Risk Group	Product/Service			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
Syndicated working finance-import oriented	Likely	Moderate	Medium	Standard documentation plus verifying lead arrangers AML/CFT compliance procedures.
100% cash covered high value auto loan	Very likely	Major	Extreme	Standard loan documentation plus additional verification of source of fund
Loan against TDR	likely	Moderate	medium	Standard documentation plus additional verification of purpose of loan.
Any purpose personal loan	Very likely	Moderate	High	Standard documentation plus verification of the actual need of the customer.
Home loan and mortgage loan	Likely	Moderate	Medium	Standard loan documentation plus close monitoring of the client on utilization of fund.

Risk Group	Business practices/delivery methods or channels			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
Direct to the customer	Very likely	Minor	Low	Standard documentation and KYC to be done.
Telesales (Hunting client over phone contact) without face to face contact	Unlikely	Major	Medium	EDD=Verification of the supporting documents and stringent check of source of fund/purpose of loan
Disbursement Cheque in other name (Not Applicant, Like Company Name) for personal loan	Very Likely	Major	Extreme	EDD & Justifying the reason of such request with proper documentation being made.
3rd party consultants or organizations are often employed for specific tasks	Likely	Moderate	Medium	Reputed/expert consultant to be appointed with proper agreement and ensuring cross check the service received
Transferring the ownership of the asset in the name of the third-party without any proper justification (Auto loan)	Very likely	Major	Extreme	To assess the relationship between them and to make required regulatory report

Risk Group	Business practices/delivery methods or channels			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
Prepayment of the loan partially/fully directly by the customer	Very likely	Moderate	High	To justify the reason of settlement

Risk Group	Country/Jurisdiction			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
Branches in the border area (Agrabad, CDA Avenue, Norsingdi and Sylhet)	likely	Moderate	Medium	Being more vigilant and extra precaution during establishment of business relationship with the client
Customer might do business in border area which increases the risk of earning illegal money	Likely	Major	High	EDD with proper justification about the source of fund and nature and purpose of loan. Close monitoring of the client. Regular follow up/update of client information.
Loan might be disbursed to clients who are involved in import oriented business with some countries known to be a tax haven or crime zone area or terrorist activities.	Unlikely	Major	Extreme	Proper follow up/monitoring of the client as well as enhanced due diligence during documentation in pre and regular visit of the client business premises in post disbursement stage.

Risk Group	Regulatory risk			
Risk	**Likelihood**	**Impact**	**Risk score**	**Treatment/Action**
Failure to collect correct and complete information of the client during KYC done	Likely	Major	High	Effective structure/methodand directions are in place to collect the required information through KYC
Customer/beneficial owner identification and verification not done properly	Likely	Moderate	Medium	Creating awareness among concerned employees on this matter.
Failure to keep record properly	Unlikely	Major	High	Put in place document retention policy to keep records properly.
Failure to scrutinize staffs properly	Likely	Moderate	High	Practicing proper mechanisms during

Risk Group	Regulatory risk			
				recruitment process to overcome the risk
Failure to train staff adequately	Unlikely	Major	High	Arranging regular in house training program as well as increased number of nomination to outside training/workshop
Not having an AML&CFT program	Unlikely	Major	Medium	Having an AML/CFT program and time to time review of it for effectiveness.
Failure to report suspicious transactions or activities	Likely	Moderate	Medium	Awareness building up among employees at branch level for such reporting as well as proactively reporting from CCU
Not submitting required report to BFIU regularly	Unlikely	Major	High	Checklist preparation with deadline for regular reporting as well as cautiousness on nonrecurring report.
Not having an AML&CFT Compliance Officer	Unlikely	Major	Medium	AML/CFT Compliance Officer is in place
Failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, IPs)	Unlikely	Major	Extreme	Strict advice and directions are communicated to concerned regarding EDD for high risk customers
Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Unlikely	Major	Extreme	Properly disseminating the freezing or suspension order to concerned persons
Not submitting accurate information or statement requested by BFIU or BB	Unlikely	Major	High	Collecting the information from more than one source to authenticate the data and sending from CCU
Failure to submit Cash Transaction Report (CTR)	Unlikely	Major	Medium	Effective mechanism has been established to make the CTR
Failure to formulate AML/CFT policy	Unlikely	Major	Medium	AML/CFT policy approved by the Board is in place
Failure to declare commitment on AML/CFT by CEO/MD	Unlikely	Moderate	Low	Commitment by CEO is in place and communicated to all employees. Besides

Risk Group	Regulatory risk			
				uploaded in company's website
Not having any Central Compliance Unit (CCU)	Unlikely	moderate	Medium	CCU is in place
Not nominating an experienced BAMLCO at each branch	likely	moderate	Medium	BAMLCO has been appointed at each branch
Not having any Customer Acceptance Policy	Unlikely	Moderate	Medium	Customer Acceptance Policy is formulated and in practice
Failed to allot a Unique Customer Identification Code for each customer	Unlikely	Minor	Low	Each customer has a unique number called CIF number.
Not following risk based approach	Likely	Moderate	Medium	We have risk based profile form in product booklet to categorize customers risk
Not performing self-assessment and independent testing procedure (ITP)	Likely	Major	High	Instruction is properly communicated to all branches for self-assessment report and ITP is done by internal audit team time to time
Not preserving in electronic method updated information of persons and entities listed in UNSCR and local sanction lists.	Likely	Major	High	A link is created with UNSCR and communicated to concerned with the purpose to use it
Not taking proper initiatives for customer learning programs on AML/CFT issues (distributing leaflets, setting posters in branches, publishing/broadcasting awareness advertisement & documentary in various media)	Likely	Moderate	Medium	Customer awareness programs have been arranged in a number of branches. Other options will be implemented in coming days
Failure to call meeting on AML/CFT issues on quarterly basis at branches	Likely	Moderate	Medium	All BAMLCOs are instructed to arrange the meeting and forward the minutes to CCU and done accordingly.
Failure to comply the requirement for high officials or head of international agency	Likely	Moderate	Medium	Already the issue is communicated to concerned employees during in house training.
Not informing or delaying to inform BFIU regarding published news of any account (deposit/loan) of any person or entity involved with ML/TF offence by CCU.	Likely	Moderate	Medium	CCU members are informed and aware about the matter to take proper action in this regard

5.3.4 Risk treatment

Manage the business risks:
Minimize and manage the risks
Apply strategies, policies and procedures

Manage the regulatory risks:
Put in place systems and controls
Carry out the risk plan and AML & CFT program

This stage is about identifying and testing methods to manage the risks the FFIL may have identified and assessed in the previous process. In doing this we will need to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk. Examples of a risk reduction or treatment step are:

- setting transaction limits for high-risk products
- having a management approval process for higher-risk products
- process to place customers in different risk categories and apply different identification and verification methods
- not accepting customers who wish to transact with a high-risk country.

Another way to reduce the risk is to use a combination of risk groups to modify the overall risk of a transaction. The FFIL may choose to use a combination of customer, product/service and country risk to modify an overall risk.

It is important to remember that identifying, for example, a customer, transaction or country as high risk does not necessarily mean that money laundering or terrorism financing is involved. The opposite is also true: just because a customer or transaction is seen as low risk does not mean the customer or transaction is not involved in money laundering or terrorism financing. Experience and common sense should be applied to the risk management process of an entity.

5.3.5 Monitor and review

Monitor & review the risk plan:
- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML&CFT program
- do internal audit or assessment
- do AML&CFT compliance report

Keeping records and regular evaluation of the risk plan and AML & CFT program is essential. The risk management plan and AML&CFT program cannot remain static as risks change over time; for example, changes to customer base, products and services, business practices and the law.

Once documented, the FFIL will develop a method to check regularly on whether AML & CFT program is working correctly and effectively. If not, the FFIL needs to work out what needs to be improved and put changes in place. This will help keep the program effective and also meet the requirements of the AML & CFT Acts and respective Rules.

5.3.6 Additional tools to help risk assessment

The following tools or ideas can be useful in helping to manage risk. It can be included in the previous risk assessment process so that the decisions are to be better informed.

5.3.6.1 Applying risk appetite to risk assessment

Risk appetite is the amount of risk a FI is prepared to accept in pursuit of its business goals. Risk appetite can be an extra guide to the risk management strategy and can also help deal with risks. It is usually expressed as an acceptable/unacceptable level of risk. Some questions to ask are:

- What risks will the FFIL accept?
- What risks will the FFIL not accept?
- What risks will the FFIL treat on a case by case basis?
- What risks will the FFIL send to a higher level for a decision?

The risk matrix can be used to show the risk appetite of our FI.

In a risk-based approach to AML & CFT the assessment of risk appetite is a judgment that must be made by the FFIL. It will be based on its business goals and strategies, and an assessment of the ML & TF risks it faces in providing the designated services to its chosen markets.

Figure 3: Sample risk matrix showing risk appetite

Very Likely	Acceptable Risk Medium	Unacceptable Risk High	Unacceptable Risk Extreme
Likely	Acceptable Risk Low	Acceptable Risk Medium	Unacceptable Risk High
Unlikely	Acceptable Risk Low	Acceptable Risk Low	Acceptable Risk Medium
	Minor	Moderate	Major

5.3.6.2 Risk tolerance

In addition to defining FI's risk appetite, the entity can also define a level of variation to how it manages that risk. This is called risk tolerance, and it provides some flexibility whilst still keeping to the risk framework that has been developed.

Chapter: Six
Risk management: some important issues

6.1 Risk Management Strategies

The FFIL may adopt the following components (where appropriate to the nature, size and complexity of its business), among others, as part of its risk management strategy:

a) reviews at senior management level of the bank's progress towards implementing stated ML&TF risk management objectives
b) clearly defined management responsibilities and accountabilities regarding ML & TF risk management
c) adequate staff resources to undertake functions associated with ML & TF risk management
d) specified staff reporting lines from ML & TF risk management system level to board or senior management level, with direct access to the board member(s) or senior manager(s) responsible for overseeing the system
e) procedural controls relevant to particular designated services
f) documentation of all ML & TF risk management policies
g) a system, whether technology based or manual, for monitoring the FI's compliance with relevant controls
h) policies to resolve identified non-compliance
i) appropriate training program(s) for staff to develop expertise in the identification of ML & TF risk(s) across the FI's designated services
j) an effective information management system which should:
   I. produce detailed and accurate financial, operational and compliance data relevant to ML & TF risk management.
   II. incorporate market information relevant to the global AML & CFT environment which may assist the FFIL to make decisions regarding its risk management strategy.
   III. enable relevant, accurate and timely information to be available to a relevant officer (for example, the AML & CFT Compliance Officer) within the organization.
   IV. to identify, quantify, assess and monitor business activities relevant to ML & TF risk(s)
   V. to monitor the effectiveness of and compliance with its internal AML & CFT systems and procedures
   VI. to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.

It should be noted that FFIL can adopt other strategies in addition to taking into account of any of the above factors (where relevant), if it considers this approach is appropriate in accordance with its risk management framework.

6.2 Ongoing Risk Monitoring

An ongoing monitoring of our risk management procedures and controls may also alert the organization to any potential failures including (but not limited to):

a) failure to include all mandatory legislative components
b) failure to gain board and/or executive approval of the AML & CFT program
c) insufficient or inappropriate employee due diligence
d) frequency and level of risk awareness training not aligned with potential exposure to ML & TF risk(s)
e) changes in business functions which are not reflected in the AML & CFT program (for example, the introduction of a new product or distribution channel)
f) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML & CFT program
g) legislation incorrectly interpreted and applied in relation to a customer identification procedure

h) customer identification and monitoring systems, policies and procedures that fail to:

i) prompt, if appropriate, for further identification and/or verification when the ML & TF risk posed by a customer increases

ii) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service

iii) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check

iv) take appropriate action where the identification document provided is neither an original nor a certified copy

v) recognize foreign identification documentation issued by a high risk jurisdiction

vi) record comprehensive details of identification documents, for example, the date of issue

vii) consult appropriate resources in order to identify high-risk customers

viii) identify when an expired or old identification document (for example, a driver's license) has been used

ix) collect any other name(s) by which the customer is known

i) lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers

j) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:

i) customer identification policies, procedures and systems

ii) identifying potential ML & TF risks

k) acceptance of documentation that may not be readily verifiable.

6.3 Higher risk scenario

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations include the following:

a) Customer risk factors

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer)
- Non-resident customers
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer form
- Business that are cash-intensive
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business

b) Country or geographic risk factors

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML & CFT systems
- Countries subject to sanctions, embargos or similar measures
- Countries identified by credible sources as having significant levels of corruption or other criminal activity
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country

c) Product, service, transaction or delivery channel risk factors

- Priority financial service
- Anonymous transactions (which may include cash)
- Non-face-to-face business relationships or transactions
- Payment received from unknown or un-associated third parties.

6.4 Lower risks Scenario

There are circumstances where the risk of money laundering or terrorist financing may be lower. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

a) **Customer risk factors**

- FIs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership
- Public administrations or enterprises.

b) Product, service, transaction or delivery channel risk factors:

- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML & CFT systems
- Countries identified by credible sources as having a low level of corruption or other criminal activity. In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

Note that having a lower money laundering and terrorist financing risk for identification and verification purposes does not necessarily mean that the same customer poses lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

6.5 Risk variables

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, FI should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship
- The level of assets to be deposited by a customer or the size of transactions undertaken
- The regularity or duration of the business relationship.

6.6 Counter Measures for Risk

6.6.1 Enhanced due diligence measures

FFIL will examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, FFIL will require 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.

6.6.2 Simplified CDD measures

Where the risks of money laundering or terrorist financing are lower, the FFIL are allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold)
- Reducing the frequency of customer identification updates
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established. Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

6.7 Ongoing due diligence

FFIL should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

Chapter: Seven
COMPLIANCE REQUIREMENT

7.1 COMPLIANCE REQUIREMENTS UNDER THE LAWS:

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

According to section 25 of MLPA, 2012 FIs'responsibilities to prevent money laundering are -

a) To maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
b) to preserve previous records of transactions of any customer's account for at least 5(five) years from the date of closure;
c) to provide with the information maintained under clauses(a) and (b) to Bangladesh Bank from time to time, on its demand;

if any suspicious transaction or attempt of such transaction as defined under clause (z)3 of section 2 is observed, to report the matter as 'Suspicious Transaction Report' to the Bangladesh Bank immediately on its own accord. (For details please consult Chapter no 9) According to section 16 of Anti Terrorism (Amendment) Act, 2012, FIs'responsibilities to combat financing of terrorism are –

(1) Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to the Bangladesh Bank without any delay. (For details please consult Chapter no 9)

(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.

Section 2(z) of MLPA, 2012"suspicious transaction" means such transactions –

(i) Which deviates from usual transactions

(ii) 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 in different time.

7.2 COMPLIANCE REQUIREMENTS UNDER CIRCULARS

7.2.1Policies for Prevention of Money Laundering and Terrorist Financing

7.2.2FAS Finance shall not open or maintain numbered or anonymous account.

7.2.3 Customer Identification:

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

- any person or institution maintaining an account of any type with a FI's or having business relationship with FIs;
- the person or institution as true beneficial owner in whose favour the account is operated;
- the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc)under the existing legal infrastructure;

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

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

7.2.4.1 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[8].

Satisfaction of the institution" means satisfaction of the appropriate authority that necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

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

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

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

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

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

7.2.5. Politically exposed Persons (PEPs)

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

While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised.

Following instructions shall have to be followed to ensure Enhanced Due Diligence:

- a risk management system shall have to be introduced to identify risks associated with the accounts opening and operating of PEPs;
- take reasonable measures to establish the source of wealth and source of funds;
- ongoing monitoring of the transactions have to be conducted; and
- the FIs should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

All instructions as detailed for PEPs shall be equally applicable if business relationship is established with family members and close associates of these persons who may pose reputation risk to the FI.

The above instructions shall also be applicable to customers or beneficial owners who become PEPs after business relationship have been established.

7.2.6. Influential Persons (IPs)

"I**nfluential** Persons(IPs) means individuals who are or have been entrusted domestically with prominent public functions , for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials"

While opening and/or operating account of Influential (IPs) enhanced due diligence shall have to be exercised.

Following instructions shall have to be followed to ensure Enhanced Due Diligence:

- a risk management system shall have to be introduced to identify risks associated with the accounts opening and operating of IPs;
- take reasonable measures to establish the source of wealth and source of funds;
- required to take information of client's profession, net wealth, explanation of transaction and regular interval will be required up dated information and recorded,
- ongoing monitoring of the transactions have to be conducted;
- Obtaining competent authority of FI's for establishment of relation with IPs, and

All instructions as detailed for IPs shall be equally applicable if business relationship is established with family members and close associates of these persons who may pose reputation risk to the FI.

The above instructions shall also be applicable to customers or beneficial owners who become PEPs after business relationship have been established.

7.2.7 Appointment and Training

7.2.7.1 Employee Screening: One of the major purposes of combating money laundering and terrorist financing activities is to protect the FIs from risks arising out of money laundering and terrorist financing. To meet this objective, FIs shall have to undertake proper screening mechanism in their different appointment procedures so that they do not face money laundering and terrorist financing risks by any of their staff.

7.2.7.2 Training for the officials: To ensure proper compliance of ML/TF activities each FI shall arrange suitable training for their officials.

7.2.7.3 Education and training for customers: Financial Institutions shall respond to customers on different matters including KYC. Financial Institutions shall time to time distribute leaflets among customers to make them aware about money laundering and terrorist financing and also arrange to stick posters in every branch at a visible place.

7.3 SUSPICIOUS TRANSACTION REPORTING (STR)

According to the provision of section 25 (1) (d) of MLPA, 2012, the FIs have to report BB proactively and immediately, facts on suspicious, unusual or doubtful transactions likely to be related to money laundering. BB has the power to call STR from FIs related to financing of terrorism according to section 15(a) of Anti terrorism (Amendment) Act, 2012.

7.4 CASH TRANSACTION REPORTING (CTR)

According to BFIU Circular no. 12 dated 29.06.2015, the FIs has to report BB monthly basis within 21 days of following month. If account cash deposit/cash withdrawn transaction through single or more transactions compounding amount is on or above 10.00 lac each day. If Reportable CTR transaction has not been occurred any month then a declaration letter will be required to submit to BFIU regarding "No transaction occurred eligible for CTR" through goAML Web's Message Board.

7.5 TARGETED FINANCIAL SANCTIONS:

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

7.6 SUPERVISORY POWER OF BANGLADESH BANK

According to the provision laid down in the section 23 of MLPA, 2012 and section 15 of Anti terrorism (Amendment) Act, 2012, Bangladesh Bank is the core implementing agency. The major supervisory powers are:

Under MLPA, 2012, Bangladesh Bank shall have the following powers and responsibilities to prevent money laundering and to resist any such activities:

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, provide with the said information to the relevant law enforcement agencies for taking necessary actions;

b)ask for any information or obtain a report from reporting organizations with regard to any transaction in which there are reasonable grounds to believe that the transaction is involved in money laundering or a predicate offence;

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;

d) Provided that such order may be extended for additional period of a maximum of 6 (six) months by 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account

e) issue, from time to time, any direction necessary for the prevention of money laundering to the reporting organizations;

f)monitor whether the reporting organizations have properly submitted information and reports requested by Bangladesh Bank and whether they have duly complied with the directions issued by it, and where necessary, carry out on-site inspections of the reporting organizations to ascertain the same;

g)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 Bank;

h) carry out any other functions necessary for the purposes of this Act.

The power and responsibilities of Bangladesh Bank under section 15(1) of Anti Terrorism (Amendment) Act, 2012 are as follows:

The Bangladesh Bank shall have the power and authority to take necessary measures to prevent and detect transaction intended to commit offence under ATA through any banking channel, and for that matter BB is empowered and authorized to -

- Call for STRs from financial institutions and keep such report confidential if law does not allow disclosure;
- Compile and preserve all statistics and records;
- Create and maintain a database of all STRs;
- Analyze the STRs;
- Issue order in writing to FIs to suspend a transaction for a period of 30 days where it has reasonable grounds to suspect that the transaction involves connection with terrorist acts, and extend the order to maximum 180 days.
- Monitor and observe the activities of FIs;
- Issue instructions to FIs directing them to take preventive measures against terrorist financing activities.
- Inspect FIs for the purpose of detection of suspicious transactions connected with terrorist financing; and
- Provide training to staff and officers of FIs for the purpose of detection and prevention of suspicious transactions as may be connected with terrorist financing.

- It is to be noted that no law enforcement authority shall have any access to the documents or files of a financial institution without approval from the chief executive of the concerned financial institution or from Bangladesh Bank.

7.7 PENALTIES UNDER MLPA:

According to section 25 (2) of MLPA, 2012, if any reporting organization violates the directions mentioned in sub-section (1) of section 25 of MLPA, 2012, Bangladesh Bank may-

(a) Impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty five) lacs on the reporting organization; and
(b) in addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities of the said organization or any of its branches, service centers, booths or agents, or as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

In addition to the above mentioned provisions there are some new provisions of penalties in the section 23 of MLPA, 2012. These are:
(3) If any reporting organization fails to provide with the requested information timely under this section, Bangladesh Bank may impose a fine on such organization which may extend to a maximum of Taka 5 (five) 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.

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

(5) If any reporting organization fails to comply with any instruction given by Bangladesh Bank under this Act, Bangladesh Bank may impose a fine on such organization which may extend to a maximum of Taka 5 (five) 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 Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.

(6) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Bank under clause (c) of sub-section 23(1) of MLPA, 2012, Bangladesh Bank may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.

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

(8) If any reporting organization is imposed fine under sub-sections 23 (3), (4), (5) and (6), Bangladesh Bank may also impose a fine not less than Taka 10 (ten) thousand but not exceeding taka 5 (five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

7.8 PENALTIES UNDER ATA:

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

7.9 SELF ASSESSMENT

As per AML circular 15, each FI should establish half yearly self assessment procedure that will assess how effectively the FI‘s AML/CFT program is working. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment should conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions and recommendations. The self assessment should advise management whether the internal procedures and statutory obligations of the FI have been properly discharged. Each branch will assess its AML/CFT activities covering the following areas on half yearly basis and submit the report to CCU within next 20 days:

- The percentage of officers/employees that received official training on AML/CFT;
- The awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and Bangladesh Bank‘s instructions and guidelines;
- The arrangement of AML/CFT related meeting on regular interval;
- The effectiveness of the customer identification during opening an individual, corporate and other account;

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

7.10 INDEPENDENT TESTING PROCEDURE

As per AML circular 15, testing is to be conducted at least annually by financial institutions' internal audit personnel, compliance department, and by an outside party such as the Institution's external auditors. The test will cover the following areas:

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

The tests include interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the financial institution's anti-money laundering procedures.

- sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- test of the validity and reasonableness of any exemption granted by the financial institution; and
- test of the record keeping system according to the provisions of the laws. 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.

CHAPTER 8:
COMPLIANCE PROGRAM

Financial institutions subject to laws should establish and maintain an effective AML/CFT program that includes at least the followings:

- Development of internal policies, procedures and controls;
- Appointment of an AML/CFT Compliance Officer;
- Ongoing employee training programs; and
- Independent audit function including internal and external audit function to test the programs.

The compliance program should be documented, approved by the Board of Directors and communicated to all levels of the organization. ***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 degree of ML and/or TF risks associated with FIs.***

8.1 DEVELOPMENT OF INTERNAL POLICIES, PROCEDURES AND CONTROLS

8.1.1 Internal Policy

Each financial institution must develop, administer, and maintain its own AML/CFT policy that ensures and monitors compliance with the laws, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes.

The written AML/CFT compliance policy at a minimum should establish clear responsibilities and accountabilities within their organizations to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the Act.

The policies should be tailored to the institution and would have to be based upon an assessment of the money laundering and terrorist financing risks, taking into account the financial institution's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering and terrorist financing.

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

It should also include a description of the roles the AML/CFT Compliance Officer(s)/Unit and other appropriate personnel will play in monitoring compliance and effectiveness of AML/CFT policies and procedures.

It should develop and implement screening programs to ensure high standards when hiring employees. Implement standards for employees who consistently fail to perform in accordance with an AML/CFT framework.

It should incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.

It should have the arrangements for program continuity despite changes in management or employee composition or structure.

The AML/CFT policies should be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/operational changes, such as additions or amendments to existing AML/CFT related rules and regulations or business.

In addition the policy should emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and should set forth the consequence of non-compliance with the applicable laws and the institution‘s policy, including the criminal, civil and disciplinary penalties and reputation harm that could ensue from any association with money laundering and terrorist financing activity.

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 programs which can deter criminals from using their facilities for money laundering and terrorist financing, thus ensuring that they comply with their obligations under the laws.

8.1.1.1 Components of Policy

- The statement of compliance policy should at a minimum include:
- A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.
- A statement that all activities carried out by the financial institution must comply with applicable governing laws and regulations.
- A statement that compliance with rules and regulations is the responsibility of each individual in the financial institution in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations cannot be an excuse for non-compliance.
- A statement that should direct staff to a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.
- A statement that employees will be held accountable for carrying out their compliance responsibilities.

8.1.1.2 Communicating the Policy

As part of its AML/CFT policy, an institution should communicate clearly to all employees on annual basis through a statement from the chief executive officer that clearly sets forth its policy against money laundering 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 institution and its senior management to comply with all laws and regulations designed to combat money laundering and terrorist financing.

8.1.2 Procedures

The standard operating procedures are often designed at a lower level in the organization and modified as needed to reflect the changes in products, personnel and promotions, and other day to day operating procedures. It will be more detailed than policies. Standard operating procedures translate policy into an acceptable and working practice. In addition to policies and procedures, there should also be a process to support and facilitate effective implementation of procedures and that should be reviewed and updated regularly.

8.1.3 Internal Control Mechanism

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

- Statement of responsibility for compliance with policy;
- Customer due diligence;
  - Customer identification/verification
  - Additional know your customer information
  - High risk customers
  - Non face to face business (if applicable)
  - Handling of politically exposed persons

- Monitoring for suspicious transaction/activity;
- Cooperation with the authorities;
- Record keeping ;
- Screening of transactions and customers;
- Training and awareness;
- Adoption of risk management practices and use of a risk-based approach.

8.2 ESTABLISHMENT OF CENTRAL COMPLIANCE UNIT

To ensure compliance of the Money Laundering Prevention Act, 2012 and ATA 2009 (as amended in 2012) each financial institution will establish arrangement for internal monitoring and control through formation of a Central Compliance Unit (CCU) under the leadership of a high official at the Head Office. In order to accomplish properly the jurisdiction and function of the CCU, each financial institution will determine institutional strategy and program. CCU will issue the instructions to be followed by the branches; these instructions will be prepared on the basis of combination of issues in monitoring of transactions, internal control, policies and procedures from the point of view of preventing money laundering & terrorist financing. CCU shall be dedicated solely to FI's related responsibilities and perform the compliance functions. The responsibilities of a CCU shall include:

a)preparing an overall assessment report after evaluating the self assessment reports received from the branches and submitting it with comments and recommendations to the chief executive of the bank;

b) Preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Audit Department on that particular quarter;

c) Submitting a half-yearly report to BFIU within 60 days after end of a quarter.

8.3 APPOINTMENT OF CHIEF AML/CFT COMPLIANCE OFFICER

Each financial institution must designate a Chief AML/CFT Compliance Officer (CAMLCO) at its head office who has sufficient authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures. The CAMLCO will directly report to the Chief Executive Officer/Managing Director for his/her responsibility. The CAMLCO will also be responsible to coordinate and monitor day to day compliance with applicable AML/CFT related laws, rules and regulations as well as with its internal policies, practices, procedures and controls.

8.3.1 Position of CAMLCO

The Chief AML/CFT Compliance Officer will be the head of CCU. The designated CAMLCO, directly or through CCU, should be a central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to financial institution's AML/CFT program. The position of the CAMLCO cannot be lower than the third rank in seniority in organizational hierarchy.

8.3.2 Qualification and experience

The CAMLCO should have a working knowledge of the diverse financial products offered by the financial institutions. The person could have obtained relevant financial institutional and compliance experience as an internal auditor or regulatory examiner, with exposure to different financial institutional products and businesses. Product and financial institutional knowledge could be obtained from being an external or internal auditor, or as an experienced operational staff. The Chief AML/CFT Compliance Officer should have a minimum of seven years of working experience, with a minimum of three years at a managerial/administrative level.

8.3.3 Responsibilities:

Each financial institution should prepare a detailed specification of the role and obligations of the CAMLCO. Depending on the scale and nature of the financial institution the designated Chief AML/CFT Compliance Officer may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions. The major responsibilities of a CAMLCO are as follows:

1. To monitor, review and coordinate application and enforcement of the financial institution's compliance policies including AML/CFT Compliance Policy. This will include - an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity, and a written AML/CFT training plan.
2. To monitor changes of laws/regulations and directives of Bangladesh Bank and revise its internal policies accordingly;
3. To respond to compliance questions and concerns of the staff and advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk;
4. To ensure that the financial institution's AML/CFT policy is complete and up-to-date, to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered by the financial institution;
5. To develop the compliance knowledge of all staff, especially the compliance personnel and conduct training courses in to the institution in this regard;
6. To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;
7. To assist in review of control procedures in the financial institution to ensure legal and regulatory compliance and in the development of adequate and sufficient testing Procedures to prevent and detect compliance lapses;
8. To monitor the business through self-testing for AML/CFT compliance and take any required corrective action;
9. To manage the STR/SAR process:

- reviewing transactions referred by divisional, regional, branch or unit compliance officers as suspicious;
- reviewing the transaction monitoring reports (directly or together with account management personnel);
- ensuring that internal Suspicious Activity Reports(SARs):
  - are prepared when appropriate;
  - reflect the uniform standard for "suspicious activity Involving possible money laundering or terrorist financing" established in its policy;

- are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy;
- are advised to other branches of the institution who are known to have a relationship with the customer;
- are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk .

- ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;
- maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner;
- managing the process for reporting suspicious activity to BFIU after appropriate internal consultation;

8.4 BRANCH ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

FAS will appoint Branch Anti-Money Laundering Compliance Officer (BAMLCO) at each of their branches. BAMLCO will be the Head of a branch (since we don't have more officers in branches presently) and have a minimum three year experience in related field. The responsibilities of a BAMLCO are as follows:

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

8.5 RESPONSIBILITIES OF OTHER EMPLOYEES

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

Function	**Role / Responsibilities**
Staff Responsible for account opening	• Perform due diligence on prospective clients prior opening an account • Be diligent regarding the identification (s) of account holder and the transactions relating to the account • Ensure all required documentation is completed satisfactorily • Complete the KYC Profile for the new customer • Ongoing monitoring of customers KYC profile and transaction activity • Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO
Customer Service Officer	• Support the Account Officer in any of the above roles • Perform the Account Officer roles in their absence
Operations Staff	• Ensure that all control points are completed prior to transaction monitoring • Be diligence on transaction trends for clients • Update customer transaction profiles in the ledger/system
Branch Manager(Unit Head)	• Ensure that the program is effective within the branch/unit

	• First point of contact for any issues
Risk Management /Credit Officer/ Internal Control Officer	• Perform Risk Assessment for the Business • Perform periodic Quality Assurance on the program in the unit • Communicate updates in laws and internal policies
Operations &technology Manager	• Ensures that the required reports and systems are in place to maintain an effective program
Controller of Branches Chief Executive Officer (CEO)	• Overall responsibility to ensure that the branches have an program in place and that it is working effectively • Overall responsibility to ensure that the Business has an AML program in place and it is working effectively
Chief Executive Officer (CEO)	▪ Overall responsibility to ensure that the Business has an AML program in place and it is working effectively.

8.6 EMPLOYEE TRAINING AND AWARENESS PROGRAM

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

8.6.1 The Need for Staff Awareness

The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institution appreciates the seriousness of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities. It is, therefore, important that financial institutions introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.

8.6.2 Education and Training Programs

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

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

8.6.3 General Training

A general training program should include the following:

- General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
- Legal framework, how AML/CFT related laws apply to FIs and their employees;

- Institution‘s policies and systems with regard to customer identification and verification, due diligence , monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

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

8.6.4 Job Specific Training

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

8.6.4.1 New Employees

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

8.6.4.2 Customer Service/Relationship Managers

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to the organization's strategy in the fight against money laundering and terrorist financing. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with non-regular (walk-in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

8.6.4.3 Processing (Back Office) Staff

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

8.6.4.4 Credit Officers:

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

8.6.4.5 Audit and compliance staff

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

8.6.4.6 Senior Management/Operations Supervisors and Managers

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

8.6.4.7 Senior Management and Board of Directors

Money laundering and terrorist financing issues and dangers should be regularly and thoroughly communicated to the board. It is important that the compliance department has strong board support, and one way to ensure that is to keep board members aware of the reputation risk that money laundering and terrorist financing poses to the institution. Major AML/CFT compliance related circulars/circular letters issued by BB should be placed to the board to bring it to the notice of the board members.

8.6.4.8 AML/CFT Compliance Officer

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

8.6.5 Training Procedures

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

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

8.6.6 Refresher Training

In addition to the above compliance requirements, training may have to be tailored to the needs of specialized areas of the institution's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Some FIs may wish to provide such training on an annual basis; others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring. Training should be conducted ongoing basis, incorporating trends and developments in an institution's business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.

8.7 INDEPENDENT AUDIT FUNCTION

8.7.1 Why the audit function is necessary

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

8.7.2 Why the audit function must be independent

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

8.7.3 Whom they report

The individuals conducting the audit should report directly to the board of directors/senior management.

8.7.4 The ways of performing audit function

Audit function shall be done by the internal audit. At the same time external auditors appointed by the FI to conduct annual audit shall also review the adequacy of AML/CFT program during their audit.

8.7.5 Internal audit

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

- Address the adequacy of AML/CFT risk assessment.
- Examine/attest the overall integrity and effectiveness of the management systems and the control environment.
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements.
- Determine personnel adherence to the financial institution's AML/CFT policies, procedures and processes.
- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations).
- Assess the adequacy of the FI's processes for identifying and reporting suspicious activity.
- Communicate the findings to the board and/or senior management in a timely manner.
- Recommend corrective action for deficiencies.

- Track previously identified deficiencies and ensure that management corrects them.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Determine when assessing the training program and materials:
  - The importance that the board and the senior management place on ongoing education, training and compliance
  - Employee accountability for ensuring AML/CFT compliance.
  - Comprehensiveness of training, in view of specific risks of individual business lines.
  - Participation of personnel from all applicable areas of the FI.
  - Frequency of training.
  - Coverage of FI's policies, procedures, processes and new rules and regulations.
  - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.
  - Penalties for noncompliance and regulatory requirements.

8.7.6 External Auditor

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

CHAPTER 9:
CUSTOMER DUE DILIGENCE

9.1 KNOW YOUR CUSTOMER PROGRAM

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

9.2 KNOW YOUR CUSTOMER (KYC) PROCEDURE

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

9.2.1 Nature of Customer's Business

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might

be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. In order to judge whether a transaction is or is not suspicious, institutions need to have a clear understanding of the business carried out by their customers.

9.2.2 Identifying Real Person

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

9.2.3 Document is not enough

The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process. The overriding principle is that every

FI must know who their customers are, and have the necessary documentary evidence to verify this. Collection of document is not enough for KYC, identification is very important.

9.2.4 Reliance on Third party

Countries may permit financial institutions to rely on third parties to perform the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.
The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information.

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

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

9.3 COMPONENTS OF KYC PROGRAM

Financial institutions in the process of designing the KYC program should include certain key elements. Such essential elements should start from the financial institutions' risk management and control procedures and should include -
(1) Customer acceptance policy,
(2) Customer identification,
(3) On-going monitoring of high risk accounts, and
(4) Identification of suspicious transactions.

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

9.3.1 Who is a Customer?

For the purpose of KYC Procedure a "Customer" is defined in AML Circular No. 24 dated 03/03/2010, as:

- 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 true beneficial owner in whose favour the account is operated;
- the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc)under the existing legal infrastructure;
- high value single transaction conducted in a single Demand Draft, Pay Order, Telegraphic Transfer by any person or institution or any person/institution involved in a financial transaction that may pose reputational and other risks to the institution. In this ase 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;

9.3.2 Customer Acceptance Policy

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

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

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

1) No account should be opened in anonymous or fictitious name.
2) Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers in to different risk grades.
3) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.

4) Not to open an account or close an account where the financial institution is unable to apply appropriate customer due diligence measures i.e. financial institution is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the financial institution. Decision by a financial institution to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

5) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

6) Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

7) The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.

9.3.3 Customer Identification

Customer identification is an essential element of KYC standards. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for financial institution to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a financial institution becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible. Once verification of identity has been satisfactorily completed, no further evidence is needed to undertake subsequent transactions. However, information should be updated or reviewed as appropriate and records must be maintained.

9.3.4 What Constitutes a Customer's Identity?

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

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

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issuance should be recorded. The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the institution's own understanding of the applicant's business.

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

9.3.5 Individual Customers

FIs shall obtain following information while opening accounts or establishing other relationships with individual customers:

- Correct name and/or names used;

- parent‘s names;
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of wealth or income
- Contact information, such as – mobile/telephone no.

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

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

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

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

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

9.3.5.1 No face-to-face contact: Where there is no face-to-face contact, photographic identification would clearly be inappropriate procedures to identify and authenticate the customer. FIs 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. FIs should not allow non face to face contact to a resident in establishing relationship.

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

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

9.3.5.4 Change in address or other details: Any subsequent change to the customer‘s name, address, or employment details of which the financial institution becomes aware should be recorded as part of the Know Your Customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

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

9.3.5.6 Introducer:

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

9.3.5.7 Persons without Standard Identification Documentation

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

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

In these cases it may be possible for the institution to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc) who knows the person. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptableto 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.

9.3.5.8 Minor

For minor, the normal identification procedures set out 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). 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.

9.3.6 Corporate Bodies and Other Entities

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for legitimate trading or economic purpose, and that it is not merely a brass plate company. where the controlling principals cannot be identified. Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, and struck off, wound-up or terminated. In addition, if the institution becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

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

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

- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the
- company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.

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

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

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

A letter issued by a corporate customer is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again. When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

9.3.6.1 Companies Registered Abroad

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

9.3.7 Partnerships and Unincorporated Businesses

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

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

9.3.8 Powers of Attorney/ Mandates to Operate Accounts

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept.

9.3.9 KYC for Internet or Online Based Customer (This is yet to include in FAS Finance)

Banking and investment business through the Internet add a new dimension to Financial Institutions' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering and fraud. It is recognized that on-line account opening services are convenient. However, it is not appropriate that Financial Institutions should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures.

However, 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 standardized account opening provisions have been satisfied in accordance with these Guidance Notes.

The development of technologies such as encryption, digital signatures, etc., and the development of new financial services and products, makes the Internet a dynamic environment offering significant business opportunities. The fast pace of technological and product development has significant regulatory and legal implications, and Bangladesh Bank is committed to keeping up-to-date with any developments on these issues through future revisions to its Guidance Notes.

9.3.10 Timing and Duration of Verification

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

However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority. This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is itself suspicious.

9.4 KNOW YOUR EMPLOYEE (KYE)

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

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

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

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

CHAPTER 10:
RECORD KEEPING

10.1 STATUTORY REQUIREMENT

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

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

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

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

Records relating to verification of identity will generally comprise:

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

Records relating to transactions will generally comprise:

Details of personal identity, including the names and addresses, etc. pertaining to:

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

Details of transaction including:

1) nature of such transactions;
2) volume of transactions customer's instruction(s) and authority (ies);
3) source(s) of funds;
4) destination(s) of funds;
5) book entries;
6) custody of documentation;
7) date of the transaction;
8) form in which funds are offered and paid out.

9) parties to the transaction
10)identity of the person who conducted the transaction on behalf of the customer

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

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

Financial institutions should ensure that records pertaining to the identification of the customer, his/her address (e.g. copies of documents like passport, national ID card, driving license, trade license, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended and should be made available to the competent authorities upon request without delay.

10.2 RETRIEVAL OF RECORDS

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

It is not always necessary to retain documents in their original hard copy form, provided that the firm has reliable procedures for holding records in microchips or electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, an institution 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 institution 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 records required.

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

10.3 CTR, STR AND INVESTIGATION

Where a FI has submitted a report of suspicious transaction to BFIU or where it is known that a customer or any transaction is under investigation, it should not destroy any records related to the customer or transaction without the consent of the BFIU or conclusion of the case even though the five-year limit may have been elapsed. To ensure the preservation of such records the financial institutions should maintain a register or tabular records of all investigations and inspection made by the investigating authority or Bangladesh Bank and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

i. the date of submission and reference of the CTR/STR/SAR;
ii. the date and nature of the enquiry;
iii. the authority who made the enquiry, investigation and reference; and
iv. details of the account(s) involved.

10.4 TRAINING RECORDS

Financial institutions will comply with the regulations concerning staff training, they shall maintain training records which include:-
(i) details of the content of the training programs provided;
(ii) the names of staff who have received the training;
(iii) the date/duration of training;
(iv) the results of any testing carried out to measure staffs understanding of the requirements; and
(v) an on-going training plan.

10.5 BRANCH LEVEL RECORD KEEPING

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

1) Information regarding Identification of the customer,
2) KYC information of a customer,
3) Transaction report,
4) Suspicious Transaction/CTR /Activity Report generated from the branch,
5) Exception report,
6) Training record,
7) Return submitted or information provided to the Head Office or competent authority.

10.6 SHARING OF RECORD/INFORMATION OF/TO A CUSTOMER

Under MLPA 2012, and ATA, 2009 (as amended in 2012), FIs shall not share account related information to investigating authority i.e., ACC or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh Bank.

CHAPTER 11:
SUSPICIOUS TRANSACTION REPORT/SUSPICIOUSACTIVITY REPORT

The final output of all compliance programs is reporting of suspicious transaction or reporting of suspicious activity. Cash Transaction Report (CTR) or Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the risk for financial institutions. So it is necessary for the safety and soundness of the institution.

11.1 DEFINITION OF STR/SAR

Generally STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be usual manner. Such report is to be submitted by financial institutions to the competent authorities.
In the section (2)(z) of MLPA, 2012 “suspicious transaction” means such transactions which deviates from usual transactions; of which there is ground to suspect that,

(1) the property is the proceeds of an offence,
(2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;
(3) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Bank from time to time.

In Anti Terrorism Act, 2009 (as amended in 2012), STR/SAR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. One important thing is that financial institutions need not to establish any proof of occurrence of a predicate offence; it is a must to submit STR/SAR only on the basis of suspicion.

11.2 OBLIGATIONS OF SUCH REPORT

As per the Money Laundering Prevention Act, 2012, FIs are obligated to submit STR/SAR to Bangladesh Bank. Such obligation also prevails for the FIs in the Anti Terrorism Act, 2009 (as amended in 2012). Other than the legislation, Bangladesh Bank has also instructed the FIs to submit STR/SAR through AML Circulars issued by Bangladesh Bank time to time.

11.3 REASONS FOR REPORTING OF STR/SAR

As discussed above, STR/SAR is very crucial for the safety and soundness of the financial institutions. The FIs should submit STR/SAR considering the followings:

It is a legal requirement in Bangladesh;
It helps protect the reputation of FIs ;
It helps to protect FIs from unfounded allegations of assisting criminals, including terrorists;
It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

11.4 IDENTIFICATION AND EVALUATION STR/SAR

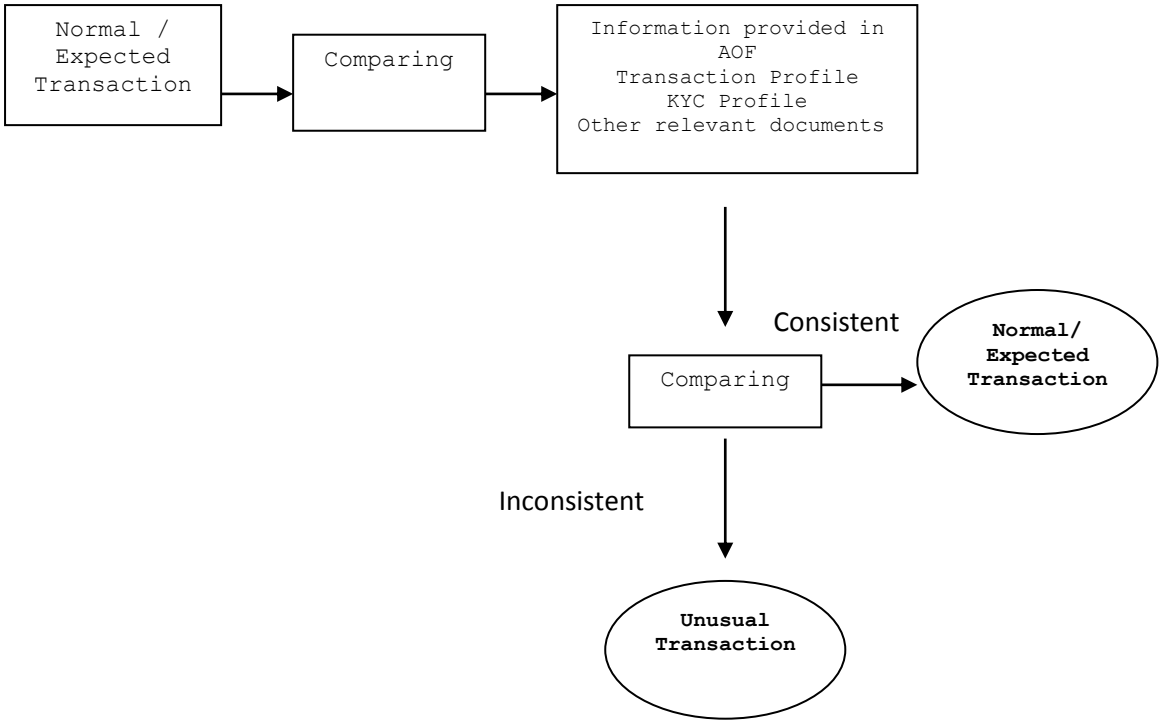
Identification of STR/SAR is very crucial for financial institutions to mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place by the financial institutions. Such suspicion may not only at the time of transaction but also at the time of doing KYC and attempt to transaction.

11.4.1 Identification of STR/SAR:

Identification of STR/SAR may be started identifying unusual transaction and activity. Such unusual transaction may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Generally the detection of unusual transactions/activities may something be sourced as follows:

Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable explanation.
By monitoring customer transactions.
By using red flag indicator.

Simply, if any transaction/activity is consistent with the provided information by the customer can be treated as normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.



As discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, FIs should conduct the following 3 stages:

a) Identification:

This stage is very vital for CTR/STR/SAR reporting. Depending on size, need and complexity of financial institutions monitoring of unusual transactions may be automated, manually or both. Some financial institutions use specialized software to detect unusual transactions or activities, however, the use of such software can only be complemented managerial oversight and not be replaced the need for constant monitoring of activity of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution and supported by adequate information systems to alert management and other appropriate staff (e.g., the compliance officer) of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should

always be an ongoing activity. Considering the nature of business FIs must be vigilant in KYC and sources of funds of the customer to identify STR/SAR.

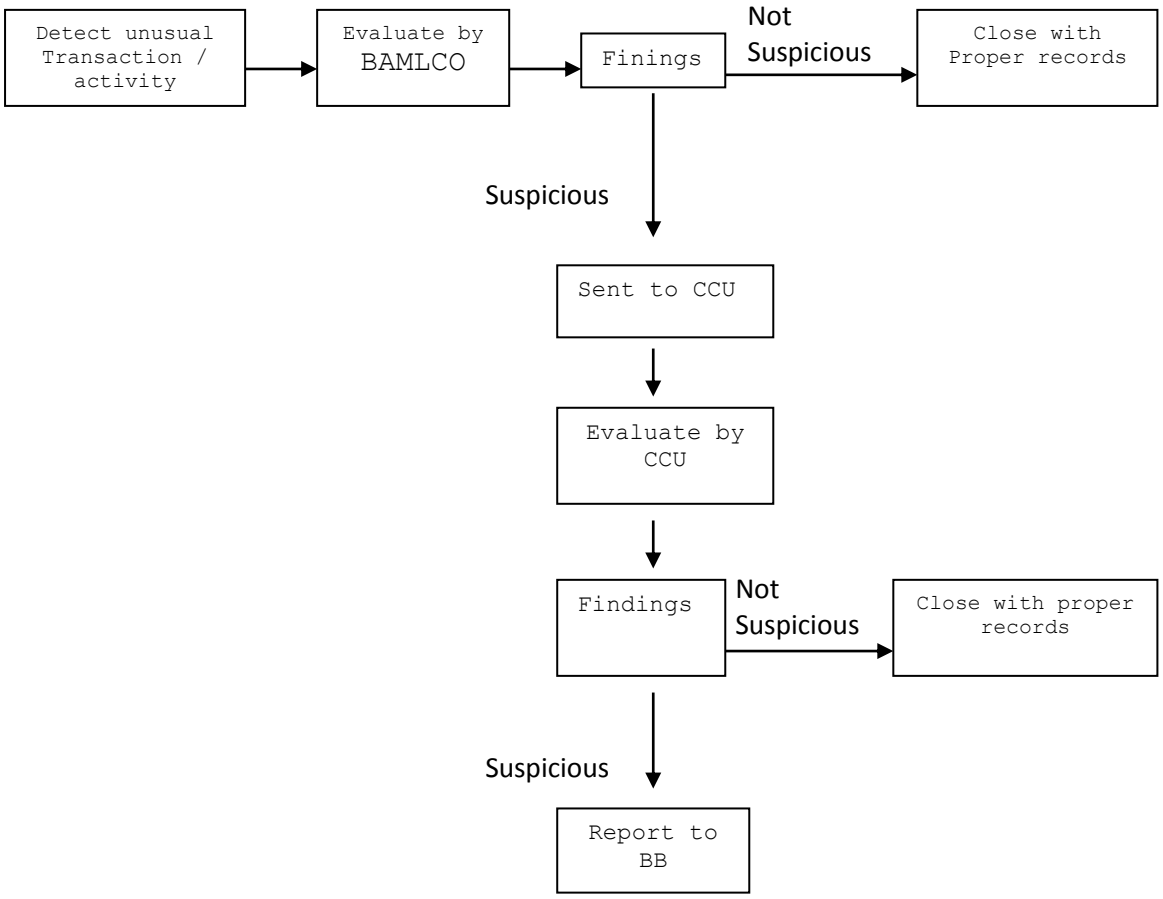
b) Evaluation:

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

c) Disclosure:

This is the final stage and FIs should submit STR/SAR to Bangladesh Bank if it is still suspicious.

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



11.5 RISK-BASED APPROACH

An integrated risk-based system depends mainly on a proper assessment of the relevant risk sectors, products, services, and clients and on the implementation of appropriate risk-focused due diligence and record-keeping. These in turn become the foundation for monitoring and compliance mechanisms that allow rigorous screening of high-risk areas and accounts. Without sufficient due diligence and risk profiling of a customer, adequate monitoring for suspicious activity would be impossible. According to the Wolfsburg Group guidelines, a risk-based monitoring system for financial institutions clients should:

- compare the client's account/transaction history to the client's specific profile information and a relevant peer group, and/or examine the clients account/transaction history against established money-laundering criteria/scenarios, in order to identify patterns of suspicious activity or anomalies;
- establish a process to compare customer or transaction-specific data against risk-scoring models;
- Be capable of recognizing patterns and of .learning. which transactions are normal for a client, rather than designating certain transactions as unusual (for example, not all large transaction are unusual and may easily be explained);
- issue alerts if unusual transactions are identified;
- track alerts in order to ensure they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required; and
- Maintain an audit trail for inspection by the institution's audit function and by financial institutions supervisors.

11.6 REPORTING OF STR/SAR

Institutions enlisted as per MLPA, 2012 and ATA, 2009 (as amended in 2012) are obligated to submit STR/SAR to Bangladesh Bank. Such report must come to the Bangladesh Bank from CCU of the respective institutions by using specified format/instruction given by the Bangladesh Bank.

11.7 TIPPING OFF

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

11.7.1 Penalties of Tipping Off

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

11.8 "SAFE HARBOR" PROVISIONS FOR REPORTING

Safe harbor laws encourage financial institutions to report all suspicious transactions by protecting financial institutions and employees from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. In section (28) of MLPA, 2012 provides the safe harbor for reporting.

11.9 RED FLAGS OR INDICATORS OF STR

11.10.1 Moving Customers: A customers who moves every month, particularly if there is nothing in that person‘s information suggesting that frequent changes in residence is normal, could be suspicious.

11.10.2 Out of market windfalls: If you think a customer who just appeared at your institution sounds too good to be true, you might be right. Pay attention to one whose address is far from your institution, especially if there is no special reason why you were given the business. Aren‘t there institutions closer to home that could provide the service? If the customer is a business, the distance to its operations may be an attempt to prevent you from verifying there is no business after all. Don‘t be bullied by your sales personnel who follow the “no question asked” philosophy of taking in new business.

11.10.3 Suspicious Customer Behavior:

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses your record-keeping or reporting duties with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be recorded.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.
- Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.
- Customer who is a student uncharacteristically transacts large sums of money.
- Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

11.10.4 Suspicious Customer Identification Circumstances:

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information when opening an account.
- Customer‘s permanent address is outside the FI‘s service area.
- Customer asks many questions about how the financial institution disseminates information about the identification of a customer.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

11.10.5 Suspicious Cash Transactions:

- Customer opens several accounts in or more names, then makes several cash deposits under the reporting threshold.
- Customer conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf.
- Corporate account has deposits and withdrawals primarily in cash than cheques.

11.10.6 Suspicious Non-Cash Deposits:

- Customer deposits large numbers of consecutively numbered money orders or round figure amounts.
- Customer deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business.
- Funds out of the accounts are not consistent with normal business or personal items of the account holder
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

11.10.7 Suspicious Activity in Credit Transactions:

- A customer‘s financial statement makes representations that do not conform to accounting principles.
- Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.

11.10.8 Suspicious Commercial Account Activity:

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.

11.10.9 Suspicious Employee Activity:

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the FI requires.
- Employee frequently is involved in unresolved exceptions or recurring exceptions on exception reports.
- Employee lives a lavish lifestyle that could not be supported by his/her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.

11.10.10 Suspicious Activity in an FI Setting:

- Request of early encashment.
- A DPS (or whatever) calling for the periodic payments in large amounts.
- Lack of concern for significant tax or other penalties assessed when cancelling a deposit.

List of Abbreviations

AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
AMLD	Anti-Money Laundering Department
APG	Asia Pacific Group on Money Laundering
ATA	Anti Terrorism Act
BAMLCO	Branch Anti-Money Laundering Compliance Officer
BB	Bangladesh Bank
BDT	Bangladesh Taka
BFIU	Bangladesh Financial Intelligence Unit
CAMLCO	Chief Anti-Money Laundering Compliance Officer
CCU	Central Compliance Unit
CDD	Customer Due Diligence
CTC	Counter Terrorism Committee
CTR	Cash Transaction Report
FATF	Financial Actions Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FSRB	FATF Style Regional Body
GPML	Global program against Money Laundering
ICRG	International Cooperation and Review Group
IOSCO	International Organization of Securities Commissions
KYC	Know Your Customer
ML	Money Laundering
MLPA	Money Laundering Prevention Act
NCC	National Coordination Committee on
NCCT	Non-cooperating Countries and Territories
OECD	Organization for Economic Co-operation and Development
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
TP	Transaction Profile
UN	United Nations
UNODC	UN Office of Drugs and Crime
UNSCR	United Nations Security Council Resolution