Money Laundering &Terrorist Financing Risk Management Guidelines

Anti Money Laundering Department
Mercantile Bank Limited

June, 2016

Focus Group

Coordinator:

Mr. Monindra Kumar Nath
Additional Managing Director & CAMLCO
Mercantile Bank Limited
Head Office, Dhaka.

Members :

Md. Nasim Alam
First Vice President & Deputy CAMLCO
Mercantile Bank Limited
Anti Money Laundering Department
Head Office, Dhaka.

Muhammad Khairul Hasan
First Assistant Vice President
Mercantile Bank Limited
Anti Money Laundering Department
Head Office, Dhaka.

Mainul Hasan
First Assistant Vice President
Mercantile Bank Limited
Anti Money Laundering Department
Head Office, Dhaka.

PREFACE

Banking is the inevitable part of an economy and plays a major contribution towards socio-economic development of a country. The sector is considered as life blood of the economy as well. As one of the most important sectors of the financial system, it forms the core of the money market and plays very dynamic role in mobilizing resources for productive investments in a country, which in turn contributes to economic development. An efficient and stable banking system is the prerequisite for overall development of the country. To maintain stability and integrity of international financial system, Financial Action Task force (FATF), an inter-governmental body established by G-7 in 1989, has set 40 recommendations for preventing money laundering and terrorist financing.

In domestic level, Bangladesh Bank, as the major regulator of the financial system of the country plays a pivotal role to stabilize and enhance the efficiency of the financial system. Considering money laundering (ML) and terrorist financing (TF) as one of the major threats to the stability and the integrity of the financial system, BB has taken several initiatives including issuance of circulars/circular letters/Guidance Notes under Money Laundering prevention Act and Anti-terrorism Act. The regulator issued a comprehensive 'Guidance Notes on Prevention of Money Laundering' in 2003 based on Money Laundering Prevention Act, 2002 which enumerated the duties and responsibilities of commercial banks of the country to prevent money laundering.

To keep pace with international initiatives and promulgated Money Laundering Prevention Act-2012 (with amendment in 2015) and Anti-Terrorism Act-2009 (with amendment in 2012 & 2013), BFIU of Bangladesh Bank has send us "Money Laundering & Terrorist Financing Risk Assessment Guidelines" vide their BFIU Circular Letter No. 01/2015 dated 08.01.2015 with an instruction to implement the guidelines in all sectors of Bank. According to Bangladesh Bank's guidelines we have prepared this guideline.

This Guidelines has been formulated in accordance with the provisions of the Money Laundering Prevention Act-2012 (with amendment in 2015), Anti-Terrorism Act-2009 (with amendment in 2012 & 2013) and the Money Laundering & Terrorist Financing Risk Assessment Guidelines and Money Laundering & Terrorist Financing Risk Management Guideline issued by BFIU and is intended to ensure that all directors and employees of Mercantile Bank Limited understand and comply with the requirements and obligations imposed on them.

The purpose of this guidance is to outline the legal and regulatory framework for Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) requirements and systems across the financial services sector. With a view to this, the document interprets the requirements of the relevant laws and regulations, and how they may be implemented in practice. It indicates good industry practices in AML and CFT procedures through a proportionate, risk-based approach; and assists the banks to design and implement the systems and controls necessary to mitigate the risks of the banks being used in connection with money laundering and the financing of terrorism.

All Directors, Senior Management and Employees of Mercantile Bank Limited have to comply with the instruction of this guideline. It will be applied to all products or services offered by Mercantile Bank Limited. **This Guideline is applicable to all domestic/foreign Branches /offices/subsidiaries of the Bank and is to be read in conjunction with related operational guidelines issued from time to time.**

CONTENTS

Annexure

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**
ARS	**Alternative Remittance System**
ATA	**Anti Terrorism Act**
BAMLCO	**Branch Anti Money Laundering Compliance Officer**
BFIU	**Bangladesh Financial Intelligence Unit**
BB	**Bangladesh Bank**
CAP	**Customer Acceptance Policy**
CCU	**Central Compliance Unit**

CAMLCO	**Chief Anti Money Laundering Compliance Officer**
CDD	**Customer Due Diligence**
DNFBPs	**Designated non-financial businesses and professions**
EDD	**Enhanced Due Diligence**
FATF	**Financial Actions Task Force**
HR	**Human Resources**
ICCD	**Internal Control & Compliance Division**
IPs	**Influential Persons**
KYC	**Know Your Customer**
KYE	**Know Your Employee**
MBL	**Mercantile Bank Limited**
ML	**Money Laundering**
MLPA	**Money Laundering Prevention Act**
MLPR	**Money Laundering Prevention Rules**
MOU	**Memorandum of understanding**
NRA	**National ML & TF Risk Assessment**
PEPs	**Politically Exposed Persons**
PF	**Proliferation Financing**
RO-FI	**Reporting Organizations-Financial Institutions**
STR	**Suspicious Transaction Report**
SAR	**Suspicious Activity Report**
TF	**Terrorist Financing**
TFS	**Targeted Financial Sanctions**
UNSCR	**UN Security Council Resolution**

AN OVERVIEW OF MONEY LAUNDERING AND TERRORIST FINANCING

1.1 INTRODUCTION

Money Laundering is happened 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 proceeds of crime 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 a society. Both money laundering and terrorist financing can weaken individual financial institution, and they are also threats 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.

1.2 DEFINING 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 is disguised to conceal their illicit origins. Most countries adopted to the following definition which was delineated in 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.

Section 2 (v) of Money Laundering Prevention Act (MLPA), 2012 of Bangladesh defines money laundering as follows:

'Money laundering' means –

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

   (1) Concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or

   (2) Assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;

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

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

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

v. converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;

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

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

viii. Participating in, associating with, conspiring, attempting, abetting, instigating or counseling to commit any offences mentioned above.

Money laundering is a criminal offence under section 4(1) of MLPA, 2012 and penalties for money laundering are-

1. Any person who commits or abets or conspires to commit the offence of money laundering, shall be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lacks, whichever is greater.
2. In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved in or related with money laundering or any predicate offence.
3. Any entity which commits an offence under this section shall be punished with a fine of not less than twice of the value of the property or taka 20(twenty) lacks, whichever

is greater and in addition to this the registration of the said entity shall be liable to be cancelled.

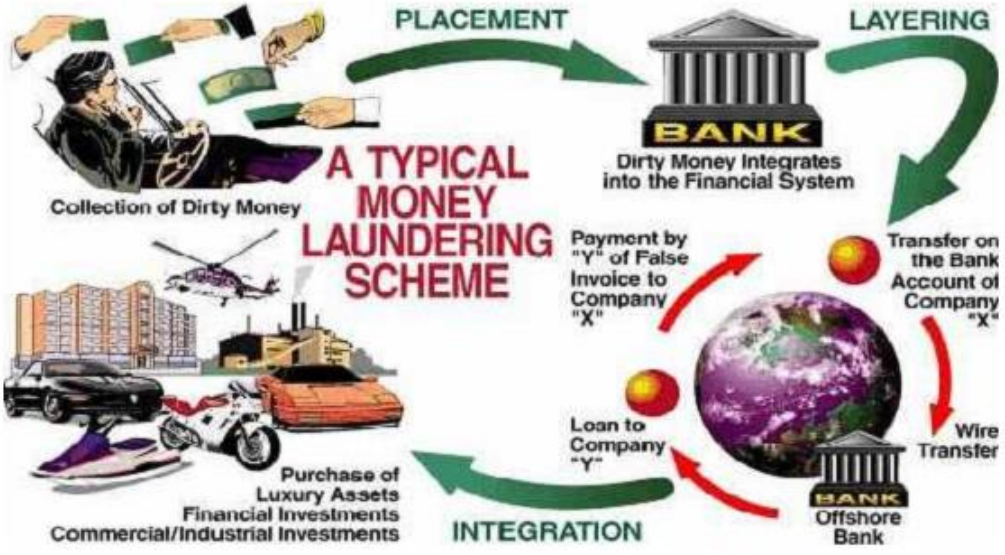
1.3 STAGES OF MONEY LAUNDERING

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

Placement – Placement is the first stage of the money laundering process, in which illegal funds or assets are brought first into the financial system directly or indirectly.

Layering - Layering is the second stage of the money laundering process, in which illegal funds or assets are moved, dispersed and disguised to conceal their origin. Funds can be hidden in the financial system through a web of complicated transactions.

Integration - Integration is the third stage of the money laundering process, in which the illegal funds or assets are successfully cleansed and appeared legitimate in the financial system.



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 WHY MONEY LAUNDERING IS DONE

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

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

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

1.5 DEFINING TERRORIST FINANCING

Terrorist financing can simply be 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 as follows:

1. If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

    a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below[1]; or
    b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

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

Bangladesh has ratified this convention and criminalized terrorism or terrorist activities under section 6(1) of Anti Terrorism Act, 2009 in line with the requirement set out in 9 (nine) conventions and protocols that were annexed I the convention.

Section 7(1) of Anti Terrorism Act (ATA), 2009, defines terrorist financing as follows:

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

a) To carry out terrorist activity;

b) By a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity;

The said person or entity shall be deemed to have committed the offence of terrorist financing.

Moreover, according to Anti Terrorism Act (ATA), 2009 conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act. The penalties for the offences for money laundering are-

(1) In case of a TF offence made by a person, he/she shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or taka 10(ten) lac, whichever is greater, may be imposed.

(2) In case of a TF offence made by an entity, the Government may listed the entity in the Schedule or proscribe and listed the entity in the Schedule, by notification in the official Gazette and in addition to that, a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is greater, may be imposed. Moreover, the head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20 (twenty) lac, whichever is greater, may be imposed unless he/she is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

1.6 THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

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

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

1.7 WHY MERCANTILE BANK MUST COMBAT ML & TF

Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a vital process to make crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupted public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences resulted from ML & TF.

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

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

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

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

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

A nation cannot afford to have its reputation and financial institutions tarnished by involvement with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions (FIs) and the underlying criminal activities like

fraud, counterfeiting, narcotics trafficking, and corruption weaken the reputation and standing of any financial institution. Actions taken by FIs to prevent money laundering are not only a regulatory requirement, but also an act of self-interest.

A financial institution tainted by money laundering accusations from regulators, law enforcement agencies, may 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 is found that an FI was used for ML & TF activities, and it did not take proper action against that ML & TF as per the laws of the country, the FI will have to face legal risk. Finally, the reputation of an FI can also be heavily affected through its involvement with ML & TF activities.

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

1.8 TARGETED FINANCIAL SANCTIONS

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

INTERNATIONAL INITIATIVES ON ML AND TF

2.1 INTRODUCTION

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

2.2 THE UNITED NATIONS

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

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

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

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

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

2.2.1 THE VIENNA CONVENTION

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

2.2.2THE 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.

2.2.3 INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM

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

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

2.2.4 SECURITY COUNCIL RESOLUTION 1267 AND SUCCESSORS

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

2.2.5 SECURITY COUNCIL RESOLUTION 1373

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

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

2.2.6 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.

2.2.7 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.

2.3 THE FINANCIAL ACTION TASK FORCE

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

2.3.1 FATF 40+9 RECOMMENDATIONS

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

2.3.2 FATF NEW STANDARDS

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

Summary of new FATF 40 standards is shown in Table A

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

2.3.3 INTERNATIONAL COOPERATION AND REVIEW GROUP (ICRG)

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

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

2.4 ASIA PACIFIC GROUP ON MONEY LAUNDERING (APG)

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

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

The APG has five key roles:

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

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

2.5 THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

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

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

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

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

2.6 THE BASEL COMMITTEE ON BANKING SUPERVISION

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

2.6.1 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.

2.6.2 BASEL CORE PRINCIPLES FOR BANKING

In 1997, the Basel Committee issued its Core Principles for Effective Banking Supervision (Core Principles), which provide a comprehensive blueprint for an effective bank supervisory system and covers a wide range of topics. These Core Principles were reviewed in September 2012 and adopted 29 Core Principles. The 29th principle deals with money laundering; it provides that- 'The supervisor determines that banks have adequate policies and processes, including strict customer due diligence rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities.'

2.6.3 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.

MAJOR NATIONAL AML & CFT INITIATIVES

3.1 INTRODUCTION

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

3.2 FOUNDING MEMBER OF APG

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

3.3 LEGAL FRAMEWORK

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

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

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

3.4 CENTRAL AND REGIONAL TASKFORCES

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

3.5 ANTI-MONEY LAUNDERING DEPARTMENT

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

3.6 BANGLADESH FINANCIAL INTELLIGENCE UNIT

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

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

3.7 NATIONAL COORDINATION COMMITTEE AND WORKING COMMITTEE

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

3.8 NATIONAL ML & TF RISK ASSESSMENT (NRA)

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

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

3.9 NATIONAL STRATEGY FOR PREVENTING ML AND TF

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

- updating National ML&TF Risk Assessment Report regularly and introducing Risk Based Approach of monitoring and supervision of all reporting organizations.
- deterring corruption induced money laundering considering corruption as a high risk.
- modernization of Border Control Mechanism and depriving perpetrators from use of proceeds of crime to prevent smuggling of gold and drugs, human trafficking, other transnational organized crimes considering the risk thereon.
- tackling illicit financial flows (IFF) by preventing the creation of proceeds of crime, curbing domestic and cross-border tax evasion and addressing trade based money laundering.
- discouraging illicit fund transfer by increasing pace of stolen assets recovery initiatives and or recovering the evaded tax.
- enhancing the capacity of BFIU in identifying and analyzing emerging ML & TF cases including ML&TF risks arising from the use of new technologies.
- enhancing compliance of all reporting agencies with special focus on new reporting agencies like NGOs/NPOs and DNFBPs.

- expanding investigative capacity and improving the quality of investigation and prosecution of ML & TF cases to deter the criminals.

- establishing identification and tracing out mechanism of TF&PF and fully implementation of targeted financial sanctions related to TF & PF effectively.
- boosting national and international coordination both at policy and operational levels.
- developing a transparent, accountable and inclusive financial system in Bangladesh.

3.10 CHIEF ANTI-MONEY LAUNDERING COMPLIANCE OFFICERs (CAMLCO) CONFERENCE

Separate annual conferences for the Chief Anti-Money Laundering Compliance Officers (CAMLCO) of Banks, Financial Institutions, Insurance Companies and Capital Market Intermediaries were arranged by BFIU. It also has arranged a number of training programs, workshops, seminars and road-shows to create awareness among the staff of reporting organizations, regulatory authorities about related issues.

3.11 EGMONT GROUP MEMBERSHIPS

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

3.12 ANTI MILITANTS AND DE-RADICALIZATION COMMITTEE

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

3.13 MEMORANDUM OF UNDERSTANDING (MOU) BETWEEN ACC AND BFIU

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

3.14 IMPLEMENTATION OF TFS

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

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

3.15 COORDINATED EFFORT ON THE IMPLEMENTATION OF THE UNSCR

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

3.16 RISK BASED APPROACH

Mercantile Bank has developed 'Money Laundering and Terrorist Financing Risk Assessment Guidelines' for identifying, assessing and mitigating ML & TF risks that the bank may encounter in doing its businesses. The guideline outlines the detail process to assess ML & TF risk under business risk considering customers, products, delivery channels and geographical positions. The guideline also include assessment of regulatory risk i.e. risk arises from non-compliance of AML & CFT measures.

This guideline will assist in identifying the bank's AML/CFT risk profile. Understanding the risk profile enables the bank to apply appropriate risk management process to the AML/CFT compliance program to mitigate risk. The risk assessment process enables management to better identify and mitigate gaps in bank's control.

The purpose of this guideline is to:

- provide general information about risks related with the products, services, delivery channels, and geographical locations;
- assist banks to assess their ML&TF risks efficiently;
- enable banks in implementing an AML&CFT program appropriate to their business having regard to the business size, nature and complexity; and
- provide a broad risk management framework based on high-level principles and procedures that a bank may wish to consider when developing and implementing a risk-based approach to identify, mitigate and manage ML&TF risks.

3.16.1 **Risk Management Framework**

The risk management framework consists of:

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

b) Risk identification;

c) Risk assessment or evaluation; and

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

3.16.1.1 **Risk identification**

There are two types of risk: business risk and regulatory risk.

Business Risks:

Bank 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).

Regulatory risks:

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 records properly
- Failure to scrutinize staffs/members properly before appointed
- Failure to train staff adequately
- Not having an AML&CFT program

- Failure to report suspicious transactions or activities
- Non submission of 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 or BB
- Non submission accurate information or statement requested by BFIU or BB.

3.16.1.2 **Risk assessment**

For assessing risk, we use ***Annex-A***, which is a simple & generic table with Risk Score and Treatment. 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)**.

Risk Score can be found by blending likelihood and impact as follows:

MBL use the risk matrix shown in ***Table-D*** (see next page) to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score is to be used to aid decision making and help in deciding what action to take in view of the overall risk. Three levels of risk (likelihood scale), three levels of impact and four levels of risk score are shown in Table B, C and D respectively.

Table B: 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

Table C: Impact scale

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

Table D: Risk score table

Rating	Impact – of an ML&TF risk
Extreme-4	Risk almost sure to happen and/or to have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level.
High-3	Risk likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.
Medium-2	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.
Low-1	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

3.16.1.3 **Risk Treatment**

Risk treatment is about identifying and testing methods to manage the risks the bank has identified and assessed in the previous process. In doing this, bank needs to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk. Based on the set strategies, policies and procedures and risk type & level & magnitude, risk treatment or action is identified for each risk (***Annex-A***).

3.16.1.4 **Risk Monitor and review**

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 entity should develop a method to check regularly on whether AML&CFT program is working correctly and well. If not, the entity 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.

3.16.1.5 **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.

<u>Applying risk appetite to risk assessment</u>

Risk appetite is the amount of risk a bank 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 bank accept?
- What risks will the bank not accept?
- What risks will the bank treat on a case by case basis?
- What risks will the bank send to a higher level for a decision?

The risk matrix Table-***E*** can be used to show the risk appetite of the bank.

In a risk-based approach to AML & CFT the assessment of risk appetite is a judgment that must be made by the bank. 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.

Table -E: Risk Matrix

LIKELIHOOD (What is the chance it will happen?)				
	Very Likely	**Acceptable Risk** Medium 2	**Unacceptable Risk** High 3	**Unacceptable Risk** Extreme 4
	Likely	**Acceptable Risk** Low 1	**Acceptable Risk** Medium 2	**Unacceptable Risk** High 3
	Unlikely	**Acceptable Risk** Low 1	**Acceptable Risk** Low 1	**Acceptable Risk** Medium 2
		Minor	**Moderate**	**Major**

IMPACT
(How serious is the risk?)

Risk tolerance

In addition to defining bank'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.

3.17 MEMORANDUM OF UNDERSTANDING (MOU) BFIU AND OTHER FIUs

To enhance the cooperation with foreign counterparts, BFIU signed Memorandum of Understanding (MoU) with other FIUs. BFIU has signed 36 (till date) MoU so far to exchange the information related to ML&TF with FIU of other countries.

AML & CFT COMPLIANCE PROGRAM OF MERCANTILE BANK LIMITED

4.1 INTRODUCTION

To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU, Mercantile Bank Limited has developed and maintained an effective AML and CFT compliance program covering senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

4.2 COMPONENT OF AML & CFT COMPLIANCE PROGRAM

The following components have been included into AML & CFT compliance program of MBL:

1. senior management role including their commitment to prevent ML, TF & PF;
2. internal policies, procedure and controls- it will include Bank's AML & CFT policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, cash transaction reporting, suspicious transaction reporting, self assessment, independent testing procedure, employee screening, record keeping and reporting to BFIU;
3. compliance structure includes establishment of central compliance Unit (CCU), Anti Money Laundering Department, appointment of chief anti-money laundering compliance officer (CAMLCO), branch anti-money laundering compliance officer (BAMLCO);
4. independent audit function- it includes the role and responsibilities of internal audit on AML & CFT compliance and external audit function;
5. awareness building program includes training, workshop, seminar for banks employees, member of the board of directors, owners and above all for the customers on AML & CFT issues.

4.3 DEVELOPMENT OF BANK'S AML & CFT COMPLIANCE PROGRAM

In order to develop the compliance program, MBL has considered all relevant laws, regulations, guidelines relating to AML & CFT and also the practices related to corporate governance. The compliance program has been finalized by members of Central Compliance Unit (CCU) of MBL.

4.4 COMMUNICATION OF COMPLIANCE PROGRAM

MBL communicates their compliance program after getting the approval from the board of directors or senior management to all of our employees, member of the board of the directors and other relevant stakeholders at home and abroad on following communicating modes:

1. Issuance of AML Circular,
2. Conducting AML & CFT related training program,
3. Issuance of letters,
4. Uploading the compliance program in the website etc.

4.5 SENIOR MANAGEMENT ROLE

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

Regarding senior management role of preventing ML, TF & PL, Anti Terrorism Act (ATA) – 2009 & BFIU Circular No. 10 dated 28.12.2014 state that

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

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

  The chief executive of the bank shall announce effective and specific commitment, give the necessary instructions to fulfill the commitments in preventing ML & TF to all the employees of all branches, agent offices, regional offices and the head office and shall ensure the implementation of the commitments. This statement of commitment shall be issued in every year.

In terms of preventing ML, TF & PF, Senior Management of Mercantile Bank Limited (MBL) includes-

1. the Members of the Board of Directors of the Bank
   and
2. the Managing Director & CEO of the Bank.

Senior Management of MBL has the accountability to ensure that the bank's policy, process and procedures towards AML & CFT are appropriately designed and implemented and are effectively operated to minimize the risk of the bank being used in connection with ML & TF. Senior Management of MBL will adopt HR Policy for ensuring the compliance of AML & CFT measures by the employees of the bank. The Board of Directors of MBL shall-

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

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

The statement of commitment of Managing Director & CEO of MBL will include the following issues:

- All employees of the Bank are required to comply with applicable laws and regulations and corporate ethical standards;
- Clear indication of balance between business and compliance, risk and mitigating measures;
- Complying with rules and regulations is the responsibility of each individual in the Bank in the normal course of their assignments. Ignorance of the rules and regulations is no excuse for non-compliance;
- Point of contact for clarification in case of ambiguity arises;
- Consequences of non-compliance as per Human Resources (HR) Policy of MBL;
- Bank's policy or strategy to prevent ML, TF & PF.

Senior Management of MBL will ensure the adequate human and other resources committed to AML & CFT. Moreover, they will ensure the autonomy of the designated officials related to AML & CFT. Senior management will take the report from the Central Compliance Unit (CCU) into consideration which will assess the operation and effectiveness of the Bank's systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner. Senior management of MBL will ensure that some potential directions have been included in Bank's HR Policy for ensuring the compliance of AML & CFT measures by the employees of the Bank.

Inclusion of potential guidelines regarding AML & CFT measures in MBL HR Policy:

In order to comply with AML & CFT measures of the anti money laundering guideline of Bangladesh Bank, some important attributes of non-compliance issues and necessary punitive actions for not complying with those issues are furnished below:

I. Non-compliance of AML & CFT measures:

There are some important measures with which employees should be complied fully to avoid the probable risks relating with AML & CFT issues as directed in ML & TF Risk Management Guidelines of BFIU.

The actions to be considered as non-compliance of AML & CFT measures are stated below:

- Opening account without KYC or incomplete KYC,
- Ignoring update of Transaction Profile which does not match the current volume of business transaction.
- Inputting erroneous & unjustified information in Account Opening Form
- Not providing correct information in time according to Regulatory bodies & HO instruction

- Not taking permission before opening of PEPs & Influence Person's account.
- Not sending correct CTR in time with forwarding
- Failure to keep essential record in a sequential and proper order for the purpose of presenting before Audit & inspection team
- Not checking the UN Security Council and domestic sanction list while opening account
- Not updating the customer's KYC before approving loan proposal
- Failure to monitor continuously that whether loan amount is diverted to unethical or unlawful business or not.

The above " non-compliance of AML & CFT measures" has been included into the Chapter-VIII, General Conduct and Discipline of HR Policy Manual(Revised-2014 as Clause#8.1.N

Actions against non-compliance:

If any employee of our bank is found reluctant to comply with the AML & CFT measures, he /she may be awarded punishment in the proportionate manner. The risk of not following proper procedure on AML or CFT issues cannot be overlooked. The person held responsible for adopting the actions which are against potential compliance issues is subject to following punishment:

i. Show-cause notice
ii. Suspension from the work
iii. Increment held up
iv. Halting promotion
v. Financial compensation
vi. Termination of job (in terms of extreme case and repeatedly ignoring compliance issues)
vii. Legal action (in the court of law) against the concerned employee (where applicable).

Action mentioned above shall be proportionate to the severity of non compliance/offence.

The "administrative actions against non-compliance of AML & CFT measures" has been included Chapter-IX, Disciplinary Action of HR Policy Manual (Revised)-2014 as Clause # 9.1.1.m.

II. Performance evaluation of employees:

Proper weight or score shall be given on the annual performance evaluation of employees for extra ordinary preventive action vis-a-vis non-compliance:

- In ACR (Annual Confidential Report) a significant percentage of total score must be retained regarding AML & CFT compliance issues.
- AML & CFT measures being vital compliance issues must be considered in the promotion and other calculation of awards given by the bank.
- The performance report of every single employee must include the score or marking arrangement on AML & CFT measures. The scoring may be projected in the following manner:

Description work/ actions	Score	Total
Receiving of Training on AML & CFT measures	1	5
Knowledge of AML guidelines & policy	2	
Knowledge of AML circulars of Mercantile Bank and reporting to the concerned authorities	1	
Co-operation with the action of BAMLCO	1	

III. Recovering the fined amount:

When any fine is imposed on bank by the BFIU, written procedure to recover the fined amount will be clearly mentioned in the HR policy for the presentation of better compliance related actions.

- If BFIU, Bangladesh Bank imposes any fine for the lapses of officials ignoring due diligence, the Human Resource Division may realize the whole portion of loss from those employees who will be responsible after proper investigation as per HR Policy Manual.

"Recovery fined amount" has been included into Chapter-IX, Disciplinary Action of HR Policy Manual (Revised)-2014 as Clause # 9.1.2.A.iv.

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

4.6 POLICIES AND PROCEDURES

Our AML & CFT policy included the following 4 (four) key elements; -

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

4.7 CUSTOMER ACCEPTANCE POLICY (CAP):

Customer is the key to success as a whole for the financial institutions but contrary to it is a recipe for failure. In the Country, Commercial Bank does not open account or deal with customer of unknown identify or have fictitious or imaginary names. Bank will accept only those clients whose identity is established by conducting due diligence appropriate to the risk profile of the client.

Mercantile Bank has developed a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. To thwart exposure of our bank to any sort of risk due to inadequate understanding our CAP has ensured explicit guidelines in setting up any kind of business relation with customer.

Mercantile Bank prepared a well defined customer acceptance policy to ensure prompt and inclusive services to all customers within the prescribed regulatory framework as well as defined processes of the Bank. In this regard the Management of Mercantile Bank has also recommended certain important themes under the guidance of Bangladesh Bank which have been incorporated to design the policy towards comprehensive coverage and implementation of customer acceptance in the Bank.

OBJECTIVES/PURPOSE AND APPLICATION OF THE POLICY:

The primary objective of the Customer Acceptance Policy are-

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

The CAP has been designed and developed considering the following factors and guiding principal:

I. To prevent illegal or criminal elements from using the Bank for money laundering activities

II. To enable the Bank to know/understand the customers and their financial dealings better which, in turn, would help the Bank to manage risks prudently

III. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws or laid down procedures.

IV. To comply with applicable laws and regulatory guidelines

V. To ensure that the concerned staffs are adequately trained in KYC, AML, CFT procedures.

The customer acceptance policy of MBL shall not be used against the disadvantaged people or the people who have not proper identification document. Our customer acceptance policy is expected to encourage the ultimate goal of transparent, accountable and inclusive financial system in Bangladesh.

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

Mercantile Bank has followed detailed and accurate customer identification procedure for opening of accounts and monitoring transactions of suspicions nature for the purpose of reporting it to be appropriate authority.. Detailed guidelines based on the Recommendations of the FATF and the paper issued on Customer Due Diligence (CDD) for Banks by Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued.

DEFINATION OF CUSTOMER:

A 'Customer' is defined as:

- A person or entity that maintains an account and/or has a business relationship with the bank;
- One on whose behalf the account is maintained (i.e. the beneficial owner) means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and
- Exercise ultimate effective control over a juridical person
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

For the purpose of KYC Procedure a "Customer" is defined in BFIU circular No. 10 dated 28/12/2014, 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 favor the account is operated;
- the true beneficial owner of the transaction of the accounts operated by the 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. ln this case if a transaction appears abnormal in relation to the usual transaction of the concerned person or institution that transaction will be treated as –"high value".

While preparing CAP policies the following important factors have been taken into consideration:

i) Customer's background
ii) Country of origin
iii) Public or high profile position
iv) Linked accounts
v) Volume of business activities
vi) Risks associated in the business of customers
vii) Other risk indicators
viii) Basic requirements for Account Opening
ix) All information available for judging the creditworthiness of borrowers.
x) All information on walk-in customers as required in AML circular

Customers are vitally important for banking business. Our motto is to extend best services to our customers. We are also aware that sometimes customers pose the risk of money laundering and financing of terrorism to the financial institutions particularly the banks. So the inadequacy or absence of KYC standards can result in serious customer and counterpart risks, especially reputation, operational, legal and compliance risks. Collecting sufficient information about our customers is the most effective defense against being used as the medium to launder the proceeds of crimes and to finance the terrorism through bank accounts. As per Sec. 25 of Money Laundering Prevention Act- 2012 MBL requires to keep satisfactory evidence of the identity of those it deals with and also requires making necessary arrangement to prevent any transaction

related to crimes as described in Anti Terrorism (Amendment) Act- 2012. It is also the responsibility of our Bank to identify suspicious transactions of their customers with due care and diligence.

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 social disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as public figures or politically exposed persons should be taken exclusively at senior management level.

The following Customer Acceptance Policy is indicating the criteria for acceptance of customers of our bank. Branch shall accept customer strictly in accordance with the said policy:

1) No account should be opened in anonymous or fictitious name. Branch will collect accurate & full name of clients and preserve documents in conformity with it. Branch will prepare proper KYC of the clients.

2) No numbered account shall be opened;

3) No banking relationship shall be established with a Shell Bank;

4) No account in the name of any person or entity listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance adopted under Chapter VII of the Carter of UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government shall be opened or operated. This list can be downloaded from the following web link-

   http://www.un.org/sc/committees/index.shtml or
   http://www.bb.org.bd/aboutus/dept/bfiu/sanction_list.php

5) Branch will accept only those customers whose appropriate identity is established by conducting due diligence to the risk profile of the client. Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grades;

6) Documents requirements and other information to be collected in respect of different categories of customers depending on perceived risk;

7) Not to open an account or close an account where the bank is unable to apply appropriate customer due diligence measures i.e. if the bank is unable to verify the identity and/or obtain documents required as per with the risk categorization due to non cooperation of the customer bank will not open or allow withdrawal of money. Decision by a bank 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;

8) 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;

9) 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;

10) 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;

11) Uniform A/C Opening Forms, KYC Profile Form and Transaction Profile Form developed in line with the guidelines of Bangladesh Bank should be properly filled in;

12) In case of opening a Politically Exposed Person (PEP) / Influential Person (IP) / Chief Executives or Top Level Officials of any International Organization account, the branch shall comply the instructions contained in BFIU Circular No. 10 dated 28.12.2014 issued by Bangladesh Bank. Such types of account will be classified as high risk and will be required very high level monitoring;

13) Source of funds, income or wealth and complete information on the actual or beneficial owners of the accounts holding 20% or more share of the account must be obtained at the time of opening of any account;

14) In case of establishing correspondent banking relationship, the branch /concerned division /department shall follow the guidelines as contained in BFIU Circular No. 10 dated 28.12.2014 issued by Bangladesh Bank meticulously;

15) In case of opening a account of Non Residents Bangladeshi the rules of Foreign Exchange Regulation Act, 1947 and the instructions under this rules promulgated by Bangladesh Bank have to be followed.

16) Customers' risk must be assessed as per parameters of risk perception as clearly defined in KYC Profile Form.

17) The branches, where locker service facilities exist, will follow the identification procedure for their customers.

It is important to bear in mind by all employees of the bank that the customer identification process does not end at the point of application. Once account relationship has been established, reasonable steps should be taken by the branch from time to time to ensure that descriptive information is kept.

MBL will ensure comprehensive implementation of the above policy as well as review of the same at regular interval through the Central Compliance Unit (CCU), Anti Money Laundering Department of Mercantile Bank Ltd. This will ensure strengthening the framework of Customer Acceptance.

All employees of MBL are instructed to be diligent in Banker- customer relationship and seek the consent of senior officials of MBL in dealing with high-risk customers. MBL always ensure high quality services at all levels, which we strive to achieve certain quantitative goals. Care must be constantly exercised not to compromise on quality. All Head of the Branches are required to follow the Customer Acceptance Policy carefully and raise the Bank to greater heights of efficiency, transparency and professionalism for complying the Money Laundering Prevention Act 2012 and Anti Terrorism (Amendment) Act, 2012.

COMPLIANCE STRUCTURE OF THE BANK

5.1 INTRODUCTION

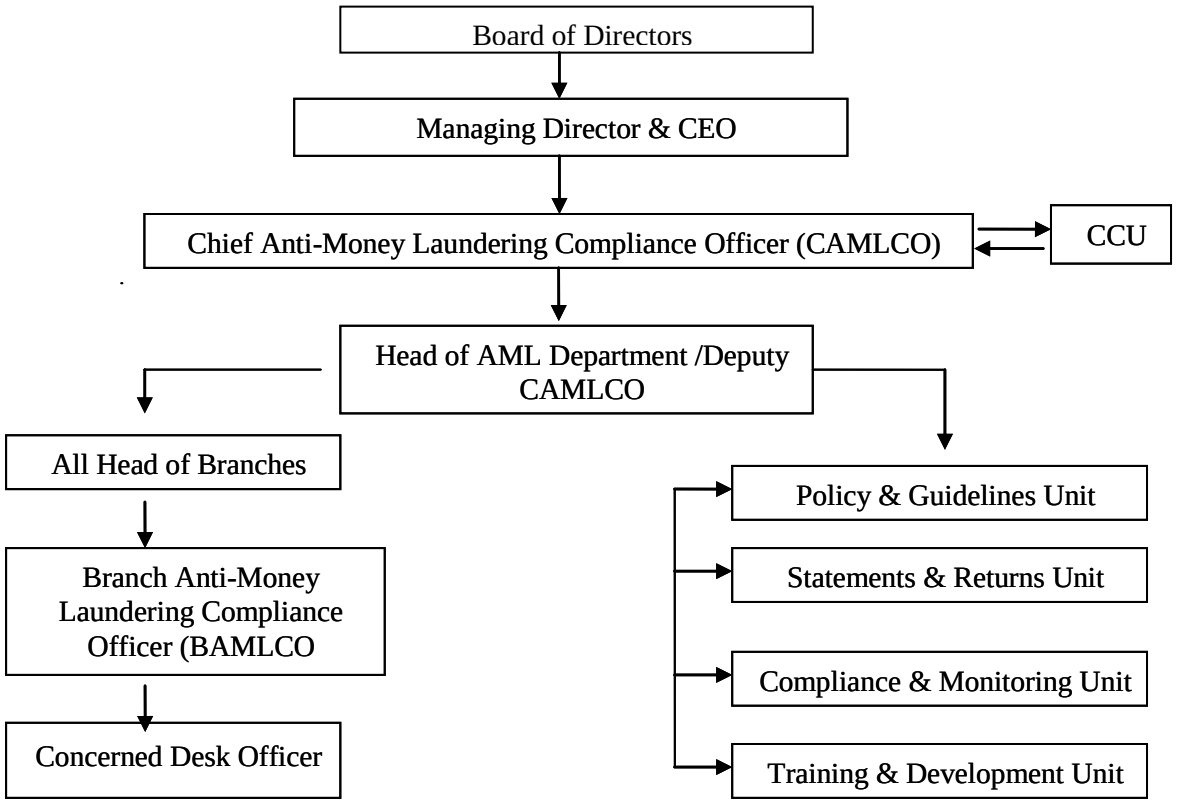
Compliance structure is an organizational setup that deals with AML & CFT compliance of the bank and the reporting procedure. The Compliance structure of Mercantile Bank includes-

- Central Compliance Unit (CCU),
- Anti Money Laundering Department (AMLD)
- Chief Anti-Money Laundering Compliance Officer (CAMLCO),
- Branch Anti-Money Laundering Compliance Officer (BAMLCO).

5.2 ORGANIZATION STRUCTURE

While complying with rules and regulations is the responsibility of each individual of Mercantile Bank in the normal course of their assignments, each individual of Head Office and Branches shall pay the role as noted there against in the effectiveness of the AML program.

5.2.1 **ORGANIZATIONAL CHART OF MERCANTILE BANK LIMITED FOR IMPLEMENTING AML/CFT POLICY:**



5.3 CENTRAL COMPLIANCE UNIT (CCU)

A Central Compliance Unit has been formed at MBL's Head Office headed by Additional Managing Director & CAMLCO. The following Heads of important Division are the member of CCU:

01	Additional Managing Director & CAMLCO	Chairman
02	Head / Deputy Head of Credit Risk Management Division	Member
03	Head of Human Resources Division	Member
04	Head of International Division	Member
05	Head of Mobile Banking Division	Member
06	Head of Information Technology Division	Member
07	Head of Risk Management Division	Member
08	Head of General Banking Division	Member
09	Head of Anti Money Laundering Department	Member Secretary

5.3.1 FUNCTIONS OF THE CENTRAL COMPLIANCE UNIT (CCU):

The CCU shall give instruction to Anti Money Laundering Department for taking necessary measures to prevent ML & TF. The member secretary of CCU will arrange meeting with other members of CCU at least once in every quarter of a year. In this meeting, members of CCU shall discuss the potential adaptation, effects and applications of instructions given in the Anti Money Laundering Act-2012, different circulars issued by BFIU, Bangladesh Bank , AML & CFT measure and other applicable laws, policy, procedures and regulations. The terms of reference of CCU are given below:

- The Unit will undertake organizational strategy and program regarding internal control policies and procedures to prevent money laundering and terrorist financing activities and will ensure implementation of the same in the Bank
- The Unit will evaluate overall monitoring process and observe changes of rules /regulations and directives of BFIU and international standards that require revision/up gradation and adaptation.
- The Unit will ensure maintenance of regular liaison with BFIU, Bangladesh Bank, External & Internal Auditors and other Law enforcing agencies through CAMLCO/ DCAMLCO
- The Unit will ensure that the Bank's AML policies and Risk Assessment Guideline under risk based approach are completed and updated.

- The Unit will monitor performance of the DCAMLCO in the head office level and BAMLCO in the branch level to ensure AML/CFT compliance.
- The Unit will monitor whether instruction circulars issued by AML Division to the branches regarding the procedure of transaction monitoring and internal control mechanism to prevent money laundering and terrorist financing are being followed.
- To monitor whether correspondent relationship are maintained as per instruction provided by AMLD.
- The Unit will oversee whether Money Laundering Prevention Act 2012, Anti Terrorism Act 2013 and other directives issued by BFIU under these two acts are being properly followed by the overseas branches and subsidiaries during rendering the activities and services.
- The Unit will supervise whether due diligence are being rendered in case of accounts of PEPs, IPs and chief or higher management of any International Organization by BAMLCO.
- To oversee KYC, responsibilities of ordering , intermediary and beneficiary bank and to update the list of agents in the website of our Bank in case of Mobile Banking Services.
- To monitor /evaluate Independent Testing Procedure to be conducted at least annually by our ICCD.
- To monitor /evaluate effectiveness of Self-Assessment procedure on half yearly basis
- Any other issue that may arise from time to time regarding AML/CFT.

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

5.4 FORMATION OF ANTI MONEY LAUNDERING DEPARTMENT (AMLD)

Mercantile Bank has formed AMLD in the head office of the bank as a unique department. DCAMLCO will be the Head of AMLD. The Bank shall always ensure sufficient manpower and other logistic support in AMLD taking any exception into consideration. The employees of the department shall remain updated on AML & CFT measures including MLPA, ATA rules and instructions issued by BFIU or Bangladesh Bank.

5.4.1 AUTHORITIES AND RESPONSIBILITIES OF THE AMLD

AMLD is the prime mover of MBL for ensuring the compliance of AML & CFT measures. The main responsibilities of this department are furnished below:

- develop banks policy, procedure and strategies in preventing ML, TF & PF;
- coordinate banks AML & CFT compliance initiatives;
- coordinate the ML & TF risk assessment of the bank and review thereon;

- present the compliance status with recommendations before the MD & CEO on half yearly basis;
- forward STR/SAR and CTR to BFIU in time and in proper manner;
- evaluate CTR to find out STR, SAR and if suspicious transaction is detected then report it to BFIU

- report summary of self assessment and independent testing procedure to BFIU in time and in proper manner;
- impart training, workshop, seminar related to AML & CFT for the employees of the bank;
- make visit to different branches to oversee the AML activities
- take required measures to submit information, report or documents in time.

AMLD\ shall have following authorities:

- ✓ Appointment of BAMLCO and assign their specific job responsibilities;
- ✓ Requisition of human resources and logistic supports for AMLD;
- ✓ For any action on AML & CFT non-compliance, HR Division shall consult with AMLD.

5.4.2 SEPARATION OF AMLD FROM INTERNAL CONTROL & COMPLIANCE (ICC)

AML department is separated from ICCD and formed as a unique department to ensuring the independent audit function in the bank. Either the division or department perform their job in different and independent way. In this regard ICC also examines the performance of AMLD and the bank's AML & CFT compliance program. Enough co-ordination and co-operation in performing their responsibility and information exchange shall have to be ensured.

5.5 CHIEF ANTI MONEY LAUNDERING COMPLIANCE OFFICER (CAMLCO)

High Official (DMD & above) shall be designated as a Chief Anti Money Laundering Compliance Officer (CAMLCO) at MBL's Head Office. At present Our CAMLCO is an Additional Managing Director. He will have sufficient authority as given by MD & CEO to implement and enforce corporate wide AML & CFT policies, procedures and measures and he will report directly to MD&CEO. The CAMLCO is responsible for oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering and terrorist financing. There will also be a Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO) in the Head office of MBL. He will remain conversant with the existing acts, rules and regulations, instructions issued by BFIU from time to tine and international standards on preventing ML & TF.

The CAMLCO, DCAMLCO and the staff of AMLD and branch level AML & CFT compliance officers all shall remain acquainted with all the staff members of the Bank. All relevant staffs must be aware of the chain through which suspicious transaction/activity reports must be passed to the CAMLCO.

5.5.1 AUTHORITIES AND RESPONSIBILITIES OF CAMLCO

Authorities-

CAMLCO shall exercise his own authority in performing his duties. MD & CEO will issue an office order conferring the authorities to CAMLCO;

- He should not take any permission or consultation from/with the MD & CEO before submission of STR/SAR and any document or information to BFIU;
- He shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- On AML & CFT issue none shall deny access to any information of the bank. If anyone denies any access to him, HR Division shall take appropriate action.
- He shall ensure his/her continuing competence.

Responsibilities-

- To monitor, review and coordinate application and enforcement of the Bank's compliance policy 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;
- To monitor changes of laws/regulations and directives of Bangladesh Bank and revise its internal policies accordingly;
- 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;
- To ensure that bank's AML/CFT policy is complete and up-to-date , to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered by the bank;
- 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;
- To assist in review of control procedures in the bank to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
- To monitor the business through self-testing for AML/CFT compliance and take any required corrective action;
- To oversee the submission of STR/SAR or any document or information to BFIU in time;
- To maintain the day-to-day operation of the bank's AML&CFT compliance;
- CAMLCO shall be liable to MD & CEO or BoD for proper functioning of AMLD and CCU;
- To review and update ML & TF risk assessment of the bank;
- To ensure that corrective actions have taken by the bank to address the deficiency identified by the BFIU or Bangladesh Bank.

5.6 BRANCH ANTI MONEY LAUNDERING COMPLIANCE OFFICER (BAMLCO)

Obligations under BFIU Circular-10, dated 28 Dec, 2014	For the implementation of all existing acts, rules, BFIU's instructions and bank's own policies on preventing Money Laundering & Terrorist Financing, bank shall nominate an experienced Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch.

As per instruction of AMLD, Head Office, Head of Branch will nominated one BAMLCO in every Branch. In most cases they will be Manager Operation or otherwise they will be high official experienced in general banking. BAMLCOs shall remain updated on the existing acts, rules and regulations, BFIU's instructions and bank's own policies on preventing Money Laundering and Terrorist Financing. The job descriptions and responsibilities of BAMLCO have been mentioned clearly in his/her appointment letter.

BAMLCO shall arrange AML & CFT meeting with other concerned important officials of the branch quarterly and shall take effective measures on the following matters after reviewing the compliance of the existing acts, rules and regulations, BFIU's instructions on preventing Money Laundering & Terrorist Financing:

- Know Your Customer,
- Transaction monitoring,
- Identifying and reporting of Suspicious Transactions,
- Record keeping,
- Training.

5.6.1 AUTHORITIES AND RESPONSIBILITIES OF BAMLCO

For preventing ML, TF & PF in the branch, the BAMLCO must perform the following responsibilities:

- ensure that the KYC of all customers have done properly and for the new customer KYC is being done properly;
- ensure that the UN Security Council and domestic sanction list checked properly before opening of account and while making any international transaction;
- keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;
- ensure regular transaction monitoring to find out any unusual transaction (In case of an automated bank, the bank should follow a triggering system against transaction profile or other suitable threshold. In case of a traditional bank, transaction should be examined at the end of day against transaction profile or other suitable threshold. Records of all transaction monitoring should be kept in the file);
- review cash transaction to find out any structuring;
- review of CTR to find out STR/SAR;
- ensure the checking of UN sanction list before making any foreign transaction;
- ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;

- compile self-assessment of the branch regularly and arrange quarterly meeting regularly;
- accumulate the training records of branch officials and take initiatives including reporting to CCU, HR and training academy;
- ensure all the required information and document are submitted properly to CCU and any freeze order or stop payment order are implemented properly;
- follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
- ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements of chapter 7;
- ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.

5.7 INTERNAL CONTROL AND COMPLIANCE

Obligations under BFIU Circular-10, dated 28 Dec, 2014	With a goal of establishing an effective AML and CFT regime, it shall have to be ensured that the Internal Audit Department of the bank is equipped with enough manpower who have enough knowledge on the existing acts, rules and regulations, BFIU's instructions on preventing money laundering & terrorist financing and bank's own policies in this matter to review the Self Assessment Report received from the branches and to execute the Independent Testing Procedure appropriately.

The Internal Control and Compliance Division (ICCD) of MBL have an important role for ensuring proper implementation of bank's AML & CFT Compliance Program. Our ICCD shall remain equipped with enough manpower and autonomy to look after the prevention of ML & TF. The ICCD has to oversee the implementation of the AML & CFT compliance program of the bank and has to review the 'Self Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

The inspection team of ICCD performs the following issues for preventing ML & TF while inspecting the Branch :

- understand ML & TF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML/CFT Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML&CFT Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;

- where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU or BB;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
    - the importance of the board and the senior management place on ongoing education, training and compliance,
    - employee accountability for ensuring AML&CFT compliance,
    - comprehensiveness of training, in view of specific risks of individual business lines,
    - training of personnel from all applicable areas of the bank,
    - frequency of training,
    - coverage of bank policies, procedures, processes and new rules and regulations,
    - coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
    - penalties for noncompliance and regulatory requirements.

5.8 EXTERNAL AUDITOR

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

CUSTOMER DUE DILIGENCE

6.1 INTRODUCTION

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources.

The CDD obligations on bank under legislation and regulation are designed to make it more difficult to abuse the banking industry for money laundering or terrorist financing. The CDD obligations compel bank to understand who their customers are to guard against the risk of committing offences under MLPA, 2012 including 'Predicate Offences' and the relevant offences under ATA, 2009.

Mercantile Bank is always committed to ensure adequate CDD measures considering the risks of money laundering and terrorist financing. Such risk sensitive CDD measures would be based on-

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

The adoption of effective KYC standards is an essential part of banks' risk management policies. To mitigate significant risks especially legal and reputational risk Branch will remain careful in ensuring adequate KYC program. Sound KYC Policies and Procedures not only contribute to the bank's overall safety and soundness, they also protect the integrity of the banking system by reducing money laundering, terrorist financing and other unlawful activities.

Branch therefore need to carry out customer due diligence for two broad reasons:

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

- to enable the organization in investigation, law enforcement by providing available information about customers in due process.

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

6.2 LEGAL OBLIGATIONS OF CDD

Obligations under MLPA, 2012	The reporting organizations shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to Bangladesh Bank.
Obligations under MLP Rules, 2013	The bank shall identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data). The verification of identity of a customer or a beneficial owner should include a series of independent checks and inquiries and not rely only on documents provided by the customer or beneficial owner. The bank shall verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person. The bank shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the bank is satisfied that it knows who the beneficial owner is. The bank shall understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship. The bank shall also conduct ongoing due diligence on the business relationship. The bank shall scrutinize the transactions undertaken by a customer throughout the relationship with the customer to ensure that the transactions are consistent with the nature, business and risk profile of the customer, including where necessary, with the source of funds.
Obligations under BFIU Circular No-10, dated 28 December, 2014	A detail provisions of CDD measures discussed in paragraph no. 3 and 5.

6.3 GENERAL RULE OF CDD

Completeness and Accuracy

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

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

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

Where Branches are unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, unable to identify the beneficial owner taking reasonable measures, unable to obtain information on the purpose and intended nature of the business relationship, branch 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

Today Identification Reference: e-TIN/National ID/Passport/Driving License is the main key record for KYC compliance. Identification information electronically and validation of the customer's identity , can then be conducted automatically from Core Banking System by using any type web service. It will help us to identity the proper person identity and reduce the work load.

Now in Bangladesh Govt. Organization & Financial Institution can verify the NID data through "Election Commission Bangladesh" Data Warehouse. Two ways they are providing this service:

1) Web Portal Service
2) Web Service (which can be use as a API)

CDD measures (Review and update)

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

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

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

Enhanced CDD measures

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

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

Enhanced CDD measures includes :

- Obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet, etc) and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship when applicable.

- Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- Making aware the concerned bank officials about the risk level of the customer.

6.4 TIMING OF CDD

Branch must apply CDD measures when it does any of the following:

a) establishing a business relationship;
b) carrying out an occasional transaction;
c) suspecting money laundering or terrorist financing; or
d) Suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification.

6.5 TRANSACTION MONITORING

Branch is monitoring the customer's transaction on a regular basis. The complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized during monitoring.

MBL has already developed a software based transaction monitoring system (MBL goAML Interface & Velocity AML Solution) where the branches /divisions of Head Office can monitor the transaction in various ways that includes but not limited to the followings:

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

6.6 EXCEPTION WHEN OPENING A BANK ACCOUNT

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

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

6.7 IN CASE WHERE CONDUCTING THE CDD MEASURE IS NOT POSSIBLE

If conducting the CDD measure becomes impossible because of the non cooperating behavior of the customer or if the collected information seemed to be unreliable, that is, Branch could not collect satisfactory information on customer identification and could

not verify that, Branch should take the following measures:

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

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

6.8 CUSOMER IDENTIFICATION:

Customer identification is an essential part of CDD measures. For the purposes of this Guidance Notes, a customer includes:

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

Whenever the opening of an account or business relationship is being considered, or a one-off transaction or series of linked transactions of BDT 5,000 or more is to be undertaken, identification procedures must be followed. Identity must also be verified in all cases where money laundering is known, or suspected.

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.

WHAT CONSTITUTES A CUSTOMER'S IDENTITY?

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

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

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

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

Once account relationship has been established, reasonable steps should be taken by the institution to ensure that descriptive information is kept up-to-date as opportunities arise. lt 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. While opening account or establishing other relationship with the customer, Branch must obtain information, documents, verifying the address & source of fund as per Annexure-B.

Record Keeping:

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

Introducer:

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

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, shall be verified.

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 shall be kept. On the other hand, valid reasons to execute mandate under the law for operating the accounts shall exist.

Timing and Duration of Verification:

The best time to undertake verification is prior to entry into the account relationship. Verification of identity must be completed before any transaction is completed in account. 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 shall not be delegated, and shall only be done in exceptional circumstances. Any such decision shall 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.

CARDS/INTERNET BANKING/MOBILE BANKING:

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

Branches shall ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that if at any point of time Bank appoints/engages agents for marketing of these cards / products are also subjected to KYC measures

KNOW YOUR CUSTOMER'S CUSTOMER:

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

Branch shall-

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

MBL reserves the right to close any account, which in its opinion has contravened the laws of the country, and indicated a reasonable degree of suspicious to be involved in illegitimate business.

6.9 VERIFICATION OF SOURCE OF FUNDS

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

6.10 VERIFICATION OF ADDRESS

Branch shall verify the address of the person at the time of establishing any business relationship or while conducting CDD. This could be done through the physical verification by the bank or by standard mail or courier service correspondence. Branch could collect any other document (recent utility bill mentioning the name and address of the customer) as per their satisfaction.

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

6.11 PERSONS WITHOUT STANDARD IDENTIFICATION DOCUMENTATION

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 anti-money laundering procedures is recommended. Internal procedures must allow for this, and must provide appropriate advice to the concerned officer 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.

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

6.12 WALK-IN/ ONE OFF/ONLINE CUSTOMERS

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

Branch shall collect complete and correct information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit MBL shall identify sources of funds as well. Branch shall obtain all information of Walk-In/One Off/ Online customer as per Annexure-D

6.13 NON FACE TO FACE CUSTOMERS

Non face to face customer means "the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the bank branch. Where there is no face-to-face contact, Branch shall not allow in establishing relationship with non-face to face customer.

6.14 CUSTOMER UNIQUE IDENTIFICATION CODE

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

6.15 CORRESPONDING BANKING

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

Mercantile Bank would establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank through collection of information as per BFIU circular-10 dated 28 December, 2014. MBL must also obtain approval from its Senior Management before establishing and continuing any correspondent relationship. MBL must be sure about the effective supervision of that foreign bank by the relevant regulatory authority. MBL shall not establish or maintain any correspondent relationship with any shell bank and not to establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank.

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

AS a corresponding bank, MBL must be sure about the appropriate CDD of the customer, if any respondent bank allow direct transactions by their customers to transact business on their behalf (i.e. payable through account). Moreover, MBL will collect the information on CDD of the respective customer from the respondent bank. Here, '**Payable through accounts' refers to "Corresponding accounts that are used directly by third parties to transact business on their behalf."**

6.16 POLITICALLY EXPOSED PERSONS (PEPs), INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

All Clients must be subject to an assessment to determine whether they are PEP's or Influential Persons or chief executives or top level officials of any international organization and their linked entities. These customers pose a higher risk of money laundering, bribery, corruption and reputational risk to the bank due to their current or former position of political power or influence, which makes them more vulnerable to corruption.

6.16.1 DEFINITION OF PEPs

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

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

6.16.2 CDD MEASURES FOR PEP'S

Before opening a PEP's Account Branch should perform the following CDD measures :

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

6.16.3 DEFINITION OF INFLUENTIAL PERSONS(IPs)

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

a) heads and deputy heads of state or government;
b) senior members of ruling party;
c) ministers, state ministers and deputy ministers;
d) members of parliament and/or national legislatures;
e) members of the governing bodies of major political parties;
f) Secretary, Additional secretary, joint secretary in the ministries;

g) Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
h) governors, deputy governors, executive directors and general managers of central bank;
i) heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
j) heads of state-owned enterprises;
k) members of the governing bodies of local political parties;
l) ambassadors, chargés d'affaires or other senior diplomats;
m) city mayors or heads of municipalities who exercise genuine political or economic power;
n) board members of state-owned enterprises of national political or economic importance.

6.16.4 CDD MEASURES FOR INFLUENTIAL PERSONS (IP)

Before opening a IP's Account Branch should perform the following CDD measures :

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

6.16.5 DEFINITION OF CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

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

6.16.6 CDD MEASURES FOR CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

Before opening a Account of CEO or top level officials of any international organization, Branch should perform the following CDD measures:

a) Branch have to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a CEO or top level officials of any international organization;
b) obtain senior managements' approval before establishing such business relationship;

c) take reasonable measures to establish the source of fund of the account of a CEO or top level officials of any international organization;
d) monitor their transactions in a regular basis; and
e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly .

6.16.7 CLOSE FAMILY MEMBERS AND CLOSE ASSOCIATES OF PEPS, INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

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

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

There may be exceptional circumstances where the individual should not be classified as a 'Close Family Member' of the PEP, such as estrangement, divorce etc. In such cases, the circumstances must be thoroughly investigated, examined and caution exercised.

In addition, where other family members such as the siblings, cousins, relatives by marriage of the PEP are deemed, by virtue of the nature of the relationship, to have a close relationship with the PEP, they should also be classified as PEPs.

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

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

In addition, it should include any person publicly or widely known to be a close business colleague of the PEP, including personal advisors, consultants, lawyers, accountants, colleagues or the PEP's fellow shareholders and any person(s) that could potentially benefit significantly from close business associations with the PEP.

6.16.8 CDD MEASURES FOR CLOSE FAMILY MEMBERS AND CLOSE ASSOCIATES OF PEPS, INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

Bank will identify if any of its customer is a family member or close associates of a PEP, IP or CEO or top level officials of any international organization. Once identified banks need to apply enhanced CDD measures that is set out in 6.3 of this guidelines. Moreover,

they need to perform the following-

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

6.17 WIRE TRANSFER

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

6.17.1 CROSS-BORDER WIRE TRANSFERS

In case of threshold cross-border wire transfers of 1000 (one thousand) or above USD or equivalent foreign currency, branch will collect full and accurate information of the originator and the same information will have to send to intermediary/beneficiary bank. Furthermore, for cross-border wire transfers, below the threshold branch will preserve the full and meaningful originator information. For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved by the branch.

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

6.17.2 DOMESTIC WIRE TRANSFERS

In case of threshold domestic wire transfers of at least 25000/- (twenty five thousands) BDT, branch will collect, preserve the full and accurate information of the originator and the information will have to send to intermediary / beneficiary bank / institutions. Furthermore, for domestic wire transfers below the threshold branch will preserve the full and meaningful originator information. For providing money of domestic wire transfers to beneficiary, branch will preserve the full and meaningful beneficiary information. Mobile financial services providing MBL should use KYC format provided time to time by Payment System Department, Bangladesh Bank, in addition to aforesaid instructions. In case of wire transfer by using debit or credit card (except buying goods and services), similar information as above has to be preserved in the payment related message/instructions.

6.17.3 DUTIES OF ORDERING, INTERMEDIARY AND BENEFICIARY BANK IN CASE OF WIRE TRANSFER

Ordering Bank:

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

Intermediary Bank:

For cross-border and domestic wire transfers, MBL working as an intermediary between ordering bank and beneficiary bank shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained. MBL shall keep the record for at least five years.

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

Beneficiary Bank:

As a beneficiary bank, MBL shall set off risk based procedure to identify wire transfers that lack required originator or required beneficiary information. In case of insufficient originator information MBL shall collect those information through mutual communication or using any other means. During the payment to receiver/beneficiary, MBL shall collect full and accurate information of receiver/beneficiary and shall preserve those information for 5 (five) years.

6.18 CDD FOR BENEFICIAL OWNERS

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

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

any other natural person who exercises control over the trust.

- Any person in equivalent or similar position for trust (as mentioned above)should consider for other types of legal arrangements.

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

6.19 RELIANCE ON THIRD PARTY

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

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

6.20 MANAGEMENT OF LEGACY ACCOUNTS

Legacy accounts refers those accounts opened before 30 April, 2002 and yet to update KYC procedures. Branch has marked these legacy accounts as "Dormant". No withdrawal shall be permitted in those accounts; however, deposit can be permitted. These accounts will be fully functional only after conducting proper CDD measures. Branch shall send the list of Dormant account to Anti Money Laundering Department, Head Office for further preservation.

RECORD KEEPING

7.1 INTRODUCTION

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

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

7.2 LEGAL OBLIGATIONS

Obligations under MLPA, 2012	The reporting organizations shall have to preserve previous records of transactions of any close account for at least 5(five) years from the date of such closure and provide with the information maintained under the clause to Bangladesh Bank.
Obligations under MLP Rules, 2013	The bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners: 1. Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity; 2. The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction; 3. The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order.

7.3 OBLIGATIONS UNDER CIRCULAR

Obligations under BFIU Circular-10; dated 28/12/2014	1. All necessary information/documents of customer's domestic and foreign transactions has to be preserved for at least 5(five) years after closing the account. 2. All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved for at least 5(five) years after closing the account. 3. All necessary information/documents of a walk-in Customer's transactions has to be preserved for at least 5 (five) years from the date of transaction. 4. Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence. 5. Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU.

7.4 RECORDS TO BE KEPT

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

The records must cover:

- customer information
- transactions
- internal and external suspicion reports
- report from CCU/AMLD/CAMLCO
- training and compliance monitoring
- information about the effectiveness of training

7.5 CUSTOMER INFORMATION

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

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

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

7.6 TRANSACTIONS

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the branch's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. Credit/debit slips, cheques should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed. MBL must retain the records of all transactions of any close account for at least 5(five) years from the date of such closure and provide with the information to Bangladesh Bank on its demand in accordance the instruction of MLPA -2012 Section 25(1) (b).

7.7 INTERNAL AND EXTERNAL REPORT

MBL will make and retain:

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

In addition, copies of any STRs made to the BFIU must be retained for five years. Records of all internal and external reports will be retained for five years from the date the report was made.

7.8 OTHER MEASURES

The records of MBL will include:

(a) in relation to training:
- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

(b) in relation to compliance monitoring
- reports by the MLRO to senior management; and
- records of consideration of those reports and of any action taken as a consequence.

7.9 FORMATS AND RETRIEVAL OF RECORDS

To satisfy the requirements of the law and to meet the purpose of record keeping, MBL is capable of retrieval without undue delay. MBL has 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. All concerned shall ensure flowing appropriate procedure in this regard.

7.10 REQUIRED FILES FOR AML/CFT COMPLIANCE IN BRANCH LEVEL

Branches are maintaining the following files for record keeping:

1. BAMLCO Office Order Preserving File
2. AML Training related Office Order File
3. AML & CFT Compliance Meeting File (Quarterly)
4. Sanction Screening File:
    a. UN & OFAC Sanction List
    b. Existing A/C' False/True Positive Statement
    c. Remittance Screening
    d. L/C Beneficiary/ Applicant, Bank Name & Vessel
    e. SWIFT Screening
5. Risk Grading File:
    a. List of High Risk A/c and related documents

    b. List of IP & PEPs A/c and related documents
6. Transaction Profile (TP) Monitoring File
7. Self Assessment Evaluation Report (Half Yearly) File
8. KYC update File
9. Thanks Letter or Address Verification Letter File
10. Transaction Monitoring File
11. CTR Monitoring File
12. STR / SAR File
    a. Find out STR / SAR at Branch Level
    b. STR sends to CCU at Head Office
13. Structuring Report File
14. Bangladesh Bank AML Inspection File
15. AML/BFIU Circulars / Circular Letters File
16. Internal AML Circular / Instruction / Memo File
17. Walking / Online Customer KYC File
18. Close Account List
19. Internal / External AML Audit Report and compliance File
20. BAMLCO Activities File (As per Instruction Circular – 893)
21. Miscellaneous File etc.

22.

REPORTING TO BFIU

8.1 LEGAL OBLIGATIONS:

Obligations under MLPA, 2012	The reporting organizations shall have to report any suspicious transaction (defined in Section 2(Z) of MLPA, 2012 and Section 2(16) of ATA, 2009) to the Bangladesh Bank immediately on its own accord.
Obligations under MLP Rules, 2013	Every bank is obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self assessment, independent testing procedure etc.) to Bangladesh Bank without any delay or in due time. Besides they have to produce any documents that is sought by Bangladesh Bank.

8.2 SUSPICIOUS TRANSACTION REPORTING

Money Laundering Prevention Act, 2012 defines suspicious transaction as follows-

'suspicious transaction' means such transactions –

- which deviates from usual transactions;
- of which there is ground to suspect that,
    - the property is the proceeds of an offence,
    - it is financing to any terrorist activity, a terrorist group or an individual terrorist;
- which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh bank from time to time.

Anti-Terrorism Act, 2009 defines suspicious transaction as follows-

'suspicious transaction' means such transactions –

- which is different from usual transactions;
- which invokes presumption that,
    - it is the proceeds of an offence under this Act,
    - it relates to financing of terrorist activities or a terrorist person or entity;
- which is any other transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.

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

8.3 IDENTIFICATION OF STR/SAR

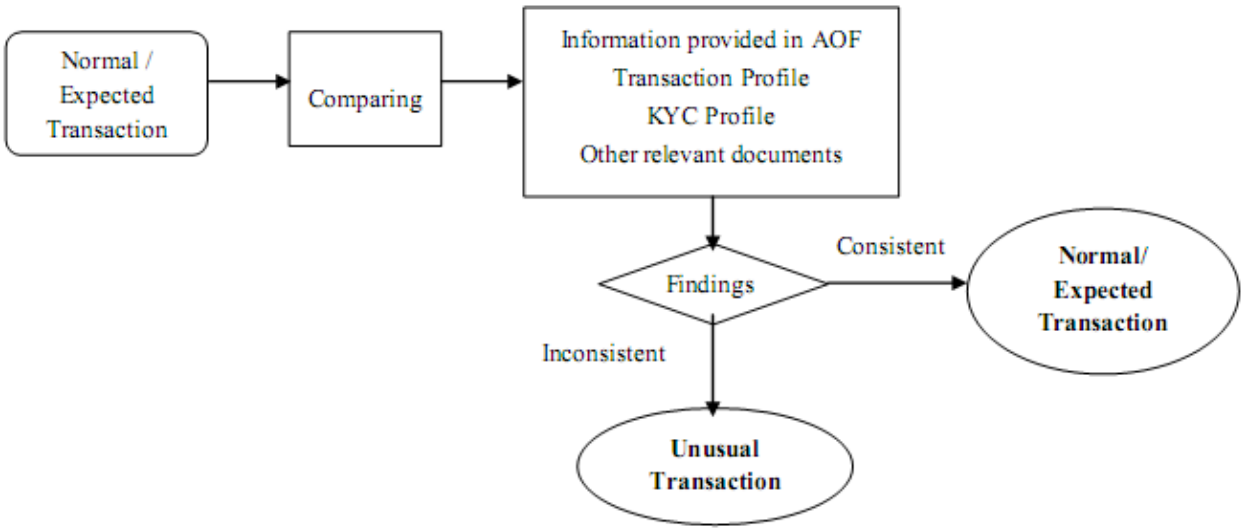
Branch normally identify the STR/SAR by scrutinizing unusual transaction and activity. Such unusual transaction may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Generally the detection of something unusual may be sourced as follows:

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

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

Branch will report STR/SAR to the Anti Money Laundering Department (AMLD), Head Office with proper documents. The report will include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the suspicion. All internal enquiries made in relation to the report will also be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

Follow chart for identifying the STR/SAR by Mercantile Bank-



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

Identification:

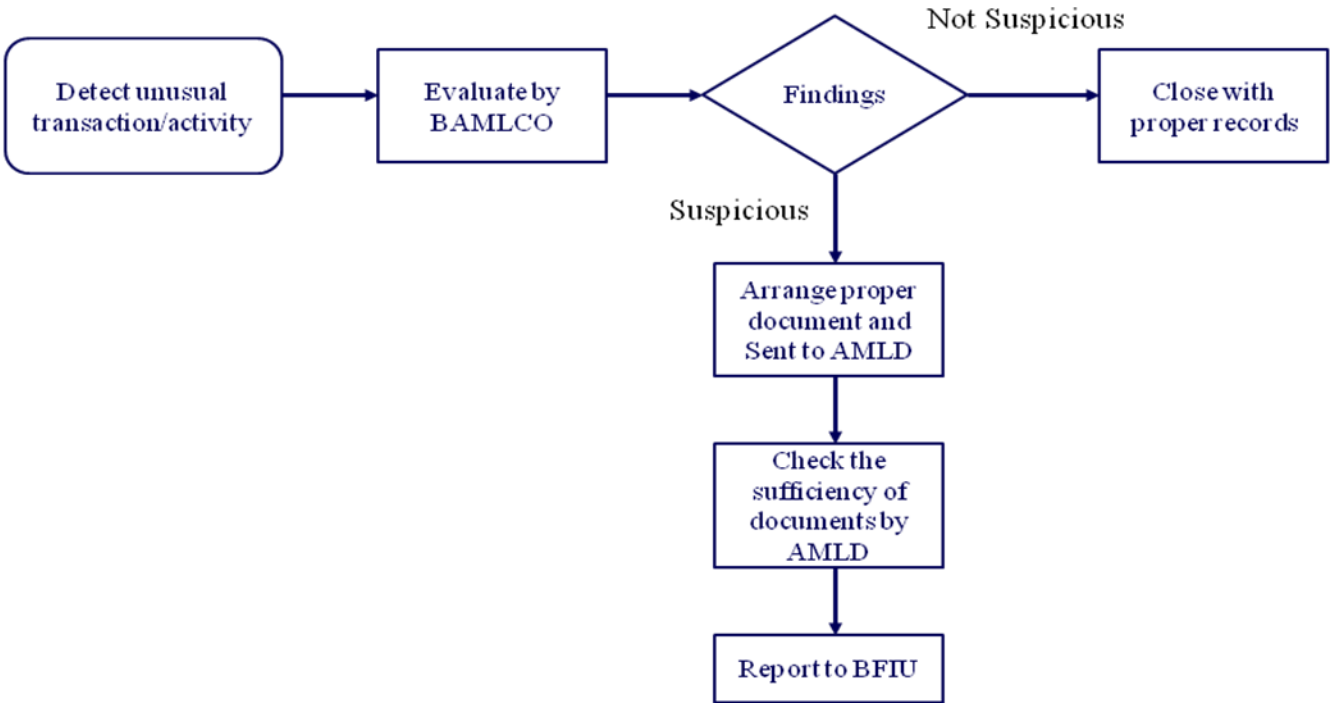
This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of bank monitoring of unusual transactions may be automated, manually or both. Mercantile Bank has been using software to detect unusual transactions or activities. Training of staff in the identification of unusual /suspicious activity is an ongoing activity of our Bank.

Evaluation:

After identification of STR/SAR at branch level, BAMLCO will evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. If BAMLCO is not satisfied, he should forward the report to AMLD. After receiving report from a branch, AMLD should check the sufficiency of the required documents. Every stages of evaluation (whether reported to BFIU or not), Branch should keep records with proper manner.

Disclosure:

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



8.4 TIPPING OFF

The officials of MBL will consider the confidentiality of the reporting of STR/SAR. They will not make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious.

8.5 CASH TRANSACTION REPORT

Every branch of MBL prepares the monthly cash transaction report and send it to AMLD in due time. If the branch has not any such transaction, it will report to AMLD as 'There is no reportable CTR'. After preparing

CTR, our branches will examine the CTR data, whether any suspicious transaction is occurred or not in the CTR. If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' to the AMLD. If no such transaction is identified, it needs to inform to the AMLD as 'No suspicious transaction has been found' while reporting the CTR and every branch needs to preserve its CTR in their own branch.

After receiving CTR data from Branches, Anti Money Laundering Department (AMLD) will prepare the accumulated CTR and send it to BFIU, Bangladesh Bank through goAML within stipulated time. AMLD has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR. Moreover, AMLD must preserve the information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

8.6 SELF ASSESSMENT REPORT

Branches of MBL prepare Self Assessment to evaluate them through a checklist that is circulated by BFIU circular no. 10, dated 28 December, 2014. Before finalizing the evaluation report, Branch will arrange a meeting about prevention of ML & TF; if the identified problems according that report are possible to solve at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations shall have to be jotted down. In the subsequent quarterly meetings on preventing money laundering and terrorist financing, the progress of the related matters shall be discussed.

After the end of every half year, the branch will submit their evaluation report along with the measures taken by the branch in this regard and adopted recommendations regarding the issue to the Internal Control and Compliance Division (ICCD) of the Head Office and the Anti Money Laundering Department within the 15th of the next month. CCU will arrange meeting to review the Self Assessment of each branch.

8.7 INDEPENDENT TESTING PROCEDURE

Independent testing has to be done through a checklist that is circulated by BFIU circular no. 10; dated 28th December, 2014 by the independent audit (i.e. performed by people not involved with the bank's AML&CFT compliance).

The individuals conducting the audit should report directly to the board of directors/senior management. Audit function shall be done by the internal audit or ICC. At the same time external auditors could be appointed (if possible) to review the adequacy of the program.

8.8 INTERNAL CONTROL & COMPLIANCE DIVISION'S (ICCD's) OBLIGATIONS REGARDING SELF ASSESSMENT OR INDEPENDENT TESTING PROCEDURE

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

While executing inspection/audit activities in various branches according to their own regular yearly inspection/audit schedule, the Internal Audit Department will examine the AML & CFT activities of the

concerned branch using the specified checklists for the Independent Testing Procedure. The ICCD will send a copy of the audit report with the rating of the branches to the AMLD, Head Office. Then AMLD send the Checklist to related Branch for compliance. After comply the lapses, Branch accordingly send their reply to AMLD.

8.9 CENTRAL COMPLIANCE UNIT'S OBLIGATIONS REGARDING SELF ASSESSMENT OR INDEPENDENT TESTING PROCEDURE

After receiving the evaluation report from the branches and inspection/audit reports from ICCD Anti Money Laundering Department, Head Office will prepare Self Assessment Report on Half yearly basis. While preparing Self Assessment Report by AMLD, the following topics must be included:

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

AMLD will submit the report to MD & CEO and Board of Directors on half yearly basis. After receiving the MD's comments & Board of Directors observations; then the Report to be submitted to BFIU, Bangladesh Bank within stipulated time.

RECRUITMENT, TRAINING AND AWARENESS

9.1 OBLIGATIONS UNDER CIRCULAR

According to instruction BFIU circular-10, Mercantile Bank Limited will follow proper Screening Mechanism in case of recruitment and ensure proper training to mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction.

Obligations under BFIU Circular-10; dated 28/12/2014	To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, bank should follow proper Screening Mechanism in case of recruitment and ensure proper training for their officials.

9.2 EMPLOYEE SCREENING

Mercantile Bank is performing its activities for proper maintaining of ML & TF risk from its customers as well as from its employee in absence of proper risk mitigating measures. MBL follows fair recruitment procedure to minimize the ML & TF risks arose by or through its employees. This fair recruitment procedure shall include implementation of fairness in judging publicly declared competitive recruitment that also includes the judgment of good character. For this we are following the under mentioned measures:

- reference check
- background check
- personal interviewing
- personal guarantee etc.

MBL will examine the consistency and capability of the employee and will arrange necessary training on AML & CFT lessons for the particular job or desk before assigning an employee in a particular job or desk,

9.3 KNOW YOUR EMPLOYEE (KYE)

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

9.4 TRAINING FOR EMPLOYEE

Every employee of MBL shall have at least basic AML & CFT training that cover all the aspects of AML & CFT measures in Bangladesh. Basic AML & CFT training is at least day long model having evaluation module of the trainees. Relevant provision of Acts, rules and circulars, guidelines, regulatory requirements, suspicious transaction or activity reporting must be covered in basic AML & CFT training course. To

keep the employees updated about AML & CFT measures, MBL impart refreshment training programs of its employees on a regular basis.

AML & CFT basic training shall cover the following-

- an overview of AML & CFT initiatives;
- relevant provisions of MLPA & ATA and the rules there on;
- Uniform Account Opening Form, KYC, TP & Risk Grading
- regulatory requirements as per BFIU circular, circular letters and guidelines;
- STR/SAR reporting procedure;
- ongoing monitoring and sanction screening mechanism;

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

9.5 AWARENESS OF SENIOR MANAGEMENT

Mercantile Bank will arrange from time to time an awareness program for all the members of its board of directors, members of the senior management and people engaged with policy making of the bank.

9.6 CUSTOMER AWARENESS

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

9.7 AWARENESS OF MASS PEOPLE

Prevention of ML & TF largely depends on awareness at all level. Public or mass people awareness on AML & CFT measures provides synergies to banks in implementing the regulatory requirement. M e r c a n t i l e Bank will arrange public awareness programs like advertisements through billboard, poster, festoon and mass media, distribution of handbills, leaflet and so on.

TERRORIST FINANCING & PROLIFERATION FINANCING

10.1 INTRODUCTION

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

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

10.2 LEGAL OBLIGATIONS

Obligations under ATA, 2009	Every Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 and if any suspicious transaction is identified, the agency shall spontaneously report it to Bangladesh Bank without any delay. The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each bank should approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, 2009; which are applicable to the bank, have been complied with or not.

10.3 OBLIGATIONS UNDER CIRCULAR

Obligations under BFIU Circular-10; dated 28/12/2015

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

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

10.4 NECESSITY OF FUNDS BY TERRORIST

Terrorist organizations need money to operate. Weapons and ammunition are expensive. Major

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

10.5 SOURCES OF FUND/RAISING OF FUND

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

10.6 MOVEMENT OF TERRORIST FUND

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

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

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

10.6.1 FORMAL FINANCIAL SECTOR

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

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

10.6.2 TRADE SECTOR

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

10.6.3 CASH COURIERS

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

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

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

10.6.4 USE OF ALTERNATIVE REMITTANCE SYSTEMS (ARS)

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

10.6.5 USE OF CHARITIES AND NON-PROFIT ORGANISATIONS

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

10.7 TARGETED FINANCIAL SANCTIONS

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

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

However, targeted financial sanctions represent a potential refinement of the sanctions tool that could be

used in conjunction with other coercive efforts, such as travel bans, to minimize the unintended effects of comprehensive sanctions and achieve greater effectiveness.

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

For effective implementation of these provisions, MBL as a reporting agency has to maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. In case there is any fund or economic resources held by the listed individuals and entities, MBL shall immediately stop payment or transaction of funds, financial assets or economic resources and report to the BFIU within the next working day with full particulars of the listed and/or the suspected individuals or entities or related or connected individual identities.

10.8 AUTOMATED SCREENING MECHANISM OF UNSCRs

For effective implementation of TFS relating to TF & PF Mercantile Bank has already implemented Automated Screening Solution. Data Soft Systems Bangladesh has provided a software name **Velocity-AML Solutions Suite** for implementing Automated Screening Solution in our bank. MBL ensure that screening has done before-

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

For proper implementation of UN sanction list, official of MBL must have enough knowledge about-

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

The descriptions and functions of **Velocity-AML Solutions Suite** are furnished below**:**

Velocity-AML Solutions Suite

Velocity is a powerful and scalable AML workflow with case management system specifically designed for facilitating AML workflow and reporting. The system integrates seamlessly with other existing AML Systems and also can be used on its own to perform on boarding (KYC), alerts reviews, CDD/EDD, and periodic reviews. The system is capable to communicate with UNSCR/OFAC/EU/UK Central Bank's list and other sanctions list through web service or can import data from those sites to work offline.

Modules of the Software**:**

- New Customer screening module Integrated with CBS
- AML Admin and On demand Screening & Related Report

- Existing Customer Screening & Related Report Module
- Payment Interdiction on Swift & Related Report Module
- KYC/CDD/EDD, TP & Related Report Module
- Case Management & Related Report Module

Workbench of the software

Velocity-AML Solutions suite is a workflow and workbench based solutions. For User perspective the system has been divided by following workbench.

- Customer officer Workbench
- BAMLCO Workbench
- DCAMLCO Workbench
- CAMLCO Workbench and
- AML Admin Workbench

Sanction list consider the software

Velocity-AML Solutions suite considers the following sanctions list but not limited. It has options to incorporate more sanction list.

- UNSCR
- OFAC SDN
- EU list
- UK List
- Central Bank List
- Bank's own list
- Hong Kong list

What to do and How to do With Sanction list

Bank's existing customer and any customer before account open will have to screen against the sanction list. Any transaction with other bank/other account will have to screen prior the transaction.

To comply and perform the screening we are using a solution called Velocity-AML Solutions suite.

The following requirements will be screened by this application :

1. Screen prior to any account opening
2. Screen against existing customer and rescreen periodically when sanction list update by the authority.
3. Before SWIFT message send and after receive any swift message screen against sanction list
4. Inward/Outward any remittance screen by the system
5. Bearer Check screen by the system

Application directly connected with UN sanction list authority website through web service. It automatically update application's database from UN sanction authority site. Than Any screening performed by the application against it's local updated database.

Transactional Review

The purpose of AML transactional review is to provide ongoing identification of suspicious activity from customer transaction data. It is generally a two-stage process whereby first, instance of potentially suspicious behavior are identified or flagged and then these instance of potentially suspicious behavior are reviewed by an analyst to determine if, ultimately a SAR should be filed.

To Identify potentially suspicious behavior we have implemented Velocity-AML solutions suite . The system fed data from our CBS system and analyze on the data .It filter, complies and summarize transactional data and flag instance of potential suspicious.

Match Algorithms Used in the Software

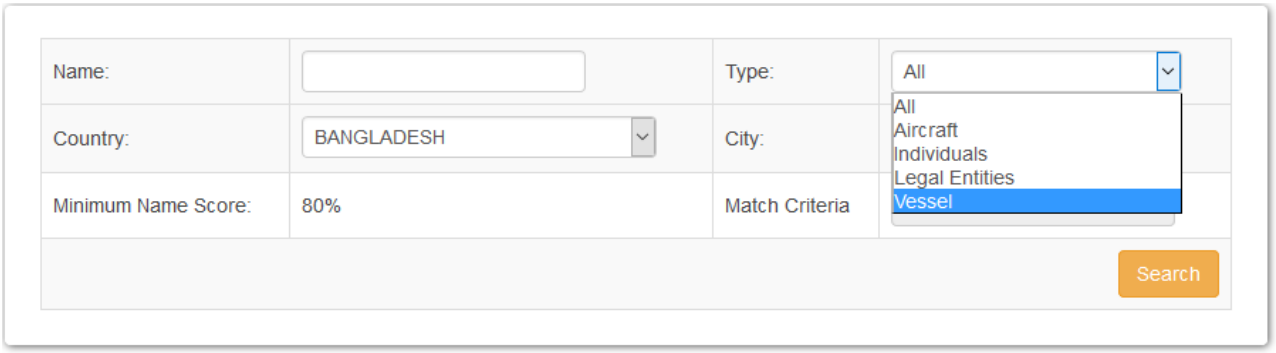
As per Bangladesh Bank's instruction, Application uses fuzzy algorithm and Phonetics algorithm individual and both in combination. Jaro-winkler use for fuzzy matching and soundex uses for phonetics matching.

False Positive Handling Procedure

False positive is a test result which incorrectly indicates that a particular condition or attribute is present. As the application uses fuzzy logic and phonetic matching algorithm, Match result returns the score/ percentage of the matching. System is configurable the matching parameters. Initially it consider the name , country and address but there have option to match father name, mother name, DOB, passport number etc.

The following series of steps we use to reduce the number of false positives:
Screen sentences separately: Filters separate names, addresses and cities from other data. They not combine these with other data in the sentence.
Screen accounts separately: Filters screen personal and corporate/Legal entity accounts separately.

Screen vessels separately and match names with vessel names: Shipping vessels or cargo ships have been a specific focus of OFAC over the past several years .So Our Application screen vessel separately in OFAC, UN sanction list along with other list.



Match found handling Procedure

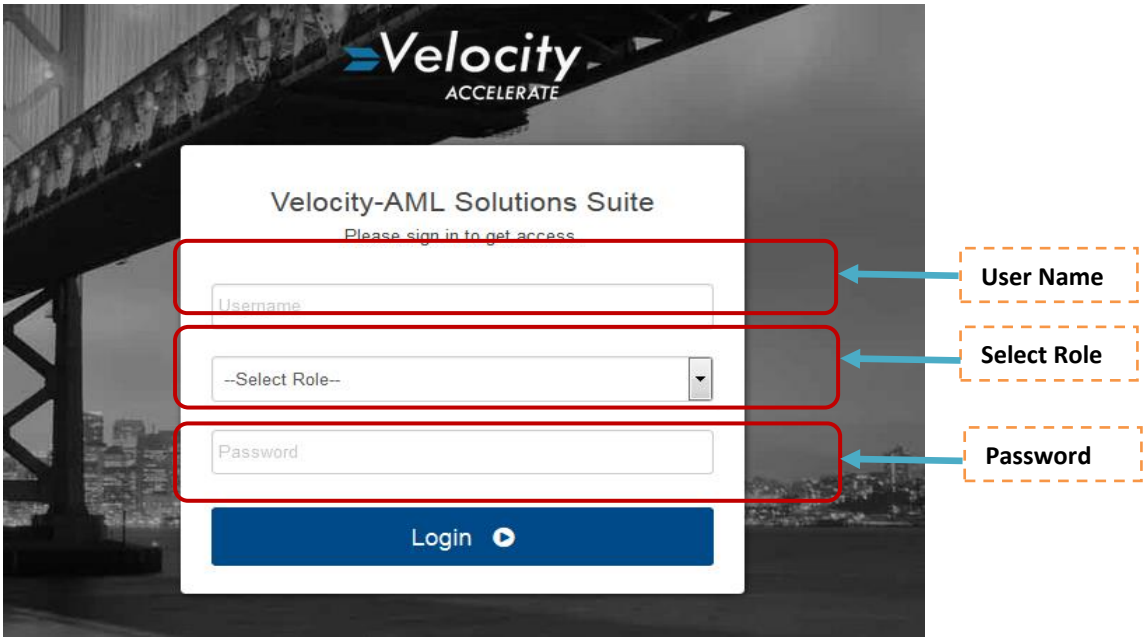
If any customer found match with any of the sanction list, system automatically hold the customer status and send upper level for approval and review. In branch level BAMLCO make decision by reviewing customer details and sanction list detail. If he seems that the customer is under sanction list, he puts his comments and justification and block the customer to make any transaction. In that case an instruction goes to CBS system and CBS routine block the customer immediately.

If any customer found the match with any sanction list, the system creates alert and notify the responsible person to clear alert. In that case responsible person take necessary action to clear alert and follow the systems workflow procedure. The system workflow is given in following section briefly.

Brief User instruction and work flow Login

Login is the startup page of the solution. Each and every user must login using this form to access the solution. User will able to login using following credentials.

1. **User Name (Enter admin provided user name)**
2. **Role (Select software role like Customer officer/ BAMLCO/DAMLCO/CAMLCO)**
3. **Password. (Enter your password)**



4. **Press enter/ click on Login button for login.**

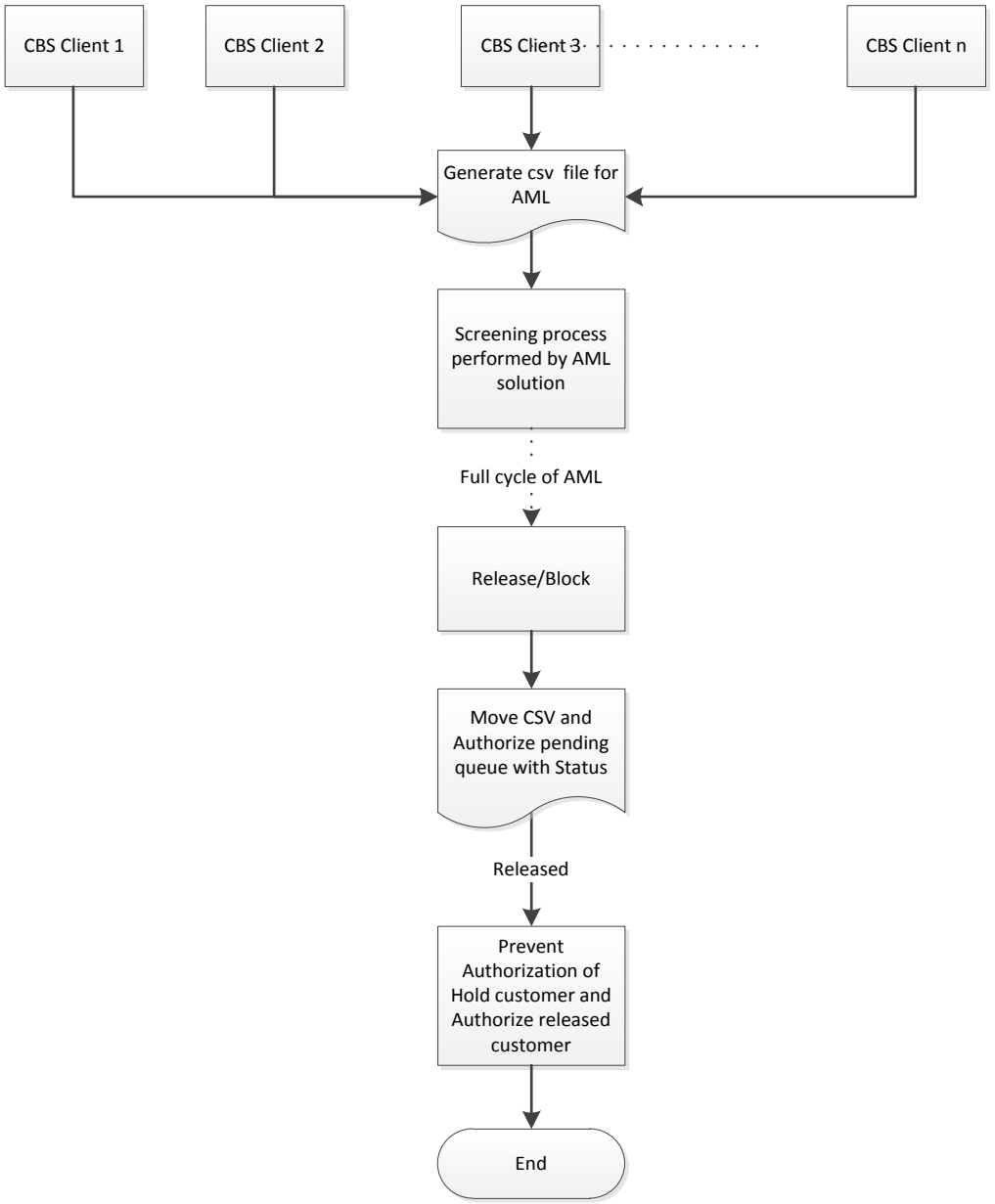
Entering valid user name, Role and password user will able to view role wise workbench to perform his task.

New Customer screening module Integrated with CBS

This module is integrated with CBS and Velocity-AML Solutions suite. Velocity-AML Solutions suite placed in between of the customer creation and authorization system.

When a CO adds a new customer in Core Banking Solutions (CBS), he will be not able to "Authorize" the customer from CBS until the customer has been screened and "Released" from Velocity-AML Solutions Suite.

Workflow of New Customer screening by MBL



1. Click on **CBS Screening** tab, the screen will appear as below-

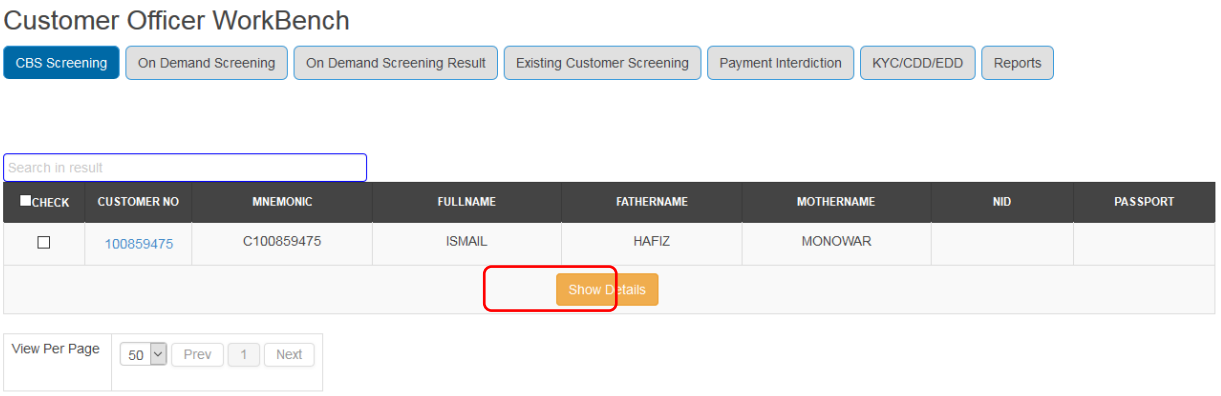


Fig: CBS Match Data List

2. Then select Individual customer or multiple customers and click Search List tab for Screening
3. After Click in Search list below Screening will appear.

4. Clicking on highlighted tag, then appear below this screen-

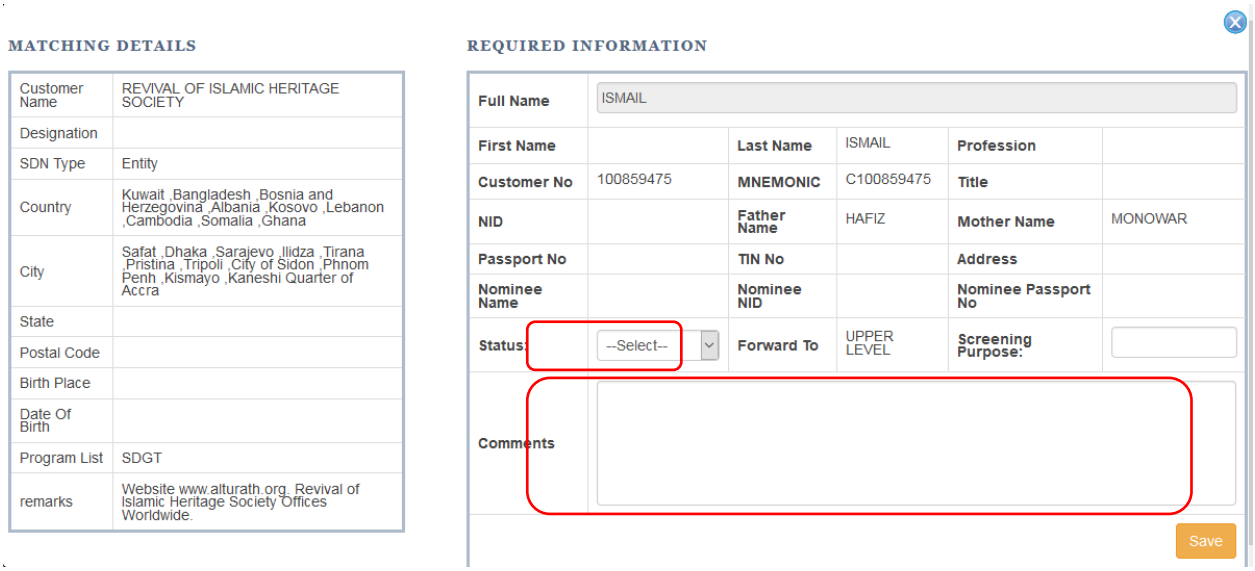


Fig: Entry Screen

5. Customer Officer can view individual customer information and fill up required information (Change Status, Select forward to upper level, etc.) and save it by click in Save Button and take a print as a PDF.

On demand screening

On demand screening module is a common screening module. It can be used for multipurpose. Initially it will use for following type of screening.

- Walking customer screening
- Remittance of cash pickup
- Bearer Check
- LC etc.

Without these it can used for multipurpose.

Customer Officer Workbench: Normally Customer officer initiate screening.

1. Screen a Customer
2. Check data from the matching data list.
3. Select Type of Entry
4. Input corresponding information.
5. If no match list found then input corresponding information.
6. Save Data with Status HOLD/FALSE POSITIVE and forward to UPPER LEVEL for further processing

BAMLCO Workbench: All data forwarded UPPER LEVEL by Customer officer is received by BAMLCO

1. Select Data from NEW Tab
2. Give Comment , Status
3. Select Forward to UPPER LEVEL if further investigation needed or select NONE
4. Save Data

DCAMLCO Workbench: All data forwarded UPPER LEVEL by BAMLCO is received by DCAMLCO

1. Select Data from NEW Tab
2. Give Comment , Status
3. Select Forward to UPPER LEVEL if further investigation needed or select NONE
4. Save Data

CAMLCO Workbench: All data forwarded UPPER LEVEL by DAMLCO is received by CAMLCO

1. Select Data from NEW Tab
2. Give Comment , Status
3. Save Data

BAMLCO/ DCAMLCO/CAMLCO can give common comments, status and forward to data for all selected Customer.

All Pending data is available in pending tab, and all close data is available in Close tab.

Remittance

Remittance officer Workbench:

1. Upload File with remittance Data
2. Select Data From New Tab Data List
3. Screening

- If no match found then save data with Status Released.
- If Match found then data is saved with matching details and send to remittance Approver for further process.

Remittance Approver Workbench: All data forwarded UPPER LEVEL by Remittance officer is received by Remittance Approver.

1. Select Data from NEW Tab
2. Give Comment , Status
3. Select Forward to UPPER LEVEL if further investigation needed or select NONE
4. Save Data

CAMLCO Workbench: All data forwarded UPPER LEVEL by Remittance Approver is received by CAMLCO

1. Select Data from NEW Tab
2. Give Comment , Status
3. Save Data

Remittance Officer, Remittance Approver can give common comments, status and forward to data for all selected Customer.

All Pending data is available in pending tab, and all close data is available in Close tab.

Existing Customer Screen

Admin Workbench:

1. Synchronize Existing Customer Data.
2. Select Branches for Screening from Screening Tab.
3. Screening

- If no match found then save data with Status Released.
- If Match found then data is send to Customer officer for further process.

Customer Officer Workbench: Normally Customer officer initiate screening for matching Customer.

1. Select Customer from list.
2. Screen and send to UPPER LEVEL with Matching Details

BAMLCO Workbench: All data forwarded UPPER LEVEL by Customer officer is received by BAMLCO

1. Select Data from NEW Tab
2. Give Comment , Status
3. Select Forward to UPPER LEVEL if further investigation needed or select NONE
4. Save Data

DCAMLCO Workbench: All data forwarded UPPER LEVEL by BAMLCO is received by DAMLCO

1. Select Data from NEW Tab
2. Give Comment , Status
3. Select Forward to UPPER LEVEL if further investigation needed or select NONE
4. Save Data

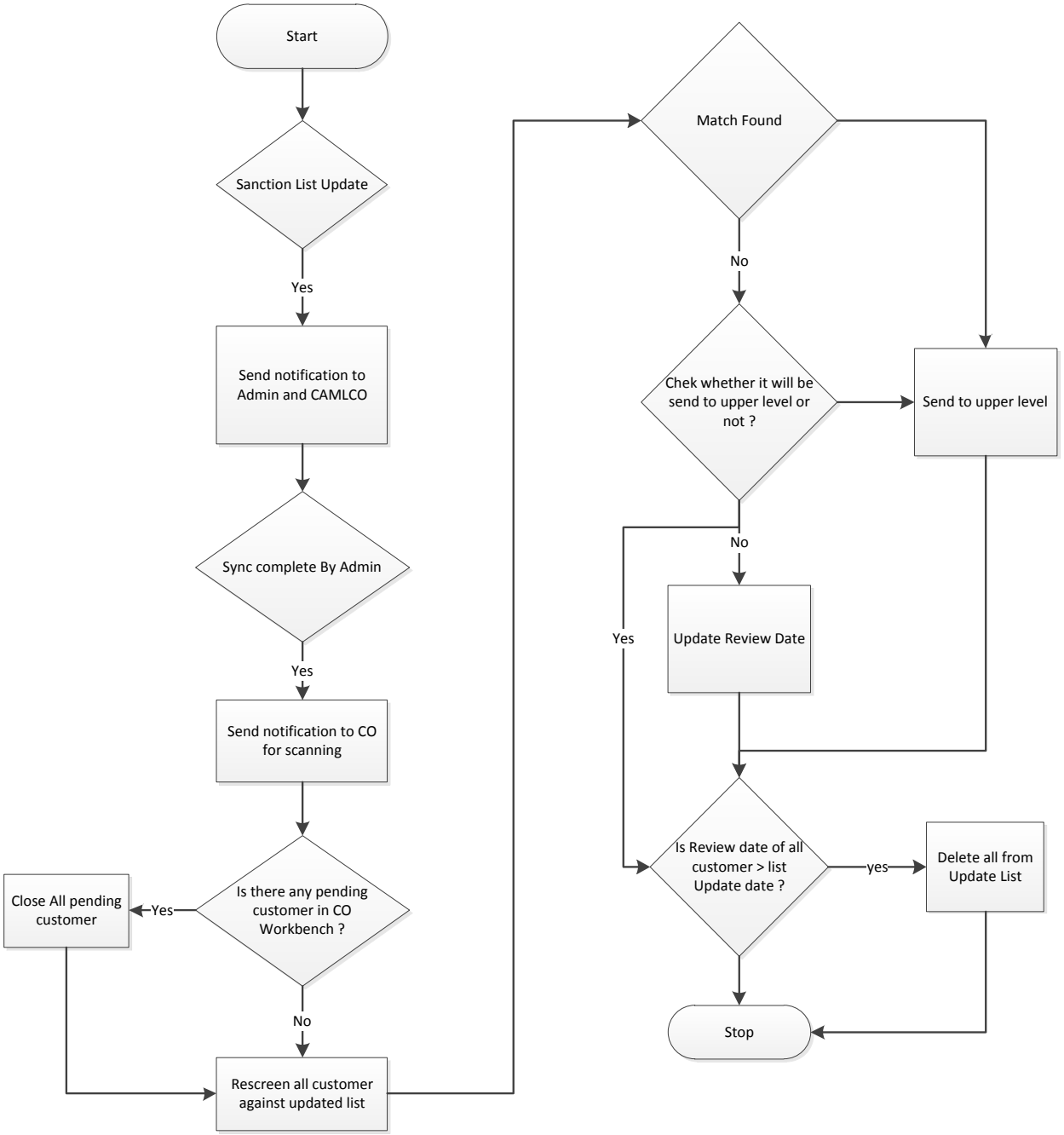
CAMLCO Workbench: All data forwarded UPPER LEVEL by DAMLCO is received by CAMLCO

1. Select Data from NEW Tab
2. Give Comment , Status
3. Save Data

BAMLCO/ DCAMLCO/CAMLCO can give common comments, status and forward to data for all selected Customer.

All Pending data is available in pending tab, and all close data is available in Close tab.

Reverse Screening: If any update in the sanction available then rescreen is performed by admin.



1. Synchronize Customer Data.
2. Rescreen data against sanction list update data
3. If no match found then save in history.
4. If Match found then data is send to Customer officer for further process.

SWIFT Screening

Incoming Message

1. AFT service will store the messages in given “AFT Input” folder. From this folder AML solution will read and scan the message. After reading if no match found then it will move the message to “CBS Input” folder and from that folder CBS will read the message.
2. If match found then AML will move the message to “Blocked In” folder. And it will wait for decision of the designated person. If he releases the message then it will move the massage to “CBS Input” folder.

Outgoing Message

1. After generating the message CBS will store the message in “CBS Out” folder. AML solution will read and scan the message. After reading if no match found then it will move the message to “AFT Out” folder and from that folder AFT will send the message.
2. If match found then AML will move the message to “Blocked Out” folder. And it will wait for decision of the designated person. If he releases the message then it will move the massage to “CBS Out” folder.

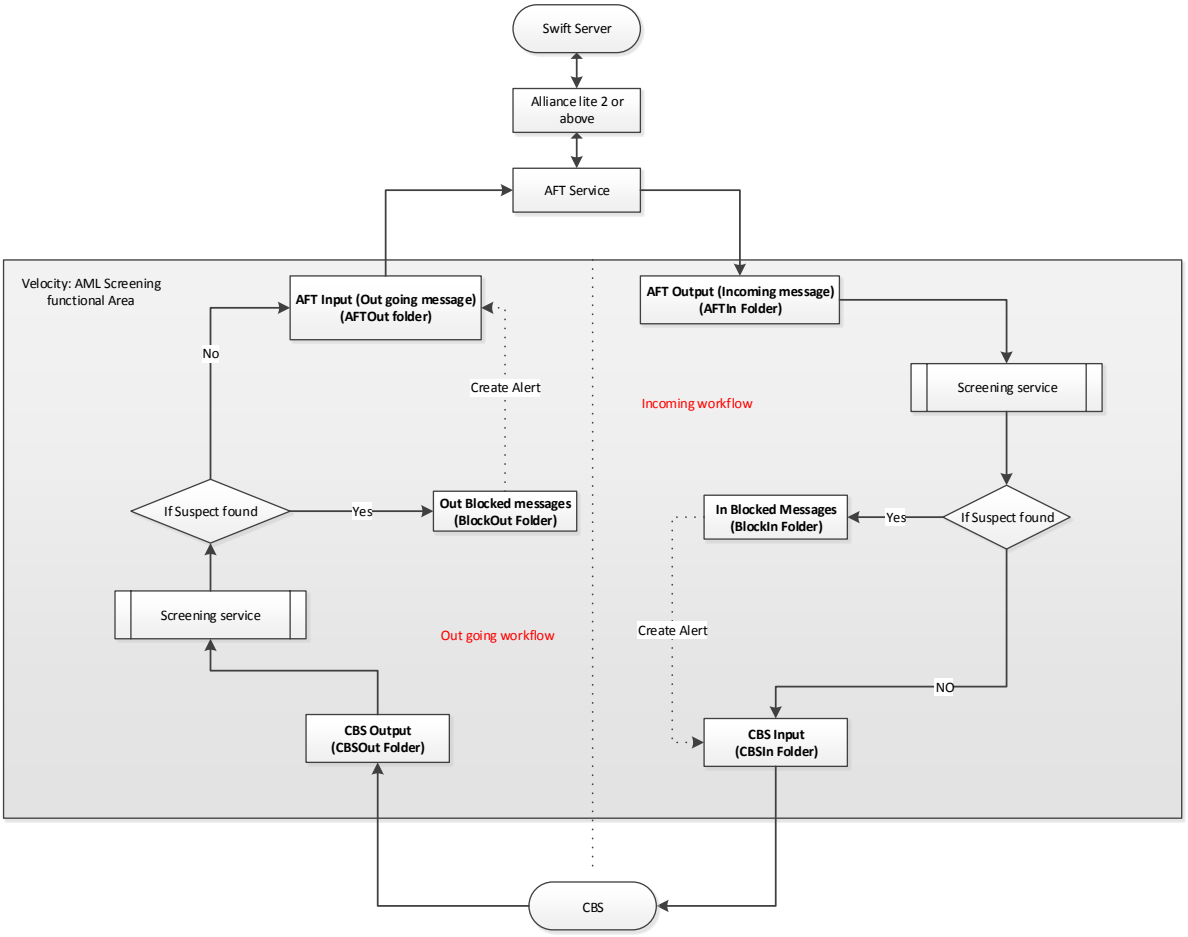
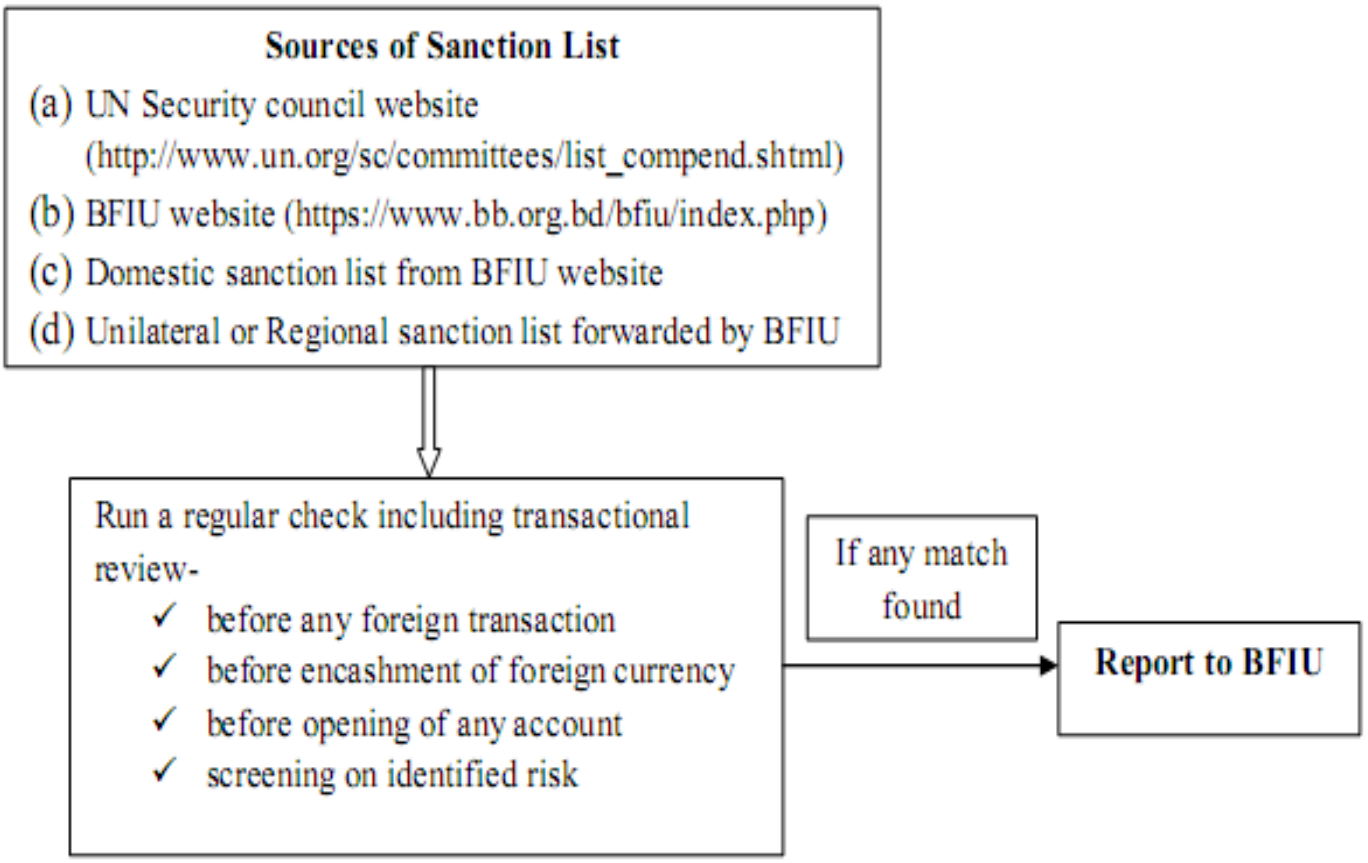


Fig: Workflow of SWIFT

10.9 ROLE OF MERCANTILE BANK IN PREVENTING TF & PF

- Mercantile Bank shall establish a procedure with the approval of Board of Directors for detection and prevention of financing of terrorism and financing in proliferation of weapons of mass destruction. MBL also issue instructions about the duties of Bank officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.
- Branch should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 and if any suspicious transaction is identified, MBL shall spontaneously report it to Bangladesh Bank without any delay.
- If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, branch has to send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to AMLD, Head Office and AMLD will report to BFIU immediately.
- Branch is maintaining and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. Branch should run regular check on the given parameters, including transactional review, to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.
- Branch should run a check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009; individuals or entities owned or controlled directly or indirectly by such persons or entities, as well as persons and entities acting on behalf of, or at the direction of, individuals or entities listed or scheduled under the Act are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.

10.10 FLOW-CHART FOR IMPLEMENTATION OF TFS BY BANK



RISK REGISTER

1. ML & TF Risk Register for Customers

Annexure- A

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank. Monitoring the transaction. Response: Acceptable Risk
Walk-in customer (beneficiary is government/semi government/ autonomous body/ bank & NBFI)	Likely	Minor	=1(Low)	CDD should be ensured. Short KYC should be obtained. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank. Response: Acceptable Risk
Walk-in customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBFI)	Likely	Moderate	=2(Medium)	CDD should be ensured. Short KYC should be obtained. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank. Response: Acceptable Risk
Non-resident customer (Bangladeshi)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank. Monitoring the transaction. Response: Acceptable Risk
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD must be applied. Monitor the transaction. Marked as STR Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
A customer making series of transactions to the same individual or entity	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Monitor the transaction. Marked as STR Response: Acceptable Risk
A customer or a group of customer making lots of transactions to the same individual or group	likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD must be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR
Customer involved in outsourcing business	likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD must be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Response: Acceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer appears to do structuring to avoid reporting threshold	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.
Customer appears to have accounts with several banks in the same area	likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction. Marked as STR Response: Acceptable Risk
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk..
Negative news about the customers' activities/ business in media or from other reliable sources	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk..
Customer is secretive and reluctant to meet in person	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitor the transaction. Verify physically. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer is a mandate who is operating account on behalf of another person/ company.	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.
Transactions by beneficiaries using Student account & Farmers account	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Obtain/check documents of beneficial owner. Monitor the transaction. Report as STR Response: Acceptable Risk
Joint account opened with minor/ women & transactions to the account	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Large deposits in the account of customer with low income	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response**:** Unacceptable Risk.
Transaction does not match with business profile	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR Response: Acceptable Risk
Customers about whom BFIU seeks information (individual)	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Monitor the transaction. Report as STR Response: Acceptable Risk
A customer whose identification is difficult to check	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Significant and unexplained geographic distance between the bank and the location of the customer	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.
Account Opening branch is far from residential address of account holder	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction. Verify physically. Encourage to opening the account to the nearest branch. Response: Acceptable Risk
Customer is a foreigner	Likely	Major	=3(High)	Obtain approval from Head Office. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Non Resident Customer	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.
Customer is a minor	Likely	Major	=3(High)	Beneficiary Owner information must be obtained. Verify the source of income. CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitor the transaction Response: Unacceptable Risk.
Customer is Housewife	Likely	Major	=3(High)	Beneficiary Owner information must be obtained. Verify the source of income. CDD should be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Monitor the transaction Report as STR Response: Unacceptable Risk.
Customers that are politically exposed persons(PEPs) or influential persons (IPs) or chief/senior officials of international organizations and their family members and close associates	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Very likely	Moderate	=3(high)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.
Customers doing significant volume transactions with higher-risk geographic locations.	Very likely	Moderate	=3(high)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitor the transaction. Report as STR Response: Unacceptable Risk.
A customer who brings in large amounts of used notes and/or small denominations	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Report as STR. CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Customer is a money changer/ courier service agent / travel agent	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any)/ acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Transaction Monitoring regularly. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer is involved in Manpower Export Business	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring Transaction. Report as STR. **Response:** Unacceptable Risk.
Customer has been refused to provide banking facilities by another bank	Likely	Major	=3(High)	Identify the reason behind non acceptance by other Banks. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Accounts opened before 30 April, 2002	Likely	Moderate	=2(Medium)	Update KYC profile Marked as dormant if KYC is not updated. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Monitor the transaction. Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customers with complex accounting and huge transaction	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Receipt of donor fund , fund from foreign source by micro finance institute (MFI)	Likely	Major	=3(High)	CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Verify source of fund. Response: Unacceptable Risk.
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Genuineness of submitted documents is difficult to ensure	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction Verify physically. Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Counterfeiting of security documents	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
High net worth with no clear identifiable sources of income	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank. Transaction is not allowed until risk is reduced Monitor the transaction regularly Response: Unacceptable Risk
Customer has been refused to provide banking facilities by another Bank	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank. Monitor the transaction regularly Response: Acceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Accounts of SME, NGOs, Trusts, Charity, Co-operative Societies, MLM Co etc.	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD must be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank. Transaction is not allowed until risk is reduced Monitor the transaction regularly Response: Unacceptable Risk
A corporate customer whose ownership structure is unusual and excessively complex	Very likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Anonymous account transactions	Very likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Wholesale Banking Customer				
Entity customer having operations in multiple locations	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Monitor the transaction. Verify physically. Encourage to opening the account to the nearest branch. Response: Acceptable Risk
Customers about whom BFIU seeks information (large corporate)	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Report as STR CDD must be ensured & EDD must be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Owner of the entity that are Influential Persons (IPs) and their family members and close associates	Likely	Major	=3(High)	Obtain senior management approval before establishing such business relationship. Transaction is not allowed until risk is reduced Verify source of fund. Report as STR CDD must be ensured & EDD must be applied. Monitor the Transaction. Response: Unacceptable Risk.
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly.. Response: Unacceptable Risk.
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Report as STR Response: Unacceptable Risk.
A customer whose identification is difficult to check.	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Owner of the entity that are Politically Exposed Persons (PEPs) or Influential Persons (IPs)/ chief / senior officials of International Organizations and their family members and close associates	Likely	Major	=3(High)	Obtain senior management approval before establishing such business relationship. Verify source of fund. Report as STR CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Monitor the Transaction. Response: Unacceptable Risk.
Charities or NPOs(especially operating in less privileged areas).	Likely	Major	=3(High)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD must be applied. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Monitoring the Transaction regularly. Response: Unacceptable Risk.
Credit Card Customer				
Customer who changes static data frequently	Likely	Major	=3(High)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Response: Unacceptable Risk.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Credit Card customer	Likely	Major	=3(High)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	Likely	Moderate	=2(Medium)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Response: Acceptable Risk
Prepaid Card customer	Likely	Minor	=1(Low)	Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied. Monitor transaction. Response: Acceptable Risk

International Trade Customer				
A new customer (Outward remittance-through SWIFT)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID(NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. To check the name of the beneficiary in the sanctioned list Marked as STR if the customer not provide the required documents Obtain the information regarding purpose of remittance. Response: Acceptable Risk
A new customer (Import/ Export)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank To check the name of the beneficiary / applicant in the sanctioned list Monitor the transaction. Valid IRC & ERC should be obtained. Response: Acceptable Risk
A new customer (Inward remittance-through SWIFT)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank To check the name of the remitter in the sanctioned list Monitor the transaction. Marked as STR if the customer not provide the required documents Response: Acceptable Risk
A new customer who wants to carry out a large transaction (Import/ Export)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank To check the name of the beneficiary / applicant in the sanctioned list Monitor the transaction. Valid IRC & ERC should be obtained. Response: Acceptable Risk

A new customer who wants to carry out a large transaction (Inward/ outward remittance)	Likely	Major	=3(High)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank To check the name of the beneficiary / remitter in the sanctioned list Monitor the transaction. Report as STR if the customer not provide the required documents Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
A customer wants to conduct business beyond its line of business (import/ export/ remittance)	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. IRC & ERC should be obtained. Report as STR if the customer not provide the required documents Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	Likely	Major	=3(High)	Obtain senior management approval before establishing such business relationship. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify source of fund. Monitor the transaction. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.

Correspondent Banks	Likely	Moderate	=2(Medium)	To be satisfied about the nature of the business of the correspondent through collection of information. Obtain senior management approval before establishing correspondent relationship. No relation with Shell Bank. CDD must be ensured & EDD must be applied before establishing correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standard for the prevention of Money Laundering & Terrorist Financing. Obtain the extensive information about their policies & procedures on prevention of Money Laundering & Terrorist Financing. Response: Acceptable Risk
Money services businesses (remittance houses, exchange houses)	Likely	Moderate	=2(Medium)	To be satisfied about the nature of the business of the correspondent through collection of information. Obtain senior management as well as Bangladesh Bank approval before establishing Agency arrangement No relation with Shell Bank. CDD must be ensured & EDD must be applied before establishing Agency arrangement with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standard for the prevention of Money Laundering & Terrorist Financing. Obtain the extensive information about their policies & procedures on prevention of Money Laundering & Terrorist Financing. Response: Acceptable Risk

2. Risk Register for Products & Services (All the products and services of a bank has to be included here)

Ri	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)	Likely	Major	=3(High)	Obtain information of Beneficiary Owner. Verify source of income. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Gift Cheque	Likely	Minor	=1(Low)	Check Standard ID(NID/passport/, Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied. Obtain information of Beneficiary before payment Response: Acceptable Risk
Locker Service	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk
Foreign currency endorsement in Passport	Likely	Minor	=1(Low)	The customer should be account holder or relative of account holder. Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied. Response: Acceptable Risk

Large transaction in the account of under privileged people	Likely	Major	=3(High)	Verify source of income. CDD mustbe ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Marked as STR Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
FDR (less than 2 million)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Response: Acceptable Risk
FDR (2 million and above)	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Special scheme deposit accounts opened with big installment and small tenure	Likely	Moderate	=2(Medium)	Verify the source of fund. CDD should be ensured Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Report as STR Response: Acceptable Risk
Multiple deposit scheme accounts opened by same customer in a branch	Likely	Moderate	=2(Medium)	Verify the source of fund. CDD should be ensured Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Report as STR Response: Acceptable Risk

Multiple deposit scheme accounts opened by same customer from different location	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced. Marked as STR Response: Unacceptable Risk.
Open DPS in the name of family member Or Installments paid from the account other than the customer's account	Likely	Major	=3(High)	Obtain the information of Beneficiary Owner. Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Stand alone DPS	Likely	Moderate	=2(Medium)	CDD should be ensured Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk
Early encashment of FDR, special scheme etc.	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk
Non face to face business relationship/transaction	Very Likely	Major	=4(Extreme)	Do not accept business relationship. Response: Unacceptable Risk
Payment received from unrelated/un-associated third parties	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Transaction is not allowed until risk is reduced Monitor the transaction. Response: Unacceptable Risk.

Retail Privilege Facilities				
Pre- Approved Credit Card with BDT 300K limit	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Enhanced ATM cash withdrawal Limit BDT 100K	Likely	Moderate	=2(Medium)	CDD should be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
SME Banking Product				
Want to open FDR where source of fund is not clear	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Early encashment of FDR	Likely	Minor	=1(Low)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured Response: Acceptable Risk
Repayment of loan EMI from source that is not clear	Likely	Major	=3(High)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.

Repayment of full loan amount before maturity	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Transaction is not allowed until risk is reduced Response: Unacceptable Risk
Loan amount utilized in sector other than the sector specified during availing the loan	Likely	Major	=3(High)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank. Report as STR Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	Likely	Major	=3(High)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Unacceptable Risk.
Source of fund used as security not clear at the time of availing loan	Likely	Major	=3(High)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Wholesale Banking Product				
Development of new product & service of bank	Likely	Moderate	=2(Medium)	CDD should be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk

Payment received from unrelated third parties	Likely	Major	=3(High)	Transaction is not allowed until risk is reduced CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the source of fund Report as STR Response: Unacceptable Risk.
High Value FDR	Likely	Major	=3(High)	Verify the source of fund. CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Term loan, SOD(FO), SOD(G-work order), SOD(Garment),SOD(PO), Loan General, Lease finance, Packing Credit, BTB L/C	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
BG(bid bond), BG(PG), BG(APG)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
L/C subsequent term loan, DP L/C	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Verify the documents Response: Acceptable Risk
C.C(H), SOD(G-Business), STL	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Verify the value of mortgage property. Response: Acceptable Risk

OBU	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Syndication Financing	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Verify the documents Monitor the transaction. Response: Acceptable Risk
Credit Card				
Supplementary Credit Card Issue	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Frequent use of Card Cheque	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk

Credit card issuance against ERQ and RFCD accounts	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
International Trade				
Line of business mismatch (import/export/remittance)	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Under/ Over invoicing (import/export/remittance)	Likely	Major	=3(High)	Verify the price of goods/services quoted in the invoice. Monitor the transaction. CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Unacceptable Risk.
Retirement of import bills in cash (import/export/remittance)	Likely	Moderate	=2(Medium)	Monitor the transaction. CDD must be ensured & EDD must be applied. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Response: Acceptable Risk

Wire transfer	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. In case of threshold cross-border wire transfer of 1000 or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected & preserved and has to be sent to intermediary/beneficiary bank. In case of threshold domestic wire transfer of at least 25,000 BDT, full and accurate information of the originator has to be collected & preserved and has to be sent to intermediary/beneficiary bank. For the domestic wire transfers below the threshold full and meaningful originator information has to be preserved. Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. Response: Acceptable Risk
Remittance **(Western Union & Others)**	Likely	Moderate	=2(Medium)	Check Standard ID (NID /, Birth Registration Certificate along with recent photo ID/ Valid passport (if any) acceptable document to the Bank CDD must be ensured & EDD must be applied. Monitor the transaction. Response: Acceptable Risk
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)	Likely	Major	=3(High)	Check Standard ID (NID /, Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Response: Unacceptable Risk.

3. Risk Register for Business practices/delivery methods or channels

Ri	Likelihood	Impact	Risk Score	Treatment/Action
Online (multiple small transaction through different branch)	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
BEFTN	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD should be ensured & EDD should be applied. Response: Acceptable Risk
BACH	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Check TP Response: Acceptable Risk
IDBP	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD should be ensured & EDD should be applied. Comply with circulars issued by Head Office from time to time Response: Acceptable Risk

Mobile Banking	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Screening Mechanism should be followed to appoint agent or cash point CDD must be ensured & EDD must be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Response: Acceptable Risk
Third party agent or broker	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Screening Mechanism should be followed to appoint agent. CDD must be ensured & EDD must be applied Response: Acceptable Risk
Direct contact with the customer	Likely	Minor	=1(low)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD should be ensured & EDD should be applied Response: Acceptable Risk
Credit Card				
New Merchant sign up	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk

High volume transaction through POS	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk
Alternate Delivery Channel				
Large amount withdrawn from ATMs	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk
Larger amount transaction from different location and different time(mid night) through ATM	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Report as STR Response: Acceptable Risk
Large amount of cash deposit in CDM	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD should be ensured & EDD should be applied. Response: Acceptable Risk
Huge fund transfer through internet	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Online/Internet	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD must be applied. Response: Acceptable Risk

Transaction Profile updated through Internet Banking	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Verify customer's email ID. Response: Acceptable Risk
Customer to business transaction-Online Payment Gateway -Internet Banking	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD must be applied. Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103) .	Likely	Moderate	=2(Medium)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD should be applied. Response: Acceptable Risk

4. Risk Register for Country/jurisdiction

Ri	Likelihood	Impact	Risk score	Treatment/Action
Import and export from/to sanction country	Very Likely	Major	=4(Extreme)	Do not accept the business relationship. Response: Unacceptable Risk
Transshipments, container, flag vessel etc. under global sanction	Likely	Major	=3(High)	Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Monitor the transaction. CDD must be ensured & EDD must be applied. Response: Unacceptable Risk.
Establishing correspondent relationship with sanction bank and/or country	Very Likely	Major	=4(Extreme)	Do not accept the business relationship. Response: Unacceptable Risk
Establishing correspondent relationship with poor AML&CFT practice country	Likely	Major	=3(High)	Particular attention should be paid & EDD must be applied while establishing a correspondent banking relationship Detailed information on the beneficial ownership of such banks shall have to be obtained. . Extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained. . Approval from senior management should be obtained Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Customer belongs to higher -risk geographic locations such as High Intensity Financial Crime Areas	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Monitor the transaction Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.

Customer belongs to countries or geographic areas identified by credible sources a providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Transaction is not allowed until risk is reduced Monitor the transaction Report as STR Response: Unacceptable Risk.
Customer belongs to High Risk ranking countries of the Basel AML index.	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Transaction is not allowed until risk is reduced Monitor the transaction Report as STR Response: Unacceptable Risk

Customer belongs to the countries identified by the bank as higher-risk because of its prior experiences or other factors.	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied while establishing a relationship Check Standard ID (NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Approval from senior management should be obtained Monitor the transaction Transaction is not allowed until risk is reduced Report as STR Response: Unacceptable Risk.
Any country identified by FATF or FSRBs- (FATF style Regional Body) as not having adequate AML&CFT systems	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Any bank that provide service to 'Shell Bank'	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Any bank that allow payable through account	Likely	Major	=3(High)	Particular attention should be paid & EDD must be applied while establishing a correspondent banking relationship Detailed information on the beneficial ownership of such banks shall have to be obtained. . Extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained. . Approval from senior management should be obtained CDD must be ensured Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Any country identified as destination of illicit financial flow	Likely	Major	=3(High)	CDD must be ensured & EDD must be applied Transaction is not allowed until risk is reduced Response: Unacceptable Risk.

Branches in a Border Area	Likely	Moderate	=2(Medium)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD should be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Physical verification. Response: Acceptable Risk
Area identified as high risk in the NRA	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Countries subject to UN embargo/sanctions	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk
Publicly known vulnerable areas	Likely	Major	=3(High)	Check Standard ID(NID/ Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank CDD must be ensured & EDD must be applied Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank Physical verification. Transaction is not allowed until risk is reduced Response: Unacceptable Risk.
Drug (Source, Destination & Trafficking Countries)	Very Likely	Major	=4(Extreme)	Do not accept as customer Response: Unacceptable Risk

5. Register for Regulatory Risk

Ri	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML/CFT guideline	Unlikely	Major	=2(Medium)	There must have AML/CFT Guidelines in the Bank.
Not forming a Central Compliance Unit (CCU)	Unlikely	Major	=2(Medium)	CCU must be formed in the Bank.
Not having an AML&CFT Compliance Officer	Unlikely	Major	=2(Medium)	There must have a BAMLCO of all the Branches of the Bank.
Not having Branch Anti Money Laundering Compliance Officer	Unlikely	Major	=2(Medium)	There must have a BAMLCO of all the Branches of the Bank.
Not having an AML&CFT program	Unlikely	Major	=2(Medium)	The concerned Department will ensure AML/CFT compliance program
No senior management commitment to comply with MLP and AT Act	Unlikely	Major	=2(Medium)	There must have senior management commitment to comply with MLP and AT Act
Failure to follow the AMLD /BFIU circular, circular letter, instructions etc.	Unlikely	Major	=2(Medium)	All AML/BFIU circular must be followed.
Not complying Freezing order issued by BFIU	Unlikely	Major	=2(Medium)	All Branches/ Divisions at Head Office must comply Freezing order issued by BFIU
Unique account opening form not followed while opening account	Unlikely	Major	=2(Medium)	All branches must follow unique account opening form while opening the account.
Non screening of new and existing customers against UNSCR Sanction and OFAC lists	Unlikely	Major	=2(Medium)	All branches must screen new and existing customers against UNSCR Sanction and OFAC lists
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Unlikely	Major	=2(Medium)	All branches must follow Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.
Complete and accurate information of customer not obtained	Unlikely	Major	=2(Medium)	All branches must obtain complete and accurate information of customer.
Failure to verify the identity proof document and address of the customer	Very likely	Major	=4(Extreme)	Close the account. Response: Unacceptable Risk

Beneficial owner identification and verification not done properly	Likely	Major	=3(High)	Check Standard ID (NID/passport/, Birth Registration Certificate along with recent photo ID/Valid passport(if any) acceptable document to the Bank Identification & verification to be done through thanks letter or physical verification (if necessary) Monitor the transaction. CDD must be ensured & EDD must be applied. Report STR. Response: Unacceptable Risk.
Customer/ Beneficial owner identification & verification not done properly	Unlikely	Major	=2(Medium)	Maintain KYC properly. Identification & verification to be done through thanks letter or physical verification (if necessary) Response: Acceptable Risk
Customer Due Diligence (CDD) not practiced properly	Unlikely	Major	=2(Medium)	CDD must be ensured & EDD must be applied properly. Response: Acceptable Risk
Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPS and influential person and senior official of international organization.)	Unlikely	Major	=2(Medium)	EDD must be applied in case of all High Risk customers. Response: Acceptable Risk
Failure to complete KYC of customer including walk in customer	Likely	Moderate	=2(Medium)	Monitor the transaction. CDD should be ensured & EDD must be applied. Report as STR. Response: Acceptable Risk
Failure to update TP and KYC of customer	Likely	Moderate	=2(Medium)	Monitor the transaction. CDD must be ensured & EDD should be applied. Marked as stop payment Report STR. Response: Acceptable Risk
Keep the legacy accounts operative without completing KYC	Likely	Moderate	=2(Medium)	CDD must be ensured & EDD should be applied. Mark the account as dormant. Response: Acceptable Risk
Failure to assess the ML & TF risk of a product or service before launching	Unlikely	Moderate	=1(Low)	AML/CFT guidelines must be followed while launching product or service. Response: Acceptable Risk
Failure to complete the KYC of Correspondent Bank	Very likely	Major	=4(Extreme)	Do not establish business relationship. Response: Unacceptable Risk

Senior Management approval not obtained before entering into a Correspondent Banking relationship	Very likely	Major	=4(Extreme)	Do not establish business relationship. Response: Unacceptable Risk
Failure to comply with the instruction of BFIU by bank Foreign subsidiary	likely	Major	=3(High)	Foreign subsidiary must be complied with the instruction of BFIU. Response: Unacceptable Risk.
Failure to keep record properly	Unlikely	Major	=2(Medium)	Preserve all records relevant with the account for 5 years after closer the account. Response: Acceptable Risk
Failure to report complete and accurate CTR on time	Unlikely	Major	=2(Medium)	The Bank shall be more careful to report complete accurate CTR on time. Response: Acceptable Risk
Failure to review CTR	Unlikely	Major	=2(Medium)	The Bank shall be more careful to review CTR . Response: Acceptable Risk
Failure to identify and monitor structuring	Unlikely	Major	=2(Medium)	The Bank shall be more careful to identify and monitor structuring Monitor the transaction. Response: Acceptable Risk
Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Unlikely	Major	=2(Medium)	The Bank shall be more careful for the timely detection and reporting of suspicious activity Monitor the transaction. Response: Acceptable Risk
Failure to conduct quarterly meeting properly	Unlikely	Major	=2(Medium)	Conduct quarterly meeting properly. Response: Acceptable Risk
Failure to report suspicious transactions	Unlikely	Major	=2(Medium)	The Bank shall be more careful to report STR duly.
Failure to conduct self assessment properly	Unlikely	Major	=2(Medium)	Conduct self assessment properly. Response: Acceptable Risk
Failure to submit statement/ report to BFIU on time	Unlikely	Major	=2(Medium)	Accountability of the concerned department should be introduced to ensure submission of all required reports to BFIU in time. Response: Acceptable Risk
Submit erroneous statement/ report to BFIU	Unlikely	Major	=2(Medium)	All Branches/Divisions at Head Office must submit accurate information requested by BFIU Response: Acceptable Risk
Not complying with any order for freezing or suspension of transaction issued by BFIU or	Unlikely	Major	=2(Medium)	All branches must complied BFIU or BB instructions. Response: Acceptable Risk

Not submitting accurate information or statement sought by BFIU or BB.	Unlikely	Major	=2(Medium)	Accurate information or statement must be submitted to BFIU or BB as per requirement. Response: Acceptable Risk
Not submitting required report to senior management regularly.	Likely	Moderate	=2(Medium)	Required reports must be submitted to senior management regularly. Response: Acceptable Risk
Failure to rectify the objections raised by BFIU or bank inspection teams on time	Likely	Major	=3(High)	All objections raised by BFIU or bank inspection teams must be rectified on time Response: Acceptable Risk
Failure to obtain information during wire transfer	Likely	Major	=3(High)	Obtain information of applicant & Beneficiary. Stop the Transaction. Transaction is not allowed until risk is reduced Response: Unacceptable Risk
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely	Major	=3(High)	Obtain information of applicant & Beneficiary. Preserve the information for minimum 5 years. Response: Unacceptable Risk.
Failure to scrutinize staff properly	Unlikely	Major	=2(Medium)	Concerned division will scrutinize staff properly before appointment. Response: Acceptable Risk
Failure to circulate BFIU guidelines and circulars to branches	Unlikely	Major	=2(Medium)	Concerned division must circulate BFIU guidelines and circulars to branches. Response: Acceptable Risk
Inadequate training/workshop arranged on AML & CFT	Unlikely	Major	=2(Medium)	Bank shall take adequate measure to provide proper training to Staff members. Response: Acceptable Risk
No independent audit function to test the AML program	Unlikely	Major	=2(Medium)	Bank must be introduced to independent audit function to test the AML program. Response: Acceptable Risk

KYC Documentation

Annexure-B

Customer type	Standard Identification document	Document for verification of source offunds	Document or strategy for Verification of
Individuals	➢Passport ➢National Id Card ➢Birth Registration Certificate (Printed copy, with seal& Signature from the Registrar) ➢Valid driving license(if any) ➢Credit Card (if any) ➢Any other documents that satisfy to the bank. NB: But in case of submitting the birth registration certificate, any other photo id (issued by a Government department or agency)of the person has to be supplied with it. If he does not have a photo id, then a certificate of Identity by any renowned people has to be submitted According to the bank's requirement. That certificate must include a photo which is duly attested by the signing renowned person. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.	➢Salary Certificate (for salaried person). ➢ Employed ID(For ascertaining level Of employment). ➢Self declaration acceptable to the bank. (commensurate with declared occupation) ➢Documents in support of beneficial owner's income(income of house wife, students etc.) ➢Trade License if the customer declared to be a businessperson ➢TIN(if any) ➢Documents of property sale. (if any) ➢Other Bank statement(if any) ➢Document of FDR encashment (if any) ➢Document of foreign remittance (if any fund comes from outside the country) ➢Document of retirement benefit. ➢Bank loan.	• Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old).The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Joint Accounts	• Passport • National Id Card • Birth Registration Certificate • (Printed copy, with seal & • signature from the Registrar) • Valid driving license (if any) • Credit Card (if any) • Any other documents (photo) that satisfy to the bank.	• Salary Certificate (for salaried person). • Employed ID (For ascertaining level of employment). • Self-declaration acceptable to the bank. (commensurate with declared occupation) • Documents in support of beneficial owner's income (income of house wife, students etc.) • Trade License if the customer declared to be a business person • TIN (if any) • Documents of property sale. (if any) • Other Bank statement (if any) • Document of FDR • encashment (if any) • Document of foreign remittance • (if any fund comes from outside the country) • Document of retirement benefit. • Bank loan	• Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency

Sole Proprietorships or Individuals doing business	• Passport • National Id Card • Birth Registration Certificate Printed copy, with seal & signature from the Registrar) • Valid driving license (if any) • Credit Card (if any) • Rent receipt of the shop (if the shop is rental) • Ownership documents of the shop (i.e purchase documents of the shop or inheritance documents) • Membership certificate of any association. (Chamber of comers, market association, trade association i.e.; Hardware association, cloth merchant association, hawker's association etc. • Any other documents that satisfy to the bank.	• Trade License • TIN • Self declaration acceptable to the bank. (commensurate with nature and volume of business) • Documents of property sale. (if injected any fund by selling personal property) • Other Bank statement (if any) • Document of FDR encashment (if any fund injected by en-cashing personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan (if any) • Personal borrowing (if any)	• Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official • Copy of utility bill/ utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency

Partnerships	• Partnership deed/ partnership letter • Registered partnership deed (if registered) • Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. • Passport of partners • National Id Card of partners • Birth Registration Certificate of partners (Printed copy, with seal & signature from the Registrar) • Valid driving license of partners (if any) • Credit Card of partners (if any) • Rent receipt of the shop (if the shop is rental) • Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents) • Membership certificate of any association. (Chamber of comers, market association, trade association i.e.; Hardware association, cloth merchant association, hawker's association etc. • Any other documents that satisfy to the bank.	• Trade License • TIN • Documents of property sale. (if injected any fund by selling personal property of a partner) • Other Bank statement (if any) • Document of FDR encashment (if any partner injected capital by enchasing Personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan • Personal Borrowing (if any)	• Acknowledgement receipt of thanks letter through postal department • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official • Copy of utility bill /utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency

Private Limited Companies	• Passport of all the directors • National Id Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • List of directors • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company.	• A copy of last available financial statements duly authenticatedby competent authority • Other Bank statement • Trade License • TIN • VAT registration • Bank loan	

Public Limited	• Passport of all the directors • National Id Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form - XII • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company.	• A copy of last available financial statements duly certified by a professional accountant • Other Bank statement (if any) • Trade License • TIN • Cash flow statement • VAT registration • Bank loan • Any other genuine source	

Government-Owned entities	• Statue of formation of the entity • Resolution of the board to open an account and identification of those who have authority to operate the account. • Passport of the operator (s) • National Id Card of the operator (s)	N/A	N/A
NGO	• National Id Card of the operator (s) • Passport of the operator(S) • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Documents of nature of the NGO • Certificate of registration issued by competent authority • Bye-laws (certified) • List of Management Committee/ Directors	• A copy of last available financial statements duly certified by a professional accountant. • Other Bank statement • TIN • Certificate of Grand / Aid	

Charities or Religious Organizations	• National Id Card of the operator (s) • Passport of the operator (s) • Resolution of the Executive • Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the Organisations • Certificate of registration issued by competent authority (if any) • Bye-laws (certified) • List of Management Committee/ Directors	• A copy of last available financial statements duly certified by a professional accountant • Other Bank statement • Certificate of Grant / Aid/ donation • Any other legal source	

Clubs or Societies	• National Id Card of the operator (s) • Passport of the operator (s) • Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the Organisations • Certificate of registration issued by competent authority (if any) • Bye-laws (certified) • List of Management Committee/ Directors	• A copy of last available financial statements duly certified by a professional (if registered) • Other Bank statement • Certificate of Grant / Aid Subscription • If unregistered declaration of authorized person/ body.	

Trusts, Foundations or similar entities	• National Id Card of the trustee (s) • Passport of the trustee(S) • Resolution of the Managing body of the Foundation/Association to open an account and identification of those who have authority to operate the account. • Certified true copy of the Trust Deed • Bye-laws (certified) • Power of attorney allowing transaction in the account.	• A copy of last available financial statements duly certified by a professional (if registered) • Other Bank statement • Donation	

Financial Institutions (NBFI)	• Passport of all the directors • National Id Card of all the directors • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form - XII • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company.	• A copy of last available financial statements duly certified by a professional accountant. • Other Bank statement • Trade License • TIN • VAT registration • Cash flow statement	

Embassies	• Valid Passport with visa of the authorized official • Clearance of the foreign ministry • Other relevant documents in support of opening account	• N/A	

Red Flags pointing to Money Laundering

Annexure-C

- The client cannot provide satisfactory evidence of identity.
- Situations where it is very difficult to verify customer information.
- Situations where the source of funds cannot be easily verified.
- Transactions in countries in which the parties are non-residents and their only purpose is a capital investment (they are not interested in living at the property they are buying).
- Frequent change of ownership of same property in unusually short time periods with no apparent business, economic or other legitimate reason and between related persons.
- Client wants to re-sell Property shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.
- Client wishes to form or purchase a company whose corporate objective is irrelevant to the client's normal profession or activities, without a reasonable explanation.
- The client sets up shell companies with nominee shareholders and/or directors.
- Client repeatedly changes Attorneys within a short period of time without any reasonable explanation.
- Client purchases property in names of other persons or uses different names on offers to purchase, closing documents and deposit receipts.
- Client deposits a large amount of cash with you to make payments which are outside of the client's profile.
- Client negotiates a purchase but wants to record a lower value on documents, paying the difference "under the table", (inadequate consideration).
- Client's documents such as identification, statement of income or employment details are provided by an intermediary who has no apparent reason to be involved, (the intermediary may be the real client).
- Transaction involves legal entities and there is no relationship seen between the transaction and the business activity of the buying company, or the company has no business activity.
- Client requests the firm to act as his agent in obtaining high sum bankers' drafts, cashiers' cheques and other cash equivalent or near cash monetary instruments or in making wire transfers to and from other banks or financial institutions, (anonymity).
- Divergence from the type, volume or frequency of transactions expected in the course of the business relationship.
- Client gives power of attorney to a non-relative to conduct large transactions (same as above).
- Use of letters of credit to move money between those countries, where such trade would not normally occur and / or is not consistent with the customer's usual business activity. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.
- The method of payment requested by the client appears inconsistent with the risk characteristics of the transaction. For example receipt of an advance payment for a shipment from a new seller in a high-risk jurisdiction.
- The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or that includes changes in regard to the beneficiary or location of payment without any apparent reason.
- Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction

of same business entity are indicators for TBML. In this regard the study of foreign exchange remittances may help detect the offence.

- The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities or sensitive / non co-operative jurisdictions.
- The commodity is transshipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense.
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.
- Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management.

Red Flags pointing to Financing of Terrorism

Behavioral Indicators:

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

Indicators linked to the financial transactions:

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

Multiple cash deposits in small amounts in an account followed by a large wire transfer to another

country.
Use of multiple, foreign bank accounts.

Annexure D

Walk-in / One-off / Online Customers

Bangladesh Bank vide their BFIU Circular -10 dated 28/12/2014 instructed us to obtain satisfactory evidence for identification of applicant / bearer who does not maintain account with us for conducting One off / Online transaction. All Branches / Concerned division of Head Office are therefore requested to preserve the following information along with appropriate documentary evidence before making transaction.

Customer's Name :	
Father's Name :	Mother's Name :
Date of birth :	Nationality :
Address :	
Documents (NID / Passport / BIN) to be obtained Number of NID / Passport / BIN:	
Telephone / Mobile Number :	
Source of Fund :	
Purpose of Deposit/ Withdrawal of Fund:	
Value of Transaction :	
Date	Signed