Introduction

Money Laundering and Terrorist Financing now a days is one of the greatest challenges that the Government and the Financial Industry face in the modern financial system. As a part of Government's efforts Bangladesh Financial Intelligence Unit (BFIU) issued series of instructions to the Scheduled Banks and Non-Bank Financial Institutions for taking effective steps to combat the money laundering activities and terrorist financing in the country's financial area.

In order to streamline the Anti-Money Laundering systems and procedures and to define the duties and responsibilities of the officials at different levels of Management these guidelines have been approved by Board in its 40th Meeting dated October 18, 2012 in the light of "Guidance Notes on Prevention of Money Laundering and Terrorist Financing" issued by BFIU vide BFIU circular no 04 dated September 16, 2012, Money Laundering Prevention Act 2012 and Anti Terrorism Act 2009 (as amended in 2012) for meticulous compliance by all concerned. This guideline is now modified to commensurate with the updated laws and regulations.

Chapter 1:
Background

1.1 Introduction

- These Guidelines have been prepared to facilitate the implementation of the Money Laundering Prevention (Amendment) Act 2015, Anti Terrorism (Amendment) Act 2013, the Rules and Directives of BFIU.

- The management of our Institution views money laundering prevention as part of their risk, management strategies and not simply as a stand-alone as required by the legislation.

1.2 What is Money Laundering?

- As defined in Section 2(V) of Money Laundering Prevention Act 2012
  - Money Laundering Prevention (Amendment) Act 2015'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, instigate or counsel to commit any offences mentioned above;

- "The U.S. Customs Service, an arm of the Department of the Treasury, provides a lengthy definition of money laundering as "the process whereby proceeds, reasonably believed to have been derived from criminal activity, are transported, transferred, transformed, converted or intermingled with legitimate funds for the purpose of concealing or disguising the

true nature, source, disposition, movement or ownership of those proceeds. The goal of the money-laundering process is to make funds derived from, or associated with, illicit activity appear legitimate."

- Another definition of Money Laundering under U.S Law is, "... the involvement in any one transaction or series of transactions that assists a criminal in keeping, concealing or disposing of proceeds derived from illegal activities."

- The EU defines it as "the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime."

1.3 Reason behind Money Laundering

Criminals engage in money laundering for three main reasons:

- First, money represents the lifeblood of the organization that engages in criminal conduct for financial gain because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and further the interests of the illegal enterprise, and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

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

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

1.4 Why we must combat Money Laundering

- Money Laundering has potentially devastating economic, security, and social consequences. Money Laundering is a process vital to making crime worthwhile. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences that result.

- Money Laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult.

- Money Laundering distorts asset and commodity prices and leads to misallocation of resources. For financial institutions it can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability and even systemic crises.

- 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.

- The International Money Fund has estimated that the magnitude of money laundering is between 2 and 5 percent of world gross domestic product, or at least USD.800 billion to USD.1.5 trillion. In some countries, these illicit proceeds dwarf government budgets, resulting in a loss of control of economic policy by governments.

- 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 officials and governments 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.

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

1.5 How to combat Money Laundering

- One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. The adoption of "know your customer" is not only a principle of good business but is also an essential tool to avoid involvement in money laundering.

- In complying with the requirements of the Act and in following these Guideline Notes the branches should at all times pay particular attention to the fundamental principle of good business practice – 'know your customer'.

1.6 The Money Laundering Cycle/Stages

- There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewellery) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities).

- Despite the variety of methods employed, the laundering is not a single act but a process accomplished in 3 basic stages which may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity.

Placement – the physical disposal of the initial proceeds derived from illegal activity. In other way Placement is when the cash proceeds from a criminal activity (the dirty money) first enter the financial system. For example, stolen goods are sold for cash, which is then deposited into a bank or FI's account. Cash can also be placed into the financial system by:

- Depositing relatively small amounts of cash into several bank or FI's accounts to avoid detection.
- Buying foreign currency, international money orders, bank drafts, travelers' cheques or other instruments with the cash.
- Buying high-value real estate.
- Buying business assets and equity investments.

Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. Other word, layering takes the form of a series of transactions designed to distance the money from the initial criminal activity, so that investigators will not be able to follow the trail and identify the perpetrators. Layering often involves the movement of funds from one country to another via electronic transfers.

- Electronic funds transfer between non-existent I fictitious companies.
- Paying large financial debts from an account funded by criminal money.
- Depositing or clearing foreign bank drafts and travelers' cheques.
- Capital market investments.

Integration – the provision of apparent legitimacy to wealth derived criminally. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds. Integration means that the proceeds of layering are finally moved back into the financial system in such a way that they appear to be normal business funds.

- Sale of legitimate businesses purchased with the proceeds of criminal money.
- Loan transaction, where the loan is secured on a criminally funded asset.
- Sale of property initially purchased with the proceeds of criminal money.
- Sale of stocks and shares.

- The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap. How the basic steps are used depends.

1.7 What is Terrorist Financing?

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

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

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

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

According to the article 7 of the Anti-Terrorism (Amendment) Act, 2013 of Bangladesh, financing of terrorism means:

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

Offences relating to financing terrorist activities.–

1. If any person or entity supplies, receives, collects or arranges any money, service or any other property, either from legitimate or illegitimate source, with the intention of the same to be used in full or partially –

   a. In the act of terrorism, or
   b. By the terrorist person(s) or entity(s) for any objective or believe to be used by them

   Then the persons or the said entity shall be deemed to have committed the offence of financing terrorist activities.

2. In framing charge of financing in terrorism, this will not depend on whether the aforesaid money, service or property as mentioned in sub-section 1, really used in any act, direction,

intention or efforts of terrorism or related to any specific act of terrorism.

3. If any person found guilty of any act as described in sub-section 1, he will be punished with imprisonment for maximum 20 years and minimum 04 years, and in addition double the amount of money involved in any such offense or taka 10 lac, whichever is higher, will be fined.

1.8 The link between Money Laundering and Terrorist Financing

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

Chapter 2:
Vulnerabilities of Financial Institutions
2.1 Vulnerabilities of Products and Services

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

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

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

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

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

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

2.1.7 Loan Backed Money Laundering

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

2.2 Structural Vulnerabilities

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

Chapter 3:
AML and CFT Policy of The UAE-Bangladesh Investment Company Limited

3.1 Overview

Money Laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities. The term "Money Laundering" is also used in relation to the financing of terrorist activity (where the funds may, or may not, originate from crime). In conducting business with due skills, care and diligence, company should comply with relevant laws, rules, regulations, codes and standards of good practice and anti-money laundering procedures should be strictly followed. Because company employees may personally be liable if any deviation is found in his/her assigned duties. The financial institution recognizes that the fight against money laundering is a team effort and has drawn a policy to combat this threat.

3.2 Policy Objective

→ Broad Objective

The objective, therefore, would be to prevent and fight Money Laundering and Terrorist Financing activity, by establishing governing standards to insulate the institution from being used as a component of financial system to launder money.

→ Specific Objective

Beside these broad objectives, the specific objectives include:

1. Enable the institution to conduct clean, commercial business, conforming to standards set by FI and Banking industry; within the framework designed by regulations and Head Office.
2. To build up awareness amongst the staff.
3. To focus on methods of Prevention of Money Laundering.
4. To prevent use of Institution's products or services for money laundering.
5. To prevent damage to the Institution's name and reputation by associating with money launderers.
6. To ensure that the institution complies with money laundering legislation / regulations.
7. To comply with applicable laws in Bangladesh with reference to ML and adhere to standards accepted internationally by the financial world on the subject.

3.3 Policy Scope

This policy addresses the responsibility of management and employees for:

- Preventing, detecting, monitoring and reporting suspected, confirmed, detected money laundering issues;
- Client identification and verification ("Know Your Customer") or KYC;
- All suspicious transactions to be noted and escalated to senior management whenever appropriate.

- Ensure suspicious transactions are reported to the CAMLCO at Head Office who will determine whether the report is required to be sent to the regulators.
- Provide the CAMLCO at the Head Office with all reasonable access to information that may be ofassistance to him in carrying his duties.
- Records are kept for all data obtained for the purpose of identification.
- Employees are trained on a regular basis on anti-money laundering measures.

3.4 Procedure

As financial institutions are committed to the prevention of money laundering, the management of UBICO has taken the following program:

- Formation of Central Compliance Unit (CCU) at Head Office headed by Chief Anti Money Laundering Compliance Officer (CAMLCO). He will examine the report received and if deemed necessary will report to BFIU for information.

- Appropriate customer identification, record keeping and reporting are primary points of consideration. The institution has a policy to keep all related documents / records for a minimum of five years even after closure of account.

Compliance is the responsibility of each employee. Therefore, all guidelines related to AML are regularly updated and circulated and ensured that all staffs are aware of the local AML laws, internal guidelines and other policies and procedures.

Chapter 4:
Compliance Requirements
4.1 Compliance Requirement under the Laws

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

According to section 25 of Money Laundering Prevention (Amendment) Act, 2015 FI's responsibilities (including other responsibilities mentioned in Rules) to prevent money laundering are –

a) To maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
b) to preserve previous accounts and records of transactions of any customer's account for at least 5(five) years from the date of closure;
c) To provide with the information maintained under clauses (a) and (b) to BFIU from time to time, on its demand;
d) if any suspicious transaction or attempt of such transaction as defined under clause (z) of section 2 is observed, to report the matter as suspicious transaction report to BFIU immediately on its own accord.

According to section 16 of Anti Terrorism (Amendment) Act, 2013, FI's responsibilities to combat financing of terrorism are –

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

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

(3) If any reporting agency fails to comply the provisions of sub-section (1), such agency shall be imposed penalty not exceeding Tk 25 (twenty five) lac set by Bangladesh Bank and Bangladesh Bank can suspend license of any branch, booth or agent of such agency.

(4) If the Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of any reporting agency fails to comply the provisions of sub-section (2), then chairman of the Board of Directors, or the Chief Executive Officer, as

the case may be, shall be imposed penalty not exceeding Tk 25 (twenty five) lac set by Bangladesh Bank and Bangladesh Bank can suspend such person from his position or inform the proper authority to take necessary action against such person.

4.2 Compliance Requirements under Circulars

4.2.1. Policies for Prevention of Money Laundering and Terrorist Financing

In pursuance of section 16 (2) of Anti Terrorism (Amendment) Act, 2013, and BFIU circular no. 04, dated 16 September 2012, all FIs must have their own policy manual approved by their Board of Directors/topmost management to prevent money laundering and terrorist financing. This policy manual must be in conformity with international standard and laws and regulations in force in Bangladesh. FIs shall from time to time review and confirm the meticulous compliance of the circulars issued by Bangladesh Bank.

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

In compliance with this circular, UBICO has formulated its own money laundering policy, duly approved by its Board. This Policy Guidelines was formulated in 2012 and now amended in accordance with the changes in relevant acts and present scenario. The Head of Finance is the CAMLCO of UBICO and Deputy Head of Finance is assigned as Deputy CAMLCO in compliances with the relevant guidance and instructions of the regulator. However, having no branch yet, UBICO needs no BAMLCO.

4.2.2. Financial Institutions shall not open or maintain numbered or anonymous account.

4.2.3 Customer Identification:

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

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

4.2.4 To protect UBICO from risks of money laundering or/and terrorist financing by customers

willful or unwilling activities, the Money Laundering Prevention Policy Manual shall clearly state how to conduct Customer Due Diligence at different stages such as:

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

a. To be sure about the customer's identity and underlying purpose of establishing relationship with the institution, UBICO shall collect adequate information up to its satisfaction.

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

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

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

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

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

4.2.5 Politically exposed Persons (PEPs)

While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised. Following instructions shall have to be followed to ensure Enhanced Due Diligence:

- a risk management system shall have to be introduced to identify risks associated with the accounts opening and operating of PEPs;
- take reasonable measures to establish the source of wealth and source of funds;

- ongoing monitoring of the transactions have to be conducted; and
- the FIs should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

All instructions as detailed for PEPs shall be equally applicable if business relationship is established with family members and close associates of these persons who may pose reputational risk to the FI. The above instructions shall also be applicable to customers or beneficial owners who become PEPs after business relationship have been established.

4.2.6 Appointment and Training

a. Employee Screening:

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

b. Training for the officials:

To ensure proper compliance of ML/TF activities UBICO shall arrange suitable training for its officials.

c. Education and training for customers:

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

4.3 Suspicious Transaction Reporting (STR)

According to the provision of section 25 (1) (d) of Money Laundering Prevention (Amendment) Act, 2015, UBICO have to report BFIU proactively and immediately, facts on suspicious, unusual or doubtful transactions likely to be related to money laundering. BB has the power to call STR from UBICO related to financing of terrorism according to section 15 of Anti Terrorism (Amendment) Act, 2013.

e. Targeted Financial Sanctions:

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

f. Supervisory Power of Bangladesh Bank:

According to the provision laid down in the section 23 of Money Laundering Prevention

(Amendment) Act, 2015 and section 15 of Anti Terrorism (Amendment) Act, 2013, BFIU is the core implementing agency. The major supervisory powers are:

Under Money Laundering Prevention (Amendment) Act, 2015, BFIU shall have the following powers and responsibilities to prevent money laundering and to resist any such activities:

(i) to analyze or review information related to cash transactions and suspicious transactions received from any reporting organization and to collect additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data on the same and, as the case may be, provide with the said information to the relevant law enforcement agencies for taking necessary actions;
(ii) ask for any information or obtain a report from reporting organizations whatever is laid down in any other law;
(iii) issue an order to any reporting organization to suspend or freeze transactions of any account for a period not exceeding 30 (thirty) days if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing any offence. Provided that such order may be extended for additional period of a maximum of 7 (seven) times by 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account;
(iv) issue, from time to time, any direction necessary for the prevention of money laundering to the reporting organizations;
(v) carry out on-site inspections of the reporting organizations, if required;
(vi) arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by BFIU;
(vii) Carry out any other functions necessary for the purposes of this Act.

The power and responsibilities of Bangladesh Bank under section 15 of Anti-Terrorism (Amendment) Act, 2013 are as follows: The Bangladesh Bank shall have the power and authority to take necessary measures to prevent and detect transaction intended to commit offence under ATA through any banking channel, and for that matter BB is empowered and authorized to –

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

terrorist financing; and

- Provide training to staff and officers of FIs for the purpose of detection and prevention of suspicious transactions as may be connected with terrorist financing.

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

4.4 Penalties under MLPA:

According to section 25 (2) of Money Laundering Prevention (Amendment) Act, 2015, if any reporting organization violates the directions mentioned in sub-section (1) of section 25 of Money Laundering Prevention (Amendment) Act, 2015, BFIU may-

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

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

In addition to the above mentioned provisions there are some new provisions of penalties in the section 23 of Money Laundering Prevention (Amendment) Act, 2015. These are:

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

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

(5) If any reporting organization fails to comply with any instruction given by BFIU under this Act, BFIU may impose a fine on such organization which may extend to a maximum of Taka 5 (five)

lacs at the rate of Taka 10 (ten) thousand per day for each of suchnon compliance and if any organization is fined more than 3(three) times in 1(one) financial year, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.

(6) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by BFIU under clause (c) of sub-section 23(1) of MLPA, 2015, BFIU may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.

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

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

4.5 Penalties under ATA:

The provision laid down in section 16 of Anti-Terrorism (Amendment) Act, 2013:

As per section 16(3), if any reporting agency fails to comply with the directions issued by Bangladesh Bank under section 16(1), the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding Taka 25 (twenty five) lacs and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

As per section 16(4), if any Board of Directors or the Chief Executive Officer in lieu of the Board of directors, whatever the name is, fails to comply with the direction of Bangladesh Bank then the Chairman or the Chief Executive Office will be liable to pay the Tk. 25 lacs as determined and directed by Bangladesh Bank and Bangladesh Bank may remove the said person and may inform the relevant authority take appropriate action again the person.

As per section 16(5), if the reporting agency fails to pay or the Chairman or Chief Executive

Officer fails to pay the fined amount or does not pay the fine as determined and directed by Bangladesh Bank as mentioned in section 3 and 4 above, Bangladesh Bank may recover the amount from the reporting agency by debiting its accounts maintained with any bank, financial institute or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

4.6 Self-Assessment

According to section 8 of BFIU circular no. 12 dated 29 June 2015, UBICO shall establish half yearly self-assessment procedure that will assess how effectively the FI's AML/CFT program is working. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment shall conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions and recommendations. The self-assessment shall advise management whether the internal procedures and statutory obligations of the FI have been properly discharged.

Once the Self Assessment is complete, observations and findings to be communicated to the Managing Director.

4.7 INDEPENDENT TESTING PROCEDURE

In UBICO, Independent Testing will be conducted at least annually as per Guidance Notes on Prevention of Money Laundering and Terrorist Financing issued by BFIU vide BFIU circular no 04 dated September 16, 2012. Issues identified in the self assessment will be specifically examined in this test, status of the issues with any mitigation measure(s), will be carefully examined in this test. Every Independent Test will conclude with a rating and submit the report to CCU.

Chapter 5:
Compliance Program

UBICO shall establish and maintain an effective AML/CFT program that includes at least the followings:

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

The compliance program shall be documented, approved by the Board of Directors and communicated to all levels of the organization.

5.1 Development of Internal Policies, Procedures and Controls

5.1.1 Internal Policy

To meet the requirement of the "Guidance Notes on Prevention of Money Laundering and Terrorist Financing" UBICO must develop, administer, and maintain its own AML/CFT policy that ensures and monitors compliance with the laws, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes. The written AML/CFT compliance policy at a minimum shall establish clear responsibilities and accountabilities within their organizations to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the Act. The policies shall be tailored to the institution and would have to be based upon an assessment of the money laundering and terrorist financing risks, taking into account the financial institution's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering and terrorist financing. It shall include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. The procedures shall address its Know Your Customer (KYC) policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transaction, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness. It shall also include a description of the roles the AML/CFT Compliance Officer(s)/Unit and other appropriate personnel will play in monitoring compliance and effectiveness of AML/CFT policies and procedures. It shall develop and implement screening programs to ensure high standards when hiring employees. Implement standards for employees who consistently fail to perform in accordance with an AML/CFT framework. It should incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel. It shall have the arrangements for program continuity despite changes in management or employee composition or structure. The AML/CFT policies shall be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/operational changes, such as additions or amendments to existing AML/CFT related rules and regulations or business. In addition the policy shall emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and shall set forth the consequence of non-

compliance with the applicable laws and the institution‘s policy, including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any association with money laundering and terrorist financing activity. The most important element of a successful AML/CFT program is the commitment of senior management, including the chief executive officer and the board of directors, to the development and enforcement of the AML/CFT programs which can deter criminals from using their facilities for money laundering and terrorist financing, thus ensuring that they comply with their obligations under the laws.

5.1.1.1 Components of Policy

The statement of compliance policy should at a minimum include:

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

5.1.1.2 Communicating the Policy

As part of its AML/CFT policy, UBICO should communicate clearly to all employees on annual basis through a statement from the chief executive officer that clearly sets forth its policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement should evidence the strong commitment of the institution and its senior management to comply with all laws and regulations designed to combat money laundering and terrorist financing.

5.1.2 Procedures

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

5.1.3 Internal Control Mechanism

The compliance program also relies on the variety of internal controls, including management report, built-in safeguards and exception report that keep the program working. FATF recommendation 18 requires that financial institutions have an internal control program.

The following elements should be included in the operational controls of any policy:

- Statement of responsibility for compliance with policy;
- Customer due diligence;
- Customer identification/verification
- Additional know your customer information
- High risk customers
- Non face to face business (if applicable)
- Handling of politically exposed persons
- Monitoring for suspicious transaction/activity;
- Cooperation with the authorities;
- Record keeping;
- Screening of transactions and customers;
- Training and awareness;
- Adoption of risk management practices and use of a risk-based approach

5.2 Establishment of Central Compliance Unit

To ensure compliance of the Money Laundering Prevention (Amendment) Act, 2015 and Anti Terrorism (Amendment) Act 2013, each financial institution will establish arrangement for internal monitoring and control through formation of a Central Compliance Unit (CCU) under the leadership of a high official. In order to accomplish properly the jurisdiction and function of the CCU, each financial institution will determine institutional strategy and program. CCU will issue the instructions to be followed; these instructions will be prepared on the basis of combination of issues in monitoring of transactions, internal control, policies and procedures from the point of view of preventing money laundering & terrorist financing. CCU shall be dedicated solely to UBICO‘s related responsibilities and perform the compliance functions.

The responsibilities of a CCU shall include:

a. preparing an overall assessment report after evaluating the self-assessment reports submitting it with comments and recommendations to the chief executive of the bank;
b. Preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Audit Department on that particular quarter;
c. Submitting a half-yearly report to BFIU within 60 days after end of a quarter.

5.3 Appointment of Chief AML/CFT Compliance Officer

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

5.3.1 Position of CAMLCO

The Chief AML/CFT Compliance Officer will be the head of CCU. The designated CAMLCO, directly or through CCU, should be a central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to financial institution's AML/CFT program.

The position of the CAMLCO cannot be lower than the third rank in seniority in organizational hierarchy.

5.3.2 Qualification and experience

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

5.3.3 Responsibilities:

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

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

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

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

5.4 Employee Training and Awareness Program

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

5.4.1 The Need for Staff Awareness

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

5.4.2 Education and Training Programs

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

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

5.4.3 General Training

A general training program should include the following:

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

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

5.4.4 Job Specific Training

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

5.4.4.1 New Employees

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

5.4.4.2 Front Office Employee

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

5.4.4.3 Credit Officers:

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

5.4.4.4 Senior Management/Operations Supervisors and Managers

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

5.4.4.5 Senior Management and Board of Directors

Money laundering and terrorist financing issues and dangers shall be regularly communicated to the board. Money laundering and terrorist financing poses to the institution. Major AML/CFT compliance related circulars/circular letters issued by BB shall also be placed to the board to bring it to the notice of the board members.

5.4.4.6 AML/CFT Compliance Officer

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

5.4.5 Refresher Training

UBICO will take necessary steps to ensure a regular training program for its new staffs covering relevant aspects.

5.5 Independent Audit Function

5.5.1 Why the audit function is necessary

To ensure the effectiveness of the AML/CFT program, UBICO shall assess the program regularly and look for new risk factors.

5.5.2 Whom they report

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

5.5.3 The ways of performing audit function

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

5.5.4 External Auditor

External UBICO shall allow the external Auditor to review the adequacy of control related to risk factors/areas of its operation/activities.

Chapter 6:

Customer Due Diligence

Customer Due Diligence (CDD) is a fundamental principle of all anti-money laundering controls. Each staff of the FI is required to perform due diligence on all prospective clients prior to opening an account. This process is completed by fulfilling the documentation requirements and also a "Know Your Customer" profile which is used to record a client's identity & source of wealth at it's most basic level. Obligations for institution's staff to perform customer due diligence have been strengthened with the introduction of a four step process. The steps are:

- Required to verify the identity of customers
- Required to take reasonable measures to identify the beneficial owner of accounts
- Required to obtain information on the purpose and intended nature of the business relationship
- Required to perform ongoing monitoring of the business relationship in order to ensure that the financial transactions are consistent with the institutions knowledge of the customer's activity, including source of funds.

The inadequacy or absence of KYC standards can subject institutions to serious customer and counter party risks, especially reputational, operational, legal and concentration risks, It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to institutions (e.g. through the withdrawal of funds by depositors, the termination of inter-institution facilities, claims against the institution, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

Reputational risk poses a major threat to institutions, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a institution's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Institutions are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme.

Operational risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of institutions' programmes, ineffective control procedures and failure to practice due diligence. A public perception that a institution is not able to manage its operational risk effectively can disrupt or adversely affect the business of the institution.

Legal risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a institution. Institutions may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, institutions can, for example, suffer fines, criminal liabilities and special penalties imposed by regulators. Indeed, a court case involving a institution may have far greater cost implications for its business than just the legal costs. Institutions

will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

Supervisory concern about concentration risk mostly applies on the assets side of the balance sheet. As a common practice, supervisors/regulators not only require institutions to have information systems to identify credit concentrations but most also set prudential limits to restrict institutions' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a institution to measure its concentration risk. This is particularly relevant in the context of related counter parties and connected lending.

CHAPTER 7:

Record Keeping

7.1 Statutory Requirement

UBICO shall observe its duties under Section 25 (1) of Money Laundering Prevention (Amendment) Act, 2015, and retain correct, full records of customers 'identification and transactions, to retain the records of customers 'identification and transactions at least for five years including requirements of legislation and Bangladesh Bank directives are fully met and that law seeks to establish.

7.2 Training Records

UBICO will comply with the regulations concerning staff training, they shall maintain training records which include: -

(i) details of the content of the training programs provided;
(ii) the names of staff who have received the training;
(iii) the date/duration of training;
(iv) the results of any testing carried out to measure staffs understanding of the requirements; and
(v) an on-going training plan.

7.3 Sharing of Record/Information of/To a Customer

Under MLPA 2015, and ATA, 2013, UBICO shall not share account related information to investigating authority i.e., ACC or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh Bank.

Chapter 8:

Suspicious Transaction Report /Suspicious Activity Report

As per the Money Laundering Prevention Act, 2012, UBICO shall submit STR/SAR through AML Circulars issued by Bangladesh Bank time to time.

8.1 Identification and Evaluation of STR/SAR

a) Identification:

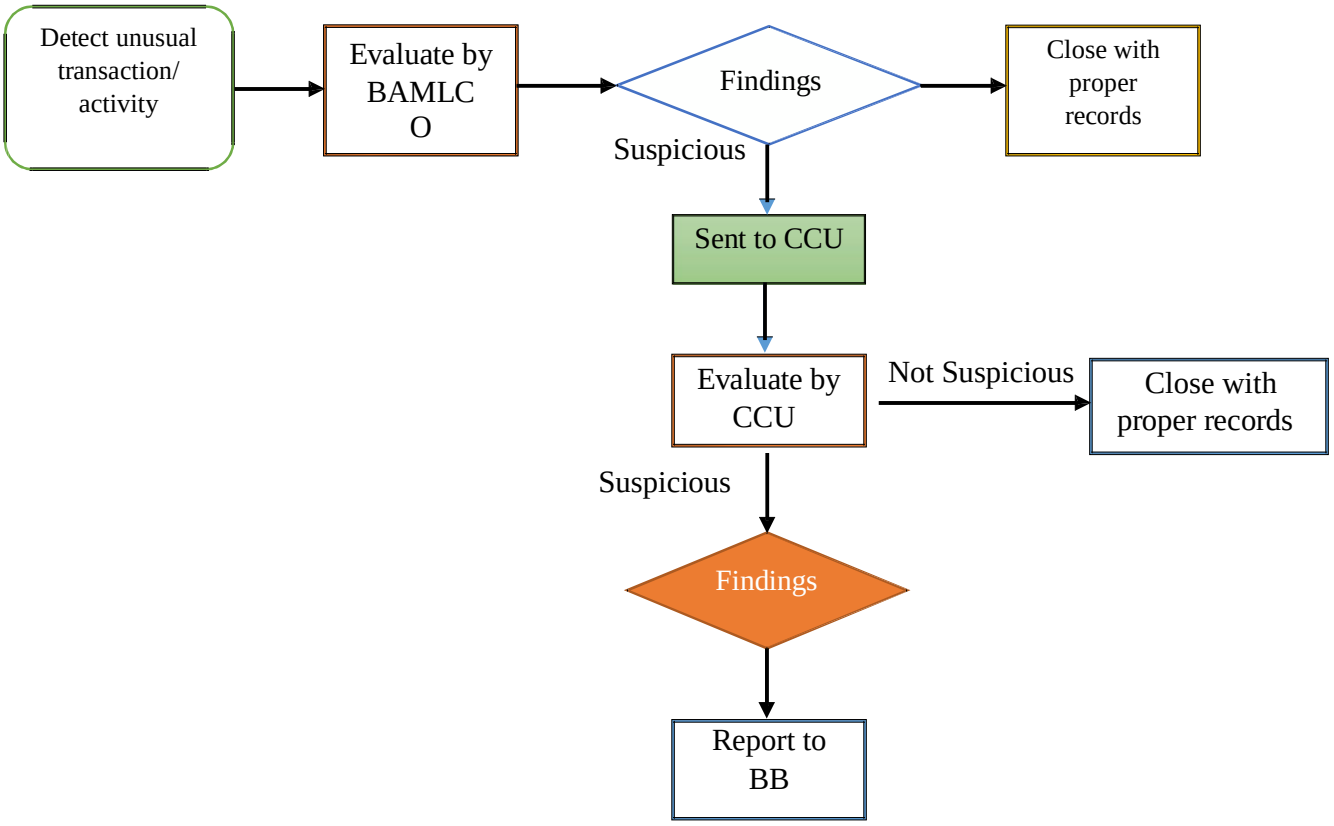
This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of financial institutions monitoring of unusual transactions may be automated, manually or both. Some financial institutions use specialized software to detect unusual transactions or activities, however, the use of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

b) Evaluation:

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

c) Disclosure:

UBICO shall submit STR/SAR to Bangladesh Bank if it is suspicious of any transection as below:



Chapter 9:

RISK BASED APPROACH

9.1 UBICO needs to take appropriate steps to identify and assess their *money laundering* and *terrorist financing* risks arisen from or through its customers, products, business practices and jurisdictional risks. This is a legal obligation as the Rule 21 of MLP Rules 2013 contains that every Reporting Organization - Financial Institution (RO-FI) shall conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. Rule 21 also contains that FIs like UBICO shall utilize this risk assessment report after having vetted by BFIU.

9.2 RISK AND RISK MANAGEMENT

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

For the AML & CFT aspects, UBICO should take into account two main sources of ML and TF risks i.e., ML & TF risk arises from or through doing their business and non-compliance of regulatory requirements.

In assessing and mitigating ML & TF risks, UBICO should consider all the financial products and services it provides to its customers, which are associated with different ML & TF risks, namely corporate finance and investment services: where UBICO provides corporate finance products such as lease finance, term loan, project finance, working capital finance, short-term finance and investment services to corporations, large and medium size enterprises and institutions. UBICO does not accept deposit in any form, nor does it provide consumer loan or credit card etc to any customer.

UBICO needs to take into consideration the following segment of its business in assessing ML & TF risk:

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

The risk management framework at a glance

1. **Risk identification:**

Identify the main ML&TF risks:
- customers
- products & services
- business practices/delivery methods or channels
- region/jurisdiction

Identify the main regulatory risks:
- failure to report STRs/SARs
- inappropriate customer verification
- inappropriate record keeping
- lack of AML/CFT program

2. **Risk assessment/evaluation**

Measure the size & importance of risk:
• Likelihood – chance of the risk happening
• Impact – the amount of loss/damage if the risk happened
• Risk Score / level of risk = likelihood X impact

3. **Risk treatment**

Manage the business risks:
• minimize and manage the risks
• apply strategies, policies and procedures
Manage the regulatory risks:
• put in place systems and controls
• carry out the risk plan and AML&CFT program

4. **Risk monitoring and review**

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

9.3 RISK IDENTIFICATION

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

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

- **Regulatory risk**

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

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

9.4 RISK ASSESSMENT

Once the risks are identified, the next step is to ***assess*** the relevant risk, which is a blend of related likelihood and impact. '***Likelihood***' means the chance of the risk occurring and '***Impact***' means the effect of any particular activity/transaction. UBICO formulates its 'likelihood' and 'impact' measures as shown next, following regulator's guidance in this respect, to evaluate the risks identified.

Likelihood scale

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

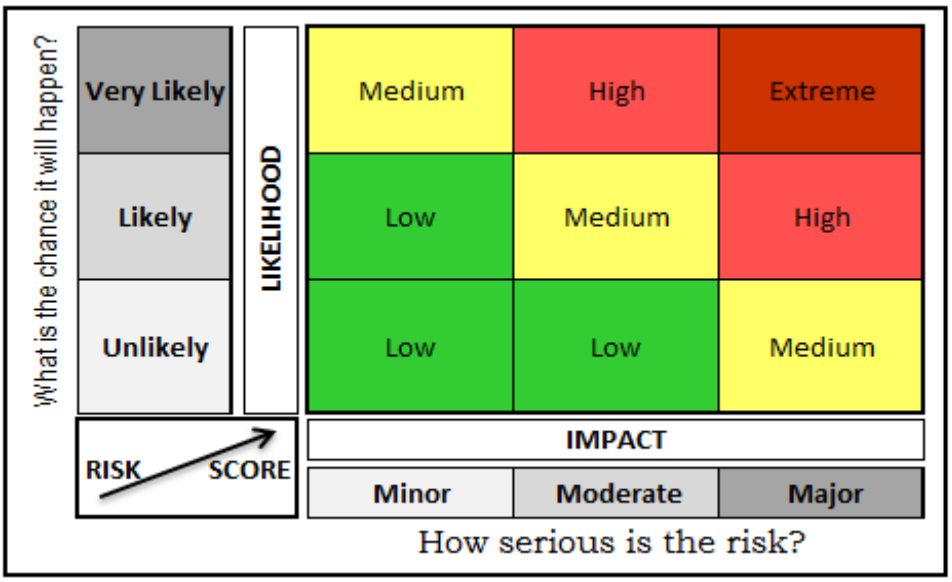
Impact scale

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 and/or terrorism financing impact.
Minor	Minor or negligible consequences or effects.

After registering a risk in the risk register, judgmental ***likelihood*** and ***impact*** are then assigned to every risk as shown in the following risk register. From blending of the likelihood and impact, the 'Risk Score' of each risk is worked out.

Likelihood X Impact = Risk Score

As shown above, each individual risk's 'likelihood' and 'impact' possibility and their combination determine its risk score. For simplicity, rather than using software or mathematical formulation, following matrix may conveniently be used to determine the risk score of any identified risk where its related 'likelihood' and 'impact' are assigned -



9.5 RISK MANAGEMENT

Now the risk score is known and populated in the Risk Register (extract below), the very next step is how management will manage or treat those risk.

9.5.1 Risk Register of UBICO

Risk Group	Customers			
Risk	**Likelihood**	**Impact**	**Risk Score**	**Treatment/Action**
New customer	Likely	Moderate	Medium	Preserve and verify KYC.
Customer whose business address and registered office are in the different geographic locations	Likely	Moderate	Medium	- Collection of details information on business and registered office.
A customer comes with early settlement of loan account	Likely	Moderate	Medium	Checking of source of fund.
Customer under separate regulator	Likely	Moderate	Medium	- Collecting update license issued by the regulator. - Follow up regulatory approval letter.

Risk Group	Products and Services			
Risk	**Likelihood**	**Impact**	**Risk Score**	**Treatment/Action**
Non face to face business relationship or transaction	Likely	Moderate	Medium	Collection of more security documents.
Loan	Likely	Moderate	Medium	Analysis of financial data.

Risk Group	Business Practice/Delivery Methods or Channels			
Risk	**Likelihood**	**Impact**	**Risk Score**	**Treatment/Action**
Direct to the customer	Unlikely	Minor	Low	Checking of standard ID.
Phone	Likely	Moderate	Medium	Proper record keeping of communication.
Email	Likely	Minor	Low	Maintaining proper record keeping.

9.5.2 Risk Treatment

It needs putting into place strategies, policies and procedures to help reduce (or treat) the risk. Examples of a risk reduction or treatment step are:

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

9.5.3 Risk Appetite – In risk management, risk appetite is the level of risk an organization is prepared to accept. It is usually expressed as an acceptable/unacceptable level of risk.

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

9.5.4 Monitor and Review - Keeping records and regular evaluation of the UBICO's 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, UBICO should develop a method to check regularly whether risk based approach of AML, CFT program is working correctly and effectively. If not, UBICO 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.

9.6 RISK VARIABLES

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

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

9.7.2 COUNTER MEASURES FOR RISK

UBICO should examine, as far as reasonably possible, the background and purpose of all complex, unusual large and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, UBICO should conduct enhanced due diligence (EDD), which include:-

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

9.7.2 Simplified CDD measures

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

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold)
- Reducing the frequency of customer identification updates
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

9.8 ONGOING DUE DILIGENCE

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

10.1 Future Plan

a) UBICO shall encourage / allow its employee to attend relevant workshop & seminar to update with AML & CFT procedure;
b) UBICO shall introduce regular assessment procedure;
c) UBICO shall communicate to its employees about its policy on prevention of money laundering or terrorist financing.

10.2 Conclusion

The management of UBICO is fully aware that the financial system shall not be and cannot be used as a channel for criminal activities.

Taking effective action against money laundering and terrorist financing makes a positive contribution to the well-being and safety of UBICO and its employees and shareholders.

List of Abbreviations

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