# Prime Finance & Investment Limited

## Anti Money Laundering & Combating Terrorist Financing

## Policy Document

## FOREWORD

Money Laundering has emerged as the alarming financial crime in the global economy. Hence, the fight against money laundering has become imperative for the global financial systems. In this context, the fight against money laundering is a priority for Prime Finance & Investment Limited so as to prevent such illicit activities thereby protecting the Company and to entire financial systems from the potential risk posed by such financial crimes.

We understand that the fight against money laundering is a team effort. Adherence to "Anti Money Laundering Policy" is essential for the safety and ethical standards of the Company's operations. We are committed to preventing ourselves from being used for criminal purposes. We are always ready to extend cooperation to regulators, prosecutors and other Government authorities to stop the Company from being used for illicit activities.

Our policy is to conduct business in compliance with all applicable laws and regulation and stop criminals from using our products and services for the purpose of money laundering. Our cooperation to our regulators is in its entirety wherein we aim to maintain the highest operating standards to safeguard the interest of our customers, our shareholders, our staff and the communities where we operate.

In conducting business with due skill, care and diligence we always seek to comply with both the letter and spirit of relevant laws, rules, regulation, code and standards of good practice. We aim to promptly address any irregularities that may arise, as we believe in transparency in our financial and regulatory reporting with swift disclosure of any breaches.

This Document lays down the Anti Money Laundering Policies and Procedures to be followed by personnel working in each functional area. However, as part of our commitment for continual improvement, each reader and follower of this manual is encouraged to identify improvement opportunities and bring them to the attention of the appropriate authority for evaluation and subsequent incorporation in the manual.

The contents of this Policy are strictly confidential and must not in any way be divulged to any person not in the service of the Company.

(Asad Khan)
Managing Director

# CONTENTS

## 1.1 Introduction

Money laundering is a process whereby identity of illegally possessed money is changed so that it appears to have originated from a legitimate source. It is the process by which dirty money is made to look clean. In other words, Money Laundering is the process whereby criminals attempt to hide and disguise the true origin and ownership of the fund. The source may include terrorism, organized crime, fraud, drug trafficking, human trafficking, etc. The money earned from above source is called "Dirty Money".

Money laundering is a major concern to the governments and regulatory authorities all over the world as it poses great threat to the international economy. Managing reputational risk and legal risk are of the top priority in the financial industry. It has been recognized as a major social problem and crime by the governments around the world.

Financial Institution is the medium for channeling the illegally or criminally earned money into the financial system. The simplest way to clean the illegally earned money is to bring-in such money to the financial system through different means such as deposits of cash, traveler's cheques, drafts, electronic transfers and other financial instruments.

## 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 are disguised to conceal their illicit origins. Money Laundering is defined in Section 2 (v) of the Money Laundering Prevention Act 2012 as follows:

‖ Money Laundering means –

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

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

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

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

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

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

(v) Converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;

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

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

(viii) Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

## 1.3 Stages of Money Laundering

There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or 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). There are a number of crimes where the initial proceeds usually take the form of cash that needs to enter the financial system by some means. Bribery, extortion, robbery and street level purchases of drugs are almost always made with cash. These proceeds of crime have to enter the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated. Despite the variety of methods employed, money laundering is not a single act but a process accomplished in 3 basic stages which are as follows:

**Placement** –

The physical disposal of the initial proceeds derived from illegal activity.

**Layering** –

Separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

**Integration** –

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

## 1.4 Defining Terrorist Financing

Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. According to the article 7 of the Anti Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means:

Offences relating to financing terrorist activities:

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

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

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

(4) If any person or entity knowingly instigates another person or entity to provide or receive or make arrangement for money, services, material support or any other property in such a manner where there are reasonable grounds to believe that the same have been used or may be used in full or partially by a terrorist person or entity or group or organization for any

purpose, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

## 1.5 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.

## 1.6 Objectives, Scope and Application of the Policy

The primary objective of the Policy is to prevent the Company (Prime Finance & Investment Limited) from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

Purposes proposed to be served by the Policy are:

i) To prevent criminal elements from using the Company for money laundering activities

ii) To enable the Company to know/understand the customers and their financial dealings better which, in turn, would help the Company to manage risks prudently

iii) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures

iv) To comply with applicable laws and regulatory guidelines

v) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

vi) To ensure that employees are accountable for carrying out their compliance requirements

This Policy is applicable to head office & all branch offices of the Company.

## 1.7 Communicating the Policy

Managing Director of the Company will communicate all employees on annual basis through a statement that sets forth its policy against money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

## 2.1 Definition of a Customer

A customer, for the purpose of the Policy is defined as:

i) a person or an entity that has a business relationship with the Company

ii) one on whose behalf the TDR/FDR/Loan account is maintained (i.e. the beneficial owner)

iii) beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

iv) any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company.

## 2.2 Key Elements of the Policy

A. Customer Acceptance Policy (CAP)
B. Customer Identification Procedures (CIP)
C. Monitoring of Transactions
D. Risk management
E. Training Program
F. Internal audit and inspection system
G. Record Keeping
H. Duties / Responsibilities and Accountability

## 2.2 (A) CUSTOMER ACCEPTANCE POLICY (CAP)

Company's Customer Acceptance Policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship in the Company broadly are:

i) No account (deposit or lease/loan) be opened in anonymous or fictitious/benami name(s)/entity(ies).

ii) Accept customers only after verifying their identity, as laid down in Customer Identification Procedures (discussed later).

iii) Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers. Also, a profile of each customer will be prepared based on risk categorization.

iv) Comply with the documentation requirements and other information to be collected, as per MLPA, ATA and guidelines/instructions issued by BFIU.

v) Not to open an account or close an existing account, where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed due to non-cooperation of the customer.

vi) Identity of a new customer to be checked so as to ensure that it does not match with any person with known criminal background or banned entities such as individual terrorists or terrorist organizations etc.

vii) Decisions to enter into business relationships with higher risk customers, such as public figures or politically exposed persons shall be taken exclusively at senior management level.

viii) Conduct extensive due diligence for an individual/entity with a high net worth whose/which source of funds is unclear.

ix) Consider customers' background, country of origin, public or high profile position, business activities or other risk indicators.

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

## 2.2 (A) (i) Indicative Guidelines

***Trust/Nominee***

Branch/offices shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branch/offices may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.
As an example, verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', branches shall take steps to verify the founder managers/directors and the beneficiaries, if defined.

***Companies and firms***

Branch/offices need to be vigilant against business entities being used by individuals as a front for maintaining relationship with Company. Branch/ office may examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

***Politically Exposed Persons (PEPs)***

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign or within the country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branch/office shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

Branch/office shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to make business relationship for PEP shall be taken at a senior level and shall be subjected to monitoring on an ongoing basis. The above norms may also be applied to the family members or close relatives of PEPs.

***Profile based on categorization***

Branches/offices shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients, business and their location etc. For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified may be categorized as low risk.

Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, Government departments & Government owned companies, regulators and statutory bodies etc.
In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

Customers those are likely to pose a higher than average risk to the Company may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Enhanced due diligence measures are to be applied based on the

risk assessment, thereby requiring intensive due diligence for higher risk customers, especially those for whom the sources of funds are not clear.

## 2.2 (B) CUSTOMER IDENTIFICATION PROCEDURES (CIP)

Customer identification requires identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Thus, the first requirement of Customer Identification Procedures (CIP) is to be satisfied that a prospective customer is actually who he/she claims to be. The second requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the banking relationship. This would enable risk profiling of the customer and also to determine the expected or predictable pattern of transactions.

Identification data, as under, would be required to be obtained in respect of different classes of customers:

For customers that are natural persons:

- Names
- Parents Names
- Date of Birth
- Address/location details (permanent, current)
- Recent photograph
- National ID card
- Passport/driving license, if any
- Copy of utility bill
- TIN
- Job ID card, in case of service holder

In respect of NRB, introduction and authentication/ verification of signatures to be made by a bank/embassy/ High Commissioner/Consulate/ Notary Public/ Persons known to the Company would be required in addition with the above.

For customers that are legal persons:

1. Legal status of the legal person/entity through proper and relevant documents.
2. Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person/entity is established and verified.
3. Understand the ownership and control structure of the customer and determine the natural and legal person.

Relevant documents mean-

For Company:

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

- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts; Satisfactory evidence of the identity of the account signatories, Subsequent changes to signatories must be verified;

- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;

- Copies of the list/register of directors.

A letter issued by a corporate customer is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. When authorized signatories change, care shall be taken to ensure that the identities of all current signatories have been verified. In addition, periodic enquiries can be effective to know whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken.

For Society/Associates/Clubs/Trust:

A copy of Resolution, trust deed, copy of bye-laws, if any, and certificate of registration in case of registered clubs, societies, association and trust.

For Firms:

In the case of Partnership firm, partnership letter/deed and introduction from a person known to the Company.

Companies Registered Abroad:

Particular care shall be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. In such a case, carry out effective checks on source of funds and the nature of the activity to be undertaken during the proposed business relationship. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

Wherever applicable, information on the nature of business activity, location, mode of payments, volume of turnover, social and financial status etc. will be collected for completing the profile of the customer.

Customer Profile:

'Customer Profile' of individual/legal entity shall be incorporated in the opening form, covering the following information, where applicable:-

1) Occupation
2) Source of funds
3) Monthly Income
4) Annual turnover
5) Date of Birth/incorporation
6) Existing credit facilities etc.

The Customer profiles incorporated in the opening forms have to be reviewed once in a year. Customers will be classified into three risk categories namely High, Medium and Low, based on the risk perception. The risk categorization will be reviewed periodically.

The Customer Identification Procedures are to be carried out at the following stages:

i) While establishing a business relationship;

ii) When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

iii) Customer identification data (including photograph/s) shall be periodically updated after the account is opened. Such verification shall be done at least once in two years in case of low risk category customers and not less than once in a year in case of high and medium risk customers.

## 2.2 (C) MONITORING AND REPORTING OF TRANSACTIONS

### 2.2 (C) *(i) Monitoring of Transactions*

Ongoing monitoring is an essential element of effective KYC procedures. Branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account.

### 2.2 (C) *(ii) High-risk accounts*

Branches/Office shall pay special attention to all complex & unusual patterns and unusually large transactions. Large transaction through cash inconsistent with the normal and expected activity shall pay special attention. Transactions involving large deposit in the form of TDR/FDR and loan against it or withdraw the fund before maturity require special attention. These types of transaction shall require approval from the senior level. High-risk accounts have to be subjected to intensify monitoring. Company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

### 2.2 (C) (iii) Cash Transactions

The Company shall transact preferably through account payee cheque/pay order. Authentic banking channel shall be used for disbursement of loan, payment of interest and payment of principal amount after maturity of deposit and in contrary accept deposit and interest income preferably through account payee cheque/pay order.

## 2.2 (C) (iv) PROCESS AND PROCEDURES TO MONITOR *SUSPICIOUS TRANSACTIONS*

The final output of all compliance programs is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the risk for the Company.

### 2.2 (C) (iv) (*a*) Definition OF STR/SAR

Generally STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be usual manner.

In the section (2) (z) of MLPA, 2012 —suspicious transaction means such transactions which deviates from usual transactions; of which there is ground to suspect that,

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

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

### 2.2 (C) (iv) (*b)* Obligations Of Suspicious Report

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

### 2.2 (C) (iv) (*c)* Identification of STR/SAR:

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

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

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

**2.2 (C) (iv) (d*)* Suspicious Customer Identification Circumstances:**

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

**2.2 (C) (iv) (e*)* Suspicious Activity in Credit Transactions:**

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

**2.2 (C) (iv) (f*)* Suspicious Commercial Account Activity**:

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

**2.2 (C) (iv) (g*)* Suspicious Activity in an FI Setting:**

- Request of early encashment without providing valid/justifiable reason
- A TDR (or whatever) calling for the periodic payments in large amounts.
- Lack of concern for significant tax or other penalties assessed when cancelling a deposit.

**2.2 (C) (iv) (h*)* STR/SAR Procedure:**

Branches are required to record and report all transactions of suspicious nature in deposit and loan etc, to Head Office and a master database shall be maintained regarding the suspicious transaction at Head Office.

The procedure to be followed is as under -

*Business Relationship Officer* ⟹ *BAMLCO* ⟹ *CAMLCO* ⟹ *CCU* ⟹ *BB*

**2.2 (C) (iv) (i*)* Terrorist finance**

In case the name of any banned organization is noticed as payee/endorsee/applicant, the first dealing officer shall report the same to the BAMLCO. Reporting of such transactions as and when detected is to be done as under:

*Reporting by Reporting to*

*Business Relationship Officer* ⟹ *BAMLCO* ⟹ *CAMLCO* ⟹ *CCU* ⟹ *BB*

Transactions which are of suspicious nature and required to be reported to BFIU-BB are given in Annexure I.

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Transactions that involve large amounts of cash inconsistent with the normal and expected profile of the customer will be subjected to detailed scrutiny. A record of such transactions will be preserved and maintained for the period as prescribed in MLPA.

### 2.2 (C) (iv) (j*)* Closure of Accounts

Where the appropriate KYC measures could not be applied due to non furnishing of information and/or non-cooperation by the customer, the account can be considered for closure or terminating the business relationship. Before exercising this option, all efforts will be made to obtain the desired information and, in the event of failure, due notice, will be given to the customer explaining the reasons for taking such a decision. In all cases, the controlling authority at the Head office shall be the competent authority to permit closure of such accounts. Customer's information shall be preserved till five years of closure of accounts.

## 2.2 (D) Risk Management

The Company has put in place an effective KYC program in place by establishing appropriate procedures and ensuring their effective implementation covering proper management oversight, systems and controls, segregation of duties, training and other related matters.

Responsibility has also been explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The nature and extent of due diligence will depend on the risk perceived by the branch/head office. However, while preparing customer profile head office/branches shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function shall provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. It would be ensured that the audit mechanism is staffed adequately with individuals who are well versed in such policies and procedures. The compliance in this regard may be put up before the Audit Committee of the Board by HO (Inspection) on half yearly intervals.

Company's Internal Audit of compliance with AML Policy will provide an independent evaluation of the same including legal and regulatory requirements. However, primary responsibility of ensuring implementation of AML/CFT Policy and related guidelines will be vested with the respective controlling Office.

Suitable checks and balances in this regard will be put in place at the time of introducing new products/procedures as also at the time of review of existing products/ procedures for overall risk and compliance management. For this purpose, each controlling office will designate an official as Money Laundering Compliance Officer (MLCO) who would ensure proper implementation and Reporting as per provisions of this Policy.

### 2.2 (D) (i) KYC for the existing accounts

While the KYC will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. On the basis of materiality and risk the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural /legal person and those of the ' beneficial owners'.

## 2.2 (E) EMPLOYEE TRAINING AND AWARENESS PROGRAM

As per FATF recommendation, a formal AML/CFT compliance program shall include an ongoing employee training program. Employees in different business functions need to understand how the Company's policy, procedures, and controls affect them in their day to day activities. As per AML circular, the Company shall arrange suitable training for their officials to ensure proper compliance of money laundering and terrorist financing prevention activities.

### 2.2 (E) (i) The Need for Staff Awareness

All 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 to ensure that all staff (permanent/contractual) are fully aware of their responsibilities.

### 2.2 (E) (ii) Education and Training Programs

All relevant staff shall be educated in the process of the —"Know Your Customer" requirements for money laundering and terrorist financing prevention purposes. The training in this respect shall 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 shall 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.

### 2.2 (E) (iii) General Training

A general training program shall 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;

### 2.2 (E) (iv) Job Specific Training

Job specific AML/CFT trainings are discussed below:

### 2.2 (E) (iv) (a) Employee Training

All employee training programs will have a module on KYC Standards/AML/CFT Measures so that employees are adequately trained on KYC/AML/CFT procedures. Records to be kept of all formal training conducted. These records have to include the names and other relevant details, dates and locations of the training.

### 2.2 (E) (iv) (b) Recruitment/Hiring of Employees

KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse channels of the Company. The Company will put in place necessary and adequate screening mechanism as an integral part of its recruitment/hiring process of personnel.

### 2.2 (E) (iv) (c) New Employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions shall be provided to all new employees who are likely to be dealing with customers, irrespective of the level of seniority. They shall 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.

### 2.2 (E) (iv) (d) Relationship Officers

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 shall be made aware of the organization's reporting system for such transactions. Training shall 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.

### 2.2 (E) (iv) (e) Processing (Back Office) Staff

The staffs, who receive completed FDR/loan application forms, must be appropriately trained in the processing and verification procedures. In addition, the need to verify the identity of the customer must be understood, and training shall be given in the organization's account opening and customer/client verification procedures. Such staff shall be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML/CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

### 2.2 (E) (iv) (f) Credit Officers:

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

### 2.2 (E) (iv) (g) Audit and compliance staff

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

### 2.2 (E) (iv) (h) 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 responsibility for supervising or managing staff. This will include the offences and penalties arising from the laws for non-reporting and for assisting money launderers and terrorist financers; internal reporting procedures and the requirements for verification of identity and the retention of records.

### 2.2 (E) (iv) (i) Senior Management and Board of Directors

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

### 2.2 (E) (iv) (j) 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 require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

### 2.2 (E) (v) Refresher Training

In addition to the above, training may have to be tailored to the needs of specialized areas of the institution's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities.

### 2.2 (E) (vi) Customer Education

The business relationship officers would be specially trained to educate the customers regarding the objectives of the KYC program. The Company 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.

### 2.2 (E) (vii) Training Procedures

An effective training program can be developed by taking the following steps:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience shall be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key shall be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.

Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file

## 2.2 (F) INTERNAL AUDIT AND INSPECTION SYSTEM

Employees of the internal audit must be sufficiently qualified to ensure that their findings and conclusions are reliable. The responsibilities of internal auditors are:

- Address the adequacy of AML/CFT risk assessment;
- Examine/attest the overall integrity and effectiveness of the management systems and the control environment;
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- Determine personnel adherence to the Company's AML/CFT policies, procedures and processes;
- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- Assess the adequacy of the Company's processes for identifying and reporting suspicious activity;
- Communicate the findings to the board and/or senior management in a timely manner;
- Recommend corrective action for deficiencies;
- Tracks previously identified deficiencies and ensure that management corrects them.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- Determine when assessing the training program and materials:
    - The importance that the board and the senior management place on ongoing education, training and compliance
    - Employee accountability for ensuring AML/CFT compliance
    - Comprehensiveness of training, in view of specific risks of individual business lines.
    - Frequency of training
    - Coverage of Company's policies, procedures, processes and new rules and regulations
    - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity
    - Penalties for noncompliance and regulatory requirements

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

## 2.2 (F) (i) Independent Testing Procedure

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

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

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

- sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- test of the validity and reasonableness of any exemption granted by the financial institution; and
- test of the record keeping system according to the provisions of the laws. Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline.

## 2.2 (G) RETENTION OF RECORDS

According to Section 25 (1) of Money Laundering Prevention Act, 2012, retain correct and full records of customers' identification and transactions while operating an account of a customer, and to retain the records of customers' identification and transactions at least for five years after closing of relationships with the customers. The records prepared and maintained by the Company on its customer relationship and transactions shall be:

- Customer Profiles
- Reports made to government authorities concerning suspicious customer activities relating to possible money laundering or other criminal conduct together with supporting documentation
- Records of all formal anti money laundering training conducted which include the names and business units of attendees and dates and locations of the training; and
- Any other document required to be retained under applicable money laundering laws/regulations.

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

i. closing of an account
ii. providing of any financial services
iii. ending of the business relationship;
iv. commencement of proceedings to recover debts payable on insolvency.

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

### 2.2 (G) (i) Retrieval of Records

The Company shall have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form, and that can be reproduced and recollected without undue delay. It is not always necessary to retain documents in their original hard copy form; it may also retain records in microchips or electronic form, as appropriate, and that these can be reproduced without undue delay.

### 2.2 (G) (ii) STR and Investigation

A report that has submitted as suspicious transaction to BFIU or where it is known that a customer or any transaction is under investigation, then any records related to the customer or transaction shall not be destroyed without the consent of the BFIU or conclusion of the case even though the five-year limit may have been elapsed.

To ensure the preservation of such records the Company shall maintain a register or tabular records of all investigations and inspection made by the investigating authority or Bangladesh Bank and all disclosures to the BFIU. The register shall be kept separate from other records and contain as a minimum the following details:

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

### 2.2 (G) (iii) Training Records

The Company 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.

### 2.2 (G) (iv) Branch Level Record Keeping

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

i. Information regarding Identification of the customer,
ii. KYC information of a customer,
iii. Transaction report,
iv. Suspicious Transaction/Activity Report generated from the branch,
v. Exception report,
vi. Training record,
vii. Return submitted or information provided to the Head Office or competent authority.

### 2.2 (G) (v) Sharing of Record/Information of/To a Customer

Under MLPA 2012, and ATA, 2009 (as amended in 2012), the Company 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.

## 2.2 (H) ESTABLISHMENT OF CENTRAL COMPLIANCE UNIT

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

The responsibilities of a CCU shall include:

i. preparing an overall assessment report after evaluating the self assessment reports received from the branches and submitting it with comments and recommendations to the Managing Director of the Company;

ii. preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Audit Department on that particular quarter;

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

## 2.2 (H) (i) Appointment of Chief AML/CFT Compliance Officer

According to Bangladesh Bank guidelines Prime Finance require to designate a Chief AML/CFT Compliance Officer (CAMLCO) at its head office who will have 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.

## 2.2 (H) (i) (a) Position of CAMLCO:

The Chief AML/CFT Compliance Officer (CAMLCO) will be the head of Central Compliance Unit (CCU). The CAMLCO, directly or through CCU, shall be a central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to Company AML/CFT program. The position of the CAMLCO cannot be lower than the third rank in seniority in organizational hierarchy.

## 2.2 (H) (i) (b) Qualification and experience:

The CAMLCO shall have a working knowledge of the diverse financial products offered by the the Company. 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 shall have a minimum of seven years of working experience, with a minimum of three years at a managerial/administrative level.

## 2.2 (H) (ii) Responsibilities:

The Company shall prepare a detailed specification of the role and obligations of the CAMLCO. Depending on the scale and nature the 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 Company'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 Company'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 shall be considered by the Company;

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:

   a) reviewing transactions referred by branch compliance officers as suspicious;

   b) reviewing the transaction monitoring reports (directly or together with account management personnel);

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

   d) ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;

   e) 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;

   f) managing the process for reporting suspicious activity to BFIU after appropriate internal consultation;

### 2.2 (H) (iii) Branch Anti-Money Laundering Compliance Officer

The Company will appoint Branch Anti-Money Laundering Compliance Officer (BAMLCO) at each of their branches. BAMLCO will be the second man of a branch and have a minimum three year experience in related field. The responsibilities of a BAMLCO are as follows:

1. Manage the transaction monitoring process

2. Report any suspicious activity to Branch Manager, and if necessary to the CAMLCO Provide training to Branch staff

3. Communicate to all staff in case of any changes in national or its own policy

4. Submit branch returns to CAMLCO timely.

### 2.2 (H) (iv) Responsibilities of other Employees:

The table below details the individual responsibilities of the employees of the Company:-

| Function | Roles / Responsibilities |
|---|---|
| Relationship Officer | ▪ Perform due diligence on prospective clients prior opening an account<br>▪ Be diligent regarding the identification (s) of account holder and the transactions relating to the account<br>▪ Ensure all required documentation is completed satisfactorily<br>▪ Complete KYC profile for the new customers<br>▪ Ongoing monitoring of customer's KYC profile and transaction activity<br>▪ Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO |
| Operations Staff | ▪ Be diligence on transaction trends for clients<br>▪ Update customer transaction profiles in the ledger/system |
| Technology Manager | ▪ Ensures that the required reports and systems are in place to maintain an effective program |
| Risk Management /Internal Control Officer | ▪ Perform Risk Assessment for the Business<br>▪ Perform periodic Quality Assurance on the program in the unit<br>▪ Communicate updates in laws and internal policies |
| Managing Director | ▪ Overall responsibility to ensure that the Business has an AML program in place and it is working effectively |

## 3.0 PENALTIES UNDER MLPA:

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

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

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

In addition to the above mentioned provisions there are some new provisions of penalties in the section 23 of MLPA, 2012. These are:

a) If any reporting organization fails to provide with the requested information timely under this section, Bangladesh Bank may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches 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.

b) If any reporting organization provides with false information or statement requested under this section, Bangladesh Bank may impose a fine on such organization not less than Taka 20 (twenty)

thousand but not exceeding Taka 5 (five) lacs and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.

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

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

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

c) 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.

## 3.0 (i) PENALTIES UNDER ATA:

The provision laid down in section 16 (3) of Anti Terrorism (Amendment) Act, 2012, if any reporting agency fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding Taka 10 (ten) lacs and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

According to section 16 (4) if any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank according to sub-section 16 (3) of ATA, Bangladesh Bank may recover the amount from the reporting agency by debiting its accounts maintained in any bank or financial institution or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

## 4.0 SELF ASSESSMENT

As per AML circular 15, the Company is required to establish half yearly self assessment procedure that will assess how effectively the Company's AML/CFT program is working. This procedure will enable 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 Company have been properly discharged. Each branch will assess its AML/CFT activities covering the following areas on half yearly basis and submit the report to CCU within next 20 days:

- The percentage of officers/employees that received official training on AML/CFT;
- The awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and Bangladesh Bank's instructions and guidelines;
- The arrangement of AML/CFT related meeting on regular interval;
- The effectiveness of the customer identification during opening an individual, corporate and other account;
- The risk categorization of customers by the branch;
- Regular update of customer profile upon reassessment;
- Identification of Suspicious Transaction Reports (STRs);
- Maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents;
- The measures taken by the branch during opening of account of PEPs;

# List of Acronyms

| | |
|---|---|
| ACC | Anti Corruption Commission |
| AML/CFT | Anti-Money Laundering/Combating the Financing of Terrorism |
| ATA | Anti Terrorism Act |
| BAMALCO | Branch Anti-Money Laundering Compliance Officer |
| BB | Bangladesh Bank |
| BFIU | Bangladesh Financial Intelligence Unit |
| CAMALCO | Chief Anti-Money Laundering Compliance Officer |
| CAP | Customer Acceptance Policy |
| CCU | Central Compliance Unit |
| CDD | Customer Due Diligence |
| CIP | Customer Identification Procedure |
| FATF | Financial Actions Task Force |
| FDR/TDR | Fixed/Term Deposit Receipt |
| FIs | Financial Institutions |
| HO | Head Office |
| KYC | Know Your Customer |
| MLPA | Money Laundering Prevention Act |
| PEP | Politically Exposed Persons |
| STR | Suspicious Transaction Report |
| SAR | Suspicious Activity Report |