Anti-Money Laundering Guidelines [Revised]

Chapter I: Definition

1.1 Background
The methods and techniques of Money Laundering (ML) are ever evolving process and changing in response to developing counter measures. For that reason, Financial Action Task Force (FATF), the international standard setter on anti money laundering (AML) and combating terrorist financing (CFT), has revised its 40 (forty) recommendations for AML and 9 (nine) special recommendations for CFT.

In line with the international standards and initiatives, Bangladesh has also amended its Money Laundering Prevention Act (MLPA), 2002 and enacted MLPA, 2009. To combat Terrorism and Terrorist Financing Anti Terrorism Act (ATA), 2009 has also been enacted. Both the Acts have empowered Bangladesh Bank (BB) to perform the anchor role in combating ML&TF through issuing instructions and directives for reporting agencies including banks. In pursuance of section 16(2) of Anti Terrorism Act, 2009 and Anti Money Laundering Department’s letter dated 04.07.2006, all banks and financial institutions must have their own policy manual approved by their Board of Directors/topmost committee to prevent money laundering and terrorist financing. This policy manual must be in conformity with international standard and laws and regulations in force in Bangladesh. Banks and the financial institutions shall from time to time review and confirm the meticulous compliance of the circulars issued by Bangladesh Bank.

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

- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;
- The 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 an offense or offenses or from an act of participation in such an offense or offenses, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

The Financial Action Task Force on Money Laundering (FATF), which is recognized as the international standard setter for anti-money laundering (AML) efforts, defines the term “money laundering” succinctly as “the processing of…criminal proceeds to disguise their illegal origin” in order to “legitimize” the ill-gotten gains of crime.
Money Laundering is defined in Section 2 (3) of the Prevention of Money Laundering Act 2009 as follows:

Money Laundering means:
   i) Transfer, conversion, bringing/ remitting funds in and out of Bangladesh the proceeds or properties acquired through commission of a predicate offence [Mentioned in 1.3] for the purpose of concealing or disguising the illicit origin of the property or illegal transfer of properties acquired or earned through legal or illegal means.
   ii) To conduct, or attempt to conduct a financial transaction with an intent to avoid a reporting requirement under this Act (the MLPA, 2009).
   iii) To do or attempt to do such activities so that the illegitimate source of the fund or property can be concealed or disguised or knowingly assist to perform or conspire to perform such activities.

1.3 Predicate Offence

The offences from which the proceeds derived from committing or attempt to commit the following offences:
1  Corruption and bribery;
2  Counterfeiting currency;
3  Counterfeiting documents;
4  Extortion;
5  Fraud;
6  Forgery;
7  Illicit arms trafficking;
8  Illicit dealing in narcotic drugs and psychotropic substances;
9  Illicit dealing in stolen and other goods;
10  Kidnapping, illegal restraint, hostage-taking;
11  Murder, grievous bodily injury;
12  Woman and child trafficking;
13  Smuggling and unauthorized cross-border transfer of domestic and foreign currency;
14  Theft or robbery or Dacoity;
15  Trafficking in human beings and illegal immigration;
16  Dowry;
17  Terrorism and Terrorist Financing;
18  Counterfeiting and Piracy of Products;
19  Environmental Crime;
20  Sexual Exploitation;
21  Taking market advantage through transactions by using price sensitive information of the capital market before it becomes public and trying to control or manipulate the market to gain personal advantage (Insider trading and market manipulation);
22  Organized Crime and
23  Any other offence which Bangladesh Bank with the approval of the Government and by notification in the Official gazette declares as predicate offence for the purpose of this Act.

1.4 Property means:
   1. Any kind of assets, whether tangible or intangible, movable or immovable, however acquired; or
2. Cash, legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.

1.5 Stages of Money Laundering

Though money or other assets can be laundered by various methods, the money laundering process is normally but not necessarily, accomplished in three stages:

**Placement:** the initial deposit of illegally derived funds either through its introduction into the financial system; through the purchase of high value goods; or by physical cross border transportation.

**Layering:** a series of transactions or movement of funds with the aim of distancing them from their source.

**Integration:** reentry of funds into the legitimate economy through investment in: real estate, luxury assets or business ventures.

1.6 Reporting organization

1. Banks
2. Financial Institutions
3. Insurance companies
4. Money changers
5. Companies or organizations remitting or transferring money
6. Other business organizations approved by Bangladesh Bank
7. Stock Dealer and Stock Broker, [Here Stock Dealer and Stock Broker means the organizations Stock Dealer, Stock Broker and Authorized Representative) defined under section 2(i) and (j) of Securities and Exchange Commission Regulations -2000].
8. Portfolio Manager and Merchant Bank, [Here Portfolio Manager and Merchant Bank means the organizations (Merchant Bank and Portfolio Manager) defined under section 2(f) and (j) of Securities and Exchange Commission Regulations -1996].
10. Asset Manager, [Asset Manager means the organizations (Mutual Fund) defined under section 2 (s) of Securities and Exchange Commission Regulations – 2001]
11. Non Profit Organization/Institution, [Non Profit Organization/Institution means organizations or institutions licensed or registered under section 28 of the Companies Act (Bangladesh) -1994].
13. Such other organizations as the Bangladesh Bank with the approval of Government may notify from time to time.
1.7 Suspicious or unusual transaction

1. A transaction that substantially deviates from the usual norm by which that transaction is usually conducted, or
2. There is reasonable cause to believe that the transaction is related to any proceeds acquired through or earned from crime or predicate offence.

1.8 Why and How to Combat Money Laundering

Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a process vital to making crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. Money laundering diminishes government tax revenue and therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult.

In order to combat Money Laundering Bank should at all time pay particular attention to the fundamental principle of good business practice—’know your customer’ (KYC). Having a sound knowledge of a customer’s business and pattern of financial transactions and commitments is one of the best methods by which Bank and its Officials will recognize attempts at money laundering.

1.9 The Offence of Money Laundering and Punishment

01. For the purpose of this Act Money laundering shall be treated as an offence
02. Any person engaged in money laundering or abetting or aiding or conspiring in the commission of such offence shall be punished with imprisonment for a term not less than six months but which may extend to seven years and in addition to this property involved with the offence shall be forfeited in favor of the state.

2.0 Punishment for Violation of Freezing / Attachment Order

Whoever contravenes the freezing order or an order of attachment passed under this Act shall be punished with imprisonment of either description for a term which may extend to one year or with fine, up to taka five thousand or both.

2.1 Divulging of Information

1. No person shall, for the purpose of frustrating the investigation or making adverse influence over the investigation, divulge any information relating to investigation or other related information to any person agent or news media.
2. Any person, organization, agent or entity authorized under this Act during the period of his/her service contract period or after retirement will refrain himself/herself from using, publishing or divulging information collected, received, retrieved and known by himself/herself except for the purpose of the Act.
3. Whoever contravenes the provision of sub-section (1) and (2), shall be liable on conviction to imprisonment of either description for a term, which may extend to two years, or fine up to Taka ten thousand or both.
2.2 Obstruction or Non Co-Operation in Investigation, Failure to Report or Supply of Information:

1. Whoever i. obstructs or refuses to assist the concerned Officer engaged in investigation under this Act or
   ii. Fails to comply without reasonable ground with a reporting obligation or fails to supply information contemplated under this Act, shall be guilty of an offence under this Section.
2. Whoever contravenes the provision of sub-section (1) shall be liable on conviction to imprisonment for a term which may extend to one year, or a fine up to Taka five thousand or both.

2.3 Providing False Information to Banks / Financial Institutions

1. Nobody knowingly shall provide false information concerning the source of funds or the identity of any account holder or the beneficial owner or nominee.
2. A person who contravenes the provision of Sub-section (1) shall be liable on conviction for an imprisonment of either description which may extend to 1 year and / or a fine up to Taka fifty thousand or both.

2.4 Investigation, Prosecution etc.

Under this Act:

i. The offences under this Act considered as the scheduled offences of Anti-Corruption Commission Act, 2004 (Act V of 2004), will be investigated by Anti-Corruption Commission or by an Officer empowered by Anti-Corruption Commission for this purpose.
ii. The Offences will be prosecuted by the Special Judge court as appointed under Criminal Law Amendment Act. 1958 (Act XL of 1958).
iii. If any conflict arises regarding investigation, prosecution and other related provisions, etc. of this Act, the provision of Anti-Corruption Commission Act, 2004 and Criminal Law Amendment Act. 1958 shall prevail.

2.5 Offence Committed by Company:

1. If any offence under this Act committed by a company, every proprietor, director, manager, secretary, or other Officer or representative who is directly involved with the offence shall be deemed to be guilty of such offence: Provided that if any person as aforesaid is not able to prove that such offence has been committed without his knowledge or he has used due diligence to prevent such offence, Explanation: In this section - (a) “Company” means any statutory body, partnership concern, association, commercial organization or organization formed with one or more than one person; (b) “Director” means any partner or member of the Board of Directors, by whatever name it is called.
2. Registration of any company, if found engaged in money laundering activity either directly or indirectly, shall be liable to be cancelled.

2.6 Protection against Proceedings Undertaken in Good Faith

No suit, prosecution either civil or criminal or other legal proceedings shall lie against government or any government officials or any reporting organizations if any person is affected or likely to be affected due to the proceedings done in good faith under this Act.
2.7 RESPONSIBILITY OF REPORTING ORGANIZATIONS IN PREVENTING MONEY LAUNDERING:

1. For the purpose of preventing and identifying money laundering reporting organizations shall:
   - keep, during the operation of accounts, the correct and full information of identification of its clients and
   - In case of closed account of any client, keep previous records of transactions of such account for at least five years from the date of closure.
   - Provide, from time to time, the records kept under clause (a) and (b) to Bangladesh Bank time to time on demand from Bangladesh Bank.
   - Inform proactively and immediately Bangladesh Bank, facts on suspicious / unusual / doubtful or transactions likely to be related to money laundering.

2. If any reporting organizations violate the directions mentioned in sub-section (1) Bangladesh Bank shall take the following actions:
   - Bangladesh Bank may impose a fine of not less than Taka ten thousand and such fine may extend to Taka five Lac upon the defaulting reporting organizations.
   - Bangladesh Bank may cancel the registration of the company or cancel the license in addition to the fine mentioned in sub-section (a). The Bangladesh Bank shall inform the permit or license authority of the reporting organizations regarding their failure to keep and furnish information under sub-section (1) so that the concerned authority may, in accordance with the relevant law or rule or regulation framed there under, take necessary action against the concerned reporting organizations for their failure or negligence.

3. Bangladesh Bank will collect the penalty money imposed under subsection (2) in its self determined manner and shall deposit the collected money into the government treasury.

2.8 INSTITUTIONAL POLICY

In order to protect Banks reputation and to meet its legal and regulatory obligations, it is essential that Bank should minimize the risk of being used by Money Launderers. With that end in view it will be an obligatory responsibility for all Bank Official, customers and management of the Bank to realize and combat the situation on this critical risk issue.

✓ Establish clear lines of internal accountability, responsibility and reporting. Primary responsibility for the prevention of money laundering rests with the nature of business which must ensure that appropriate internal controls are in place and operating effectively and that bank Officials are adequately trained. The business is supported in meeting this responsibility by the Legal and Compliance function and by Bank Investigations.
✓ Given its importance in reputational and regulatory terms, the effectiveness of the money laundering prevention regime across all businesses should form part of the governance oversight responsibilities of all branch managers.
✓ Document, implement and maintain, procedures and controls which interpret Bank Policy and Bank Standards for each business in the context of applicable laws and
regulations and corporate ethical standards. Compliance with such procedures and controls and with Bank Policy and Bank Standards will be effectively monitored.

✓ Establish an effective ‘Know Your Customer’ Policy for the Branch Manager which will contain a clear statement of management’s overall expectation matching local regulations and establishing specific line of responsibilities.

✓ Co-operate with any lawful request for information made by government agencies during their investigations into money laundering.

✓ Support governments, law enforcement agencies and Bangladesh Bank in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal purposes.

✓ Report money laundering issues to Head Office Management on a regular basis. The Branch Manager responsible to combat Money Laundering shall determine and communicate the content, format and frequency for management reporting.

2.9 SENIOR MANAGEMENT COMMITMENT
The most important element of a successful anti-money-laundering program is the commitment of senior management, including the Chief Executive Officer and the Board of Directors, to the development and enforcement of the anti-money-laundering objectives which can deter criminals from using their facilities for money laundering, thus ensuring that they comply with their obligations under the law.

Senior management must send the signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of its anti money laundering policy the Bank will communicate clearly to all employees on an annual basis 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 Bank and its Senior Management to comply with all laws and regulations designed to combat money laundering. The statement of compliance policy is:

✓ That all employees of the Bank are required to comply with applicable laws and regulations and corporate ethical standards.

✓ That all activities carried on by the Bank must comply with applicable governing laws and regulations.

✓ That complying with rules and regulations is the responsibility of each individual in the Bank 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 is no excuse for non-compliance.

✓ That the statement should direct Officials to a compliance Officer or other knowledgeable individuals when there is a question regarding compliance matters.

✓ That a certification that Official will be held accountable for carrying out their compliance responsibilities.

3.0 DISCLAIMER
This Guideline is intended to provide general advice to the employees of BASIC Bank Limited. It should never be relied on as a substitute for Money Laundering Prevention Act 2009 and Bangladesh Bank Guidelines.
Chapter II: Process to Implement AML

1.1 Formation of Central Anti-Money Laundering Compliance Unit (CCU)

With a view to implementing any policy it is imperative that an organization should have an organogram depicting the position of people working there with job description and responsibilities having dot lines for making them accountable to the organization for their activities. Anti-money laundering program has been taken up as a serious and important policy to be implemented in our Bank for which a Central Compliance Unit [CCU] is functioning in the Bank headed by a senior executive.

The Central Compliance Unit shall directly report to the Managing Director through the Chief Anti Money Laundering Compliance Officer [CAMLCO]. The Central Compliance Unit shall report to the Regulatory Body i.e. Bangladesh Bank for any matter relating to money laundering or any transaction susceptible to money laundering under intimation to the Chief Anti Money Laundering Compliance Officer and the Managing Director.

1.2 Job description and responsibilities of Head of Central Compliance Unit:

i. To monitor, review and coordinate application and enforcement of the Bank’s compliance policies including Anti-Money Laundering Compliance Policy. This will include anti-money laundering risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transactions and account operational records.

ii. To monitor changes in laws, rules and regulations and also the instructions of Bangladesh Bank which may require the AML program to be revised from time to time.

iii. To respond to questions relating to compliance and concerns of employees and advise operational units in Head Office, Branches and Booth(s).

iv. To assist Operational Units in Head Office, Branches and Booth(s) in providing solutions to problems cropped up from activities or transactions related to money laundering.

v. To ensure that the Bank’s AML program is comprehensive and updated.

vi. To maintain ongoing awareness of new and changing business activities susceptible to money laundering risks and identify potential compliance issues deemed to be reasonably vulnerable to money laundering risks.

vii. To develop knowledge of all employees, particularly the compliance officers in respect of AML program.

viii. To develop and maintain ongoing relationships with regulatory authorities, external and internal audit teams, Head of Branches and Booth(s) for assisting them in early identification of issues which may be susceptible to money laundering risks.

ix. To assist in review of control procedures in the Bank so as to ensure legal and regulatory compliance and in the development of adequate testing procedures to detect and prevent lapses in compliance issues.

x. To monitor business self-testing for AML compliance and take corrective action.

xi. To manage Suspicious Activity Reporting Process which refers to:
   ✓ Reviewing transactions referred by operational units in Head Office, Branches and Booth(s) as suspicious.
   ✓ Reviewing the Transaction Monitoring Reports
   ✓ Ensuring that internal suspicious activity reports:
o are prepared as and when they appear to be appropriate.
o reflect the uniform standard for “suspicious activity involving possible money laundering established in the policy”.
o are accompanied by documentation of the Branches’ decisions to retain or terminate the account, as required under the policy.
o are advised to other branches who may have relationship with customer.
o are reported to the CAMLCO and the Managing Director when the suspicious activity is adjudged to represent sufficient risk to the Bank including reputational risk.

✓ Ensuring that a documented plan of corrective action appropriate for the seriousness of the suspicious activity.
✓ 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 Bangladesh Bank authorities after appropriate internal consultations.

1.3 Nomination of Chief Anti-Money Laundering Compliance Officer

The Managing Director will nominate a Chief Anti-Money Laundering Compliance Officer (CAMLCO) in the position of Deputy Managing Director, who will have sufficient authority to implement and enforce corporate-wide anti-money laundering policies, procedures and measures. CAMLCO will report directly to the Managing Director and Board of Directors as well as have sufficient clout to investigate potentially suspicious activities. The CAMLCO has a significant degree of responsibility and should be familiar with all aspects of the legislation.

The CAMLCO may carry out his or her responsibilities through the Central Compliance Unit. The CAMLCO will be a central point of contact for communicating with the regulatory agencies regarding issues related to the financial institution’s anti-money laundering program.

The CAMLCO may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remains responsible and accountable for the operation of the designated functions. Considering the complexity of the operation, the Head of the Central Compliance Unit may act Deputy CAMLCO of the bank.

The CAMLCO will coordinate and monitor day to day compliance with applicable money laundering laws, rules and regulations; the Institution’s AML Policy and the practices, procedures and controls implemented by the bank.

All reports of suspicious activities must reach the CAMLCO at Head Office and only the CAMLCO should have the authority to determine whether a disclosure in accordance with the regulation is appropriate.

Chief Anti Money Laundering Compliance Officer (CAMLCO) has the responsibility for communicating reports of suspicious transactions to the Anti-Money Laundering Department of Bangladesh Bank and will provide the liaison between the Branch and the Bangladesh Bank.
1.4 Nomination of Branch Anti-Money Laundering Compliance Officer (BAMLCO)

The Branch In-Charge will act as Branch Anti-Money Laundering Compliance Officer with intimation to the CAMLCO. The BAMLCO will ensure that his/her branch is carrying out AML policies and procedures as required. The BAMLCO must have sound knowledge of AML regulatory issues and product knowledge associated with a broad range of relevant financial services, banking activities and must be familiar with the ways in which any of Bank’s products or services may be abused by money launderers. The BAMLCO will report to the CAMLCO regularly on compliance issues and the need for any revisions to policies and procedures.

1.5 Organogram

Besides the above, a brief description of role and responsibilities of individual officer/executive involved in anti-money laundering program of the Bank is given below:

<table>
<thead>
<tr>
<th>Function</th>
<th>Role / Responsibilities</th>
</tr>
</thead>
</table>
| Account Officer/Relationship Manager/Officers involved in Account opening | ▪ To exercise due diligence in establishing the identity of customer prior to opening the Account.  
  ▪ To obtain as much information as possible on the customer that might help proper consideration of the nature and type of account.  
  ▪ To ensure that all required documents in respect of account opening are obtained and proper documentation is complete in case of loan account.  
  ▪ To ensure that transaction profile is obtained and reviewed when transactions are being carried out.  
  ▪ To obtain documentary evidence of large cash transactions are being carried out.  
  ▪ To report to BAMLCO for any suspicious transaction, deems necessary. |
| Operations Officer              | ▪ Obtain documentary evidence of large cash deposits.  
  ▪ Ensure that all control points are completed prior to transaction monitoring.  
  ▪ Ongoing diligence on transaction trends for clients.  
  ▪ Update customer transaction profiles in the ledger/system.  
  ▪ Perform AML risk assessment for the Business.  
  ▪ Perform periodic quality assurance on the AML program in the Branch. |
| BAMLCO                          | ▪ To manage transaction monitoring process  
  ▪ To report on suspicious transaction to CAMLCO  
  ▪ To make Officials of Branch aware of AML program.  
  ▪ To update Bank’s AML Policy in line with any change or revision in the country’s AML policy.  
  ▪ To submit Branch Returns to Central Compliance Unit  
  ▪ To ensure that AML program is effectively accomplished in the Branch or Booth.  
  ▪ To act as first point of contact in respect of any AML issues |
| Central Compliance Unit         | Narrated elaborately in serial no. 1.2 above |
| CAMLCO                          | Narrated elaborately in serial no. 1.3 above |
| Managing Director               | ▪ Overall responsibility to ensure that the Bank has an AML program in place and that it is working effectively |
Chapter III: Anti Money Laundering Processes

1.1 Know Your Customer (KYC) Policies

As per requirement of Money Laundering Prevention Act 2009 the Bank needs to seek satisfactory evidence of the identity of those with whom it deals.

Having sufficient information about customer - “knowing your customer” (KYC) - and making use of that information will underpin all anti-money laundering efforts, and will be the most effective defense against being used to launder the proceeds of crime.

The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. The Bank will seek and retain full information of its customers by using KYC profile form and update it as and when required.

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise.

So, it needs to be sure that the institution is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any bank or investment account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally.

1.2 Know Your Customer Procedures

KYC procedure starts from opening account in the name of different clients irrespective of borrowers and depositors. Each officer involved in account opening will be required to perform due diligence on all prospective clients prior to opening an account. This process will be completed by fulfilling the documentation requirements e.g., Account Application, Bank References, Source of funds and Identification for example and also a ‘Know Your Customer’ profile which will be used to record a client’s source of wealth, expected transaction activity at it’s most basic level.

KYC profile gives the basic information about the customer like, Name, Address, Tel/Fax Numbers, line of business, Annual sales.

Once the identification procedures have been completed and the client relationship is established, the concerned officer will monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened.

The KYC Profile information will also include the observations of the concerned officers when they visit the customer’s business place like, the business place is owned or rented, the
type of clients visited, mode of transaction. He/she will record his/her observations and sign the KYC Profile form.

In the case of high net worth Accounts, the information will include net worth of the customer, source of funds etc

The KYC Profile leads to Risk Classification of the Account as High/Low Risk.

1.3 Risk categorization – Based on Activity/KYC Profile

When opening accounts, the concerned officer will assess the risk that the accounts could be used for “money laundering”, and will classify the accounts as either High Risk or Low Risk. The risk assessment may be made using the KYC Profile Form in which following seven risk categories are scored using a scale of 1 to 5 where scale 4-5 denotes High Risk, 3- Medium Risk and 1-2 Low Risk:

- Occupation or nature of customer’s business
- Net worth / sales turnover of the customer
- Mode of opening the account
- Expected value of monthly transactions
- Expected number of monthly transactions
- Expected value of monthly cash transactions
- Expected number of monthly cash transactions

The risk scoring of less than 14 indicates low risk and more than 14 would indicate high risk. The risk assessment scores are to be documented in the KYC Profile Form. However, the concerned officer may override this automatic risk assessment to “Low Risk” if it believes that there are appropriate mitigants to the risk. This override decision must be documented (reasons why) and approved by the BAMLCO.

KYC Profiles and Transaction Profiles must be updated and re-approved at least annually for “High Risk” accounts. There is no requirement for periodic updating of profiles for “Low Risk” transactional accounts. These should, of course, be updated if and when an account is reclassified to “High Risk”, or as needed in the event of investigations of suspicious transactions or other concern.
1.4 Customer Identification

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

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

To protect bank from risks of money laundering or/and terrorist financing by customers willful or unwilling activities, the Money Laundering Prevention Guideline clearly states 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;
- while remitting money and providing other services at the request of non account holders; and
- while there is reasonable ground to suspect about the adequacy or veracity of previously obtained customer identification data.

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

**Explanation:** “Satisfaction of the institution” means satisfaction of the appropriate authority that necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

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

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

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

- 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:
  i. he has controlling share of a company or/and
  ii. hold 20% or more shares of a company.

**Politically exposed Persons (PEPs)**

While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised. PEPs means “Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials”. All instructions as detailed for PEPs shall equally apply if business relationship is established with the family members and close associates of these persons who may pose reputational risk to the bank.

Following instructions shall have to be followed to ensure Enhanced Due Diligence, while opening and operating the account of Politically Exposed Persons (PEPs):

i. a risk management system shall have to be introduced to identify risks associated with the opening and operating accounts of PEPs;
ii. obtain senior management approval for establishing business relationships with such customers;
iii. take reasonable measures to establish the source of wealth and source of funds;
iv. ongoing monitoring of the transactions have to be conducted; and
v. the banks/financial institutions should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

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

**Correspondent Banking**

Instructions for establishing corresponding relationship are as follows:

i. For the purpose of this circular correspondent banking shall mean providing services which are approved by Bangladesh Bank like credit, deposit, collection, clearing, payment or other similar services by one bank (correspondent) to another bank (respondent).
ii. While establishing and continuing correspondent banking relationship following drill should be observed so that banking system can not be abused for the purpose of money laundering:
- Before providing correspondent banking service senior management approval must be obtained on being satisfied about the nature of the business of the respondent bank through collection of information as per annexure-1
- Banks should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.
- Banks should not establish or continue a correspondent banking relationship with any shell bank. [Here shell bank refers to such banks as are incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with a regulated financial group.]
- Correspondent banking relationship shall not be established or continued with those respondent banks that established correspondent banking relationship or maintain account with a shell bank.
- Bank should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries and territories enlisted in Financial Action Task Force’s Noncooperating Countries and Territories list). Enhanced due diligence shall be required in such cases. Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.
- Enhanced Due Diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customers to transact business on their behalf (i.e. payable through account)
- The instructions described in this circular shall be applicable to the entire existing correspondent banking relationship.

**Branches and subsidiaries situated/located in foreign jurisdiction**

1. Reporting organizations (in applicable cases) under Money Laundering Prevention Act, 2009 and Anti Terrorism Act, 2009 having branches and subsidiaries abroad shall also comply with the provisions of Money Laundering Prevention Act, 2009 and Anti Terrorism Act, 2009.
2. If branch or a subsidiary located abroad, for any reason fails to comply with the instructions of Money Laundering Prevention Act, 2009 and Anti Terrorism Act, 2009 it shall without any delay report to such cases to Anti Money Laundering Department mentioning the reason of the failure.

**1.5 What Constitutes a Person’s Identity?**

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

- the physical identity (e.g. name, date of birth, TIN/voter registration/passport/ID number, etc.); and
- the activity undertaken.
Confirmation of a person’s address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issue should be recorded.

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

When commencing a business relationship, it needs to consider recording the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. Documentation about the nature of the applicant’s business should also cover the origin of funds to be used during the relationship. For example, funds may be transferred from a bank or the applicant’s employer, or be the proceeds of a matured insurance policy, etc.

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

### 1.6 Individual Customers

Where verification of identity is required, the following information should be obtained from all individual applicants for opening accounts or other relationships, and should be independently verified by the concerned officer itself:

- True name and/or names used;
- Parent’s names;
- Date of birth;
- Current and permanent address;
- Details of occupation/employment and sources of wealth or income

One or more of the following steps is recommended to verify addresses:

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

The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.
3. The date of birth is important as an identifier in support of the name, and is helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard. It is also helpful for residence/nationality to be ascertained to assist risk assessment procedures and to ensure that the Bank does not breach UN or other international financial sanctions.

4. Identification of documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.:

(i) Current valid passport;
(ii) Valid driving license;
(iii) Voter ID Card;
(iv) Armed Forces ID card;
(v) A Bangladeshi employer ID card bearing the photograph and signature of the applicant; or
(vi) A certificate from any local government organs such as Union Council Chairman, Ward Commissioner, etc. or any respectable person acceptable to the Bank.

5. Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which the concerned officer is unfamiliar, either because of origin, format or language, he must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. The concerned officers should also be aware of the authenticity of passports.

6. Where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should be undertaken to guard against impersonation.

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

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

9. Any subsequent change to the customer’s name, address, or employment details of which the concerned officer becomes aware should be recorded as part of the know your customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

10. Where this is not possible, the relevant details should be recorded on the applicant's file. In case of one-off transactions the details should be recorded in a manner which allows cross reference to transaction records. Such institutions may find it convenient to record
identification details on a separate form similar to the example in Annexure F, to be retained with copies of any supporting material obtained.

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

1.7 Persons without Standard Identification Documentation

Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous anti-money laundering procedures is recommended. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

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

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

The Branch In-Charge may authorize the opening of a business relationship if he/she is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer’s file, and must also retain this information in the same manner and for the same period of time as other identification records.

For students or other young people, the normal identification procedures set out above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant’s educational institution.

Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.
1.8 Corporate Bodies and other Entities

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company’s assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a “brass plate company” where the controlling principals cannot be identified.

Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if the institution becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

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

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.

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

**The following documents should normally be obtained from companies:**

- Certified true copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified true copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company’s
assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;

- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.

Where the business relationship is being opened in a different name from that of the applicant, it needs to find out the reason for using the second name makes sense.

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

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

A letter issued by a corporate customer similar to Annexure E is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the concerned officer already knows their identities and identification records already accord with the requirements of this guideline, there is no need to verify identity again.

When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

1.9 Partnerships and Unincorporated Businesses

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

Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable). An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

1.10 Powers of Attorney/ Mandates to Operate Accounts

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

1.11 Internet or Online Banking

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

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

1.12 Walk-in Customers for TT, DD, PO etc.

The AML Circular # 2 requires the bank to obtain satisfactory evidence of identification of applicants for floor services like TT, DD, PO etc. who do not maintain accounts with the bank for conducting the above-noted services.

In case of remitting money through TT, DD, PO etc. for walk-in customers, he/she will kindly be requested to provide the details, together with appropriate documentary evidence, before the transaction may proceed. The details record will be retained by using a form given in Annexure F of this guideline which will allow cross reference to transaction records.

1.13 Provision of Safe Custody and Safety Deposit Boxes

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

1.14 Timing and Duration of Verification

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

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

1.15 Transaction Monitoring Process

The concerned officer is expected to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the Customer given in Annexure-C of this guideline as to whether transactions are well covered in terms of all guidelines laid down by Bangladesh Bank and other laws. Possible areas to monitor could be:

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

Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. This will be declared in a Transaction Profile (TP) at the time of opening account from the customer. Ideally any deviation from the normally expected TP should be reviewed with human judgment and interaction with customer. Such reviews may result in changing the expected profile or closing the customer account.

It may not be feasible for some specific branches having very large number of customers to track every single account against the TP where a risk based approach will be taken for monitoring transactions based on use of “Customer Categories” and “Transaction Limits” (individual and aggregate) established within the branch. The Customer Category will be assigned at account inception - and may be periodically revised - and will be documented on the Transaction Profile. Transaction Limits will be established by the business subject to agreement by Branch AMLCO. The Customer Categories and Transaction Limits will be maintained in the manual ledgers or computer systems.

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

The concerned officer will review and sign-off on such exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the “transaction limit” established for that category of customer. The concerned officer will document his/her review by initial on the report, and where necessary will prepare internal Suspicious Activity Reports (SARs) with action plans for approval by the Branch AMLCO. A copy of the transaction identified will be attached to the SARs.
The AMLCO will review the SARs and responses from the concerned officer. If the explanation for the exception does not appear reasonable then the branch AMLCO should review the transactions prior to considering submitting them to the CAMLCO. If the Branch AMLCO believes the transaction should be reported then the AMLCO will supply the relevant details to the CAMLCO.

The CAMLCO will investigate any reported accounts and will send a status report on any of the accounts reported. No further action should be taken on the account until notification has been received.

If, after confirming with the client, the transaction trend is to continue the concerned officer is responsible for documenting the reasons why the transaction profile has changed and should amend the KYC profile accordingly.

1.17 Reporting of Cash Transaction Report (CTR)

The Anti-Money Laundering Compliance Officer (AMLCO) will monitor and analyze the daily cash transaction and prepare daily Cash Transaction Report (CTR) as per format given in appendix – Ka of AML circular – 10 in case of cash deposit, cash withdrawal and cash remittance/online deposit of Tk.7.00 lac above in a single transaction or multiple transactions in any account in a single day. He or she will send CTRs to the CCU by the 1st week of subsequent month for onward submission of the same to Bangladesh Bank. Separate CTR report will be needed to prepare for cash deposit, withdrawal and remittance/online deposit.

The AMLCO will analyze the CTR(s) meticulously before reporting the same to the CCU. If something is found suspicious/unnusual, the AMLCO will provide details of transactions and add his comment regarding the reason for treating the transaction as unusual/suspicious as per format given in Appendix–Kha of AML Circular-10.

1.18 Recognition of Suspicious Transactions

As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. It is more than the absence of certainty that someone is innocent. A person would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime. However, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

Questions that the concerned officers must consider when determining whether an established customer’s transaction must be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer’s business or personal activities?
- Has the pattern of transactions conducted by the customer changed?
- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Examples of what might constitute suspicious transactions are given in Annexure G. These are not intended to be exhaustive and only provide examples of the most basic way by which money may be laundered. However, identification of any of the types of transactions listed in Annexure G should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

1.19 Suspicious Activity Reporting Process

All employees of the bank are to remain conscious and alert to identify unusual/suspicious transactions and just after detection of unusual/suspicious transactions which may have connections with money laundering as per article 19(1) (Ga) of Money Laundering Prevention Act, 2002 will be reported in writing as per proforma at Appendix-Ga of AML Circular–02 and Appendix–Kha of AML Circular–10 to the nominated compliance officer of the of the branch.

Where the employee continues to encounter suspicious activities on an account, which he/she has previously reported to AMLCO, he/she will continue to make reports to AMLCO whenever a further suspicious transaction occurs, and the AMLCO will determine whether a disclosure in accordance with the regulations is appropriate.

The Compliance Officer will immediately analyze the reported incident properly and record in writing with reasons in details whether the transaction is connected with money laundering or not. If the reported issue appears to be connected with money laundering he will send immediately the details of the incident along with a copy of the above forms to the Central Compliance Unit. Central Compliance Unit will examine and analyze the reports received and record its observation on the above form Ga and STR and if the incident is considered to be reportable to Bangladesh Bank, the same should be sent immediately to Anti-Money Laundering Department, Bangladesh Bank, Head Office. If nothing is found unusual/suspicious, the CAMLCO will send STR(s) to Bangladesh Bank by adding his comment “Nothing unusual/suspicious is found”.

On the issue of reported unusual/suspicious transactions, no officer of the bank will disclose the same to the clients or any other persons so that the investigation are hampered or influenced adversely.

Only the CAMLCO will have the authority to determine whether a disclosure in accordance with the regulation is appropriate. However the AMLCO can be permitted to add his comments to the suspicion report indicating any evidence as to why he/she believes the suspicion is not justified. The Chief Anti Money Laundering Compliance Officer will be responsible for communicating reports on suspicious transactions to the Anti-Money Laundering Department of Bangladesh Bank and for maintaining the liaison between the institution and the Bangladesh Bank.

The bank will refrain from carrying out transactions which it knows or suspects to be related to money laundering until anti-money laundering compliance unit has apprised the Bangladesh Bank. Where it is impossible in the circumstances to refrain from executing a suspicious transaction before reporting to the Bangladesh Bank or where reporting it is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the
anti-money laundering compliance unit shall apprise the Bangladesh Bank immediately afterwards.

The CAMLCO will keep a written record of every matter reported to him, of whether or not the suggestion was negated or reported, and of his reasons for his decision.

1.20 System of Independent Procedures Testing

Testing is to be conducted at least annually by the internal audit personnel and compliance department. The tests include:

- interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the bank’s anti-money laundering procedures;
- a sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- a test of the validity and reasonableness of any exemptions granted by the anti-money laundering compliance unit; and
- a test of the record keeping system according to the provisions of the Act.

Any deficiencies will be identified and reported to the CAMLCO together with a request for a response indicating corrective action taken or to be taken and a deadline
Chapter IV: Record Keeping

1.1 Statutory Requirements

The requirement contained in Section 19 Ka of the Act to retain correct and full records of customers’ identification and transactions at least for five years after termination of relationships with the customers is an essential constituent of the audit trail that the law seeks to establish.

Where there has been a report of a suspicious activity or the management is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client will be retained until confirmation is received that the matter has been concluded.

1.2 Documents Verifying Evidence of Identity and Transaction Records

Records relating to verification of identity will generally comprise:

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

Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. as prescribed by Bangladesh Bank under AML Circular # 2 and subsequent directives pertaining to:
  1. the customer;
  2. the beneficial owner of the account or product;
  3. the non-account holder conducting any significant one-off transaction;
  4. any counter-party;

- details of transaction including:
  5. the nature of such transactions;
  6. Customer’s instruction(s) and authority (ies);
  7. source (s) and volume of funds;
  8. destination (s) of funds;
  9. book entries;
  10. custody of documentation;
  11. the date of the transaction;
  12. the form (e.g. cash, cheque) in which funds are offered and paid out.

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. the carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
ii. the ending of the business relationship; or
iii. the commencement of proceedings to recover debts payable on insolvency.
1.3 Formats and Retrieval of Records

To satisfy the requirements of the law, it is important that records are capable of retrieval without undue delay. It is not necessary to retain documents in their original hard copy form, provided the availability of reliable procedures for holding records in microfiche or electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, the concerned officer/AMLCO may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on the bank itself and the onus is thus on the business to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required.

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

1.4 Wire Transfer Transactions

Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of telegraphic transfers (TT) and electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in a TT and electronic payment message instruction.

Following the recent focus on terrorist financing, the concerned officers are required to include accurate and meaningful originator (name, account number, and where possible address) and beneficiary information (account name and/or account number) on all outgoing funds transfers and related messages that are sent, and this information should remain with the transfer or related message throughout the payment chain. The records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a minimum of five years.

1.5 Investigations

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

Central anti-money Laundering compliance unit will maintain a register or tabular records of all investigations made to it by the Bangladesh Bank and all disclosures to the Bangladesh Bank. The register will be kept separate from other records and contain as a minimum the following details:

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

So that the management can demonstrate that it has complied with the regulations concerning staff training, it will conduct training through training cell and should maintain 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 on which the training was delivered;
(iv) the results of any testing carried out to measure staff understanding of the money laundering requirements; and
(v) an on-going training plan.
Chapter V: Training and Awareness

1.1 The need for staff awareness

All the staff will 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 will be trained to co-operate fully and to provide a prompt report of any suspicious transactions. It is, therefore, important that the bank introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.

The management will ensure that the staffs are adequately trained in relation to identification, reporting and record retention to ensure that they are adequately trained to discharge their responsibilities. So the Bank will take appropriate measures to make employees aware of:

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

All relevant staff will be educated in the process of the “know your customer” requirements for money laundering prevention purposes. The training in this respect will 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 will be alert to any change in the pattern of a customer’s transactions or circumstances that might constitute criminal activity.

Although 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 form of high-level general awareness raising training will therefore needed.

1.2 Training to New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting any suspicious transactions to the Anti Money Laundering Compliance Officer (AMLCO) will be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They will 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.

1.3 Training of Customer Service/Tellers/Foreign Exchange Dealers

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are vital to the organization’s strategy in the fight against money laundering. They will be made aware of their legal responsibilities and will be made aware of the organization’s reporting system for such transactions. Training will 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.

1.4 Training Processing (Back Office) Staff
Those members of staff who receive completed Account Opening, Payment Order/DD/TT/FDR application forms and cheques for deposit into customer’s account or other investments will receive appropriate training in the processing and verification procedures. Those members of staff, who are in a position to deal with account opening, or to accept new customers, must receive the training given to cashiers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training will be given in the Bank's account opening and customer/client verification procedures. Such staff will be made aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Anti Money Laundering Compliance Officer whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

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

1.6 Training of Anti Money Laundering Compliance Officer
In depth training on all aspects of the Money Laundering Legislation, Bangladesh Bank directives and internal policies will be required for the Anti Money Laundering Compliance Officer. In addition, the AMLCO 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.

1.7 Refresher Training
In addition to the above relatively standard requirements, training may have to be tailored to the needs of specialized areas of the Bank’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.
<table>
<thead>
<tr>
<th>S1.</th>
<th>Description</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Have you carried out a review of processes in your business to identify where money laundering is most likely to occur?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>02</td>
<td>Is this review regularly updated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>03</td>
<td>Have you established procedures and controls to prevent or detect money laundering?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>Is the effectiveness of such controls tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05</td>
<td>Do online or electronic transactions circumvent these controls?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06</td>
<td>Do you have a comprehensive written policy on money laundering?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>07</td>
<td>Is all staff aware of this policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08</td>
<td>Does your money laundering policy include clear guidelines on accepting corporate hospitality and gifts?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>09</td>
<td>Is all staff aware of their responsibilities with regard to money laundering?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Do they receive regular money laundering training?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Are all members of staff sufficiently capable of identifying suspicious transactions?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Are your systems capable of highlighting suspicious transactions (i.e. those not conforming to usual parameters)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Do all members of staff know the identity of their Anti Money Laundering Compliance Officer (AMLCO)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Are your systems capable of providing the AMLCO with all the information required for the Annual Management Report?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Do you thoroughly check and verify the identity of all your clients?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Do you have client accounts in the name of fictitious persons/ entities?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Do you know the identity of the beneficial owner of all your corporate clients?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Is this identity verified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Are all suspicious transactions reported to Bangladesh Bank?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CHECK LIST FOR BRANCH LEVEL INVESTIGATION

1. Branch Anti-Money Laundering Compliance Officer

- Does the branch have a compliance officer?
- Does he/she have sufficient experience and seniority?
- Does he/she have necessary support of senior management to perform his responsibilities?
- Is he/she well conversant about the AML Act 2002, AML circulars and Guidelines Notes on Prevention of Money Laundering?
- Did he/she attend any formal training in the last one-year?
- Does he/she keep himself/herself updated with the change in regulations?
- How many suspicious transaction reports has he/she received so far from the dealing officers of the branch?
- How many suspicious transactions has he/she reported to the AMLCO so far?
- Does the AMLCO carry out monitoring and review of sufficient quality and frequency to satisfy himself/herself that the business and operations are in compliance?
- Does the monitoring carried out by the AMLCO appear adequate including relevant high-risk accounts/activities?
- From a sample of reviews carried out by the AMLCO consider whether they are of sufficient depth and quality.

2. Staff/officers awareness

- How many staff/officers are there in the branch?
- How many staff/officers received formal training on AML program?
- Are the staff/officers of the branch familiar with the banks own anti-money laundering policies, procedures and programs as well as national policies and BB guidelines?

3. Sound KYC Procedures

**KYC for account holders:**

- Obtain and review the account opening procedures and documentation. Do these comply with the requirement of BB Guidance Notes?
- Test samples new accounts-personal, corporate or other to check that satisfactory identification has been obtained, verified and recorded.
- Does the bank have separate KYC profile proforma?
- Test a sample KYC profiles to check whether all relevant information have been obtained.
- Does the branch cover KYC for all products of the bank?
- Does the branch classify their customers on the basis of risk involved?
- Obtain and review the classification procedures to check whether the procedures followed are satisfactory.
- In any additional information obtained in respect of high-risk customers?
- Obtain a high-risk customer KYC profile and examine whether all relevant information/documentation/requirements have been met.
- What is the Customer Acceptance Policy?
Does the branch verify the identification and other information supplied by its customers? If verified, is the method of verification sufficient/satisfactory?

Does the branch review and up-date the KYC on periodical basis?

KYC for walk in/one-off customers:

 Does the branch make KYC for one-off/walk in customers?

 Obtain a sample of KYC for such customer and review to check whether verification of identity is reasonable practicable.

4. Transaction Profile (TP) monitoring

 Has the branch obtained transaction profile from all its customer?

 Obtain a sample copy of TP and examine whether all requirements for transaction monitoring have been met.

 Does the branch monitor the customer transaction with the TP on regular basis?

 If not, is there any threshold for monitoring the transaction of the customers?

 Whether the monitoring mechanism for 4 above is sufficient/adequate.

 Does the branch monitor the inward/outward remittances including Foreign Remittance?

 If so, is the system followed by the branch sufficient/adequate?

 Does the branch review and up-date the transaction profile on periodical basis?

5. Suspicious Transaction Reporting

 How are unusual transaction identified?

 Do all staff/officers of the branch know all system of reporting suspicious transaction?

 How many unusual/suspicious transaction has been reported to the AMLCO?

 Obtain a few STRs and check whether internal reporting of suspicious transaction covers the procedures?

6. Submission of Returns to CAMLCO

 How many returns are scheduled to be submitted to the CAMLCO?

 Does the branch submit the returns on timely basis?

 Obtain copy of a set of returns and check whether information contained in the returns is accurate and complete.

7. Record Keeping

 Are there procedures in place to ensure preservation of record in respect of customer identification (KYC) and transaction in accordance with the regulatory and banks own requirements?

 Check whether records are kept in accordance with the requirement.

 Check whether records are provided to CAMLCO or regulatory authority as per their requirement.

 Check on sample basis the correspondences made by branch with CAMLCO or regulatory authority and determine if branch management has taken appropriate corrective action.

8. Overall branch management on AML function

 Review prior audit/inspection report of the branch (internal and external) to check whether any violations or weakness are noted regarding AML Program.

 Is the instruction contained in letter no. complied with?

 Is the overall AML function of the branch satisfactory?
CHECK LIST FOR HEAD OFFICE LEVEL INVESTIGATION

1. Senior Management Commitment

✓ Is the Senior Management committed to implement the AML Act and Guidance Notes?
✓ Has the Board of Directors of the Bank adopted a written AML Program?
✓ Is the AML program adopted by the Board sufficient to comply with the AML Act and guidelines issued by BB?
✓ Does the Senior Management follow up the AML program regularly?

2. Anti-Money Laundering Compliance Unit

✓ Does the bank have a complete Anti-money Laundering Compliance Unit?
✓ Does the CAMLCO have sufficient authority to implement and enforce the policies, procedures/programs?
✓ Does the CAMLCO have the sufficient support of Senior Management to perform his responsibilities?
✓ Is the CAMLCO sufficiently senior and experienced to command the necessary authority?
✓ Is the CAMLCO sufficiently independent?
✓ How and when does the CAMLCO report to the Senior Management for his responsibilities?
✓ Does the CAMLCO keep up to date with the changes in regulations and amend procedures accordingly?
✓ Does he/she follow the appropriate process for reporting suspicious transaction to BB?
✓ How many suspicious transaction report has CAMLCO received so far from the branches?
✓ How many suspicious transactions have been reported to BB so far?
✓ Does the Internal Control (Audit Dept.) of the bank examine whether compliance of AML program is properly followed at branch level?
✓ Are arrangements in place for the CAMLCO to review the work carried out by Internal Audit, External Audit, BB Inspection Report (Comprehensive and Special) etc?
✓ Does the Anti-money Laundering Compliance Unit has any project/plan to obtain KYC and transaction profile of the pre-2002 accounts?
✓ Has the Anti-money Laundering Compliance Unit issued any clear-cut instructions to classify the accounts based on activity/KYC profile?
✓ Is the overall performance of CAMLCO considered to be satisfied?
✓ Check the correspondence made by Anti-money Laundering Compliance Unit or any other department of the Head Office of the bank with AMLD of Bangladesh Bank and determine whether Management of the bank has taken appropriate corrective action.

3. Bi-Monthly/Quarterly Submission of Returns

✓ Does Anti-money Laundering Compliance Unit submit the required returns to BB regularly?
✓ Is the information contained in the returns accurate and sufficient?
✓ Examine some sample files and check whether the matters have been dealt with properly.
4. Training

✓ How many officers/staff of the bank have been trained up in the 1st Phase (Number & Percentage)?
✓ How many officers/staff have been trained in the 2nd Phase?
✓ Are records maintained of officers/staff who have attended anti-money laundering training?
✓ Are any checks carried out to assess the understanding of the trainee?
✓ Is anti-money laundering training included as part of more general training programs?
✓ Obtain copies of some relevant training materials and supporting documentation. How is training material updated?
✓ Did the CAMLCO attend any formal training programs in the last three years?

5. Record Keeping

✓ Check whether records are held in accordance with the requirements.
✓ Check whether records are provided to Regulatory Authority as per their requirement.