MANAGING CORE RISK IN BANKING

Money Laundering & Terrorist Financing Risk Management Guidelines

Social Islami Bank Limited

Money Laundering & Terrorist Financing Risk Management Guidelines Of Social Islami Bank Limited

Revised on June 2016

CONTENTS

AN OVERVIEW OF MONEY LAUNDERING AND TERRORIST FINANCING

1.1 DEFINING MONEY LAUNDERING

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

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

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

- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

The Financial Action Task Force (FATF), the international standard setter for anti-money laundering (AML) and combating financing of terrorism (CFT) efforts, recommends that money laundering should be criminalized in line with the Vienna Convention and Palermo Convention. Like other countries of the world, Bangladesh has criminalized money laundering in line with those conventions. Moreover, Bangladesh also considers some domestic concerns like 'smuggling of money or property from Bangladesh' in criminalizing money laundering.

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

'Money laundering' means-

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

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

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

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

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

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

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

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

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

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

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

1. Any person who commits or abets or conspires to commit the offence of money laundering, shall be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lacks, whichever is higher.

2. In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which is directly or indirectly involved in or related with money laundering or any predicate offence.

3. Any entity which commits an offence under this section shall be punished with a fine of not less than twice the value of the property or taka 20(twenty) lacks, whichever is higher and in addition to this the registration of the said entity shall be liable to be cancelled.

1.2 STAGES OF MONEY LAUNDERING

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

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

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

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

1.3 WHY MONEY LAUNDERING IS DONE

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

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

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

1.4 DEFINING TERRORIST FINANCING

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

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

    a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below[1]; or

    b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

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

[1] International Convention for the Suppression of the Financing of Terrorism (1999), Article 2, http://www.un.org/law/cod/finterr.htm. The treaties referred to annex in sub-paragraph 1(a) shall be available in this web link.

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

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

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

a) to carry out terrorist activity;

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

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

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

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

(2) In case of a TF offence made by an entity, the Government may list the entity in the Schedule or proscribe and list the entity in the Schedule, by notification in the official Gazette and in addition to that, a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is higher, may be imposed. Moreover, the head of that entity, whether he is designated as Chairman,

Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20 (twenty) lac, whichever is higher, may be imposed unless he/she is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

1.5 THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

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

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

1.6 TARGETED FINANCIAL SANCTIONS

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

TFS related to terrorism and terrorist financing-

FATF recommendation 6 requires 'Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)'.

TFS related to Proliferation-

FATF recommendation 7 requires 'Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations'.

AML & CFT COMPLIANCE PROGRAM OF BANK

2.1 INTRODUCTION

To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU, bank should develop and maintain an effective AML and CFT compliance program. This should cover at least senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

2.2 COMPONENT OF AML & CFT COMPLIANCE PROGRAM

The compliance program of bank should be documented and communicated to all levels of the organization after getting approval by its Board of Directors or the highest management committee (as applicable). In developing an AML&CFT compliance program, attention should be paid to the size and range of activities, complexity of operations, and the nature and degree of ML & TF risk faced by the bank. The program must include-

1. senior management role including their commitment to prevent ML, TF & PF;

2. internal policies, procedure and controls- it should include Bank' policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, self-assessment, independent testing procedure, employee screening, record keeping and reporting to BFIU;

3. compliance structure includes establishment of central compliance Unit (CCU), appointment of chief anti-money laundering compliance officer (CAMLCO), branch anti-money laundering compliance officer (BAMLCO);

4. independent audit function- it includes the role and responsibilities of internal audit on AML & CFT compliance and external audit function;

5. awareness building program includes training, workshop, seminar for bank employees, members of the board of directors, owners and above all for the customers on AML & CFT issues.

2.3 DEVELOPMENT OF BANK'S AML & CFT COMPLIANCE PROGRAM

In developing its own AML & CFT compliance program, bank may consider any relevant document including relevant guidelines of Bangladesh Bank as a basis for it. Bank should also consider all relevant laws, regulations, guidelines relating to AML & CFT and also the practices related to corporate governance. In drafting the compliance program, bank should involve all its relevant departments or divisions like general banking, credit, foreign exchange, information technology, international division, alternative delivery channels, internal audit and compliance and above all central compliance unit. Their involvement should be documented or reflected in the compliance program. Proper attention should be given to the size and range of activities, complexity of operations, customer base, use of technology, diversity of product, delivery channel, external linkage, geographic location and the output of ML & TF risk assessment of the bank. Bank can use Bengali and/or English language in drafting compliance program. If the compliance program developed in English then bank may develop a Bangla version of it to make it more communicative.

2.4 COMMUNICATION OF COMPLIANCE PROGRAM

Bank should communicate its compliance program immediately after the approval from the board of directors or from the highest authority to all of its employees, members of the board of the directors and other relevant stakeholders at home and abroad. Bank should select proper channel that is the best suited to the bank to communicate with the compliance program. Bank should also upload the compliance program in their website for their customers or other stakeholders.

2.5 SENIOR MANAGEMENT ROLE

For the purposes of preventing ML, TF & PF, senior management includes members of the board of directors of the bank, or the member of the highest management committee in absence of the board of directors and the Chief Executive Officer (CEO) or the Managing Director (MD) of the bank.

Obligations under Law (ATA, 2009)-

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

Obligations under BFIU Circular (Circular-10; dated- 28 Dec, 2014)-

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

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

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

Board of Directors (BoD) or Highest Management committee (in absence of BoD) shall –

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

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

Statement of commitment of CEO or MD of bank should include the followings-

- Bank's policy or strategy to prevent ML, TF & PF;
- Emphasize on effective implementation of bank's AML&CFT compliance programme;
- Clear indication of balance between business and compliance, risk and mitigating measures;
- Compliance is the responsibility of each employee during their normal course of assignment and ignorance shall not be considered as the excuse for non-compliance;
- Point of contact for clarification in case of any ambiguity;
- Consequences of non-compliance as per human resources (HR) policy of the bank.

Senior management of bank has accountability to ensure that the bank's policy, process and procedures towards AML & CFT are appropriately designed and implemented, and are effectively operated to minimize the risk of the bank being used in connection with ML & TF.

Senior management must ensure the adequacy of the human and other resources devoted to AML & CFT. Moreover, they need to ensure the autonomy of the designated officials related to AML & CFT. Senior management should take the report from the Central Compliance Unit (CCU) into consideration which will assess the operation and effectiveness of the bank's systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner.

Senior management of bank should adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the bank.

Bank's HR Policy should include at least following issues for proper implementation of AML & CFT measures:

- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- Proper weight should be given in the annual performance evaluation of employees for extra ordinary preventive action vis a vis for non-compliance;
- Written procedure to recover the penalty amount from the concerned employee if the fine is imposed on employee by the BFIU;
- Other measures that shall be taken in case of non-compliance by the bank.

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

2.6 POLICIES AND PROCEDURES

An AML & CFT policy usually includes the 4 (four) key elements; they are -

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

2.6.1 WRITTEN AML & CFT COMPLIANCE POLICY

At a minimum, the board of directors or the management committee of bank must develop, administer, and maintain an AML & CFT compliance policy that ensures and monitors compliance with the Acts, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes.

The written AML&CFT compliance policy at a minimum should establish clear responsibilities and accountabilities within their organizations to ensure that policies, procedures, and

controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the law.

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

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

It should also include a description of the roles the AML&CFT Compliance Officers(s)/Unit and other appropriate personnel will play in monitoring compliance with and effectiveness of AML&CFT policies and procedures. It should develop and implement screening programs to ensure high standards when hiring employees. It should also implement standards for employees who consistently fail to perform in accordance with an AML&CFT framework. It should incorporate AML&CFT compliance into job descriptions and performance evaluations of appropriate personnel. It should have the arrangements for program continuity despite changes in management or employee composition or structure.

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

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

2.6.2 PROCEDURES

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

2.7 CUSTOMER ACCEPTANCE POLICY

Bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place to set-up any kind of business relationship with the bank. A concrete Customer Acceptance Policy is very important so that inadequate understanding of a customer's background and purpose for utilizing a bank account or any other banking product/service may not expose the Bank to a number of risks. The primary objectives of a Customer Acceptance Policy are –

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

The customer acceptance policy of bank should not be used against the disadvantaged people or the people who have not proper identification document. A customer acceptance

policy should encourage the ultimate goal of transparent, accountable and inclusive financial system in Bangladesh.

Bank needs to ensure that it will accept only those customers whose appropriate identity is established by conducting due diligence to the risk profile of the client. Parameters of risk perception must be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to enable categorization of customers into different risk grade.

Bank should not open an account where it is unable to apply appropriate customer due diligence measures i.e. if the bank is unable to verify the identity and/or obtain documents required as per risk categorization due to non-cooperation of the customer bank will not open or allow withdrawal of money. Decision by bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such decision.

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

Necessary checks should be made before opening a new account so that the bank can ensure the identity of the customer does not match with any person with known criminal background or with proscribed entities such as individual terrorists or terrorist organizations etc.

Customer acceptance policy of bank must include-

- No account in anonymous or fictitious name or account only with numbers shall be opened;
- No banking relationship shall be established with a Shell Bank; and
- No account in the name of any person or entity listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance adopted under Chapter VII of the Carter of UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government shall be opened or operated.

N.B: 'Person or entities listed under various resolutions of United Nations Security Council' can be downloaded from http:// www.un.org/sc/committees/ list compend. shtml and the list of Bangladesh Government can be found at the schedule of Anti-Terrorism Act, 2009.

COMPLIANCE STRUCTURE OF BANK

3.1 INTRODUCTION

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

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

3.2 CENTRAL COMPLIANCE UNIT

Obligations under BFIU Circular-10, dated 28 Dec, 2014 -

"To keep the banking sector free from the risks related to Money Laundering & Terrorist Financing and for the effective/proper compliance of all existing acts, rules and instructions issued by BFIU time to time, every bank should set up a Central Compliance Unit (CCU) that will be directly monitored by the Managing Director or the Chief Executive Officer of the bank.

The central compliance unit must be headed by a high official, who will be known as the Chief Anti Money Laundering Compliance Officer (CAMLCO). In this case, 'High official' will be considered as an official up to 2 (two) steps below the managing director/ chief executive officer. But, for a foreign bank, mentioned 'high official' must be a member of the Management Committee (ManCom). If the CAMLCO is changed, it should be informed to BFIU without delay. Before assigning other duties of the bank to the CAMLCO, the management has to ensure that the AML & CFT activities of the bank will not be hampered.

The banks can also nominate one or more deputy of the CAMLCO, who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (D-CAMLCO). The D-CAMLCO will be at least in the rank of 'Assistant General Manager' or 'Vice President' of the bank. The CAMLCO and DCAMLCO have to have detailed knowledge of the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML & TF."

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

3.2.1 FORMATION OF CCU

In light of the directives mentioned in BFIU Circular-10, dated 28 Dec, 2014 CCU should be established in the head office of the bank or any suitable place as a permanent set-up with specific organogram like other department or division of a bank. Adequate human resources and other logistic support should be provided based on the size and nature of the bank but human resources shall not be less than 5 (five) officials in any case. The bank should determine additional human resource in the CCU by considering the number of branches, technology used, geographical presence and customer base. Among the 5 (five) officials in the CCU, at least 2 (two) officials must be familiar with general banking and 1 (one) with information technology of the bank. The employee of the CCU must have enough knowledge on AML & CFT measures of Bangladesh including MLPA, ATA and rules and instructions issued by BFIU or Bangladesh Bank.

3.2.2 AUTHORITIES AND RESPONSIBILITIES OF THE CCU

CCU is the prime mover of the bank for ensuring the compliance of AML & CFT measures. Its main responsibilities are to-

1) develop banks policy, procedure and strategies in preventing ML, TF & PF;
2) coordinate banks AML & CFT compliance initiatives;
3) coordinate the ML & TF risk assessment of the bank and review thereon;
4) present the compliance status with recommendations before the CEO or MD on half yearly basis;
5) forward STR/SAR and CTR to BFIU in time and in proper manner;
6) report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner;
7) impart training, workshop, seminar related to AML & CFT for the employee of the bank;
8) take required measures to submit information, report or documents in time.

For shouldering these responsibilities bank authority may consider giving the following authority to CCU-

1) appointment of BAMLCO and assign their specific job responsibilities;
2) requisition of human resources and logistic supports for CCU;
3) make suggestion or administrative sanction for non-compliance by the employees.

3.2.3 SEPARATION OF CCU FROM Internal Control & Compliance Division (ICCD) (Internal Audit Department)

For ensuring the independent audit function in the bank CCU should be completely separated from internal audit or compliance and control (ICC). Either the division or unit may perform same job but in different and independent way. In this regard ICC also examines the performance of CCU and the bank's AML & CFT compliance program. To ensure this autonomy there shall not be any member from ICC to CCU and vis-a-vis; but there should be enough co-ordination and co-operation in performing their responsibility and information exchange. There should not be any impediment to transfer employee from ICC to CCU and vis-à-vis but no one should be posted in these 2 (two) departments/units at the same time.

3.3 CHIEF ANTI MONEY LAUNDERING COMPLIANCE OFFICER (CAMLCO)

As per directives mentioned in BFIU Circular-10, dated 28 Dec, 2014:

- Bank must designate a Chief Anti Money Laundering Compliance Officer (CAMLCO) at its head office who has sufficient authority to implement and enforce corporate wide AML&CFT policies, procedures and measures and who will report directly to CEO or MD. This provides evidence of senior management's commitment to efforts to combat money laundering and terrorist financing and, more importantly, provides added assurance that the officer will have sufficient influence to enquire about potentially suspicious activities. The CAMLCO is responsible for oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering and terrorist financing.
- The position within the organization of the person appointed as CAMLCO will vary according to the size of a bank and the nature of its business, but he or she should be sufficiently senior to command the necessary authority but should not be more than 2 steps below the MD or CEO. Each bank should prepare a detailed specification of the role and obligations of the CAMLCO.
- The designated CAMLCO, directly or through the CCU, should be the central point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML&CFT program. Depending on the scale and nature of the bank the designated CAMLCO may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions.

- ❖ All staffs engaged in the bank at all levels must be made aware of the identity of the CAMLCO, his deputy and the staff and branch/unit level AML&CFT compliance officers, and the procedure to follow when making a suspicious transaction/activity report. All relevant staffs must be aware of the chain through which suspicious transaction/activity reports should be passed to the CAMLCO.
- ❖ As the CAMLCO is responsible for the oversight of all aspects of the bank's AML&CFT activities and is the focal point for all activity within the bank relating to ML & TF his/her job description should clearly set out the extent of the responsibilities given to him/her. The CAMLCO will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering/terrorist financing is put into practice.

3.3.1 AUTHORITIES AND RESPONSIBILITIES OF CAMLCO

Authorities-

- CAMLCO should be able to act on his own authority;
- He/she should not consult or seek any permission from the MD or CEO before submission of STR/SAR and any document or information to BFIU;
- He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He/she must have access to any information of the bank;
- He/she shall ensure his/her continuing competence.

Responsibilities-

- CAMLCO must ensure overall AML&CFT compliance of the bank;
- oversee the submission of STR/SAR or any document or information to BFIU in time;
- maintain the day-to-day operation of the bank's AML&CFT compliance;
- CAMLCO shall be liable to MD , CEO or BoD for proper functioning of CCU;
- CAMLCO shall review and update ML & TF risk assessment of the bank;
- ensure that corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.

3.4 BRANCH ANTI MONEY LAUNDERING COMPLIANCE OFFICER (BAMLCO)

Obligations under BFIU Circular-10, dated 28 Dec, 2014 -

"For the implementation of all existing acts, rules, BFIU's instructions and bank's own policies on preventing Money Laundering & Terrorist Financing, bank shall nominate an experienced Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch."

The manager, the second man of the branch or a high official experienced in general banking shall be nominated as the BAMLCO. The BAMLCO has to have detailed knowledge of the existing acts, rules and regulations, BFIU preventing Money Laundering and Terrorist Financing. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her appointment letter.

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

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

3.4.1 AUTHORITIES AND RESPONSIBILITIES OF BAMLCO

For preventing ML, TF & PF in the branch, the BAMLCO should perform the following

responsibilities:

- ensure that the KYC of all customers have been done properly and for the new customer KYC is being done properly;
- ensure that the UN Security Council and domestic sanction list are checked properly before opening of account and while making any international transaction;
- keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;
- ensure regular transaction monitoring to find out any unusual transaction (In case of an automated bank, the bank should follow a triggering system against transaction profile or other suitable threshold. In case of a traditional bank, transaction should be examined at the end of day against transaction profile or other suitable threshold. Records of all transaction monitoring should be kept in the file);
- review cash transaction to find out any structuring;
- review CTR to find out STR/SAR;
- ensure the checking of UN sanction list before making any foreign transaction;
- ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
- compile self-assessment of the branch regularly and arrange quarterly meeting regularly;
- accumulate the training records of branch officials and take initiatives including reporting to CCU, HR and training academy;
- ensure all the required information and document are submitted properly to CCU and any freeze order or stop payment order are implemented properly;
- follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
- ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements of chapter 7;
- ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.

3.5 INTERNAL CONTROL AND COMPLIANCE

Obligations under BFIU Circular-10, dated 28 Dec, 2014

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

Internal Audit or Internal Control and Compliance (ICC) of a bank shall have an important role for ensuring proper implementation of bank's AML & CFT Compliance Program. Every bank needs to ensure that ICC is equipped with enough manpower and autonomy to look after the prevention of ML&TF. The ICC has to oversee the implementation of the AML & CFT compliance program of the bank and has to review the 'Self-Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

To ensure the effectiveness of the AML&CFT compliance program, bank should assess the program regularly and look for new risk factors. FATF recommendation 18 suggests that-

'Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML&CFT purposes. Financial institutions should be required to ensure that their foreign branches and majority owned

subsidiaries apply AML&CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing'.

Bank's internal auditors should be well resourced and enjoy a degree of independence within the bank. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable.

The internal audit must-

- understand ML & TF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML/CFT Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML&CFT Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU or BB;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
    - the importance of the board and the senior management place on ongoing education, training and compliance,
    - employee accountability for ensuring AML&CFT compliance,
    - comprehensiveness of training, in view of specific risks of individual business lines,
    - training of personnel from all applicable areas of the bank,
    - frequency of training,
    - coverage of bank policies, procedures, processes and new rules and regulations,
    - coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
    - penalties for noncompliance and regulatory requirements,

3.6 EXTERNAL AUDITOR

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

CUSTOMER DUE DILIGENCE

4.1 INTRODUCTION

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources. The CDD obligations compel banks to understand who their customers are, to guard against the risk of committing offences under MLPA, 2012 including 'Predicate Offences' and the relevant offences under ATA, 2009.

Therefore, banks should be able to demonstrate to their supervisory authority to put in place, implement adequate CDD measures considering the risks of money laundering and terrorist financing. Such risk sensitive CDD measures should be based on-

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

The adoption of effective KYC standards is an essential part of banks' risk management policies. Banks with inadequate KYC program may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the bank's overall safety and soundness, they also protect the integrity of the banking system by reducing money laundering, terrorist financing and other unlawful activities.

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

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

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

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

4.2 LEGAL OBLIGATIONS OF CDD

Obligations under MLPA, 2012 -

"The reporting organizations shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to Bangladesh Bank."

Obligations under MLP Rules, 2013 -

"The bank shall identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data). The verification of identity of a customer or a beneficial owner should include a series of independent checks and inquiries and not rely only on documents provided by the customer or beneficial owner. The bank shall verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person.

The bank shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the bank is satisfied that it knows who the beneficial owner is.

The bank shall understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship. The bank shall also conduct ongoing due diligence on the business relationship.

The bank shall scrutinize the transactions undertaken by a customer throughout the relationship with the customer to ensure that the transactions are consistent with the nature, business and risk profile of the customer, including where necessary, with the source of funds."

Obligations under BFIU Circular No-10, dated 28 December, 2014

"Details of CDD measures have been discussed in paragraph no. 3, 4 and 5."

4.3 GENERAL RULE OF CDD

Completeness and Accuracy

Bank require to be certain about the customer's identity and underlying purpose of establishing relationship with the bank, and should collect sufficient information up to its satisfaction. **"Satisfaction of the bank"** 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.

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

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

The verification procedures establishing the identity of a prospective customer should basically be the same whatever type of account or service is required. The best would be to obtain from the prospective customer the identification documents which is most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity, so verification will generally be a cumulative process. The overriding principle is that bank must know who its customers are, and have the necessary documentary evidences to verify this.

Where the bank is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, unable to identify the beneficial owner taking reasonable measures, unable to obtain information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer. Annexure-B provides an example of collection of documents that bank find it useful for their purpose.

Ongoing CDD measures (Review and update)

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

Any subsequent change to the customer's name, address, or employment details of which the bank becomes aware should be recorded as part of the CDD process. Generally this would be undertaken as part of good business practice and due diligence but also serves for prevention of money laundering and terrorist financing. Bank should collect customer declaration about the Transaction Profile of customer account in the specified form. After reviewing the nature of the customer, the source of money in the account and the nature of transaction, bank should again collect the Transaction Profile along with the amendments in it from the customer by reviewing the transactions of the customer within 6 (six) months of establishing business relation and assessing the effectiveness with a logical consideration.

Enhanced CDD measures

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

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

Enhanced CDD measures include:

- Obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet etc) and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship when applicable.
- Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- Making the concerned bank officials aware of the risk level of the customer.

4.4 TIMING OF CDD

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

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

4.5 TRANSACTION MONITORING

Bank needs to monitor the transactions of customers on regular basis. The complex transaction, transactions with deviation from normal transaction and the transactions that do not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized during monitoring. An effective system has to be developed by the bank to review the risk by maintaining a specific time interval; and according to the review, Enhanced Due Diligence has to be maintained for high risk category accounts.

Bank should put in place various ways of transaction monitoring mechanism within their branches that include but not limited to the followings:

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

4.6 EXCEPTION WHEN OPENING A BANK ACCOUNT

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

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

4.7 IN CASE WHERE CONDUCTING THE CDD MEASURE IS NOT POSSIBLE

If conducting the CDD measure becomes impossible because of the non-cooperating behavior of the customer or if the collected information seems to be unreliable, that is, bank could not collect satisfactory information on customer identification and could not verify that, bank should take the following measures:

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

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

If the bank concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be sent to the BFIU. The bank must then retain the funds until consent has been given to return the funds to the source from which they came.

If the bank concludes that there are no grounds for making a report, it will need to make a decision on the appropriate course of action. This may be retaining the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or returning the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

4.8 CUSTOMER IDENTIFICATION

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

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

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for bank to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if the bank at any time becomes aware that it lacks sufficient information about an existing customer, it will take steps to ensure that all relevant information is obtained as quickly as possible.

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

Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken. Records must be maintained as set out in Chapter V, and information should be updated or reviewed as appropriate.

4.9 VERIFICATION OF SOURCE OF FUNDS

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

4.10 VERIFICATION OF ADDRESS

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

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

4.11 PERSONS WITHOUT STANDARD IDENTIFICATION DOCUMENTATION

Most of the 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, street children or people, students and minors shall 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 considering risk profile of the prospective customers without compromising sufficiently rigorous anti-money laundering procedures is recommended. Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances.

Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address. A manager may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

For students or other young people, the normal identification procedures set out as 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.

4.12 WALK-IN/ ONE OFF CUSTOMERS

Bank should collect complete and correct information while serving Walk-in customer, i.e. a customer without having account. Bank should know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT. Detailed provisions are discussed in the paragraph 4.17 of this Guidelines.

Bank should collect complete and correct information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit bank should identify sources of funds as well.

4.13 NON FACE TO FACE CUSTOMERS

Bank should assess money laundering and terrorist financing risks while providing service to non-face to face customers and develop the policy and techniques to mitigate the risks, as well as will review that from time to time. 'Non face to face customer' refers to "the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the bank branch".

4.14 CUSTOMER UNIQUE IDENTIFICATION CODE

Bank should use unique identification code for any customer maintaining more than one account or availing more than one facility. Such unique identification system could facilitate bank to avoid redundancy, and saves time and resources. This mechanism also enables bank to monitor customer transactions effectively.

4.15 CORRESPONDING BANKING

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

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

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

ownership of such banks and extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained.

If any respondent bank allow direct transactions by their customers to transact business on their behalf (i.e. payable through account), the corresponding bank must be sure about the appropriate CDD of the customer done by the respondent bank. Moreover, it must be sure that collecting the information on CDD of the respective customer is possible by the respondent bank on request of the correspondent bank. Here, '**Payable through accounts**' refers to "Corresponding accounts that are used directly by third parties to transact business on their behalf."

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

All Clients must be subject to an assessment to determine whether they are PEP's or Influential Persons or chief executives or top level officials of any international organization and their linked entities. These customers pose a higher risk of money laundering, bribery, corruption and reputational risk to the bank due to their current or former position of political power or influence, which makes them more vulnerable to corruption. Relationships with these customers may increase the risk to the bank due to the possibility of that individuals holding such positions may misuse their power and influence for personal gain or advantage or for the personal gain or advantage of their Close Family Members and Close Associates. The person's status (PEP's, Influential Persons and chief executives or top level officials of any international organization) itself does not incriminate individuals or entities. It does, however, put a prospective or existing Client into a higher risk category.

4.16.1 DEFINITION OF PEPs

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

1. heads and deputy heads of state or government;
2. senior members of ruling party;
3. ministers, deputy ministers and assistant ministers;
4. members of parliament and/or national legislatures;
5. members of the governing bodies of major political parties;
6. members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
7. heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
8. heads of state-owned enterprises

4.16.2 CDD MEASURES FOR PEP'S

Bank needs to identify whether any of their customer is a PEP. Once identified bank needs to apply enhanced CDD measures that is set out in 6.3 of this guidelines. Moreover, they need to perform the following-

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

4.16.3 DEFINITION OF INFLUENTIAL PERSONS

'**Influential persons'** refers to, "Individuals who are or have been entrusted with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials."

The following individuals must always be classed as Influential persons:

- heads and deputy heads of state or government;
- senior members of ruling party;
- ministers, state ministers and deputy ministers;
- members of parliament and/or national legislatures;
- members of the governing bodies of major political parties;
- Secretary, Additional secretary, joint secretary in the ministries;
- Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- governors, deputy governors, executive directors and general managers of central bank;
- heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
- heads of state-owned enterprises;
- members of the governing bodies of local political parties;
- ambassadors, *chargés d'affaires* or other senior diplomats;
- city mayors or heads of municipalities who exercise genuine political or economic power;
- board members of state-owned enterprises of national political or economic importance.

Whether an individual is an influential person or not will depend on the prominence or importance of the function that he/she holds, and the level of corruption in the country, the reputation and personal links of the individual and whether he/she has any links to industries that are prone to corruption. If the individual does not hold sufficient influence to enable them to abuse his/her power for gain, they should not be classified as an influential person.

4.16.4 CDD MEASURES FOR INFLUENTIAL PERSONS

Bank need to identify whether any of their customer is an IP. Once identified bank need to apply enhanced CDD measures that is set out in 4.3 of this guidelines.

Moreover, bank needs to perform the following-

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

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

'Chief executive of any international organization or any top level official' refers to, "Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the boards or equivalent functions." The heads of international organizations and agencies that exercise genuine political or economic influence (e.g. the United Nations,

the International Monetary Fund, the World Bank, the World Trade Organization, the International Labor Organization) must always be classed as this category.

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

Bank needs to identify whether any of their customer is a CEO or top level officials of any international organization. Once identified bank needs to apply enhanced CDD measures that is set out in 4.3 of this guidelines. Moreover, bank needs to perform the following-

1) Bank has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a CEO or top level officials of any international organization;
2) obtain senior managements' approval before establishing such business relationship;
3) take reasonable measures to establish the source of fund of the account of a CEO or top level officials of any international organization;
4) monitor their transactions in a regular basis; and
5) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly .

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

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

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

There may be exceptional circumstances where the individual should not be classified as a 'Close Family Member' of the PEP, such as estrangement, divorce etc. In such cases, the circumstances must be thoroughly investigated, examined and caution exercised. In addition, where other family members such as the siblings, cousins, relatives by marriage of the PEP are deemed, by virtue of the nature of the relationship, to have a close relationship with the PEP, they should also be classified as PEPs.

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

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

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

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

Bank need to identify whether any of their customer is a family member or close associates of a PEP, IP or CEO or top level officials of any international organization. Once identified bank needs to apply enhanced CDD measures that is set out in 4.3 of this guidelines. Moreover, they need to perform the following-

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

4.17 WIRE TRANSFER

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

4.17.1 CROSS-BORDER WIRE TRANSFERS

Under general or special consideration in case of threshold cross-border wire transfers of 1000 (one thousand) or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank. Furthermore, for cross-border wire transfers, below the threshold full and meaningful originator information has to be preserved. For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved.

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

4.17.2 DOMESTIC WIRE TRANSFERS

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

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

Ordering Bank:

The ordering bank should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information. These information

has to be preserved minimum for 5 (five) years.

Intermediary Bank:

For cross-border and domestic wire transfers, any bank working as an intermediary between ordering bank and beneficiary bank, should ensure that all originator and beneficiary information that accompanies a wire transfer is retained. A record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution (or as necessary another intermediary financial institution).

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

Beneficiary Bank:

A beneficiary financial institution should initiate risk based procedure to identify wire transfers that lack required originator or required beneficiary information. In case of insufficient originator information concerned parties should collect those information through mutual communication or using any other means. During the payment to receiver/beneficiary, the bank should collect full and accurate information of receiver/beneficiary and should preserve those information for 5 (five) years.

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

4.18 CDD FOR BENEFICIAL OWNERS

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

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

- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercises control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) should consider for other types of legal arrangements.
- Where, a natural or legal persons who holds controlling interest, listed on a stock exchange and subjects to disclosure requirements or majority owned subsidiaries of such listed companies may exempted from identifying or verifying beneficial

ownership requirements.

4.19 RELIANCE ON THIRD PARTY

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

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

4.20 MANAGEMENT OF LEGACY ACCOUNTS

Legacy accounts refers those accounts opened before 30 April, 2002 and yet to update KYC procedures. These legacy accounts will be treated as "Dormant". No withdrawal will be permitted in those accounts; however, deposit can be permitted. These accounts will be fully functional only after conducting proper CDD measures. Branch Compliance Unit and Central Compliance Unit both will preserve data of such accounts at their end.

RECORD KEEPING

5.1 INTRODUCTION

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

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

5.2 LEGAL OBLIGATIONS

Obligations under MLPA, 2012 -

"The reporting organizations shall have to preserve previous records of transactions of any close account for at least 5(five) years from the date of such closure and provide with the information maintained under the clause to Bangladesh Bank."

Obligations under MLP Rules, 2013 -

"The bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners:

(1) Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;

(2) The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction;

(3) The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order."

5.3 OBLIGATIONS UNDER CIRCULAR

Obligations under BFIU Circular-10; dated 28/12/2014-

"(1) All necessary information/documents of customer's domestic and foreign transactions has to be preserved for at least 5(five) years after closing the account.

(2) All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved for at least 5(five) years after closing the account.

(3) All necessary information/documents of a walk-in Customer's transactions has to be preserved for at least 5 (five) years from the date of transaction.

(4) Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence.

(5) Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU."

5.4 RECORDS TO BE KEPT

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

Bank's records should cover:

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

5.5 CUSTOMER INFORMATION

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

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

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

5.6 TRANSACTIONS

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the bank's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed.

5.7 INTERNAL AND EXTERNAL REPORTS

Bank should make and retain:

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

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

5.8 OTHER MEASURES

Bank's records should include:

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

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

5.9 FORMATS AND RETRIEVAL OF RECORDS

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

It is not always necessary to retain documents in their original hard copy form, provided that the bank has reliable procedures for keeping records in electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, bank 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 responsibility is thus on the bank 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.

REPORTING TO BFIU

6.1 LEGAL OBLIGATIONS

Obligations under MLPA, 2012 -

"The reporting organizations shall have to report any suspicious transaction (defined in Section 2(Z) of MLPA, 2012 and Section 2(16) of ATA, 2009) to the Bangladesh Bank immediately on its own accord."

Obligations under MLP Rules, 2013 -

"Every bank is obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self-assessment, independent testing procedure etc.) to Bangladesh Bank without any delay or in due time. Besides they have to produce any documents that is sought by Bangladesh Bank."

6.2 SUSPICIOUS TRANSACTION REPORTING

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

'suspicious transaction' means such transactions-

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

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

'suspicious transaction' means such transactions-

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

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

Generally STR/SAR means a formatted report of suspicious transactions/activities where there is reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seems to be usual manner. Such report is to be submitted by banks to the competent authorities i.e. to BFIU. Suspicion basically involves a personal and subjective assessment. The bank has to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

6.3 IDENTIFICATION OF STR/SAR

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

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

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

All suspicions reported to the CCU will be documented, or recorded electronically. The report will include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the suspicion. All internal enquiries made in relation to the report will also be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

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

- **Identification:**

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

- **Evaluation:**

  This part must be in place at branch level and Central Compliance Unit (CCU). After identification of STR/SAR at branch level, BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. If BAMLCO is not satisfied, he should forward the report to CCU. After receiving report from branch, CCU should check the sufficiency of the required documents. Every stages of evaluation (whether reported to BFIU or not), bank should keep records with proper manner.

- **Disclosure:**

  This is the final stage and bank should submit STR/SAR to BFIU if it still looks suspicious.

6.4 TIPPING OFF

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

6.5 CASH TRANSACTION REPORT

Every branch will prepare the monthly cash transaction report and send it to CCU in due

time. If the branch have not any such transaction, it should report it to the CCU as 'There is no reportable CTR'. Simultaneously, branches need to identify whether there is any suspicious transaction reviewing the cash transactions. If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' to the CCU. If no such transaction is identified, it needs to inform to the CCU as 'No suspicious transaction has been found' while reporting the CTR. Besides, every branch needs to preserve its CTR in their own branch.

The Central Compliance Unit (CCU) needs to prepare the accumulated CTR received from its all branches. The CCU must ensure the accuracy and timelines while reporting to BFIU. Moreover CCU has to review all the cash transaction from the branches above the threshold and search for any suspicious transaction. If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' to the CCU. CCU has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR. Moreover, CCU must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

6.6 SELF ASSESSMENT REPORT

According to the instructions of BFIU, branches need to conduct the Self-Assessment to evaluate them on a half yearly basis. Self-Assessment has to be done through a checklist that is circulated by BFIU circular no. 10; dated 28th December, 2014. Before finalizing the evaluation report, there will have to be a meeting presided over by the branch manager with all concerned officials of the branch. In that meeting, there will be a discussion on the branch evaluation report; if the identified problems according that report are possible to solve at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations will have to be jotted down. In the subsequent quarterly meetings on preventing money laundering and terrorist financing, the progress of the related matters should be discussed.

After the end of every half year, the branch evaluation report along with the measures taken by the branch in this regard and adopted recommendations regarding the issue should be submitted to the Internal Control & Compliance Division (ICCD) (Internal Audit Department) of the Head Office and the Central Compliance Unit within the 15th of the next month.

6.7 INDEPENDENT TESTING PROCEDURE

Independent testing has to be done through a checklist that is circulated by BFIU circular no. 10; dated 28th December, 2014. The audit must be independent (i.e. performed by people not involved with the bank's AML&CFT compliance). Audit is a kind of assessment of checking of a planned activity. The individuals conducting the audit should report directly to the board of directors/senior management. Audit function will be done by the Internal Control & Compliance Division (ICCD) (Internal Audit Department). At the same time external auditors could be appointed (if possible) to review the adequacy of the program.

6.8 INTERNAL CONTROL & COMPLIANCE DIVISION'S (ICCD) (INTERNAL AUDIT DEPARTMENT'S) OBLIGATIONS REGARDING SELF ASSESSMENT OR INDEPENDENT TESTING PROCEDURE

The Internal Control & Compliance Division (ICCD) (Internal Audit Department) shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the CCU.

While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the Internal Control & Compliance Division (ICCD) (Internal Audit Department) should examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure. The Internal Control & Compliance Division (ICCD) (Internal Audit Department) should send a copy of the report with the rating of the branches inspected/audited by the ICCD to the CCU of the bank.

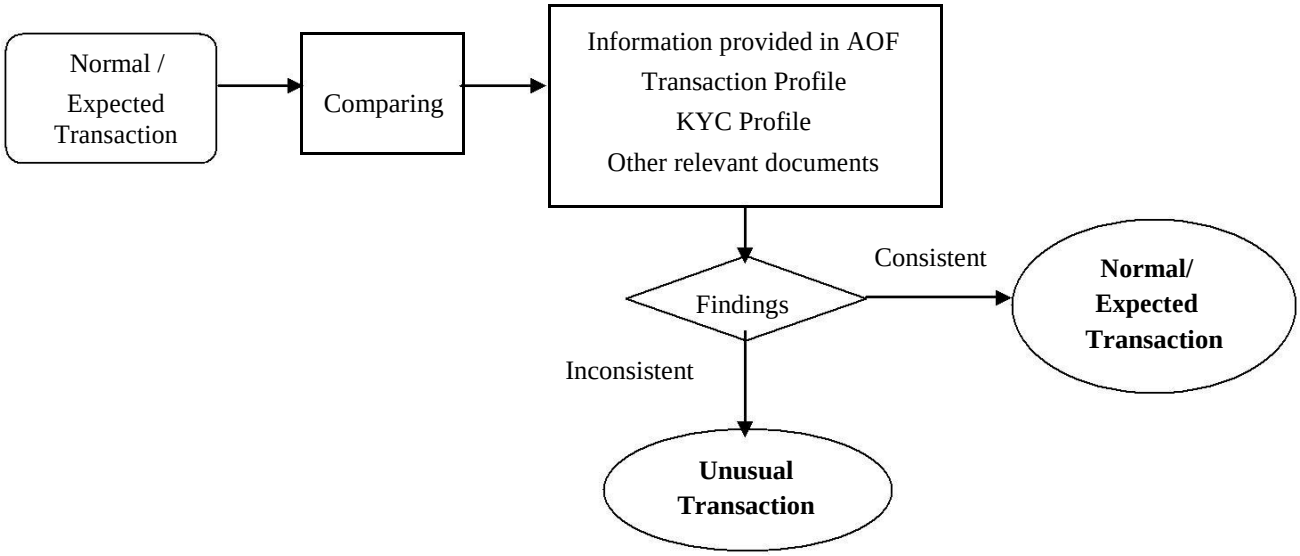
6.9 CENTRAL COMPLIANCE UNIT'S OBLIGATIONS REGARDING SELF ASSESSMENT OR INDEPENDENT TESTING PROCEDURE

Based on the received branch evaluation reports from the branches and submitted inspection/audit reports by the Internal Control & Compliance Division (ICCD) (Internal Audit Department), the Central Compliance Unit shall prepare a checklist based evaluation report on the inspected branches in a considered half year time. In that report, beside other topics, the following topics must be included:

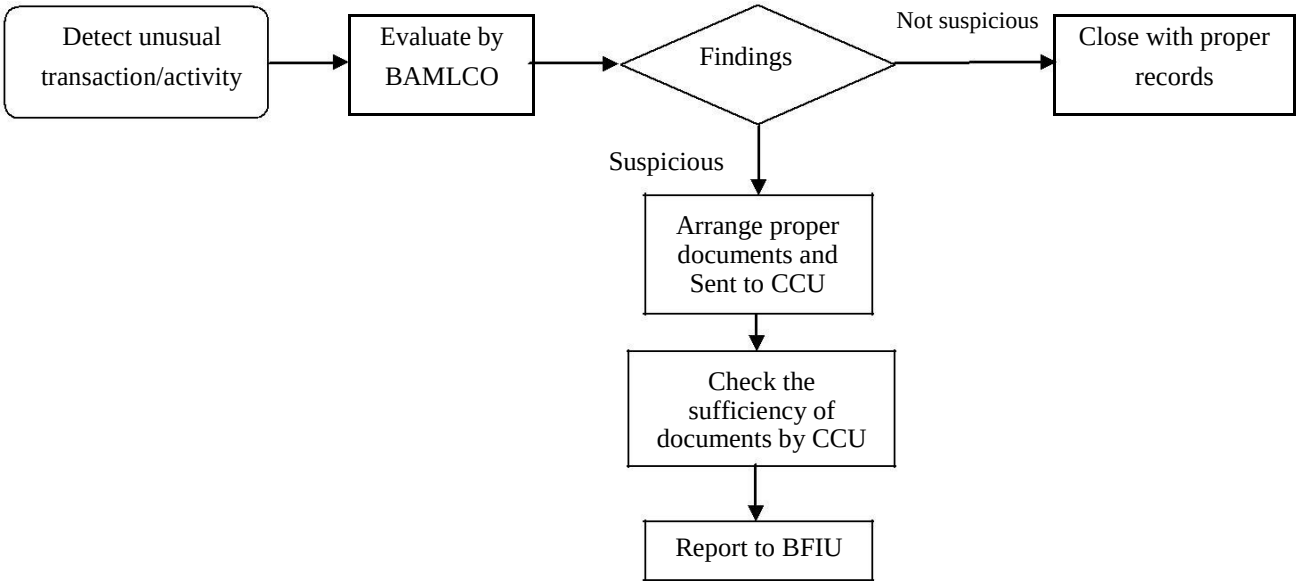
(a) Total number of branch and number of self-assessment report received from the branches;
(b) The number of branches inspected/audited by the ICCD at the time of reporting and the status of the branches (branch wise achieved number);
(c) Same kinds of irregularities that have been seen in maximum number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

6.10 FLOW-CHART FOR IDENTIFICATION OF STR/SAR

The following chart shows the graphical presentation of identification of STR/SAR-



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



RECRUITMENT, TRAINING AND AWARENESS

7.1 OBLIGATIONS UNDER CIRCULAR

Obligations under BFIU Circular-10; dated 28/12/2014

To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, bank should follow proper Screening Mechanism in case of recruitment and ensure proper training for their officials.

7.2 EMPLOYEE SCREENING

Social Islami Bank Limited (SIBL) has to follow fair recruitment procedure to minimize ML & TF risks arose by or through its employees. This fair recruitment procedure will not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, bank is required to follow the following measures (at least one from below):

- reference check
- background check
- screening through or clearance from Law Enforcement Agency
- personal interviewing
- personal guarantee etc.

Before assigning an employee in a particular job or desk, bank will examine the consistency and capability of the employee and be ensured that the employee will have necessary training on AML & CFT lessons for the particular job or desk.

7.3 KNOW YOUR EMPLOYEE (KYE)

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

7.4 TRAINING FOR EMPLOYEE

Every employee of the bank will have at least basic AML & CFT training that should cover all the aspects of AML & CFT measures in Bangladesh. Basic AML & CFT training will be at least day long model having evaluation module of the trainees. Relevant provision of Acts, rules and circulars, guidelines, regulatory requirements, suspicious transaction or activity reporting will be covered in basic AML & CFT training course. To keep the employees updated about AML & CFT measures, the bank will arrange refreshment training programs of its employees on a regular basis.

AML & CFT basic training will cover the following-

- an overview of AML & CFT initiatives;
- relevant provisions of MLPA & ATA and the rules there on;
- regulatory requirements as per BFIU circular, circular letters and guidelines;

- STR/SAR reporting procedure;
- ongoing monitoring and sanction screening mechanism;

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

7.5 AWARENESS OF SENIOR MANAGEMENT

Bank is required to arrange, at least once in a year, an awareness program for all the members of its board of directors or in absence of board of directors, members of the highest policy making committee and people engaged with policy making of the bank.

7.6 CUSTOMER AWARENESS

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

7.7 AWARENESS OF MASS PEOPLE

Bank is encouraged to arrange public awareness programs on AML & CFT issues like advertisements through billboard, poster, festoon and mass media, distribution of handbills, leaflet and so on.

TERRORIST FINANCING & PROLIFERATION FINANCING

8.1 INTRODUCTION

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

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

Regardless of whether the funds in a transaction are related to terrorists or terrorist activities, business relationships with such individuals or other closely associated persons or entities could, under certain circumstances, expose a bank to significant reputational, operational, and legal risk. This risk is even more serious if the person or entity involved is later shown to have benefited from the lack of effective monitoring or willful blindness of a particular bank and thus was to carry out terrorist acts.

8.2 LEGAL OBLIGATIONS

Obligations under ATA, 2009 -

"Every Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 and if any suspicious transaction is identified, the agency shall spontaneously report it to Bangladesh Bank without any delay.

The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each bank should approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, 2009; which are applicable to the bank, have been complied with or not."

8.3 OBLIGATIONS UNDER CIRCULAR

Obligations under BFIU Circular-10; dated 28/12/2014 -

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

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

8.4 NECESSITY OF FUNDS BY TERRORIST

Terrorist organizations need money to operate. Weapons and ammunition are expensive. Major international operations require substantial investments for personnel, training, travel and logistics. Organizations must have substantial fundraising operations, as well as mechanisms for moving funds to the organization and later to terrorist operators. These functions entail considerable risk of detection by authorities, but also pose major challenges

to both the terrorists and intelligence agencies.

8.5 SOURCES OF FUND/RAISING OF FUND

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

8.6 MOVEMENT OF TERRORIST FUND

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

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

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

8.6.1 FORMAL FINANCIAL SECTOR

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

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

8.6.2 TRADE SECTOR

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

8.6.3 CASH COURIERS

The physical movement of cash is one way terrorists can move funds without encountering the AML/CFT safeguards established in financial institutions. It has been suggested that some groups have converted cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside of the financial system. The movement of cash across the borders is prevalent in the cash based economy and where the electronic banking system remains embryonic or is little used by the populace.

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

8.6.4 USE OF ALTERNATIVE REMITTANCE SYSTEMS (ARS)

Alternative remittance systems (ARS) are used by terrorist organizations for convenience and access. ARS have the additional attraction of weaker and/or less opaque record-keeping

and in many locations may be subject to generally less stringent regulatory oversight. Although FATF standards call for significantly strengthened controls over such service providers, the level of anonymity and the rapidity that such systems offer have served to make them a favored mechanism for terrorists.

8.6.5 USE OF CHARITIES AND NON-PROFIT ORGANISATIONS

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

8.7 TARGETED FINANCIAL SANCTIONS

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

For effective implementation of these provisions, detailed mechanism has been developed in Anti-terrorism Rules, 2013. Under rule 16 of AT rules, 2013, banks as a reporting agency has to maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. In case there is any fund or economic resources held by the listed individuals and entities, the banks should immediately stop payment or transaction of funds, financial assets or economic resources and report to the BFIU within the next working day with full particulars of the listed and/or the suspected individuals or entities or related or connected individual identities.

8.8 AUTOMATED SCREENING MECHANISM OF UNSCRs

For effective implementation of TFS relating to TF & PF banks are required to have automated screening mechanism that could prohibit any listed individuals or entities to enter into the banking channel. The banks should operate in such system whether they could detect any listed individuals or entities prior to establish any relationship with them. In particular, banks need to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individuals or entities could not use the formal financial channel. In a word, bank shall ensure that screening has done before -

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

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

- legal obligation and consequences of non-compliance;
- sources of information;
- what to do and how to do with sanction list;
- transactional review;
- how to deal with ‘false positives’;

- how to deal with actual match;
- how to deal with 'aggrieved person or entity';
- how to exercise 'exemption' requirements;

- listing & de-listing process.

8.9 ROLE OF BANK IN PREVENTING TF & PF

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

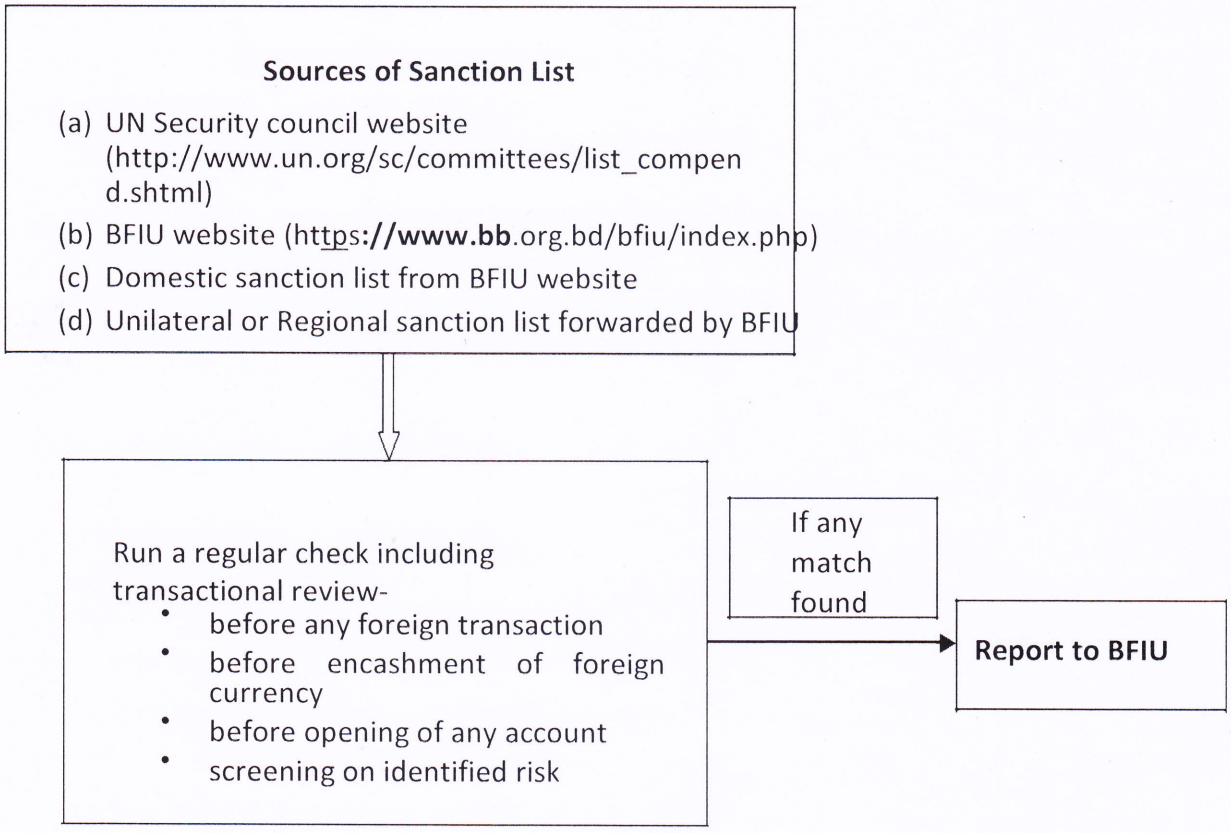
- Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 and if any suspicious transaction is identified, bank will spontaneously report it to Bangladesh Bank without any delay.

- If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, bank will send the details of the accounts (if any is found with the bank) of any persons who are engaged in those activities to BFIU immediately.

- Bank should maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. Bank should run regular check on the given parameters, including transactional review, to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with the bank.

- Bank should run a check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009; individuals or entities owned or controlled directly or indirectly by such persons or entities, as well as persons and entities acting on behalf of, or at the direction of, individuals or entities listed or scheduled under the Act are holding any funds, financial assets or economic resources or related services or having any form of relationship with the bank.

10.8 FLOW-CHART FOR IMPLEMENTATION OF TFS BY BANK



Annexure- A

RISK REGISTER

1. ML & TF Risk Register for Customers

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer				
Walk-in customer (beneficiary is government/ semi government/ autonomous body/ bank & NBFI)				
Walk-in customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBFI)				
Non-resident customer (Bangladeshi)				
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)				
A customer making series of transactions to the same individual or entity				
Customer involved in outsourcing business				
Customer appears to do structuring to avoid reporting threshold				
Customer appears to have accounts with several banks in the same area				
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting				
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court				
Negative news about the cust business in media or from other reliable sources				
Customer is secretive and reluctant to meet in person				
Customer is a mandate who is operating account on behalf of another person/ company.				
Large deposits in the account of customer with low income				
Customers about whom BFIU seeks information (individual)				
A customer whose identification is difficult to check				

Significant and unexplained geographic distance between the bank and the location of the customer				
Customer is a foreigner				
Customer is a minor				
Customer is Housewife				
Customers that are politically exposed persons (PEPs) or influential persons (IPs) or chief/senior officials of international organizations and their family members and close associates				
Customer opens account in the name of his/her family member who intends to credit large amount of deposits				
Customers doing significant volume of transactions with higher -risk geographic locations.				
A customer who brings in large amounts of used notes and/or small denominations				
Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)				
Customer is a money changer/ courier service agent / travel agent				
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above				
Customer is involved in Manpower Export Business				
Customer has been refused to provide banking facilities by another bank				
Accounts opened before 30 April, 2002				
Customers with complex accounting and huge transaction				
Receipt of donor fund , fund from foreign source by micro finance institute (MFI)				
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source				
Wholesale Banking Customer				
Entity customer having operations in multiple locations				

Customers about whom BFIU seeks information (large corporate)				
Owner of the entity that are Influential Persons (IPs) and their family members and close associates				
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)				
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).				
A customer whose identification is difficult to check.				
Owner of the entity that are Politically Exposed Persons (PEPs) or chief / senior officials of International Organizations and their family members and close associates				
Charities or NPOs (especially operating in less privileged areas).				
Credit Card Customer				
Customer who changes static data frequently				
Credit Card customer				
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments				
Prepaid Card customer				
International Trade Customer				
A new customer (Outward remittance-through SWIFT)				
A new customer (Import/ Export)				
A new customer (Inward remittance-through SWIFT)				
A new customer who wants to carry out a large transaction (Import/ Export)				
A new customer who wants to carry out a large transaction (Inward/ outward remittance)				
A customer wants to conduct business beyond its line of business (import/ export/ remittance)				
Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates				
A new customer who wants to carry out a large transaction (Import/ Export)				
Correspondent Banks				
Money services businesses (remittance houses, exchange houses)				

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

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)				
Gift Cheque				
Locker Service				
Foreign currency endorsement in Passport				
Large transaction in the account of under privileged people				
FDR (less than 2 million)				
FDR (2 million and above)				
Special scheme deposit accounts opened with big installment and small tenure				
Multiple deposit scheme accounts opened by same customer in a branch				
Multiple deposit scheme accounts opened by same customer from different location				
Open DPS in the name of family member Or Installments paid from the account other than the customer's acco				
Stand alone DPS				
Early encashment of FDR, special scheme etc.				
Non face to face business relationship /transaction				
Payment received from unrelated/un-associated third parties				
Retail Privilege Facilities				
Pre- Approved Credit Card with BDT 300K limit				
Enhanced ATM cash withdrawal Limit BDT 100K				
SME Banking Product				
Want to open FDR where source of fund is not clear				
Early encashment of FDR				
Repayment of loan EMI from source that is not clear				

Repayment of full loan amount before maturity				
Loan amount utilized in sector other than the sector specified during availing the loan				
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount				
Source of fund used as security not clear at the time of availing loan				
Wholesale Banking Product				
Development of new product & service of bank				
Payment received from unrelated third parties				
High Value FDR				
Term loan, SOD(FO), SOD(G-work order), SOD(Garment),SOD(PO), Loan General, Lease finance, Packing Credit, BTB L/C				
BG(bid bond), BG(PG), BG(APG)				
L/C subsequent term loan, DP L/C				
C.C(H), SOD(G-Business), STL				
OBU				
Syndication Financing				
Credit Card				
Supplementary Credit Card Issue				
Frequent use of Card Cheque				
BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)				
Credit card issuance against ERQ and RFCD accounts				
International Trade				
Line of business mismatch (import/export/remittance)				
Under/ Over invoicing (import/export/remittance)				
Retirement of import bills in cash (import/export/remittance)				
Wire transfer				
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)				

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Online (multiple small transaction through different branch)				
BEFTN				
BACH				
IDBP				
Mobile Banking				
Third party agent or broker				
Credit Card				
New Merchant sign up				
High volume transaction through POS				
Alternate Delivery Channel				
Large amount withdrawn from ATMs				
Larger amount transaction from different location and different time(mid night) through ATM				
Large amount of cash deposit in CDM				
Huge fund transfer through internet				
Transaction Profile updated through Internet Banking				
Customer to business transaction-Online Payment Gateway -Internet Banking				
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)				
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103) .				

4. Risk Register for Country/jurisdiction

Risk	Likelihood	Impact	Risk score	Treatment/Action
Import and export form/to sanction country				
Transshipments, container, flag vessel etc. under global sanction				
Establishing correspondent relationship with sanction bank and/or country				
Establishing correspondent relationship with poor AML&CFT practice country				

Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas				
Customer belongs to countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.				
Customer belongs to High Risk ranking countries of the Basel AML index.				
Customer belongs to the countries identified by the bank as higher -risk because of its prior experiences or other factors.				
Any country identified by FATF or FSRBs-(FATF style Regional Body) as not having adequate AML&CFT systems				
Any bank that provi				
Any bank that allow payable through account				
Any country identified as destination of illicit financial flow				
Branches in a Border Area				
Area identified as high risk in the NRA				
Countries subject to UN embargo/sanctions				

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML/CFT guideline				
Not forming a Central Compliance Unit (CCU)				
Not having an AML&CFT Compliance Officer				
Not having Branch Anti Money Laundering Compliance Officer				
Not having an AML&CFT program				
No senior management commitment to comply with MLP and AT Act				
Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.				
Unique account opening form not followed while opening account				
Non screening of new and existing customers against UNSCR Sanction and OFAC lists				

Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.				
Complete and accurate information of customer not obtained				
Failure to verify the identity proof document and address of the customer				
Beneficial owner identification and verification not done properly				
Customer Due Diligence (CDD) not practiced properly				
Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPS and influential person and senior official of international organization.)				
Failure to complete KYC of customer including walk in customer				
Failure to update TP and KYC of customer				
Keep the legacy accounts operative without completing KYC				
Failure to assess the ML & TF risk of a product or service before launching				
Failure to complete the KYC of Correspondent Bank				
Senior Management approval not obtained before entering into a Correspondent Banking relationship				
Failure to comply with the instruction of BFIU by bank Foreign subsidiary				
Failure to keep record properly				
Failure to report complete and accurate CTR on time				
Failure to review CTR				
Failure to identify and monitor structuring				
Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity				
Failure to conduct quarterly meeting properly				
Failure to report suspicious transactions (STR)				
Failure to conduct self assessment properly				
Failure to submit statement/ report to BFIU on time				
Submit erroneous statement/ report to BFIU				

Not complying with any order for freezing or suspension of transaction issued by BFIU or BB				
Not submitting accurate information or statement sought by BFIU or BB.				
Not submitting required report to senior management regularly				
Failure to rectify the objections raised by BFIU or bank inspection teams on time				
Failure to obtain information during wire transfer				
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank				
Failure to scrutinize staff properly				
Failure to circulate BFIU guidelines and circulars to branches				
Inadequate training/ workshop arranged on AML & CFT				
No independent audit function to test the AML program				

Annexure- B

KYC Documentation

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

Joint Accounts	➢ Passport ➢ National Id Card ➢ Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) ➢ Valid driving license (if any) ➢ Credit Card (if any) ➢ Any other documents (photo) that satisfy to the bank.	➢ Salary Certificate (for salaried person). ➢ Employed ID (For ascertaining level of employment). ➢ Self declaration acceptable to the bank. (commensurate with declared occupation) ➢ Documents in support of benefici ➢ income (income of house wife, students etc.) ➢ Trade License if the customer declared to be a business person ➢ TIN (if any) ➢ Documents of property sale. (if any) ➢ Other Bank statement (if any) ➢ Document of FDR encashment (if any) ➢ Document of foreign remittance (if any fund comes from outside the country) ➢ Document of retirement benefit. ➢ Bank loan.	➢ Acknowledgement receipt of thanks letter through postal department. ➢ Proof of delivery of thanks letter through courier. ➢ Third party verification report. ➢ Physical verification report of bank official ➢ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or name. Residential address appearing on an official document prepared by a Government Agency
Sole Proprietorships or Individuals doing business	➢ Passport ➢ National Id Card ➢ Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) ➢ Valid driving license (if any) ➢ Credit Card (if any) ➢ Rent receipt of the shop (if the shop is rental) ➢ Ownership documents of the shop (i.e purchase documents of the shop or inheritance documents) ➢ Membership certificate of any association. (Chamber of comers, market association,	➢ Trade License ➢ TIN ➢ Self declaration acceptable to the bank. (commensurate with nature and volume of business) ➢ Documents of property sale. (if injected any fund by selling personal property) ➢ Other Bank statement (if any)	➢ Acknowledgement receipt of thanks letter through postal department. ➢ Proof of delivery of thanks letter through courier. ➢ Third party verification report. ➢ Physical verification report of bank official ➢ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or name. ➢ Residential address appearing on an official document prepared by

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

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

Government-Owned entities	➢ Statue of formation of the entity ➢ Resolution of the board to open an account and identification of those who have authority to operate the account. ➢ Passport of the operator (s) ➢ National Id Card of the operator (s)	N/A	N/A
NGO	➢ National Id Card of the operator (s) ➢ Passport of the operator (s) ➢ Resolution of the board of directors to open an account and identification of those who have authority to operate the account. ➢ Documents of nature of the NGO ➢ Certificate of registration issued by competent authority ➢ Bye-laws (certified) ➢ List of Management Committee/ Directors	➢ A copy of last available financial statements duly certified by a professional accountant. ➢ Other Bank statement ➢ TIN ➢ Certificate of Grand / Aid	
Charities or Religious Organisations	➢ National Id Card of the operator (s) ➢ Passport of the operator (s) ➢ Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. ➢ Documents of nature of the Organisations ➢ Certificate of registration issued by competent authority (if any) ➢ Bye-laws (certified) ➢ List of Management Committee/ Directors	➢ A copy of last available financial statements duly certified by a professional accountant ➢ Other Bank statement ➢ Certificate of Grant / Aid/ donation ➢ Any other legal source	
Clubs or Societies	➢ National Id Card of the operator (s) ➢ Passport of the operator (s) ➢ Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. ➢ Documents of nature of the Organisations	➢ A copy of last available financial statements duly certified by a professional (if registered) ➢ Other Bank statement ➢ Certificate of Grant / Aid	

	➢ Certificate of registration issued by competent authority (if any) ➢ Bye-laws (certified) ➢ List of Management Committee/ Directors	➢ Subscription ➢ If unregistered declaration of authorized person/ body.	
Trusts, Foundations or similar entities	➢ National Id Card of the trustee (s) ➢ Passport of the trustee (s) ➢ Resolution of the Managing body of the Foundation/Association to open an account and identification of those who have authority to operate the account. ➢ Certified true copy of the Trust Deed ➢ Bye-laws (certified) ➢ Power of attorney allowing transaction in the account.	➢ A copy of last available financial statements duly certified by a professional (if registered) ➢ Other Bank statement ➢ Donation	
Financial Institutions (NBFI)	➢ Passport of all the directors ➢ National Id Card of all the directors ➢ Certificate of incorporation ➢ Memorandum and Articles of Association ➢ Certificate of commencement of business ➢ List of directors in form -XII ➢ Resolution of the board of directors to open an account and identification of those who have authority to operate the account. ➢ Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. ➢ Nature of the business ➢ Expected monthly turnover ➢ Identity of beneficial owners, holding 20% interest or more of having control over the company's ass person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time	➢ A copy of last available financial statements duly certified by a professional accountant. ➢ Other Bank statement ➢ Trade License ➢ TIN ➢ VAT registration ➢ Cash flow statement	

	employee , officer or director of the company. ➢		
Embassies	Valid Passport with visa of the authorized official ➢ Clearance of the foreign ministry ➢ Other relevant documents in support of opening account	N/A	

Important - This is an example of documents that may be taken by a bank in case of establishing business relationship with its clients. But it is a mere example only, the bank should urge correct and accurate information that could satisfy the bank itself.

Annexure- C

Red Flags pointing to Money Laundering

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

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

Red Flags pointing to Financing of Terrorism

Behavioral Indicators:

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

Indicators linked to the financial transactions:

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

Annexure- D

সোস্যাল ইসলামী ব্যাংক লিমিটেড
মানিলন্ডারিং প্রতিরোধ ইউনিট
প্রধান কার্যালয়,ঢাকা।

তারিখঃ ১৯-০৪-২০১৫ ইং

"সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তারে অর্থায়ন প্রতিরোধ সংক্রান্ত নীতিমালা" (Policy for Prevention of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction)

"বিএফআইইউ সার্কুলার নং-১০ তারিখঃ ২৮-১২-২০১৪ ইং এর ১.৩ নং এবং ১.৪ নং অনুচ্ছেদে বর্ণিত নির্দেশনানুসারে গঠিত প্রধান কার্যালয়ের কেন্দ্রীয় পরিপালন ইউনিট (Central Compliance Unit) এবং শাখা পর্যায়ে শাখা পরিপালন ইউনিট (Branch Compliance Unit) সন্ত্রাস বিরোধী আইন, ২০০৯, সন্ত্রাস বিরোধী আইন (সংশোধিত), ২০১২ এবং সন্ত্রাস বিরোধী আইন (সংশোধিত), ২০১৩, এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়ন প্রতিরোধ সংক্রান্ত বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট জারীকৃত নির্দেশনা পরিপালন ও আভ্যন্তরীণ পরিবীক্ষণের দায়িত্ব পালন করবে।

সন্ত্রাস বিরোধী আইন, ২০০৯, সন্ত্রাস বিরোধী আইন (সংশোধিত), ২০১২ এবং সন্ত্রাস বিরোধী আইন (সংশোধিত), ২০১৩ এর নির্দেশনা পরিপালনের ক্ষেত্রে কোন গ্রাহকের কোন লেনদেন বা লেনদেনের প্রচেষ্টা হতে যদি এ মর্মে সন্দেহ করার যুক্তিসঙ্গত কারণ সৃষ্টি হয় যে, কোন অর্থ বা লেনদেন সন্ত্রাস বিরোধী আইন, ২০০৯, সন্ত্রাস বিরোধী আইন (সংশোধিত), ২০১২ এবং সন্ত্রাস বিরোধী আইন (সংশোধিত), ২০১৩ অনুসারে সন্ত্রাসী কার্যে অর্থ যোগানের সাথে সংশ্লিষ্ট এবং ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নের সাথে সংশ্লিষ্ট তবে সঙ্গে সঙ্গে বিষয়টি বিএফআইইউ সার্কুলার নং-১০ তারিখঃ ২৮-১২-২০১৪ ইং এর পরিশিষ্ট-গ মোতাবেক একইদিনে শাখা মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা (BAMLCO) অথবা শাখা পরিপালন ইউনিট ইনচার্জ এর মন্তব্য সহকারে একটি রিপোর্ট প্রধান কার্যালয়ের কেন্দ্রীয় পরিপালন ইউনিটে প্রেরণ করবে। কেন্দ্রীয় পরিপালন ইউনিট প্রাপ্ত রিপোর্টটি পরীক্ষণ ও পর্যালোচনান্তে মতামত সন্নিবেশ করবে এবং রিপোর্টকরণ যোগ্য বিবেচনার ক্ষেত্রে গোপনীয়তার সঙ্গে সর্বোচ্চ ০৩ (তিন) কর্মদিবসের মধ্যে বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটে প্রেরণ করবে।

শাখা সমূহ ১) নতুন হিসাব খোলা এবং গ্রাহকের হিসাব পরিচালনাকালে গ্রাহকের পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংরক্ষণ করণ, ২) কোন গ্রাহকের হিসাব বন্ধ হলে বন্ধ হওয়ার তারিখ হতে অনূন্য ৫(পাঁচ) বৎসর পর্যন্ত উক্ত হিসাবের লেনদেন সংক্রান্ত তথ্য সংরক্ষণ করণ, ৩) উপরোক্ত ১ ও ২ এর অধীন সংরক্ষিত তথ্যাদি বাংলাদেশ ব্যাংকের চাহিদা মোতাবেক, সময় সময়, সরবরাহ নিশ্চিতকরণে যথাযথ ব্যবস্থা গ্রহণ করা, ৪) কোন হিসাব সন্ত্রাসী কার্যে অর্থ যোগানের সঙ্গে জড়িত থাকিতে পারে এরূপ সন্দেহ হলে স্ব-উদ্যোগে প্রধান কার্যালয়স্থিত কেন্দ্রীয় পরিপালন ইউনিটে অবিলম্বে অবহিত করা, যাতে তা দ্রুততম সময়ে বাংলাদেশ ব্যাংককে অবহিত করা যায়। এছাড়া বাংলাদেশ ব্যাংক কর্তৃক সংশ্লিষ্ট বিষয়ে জারীকৃত ও ভবিষ্যতে জারিতব্য নির্দেশনা শাখাসমূহ পরিপালন করবে।

সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়ন সম্পর্কিত সংবাদ গণমাধ্যমে প্রকাশ হবার সাথে সাথে উক্ত কর্মকান্ডের সাথে জড়িত কোন ব্যক্তি বা সত্তার কোন ব্যাংক হিসাব পরিচালিত হয়ে থাকলে এ বিষয়ক বিস্তারিত তথ্য সংশ্লিষ্ট শাখা অবিলম্বে কেন্দ্রীয় পরিপালন ইউনিটে প্রেরণ করবে, যেন তা দ্রুততম সময়ে বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটে প্রেরণ করা যায়।

বিএফআইইউ সার্কুলার নং-১০ তারিখঃ ২৮-১২-২০১৪ ইং এর অনুচ্ছেদ ২(৩) অনুসারে জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলুশনের আওতায় সন্ত্রাস ও সন্ত্রাসীকার্যে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার কোন হিসাব খোলা যাবে না বা পরিচালনা করা যাবে না। জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলুশনের আওতায় তালিকাভুক্ত ব্যক্তি বা সত্তা বলতে সন্ত্রাস বিরোধী বিধিমালা, ২০১৩ এর ২ (ছ) নং বিধিতে সংজ্ঞায়িত রেজুলুশনের আওতায় তালিকাভুক্ত ব্যক্তি বা সত্তাকে বুঝাবে। এই তালিকাসমূহ http://www.un.org/sc/committees/index.shtml বা http:// www. bb.org.bd/ aboutus/dept/bfiu/sanction_list.php ওয়েবলিংক হতে সংগ্রহ করা যাবে। বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তা বলতে সন্ত্রাস বিরোধী আইন, ২০০৯ এর ১৮ নম্বর ধারায় প্রদত্ত ক্ষমতাবলে বাংলাদেশ সরকার কর্তৃক সময়ে সময়ে সরকারি গেজেট প্রজ্ঞাপন দ্বারা তফসিলভুক্ত কোন ব্যক্তি বা সত্তাকে বুঝাবে।

জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলুশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার হালনাগাদ তথ্য ইলেক্ট্রনিক পদ্ধতিতে সংরক্ষণ করা হবে।

"সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তারে অর্থায়ন প্রতিরোধ সংক্রান্ত নীতিমালা" (Policy for Prevention of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction)

প্রতিটি শাখা (প্রধান কার্যালয়স্থিত সংশ্লিষ্ট ডিভিশন/বিভাগ/ইউনিট/সেল সহ) জাতিসংঘের নিরাপত্তা পরিষদের কোন রেজুলুশনের আওতায় বা বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তার নামে অথবা প্রত্যক্ষ বা পরোক্ষভাবে তাদের নিয়ন্ত্রণাধীন/স্বার্থসংশ্লিষ্ট কোন ব্যক্তি বা সত্তার নামে ব্যাংক হিসাব রয়েছে কিনা বা কোন লেনদেন সংঘটিত হয়েছে কিনা তা চিহ্নিত করার জন্য নিয়মিত লেনদেন মনিটর করবে এবং প্রয়োজনে লেনদেন পর্যালোচনা করবে। তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তা অথবা প্রত্যক্ষ বা পরোক্ষভাবে তাদের নিয়ন্ত্রণাধীন/স্বার্থসংশ্লিষ্ট কোন ব্যক্তি বা সত্তার কোন ব্যাংক হিসাব বা লেনদেন চিহ্নিত হওয়ার সাথে সাথে সংশ্লিষ্ট শাখা (প্রধান কার্যালয়স্থিত সংশ্লিষ্ট ডিভিশন/বিভাগ/ইউনিট/সেল সহ) উক্ত হিসাবের লেনদেন বা লেনদেনটি স্থগিত করে একইদিনে কেন্দ্রীয় পরিপালন ইউনিটকে অবহিত করবে যেন পরবর্তী কর্ম দিবসের মধ্যে এ বিষয়ক বিস্তারিত তথ্য বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটকে অবহিত করা যায়।

যদি অয়্যার ট্রান্সফার সংক্রান্ত লেনদেনের আবেদনকারী কিংবা বেনিফিশিয়ারী জাতিসংঘের নিরাপত্তা পরিষদের কোন রেজুলুশনের আওতায় বা বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তা হয় তবে তা চিহ্নিত হওয়ার সাথে সাথে সংশ্লিষ্ট শাখা (প্রধান কার্যালয়স্থিত সংশ্লিষ্ট ডিভিশন/বিভাগ/ইউনিট/সেল সহ) উক্ত লেনদেনটি স্থগিত করে একইদিনে কেন্দ্রীয় পরিপালন ইউনিটকে অবহিত করবে যেন পরবর্তী কর্ম দিবসের মধ্যে এ বিষয়ক বিস্তারিত তথ্য বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটকে অবহিত করা যায়।

জাতিসংঘের নিরাপত্তা পরিষদ কর্তৃক গৃহীত রেজুলুশন ১৩৭৩ (২০০১) এর আওতায় বিদেশী সরকার বা বিদেশী এফআইইউ এর অনুরোধে বিএফআইইউ হতে প্রেরিত বা উক্ত রেজুলুশনের আওতায় বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তার সাথে ব্যাংক হিসাব বা অন্য কোন সম্পর্ক রয়েছে কিনা তা চিহ্নিত করার জন্য ব্যাংক নিয়মিত লেনদেন মনিটর করবে এবং প্রয়োজনে লেনদেন পর্যালোচনা করবে। তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তার কোন ব্যাংক হিসাব চিহ্নিত হওয়ার সাথে সাথে সংশ্লিষ্ট শাখা (প্রধান কার্যালয়স্থিত সংশ্লিষ্ট ডিভিশন/বিভাগ/ইউনিট/সেল সহ) উক্ত হিসাবের লেনদেন স্থগিত করে একইদিনে কেন্দ্রীয় পরিপালন ইউনিটকে অবহিত করবে যেন পরবর্তী কর্ম দিবসের মধ্যে এ বিষয়ক বিস্তারিত তথ্য বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটকে অবহিত করা যায়।

আন্তর্জাতিক বাণিজ্যিক লেনদেনের ক্ষেত্রে প্রত্যেকটি ব্যাংক উক্ত লেনদেন সম্পাদনের পূর্বে লেনদেনের সাথে সম্পর্কিত পক্ষসমূহ জাতিসংঘের নিরাপত্তা পরিষদের কোন রেজুলুশনের আওতায় বা বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তা কিনা তা চিহ্নিত করার জন্য লেনদেনটি পর্যালোচনা করবে। তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তার সংশ্লিষ্টতা চিহ্নিত হওয়ার সাথে সাথে সংশ্লিষ্ট শাখা (প্রধান কার্যালয়স্থিত সংশ্লিষ্ট ডিভিশন/বিভাগ/ইউনিট/সেল সহ) উক্ত লেনদেনটি স্থগিত করে একইদিনে কেন্দ্রীয় পরিপালন ইউনিটকে অবহিত করবে যেন পরবর্তী কর্ম দিবসের মধ্যে এ বিষয়ক বিস্তারিত তথ্য বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটকে অবহিত করা যায়।"

Annexure- E

সোস্যাল ইসলামী ব্যাংক লিমিটেড
মানিলন্ডারিং প্রতিরোধ ইউনিট
প্রধান কার্যালয়,ঢাকা।

তারিখঃ ০৬-০৫-২০১৫ ইং

"গ্রাহক নির্বাচনে অনুসরণীয় নীতিমালা (Customer Acceptance Policy)"

ক্রম	শিরোনাম	নীতি	পদ্ধতি
১	ব্যক্তিক হিসাবের প্রাথমিক যোগ্যতা	প্রাপ্ত বয়স্ক, সুস্থ মস্তিষ্ক সম্পন্ন এবং দেউলিয়া নয় এমন যে কোন বাংলাদেশী নাগরিক/নাগরিকগণ নিজ নামে বা যৌথ নামে ব্যাংক হিসাব খুলতে পারবেন ও সেবা গ্রহণ করতে পারবেন।	প্রচলিত আইন ও নিয়মের পাশাপাশি মানি লন্ডারিং প্রতিরোধ আইন ২০১২, সন্ত্রাস বিরোধী আইন ২০০৯, সন্ত্রাস বিরোধী আইন (সংশোধিত) ২০১২, সন্ত্রাস বিরোধী আইন (সংশোধিত) ২০১৩, মানি লন্ডারিং প্রতিরোধ বিধিমালা ২০১৩, সন্ত্রাস বিরোধী বিধিমালা ২০১৩ এবং মানি লন্ডারিং প্রতিরোধ সার্কুলার ও সার্কুলার লেটারসমূহের নির্দেশনা আবশ্যিকভাবে অনুসরণ করতে হবে। গ্রাহকের কেওয়াইসি, টিপি, অর্থের উৎস এবং ঝুঁকি ভিত্তিক গ্রাহক বিভাজন নিশ্চিত করতে হবে।
২	নাবালক	নাবালকদের বয়স উল্লেখপূর্বক তাদের পক্ষে তাদের অভিভাবক হিসাব খুলতে পারবেন।	নাবালক ও অভিভাবকের উভয়েরই কেওয়াইসি করতে হবে, উভয়ের মধ্যকার সম্পর্ক ও অর্থের উৎস যৌক্তিক পর্যায়ে নিশ্চিত করতে হবে।
৩	নিরক্ষর ব্যক্তি	যে কোন নিরক্ষর ব্যক্তি প্রচলিত নিয়ম অনুসরণ করে হিসাব খুলতে পারবে।	নিরক্ষর ব্যক্তির কেওয়াইসি সম্পন্ন করতে হবে। কেবলমাত্র আমানতকারীর ব্যক্তিগত উপস্থিতিতে হিসাব খোলা ও হিসাব হতে টাকা উত্তোলন করা যাবে।
৪	গ্রাহকের তথ্য যাচাই	যে সকল ক্ষেত্রে গ্রাহকের পরিচিতির স্বপক্ষে দলিলাদি সংগ্রহ করা যাবে না বা তথ্যের সত্যতা যাচাই করা যাবে না, ব্যাংক সে সকল হিসাব খুলবে না এবং পরিচালনা করবে না।	-
৫	Politically Exposed Persons (PEPs), প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তা	বিএফআইইউ সার্কুলার নং-১০ তারিখঃ ২৮-১২-২০১৪ ইং এ বর্ণিত Politically Exposed Persons (PEPs), প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তা এর হিসাব ব্যাংক খুলতে পারবে।	Politically Exposed Persons (PEPs), প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার হিসাব খোলার ক্ষেত্রে বিএফআইইউ সার্কুলার নং-১০ তারিখঃ ২৮-১২-২০১৪ ইং এর নির্দেশনা অনুসরণ করতে হবে।
৬	অনিবাসী বাংলাদেশী এবং বিদেশী নাগরিক	ব্যাংক প্রচলিত পদ্ধতি অনুসরণ করে অনিবাসী বাংলাদেশী এবং বিদেশী নাগরিকের ব্যাংক হিসাব খুলতে পারবে।	গ্রাহকের কেওয়াইসি, টিপি, অর্থের উৎস এবং ঝুঁকি ভিত্তিক গ্রাহক বিভাজন নিশ্চিত করতে হবে। অনিবাসী বাংলাদেশীদের হিসাব খোলার ক্ষেত্রে Foreign Exchange Regulation Act, 1947 এর বিধানাবলী ও এর আওতায় বাংলাদেশ ব্যাংক কর্তৃক জারীকৃত নির্দেশনাসমূহ এবং Guidelines for Foreign Exchange Transaction যথাযথভাবে অনুসরণ করতে হবে।
৭	করেসপন্ডেন্ট ব্যাংকিং	ব্যাংক বৈদেশিক বাণিজ্য সম্পাদনের জন্য বিদেশে অবস্থিত ব্যাংকের সাথে করেসপন্ডেন্ট ব্যাংকিং সম্পর্ক স্থাপন করতে পারবে।	করেসপন্ডেন্ট ব্যাংকিং সম্পর্ক স্থাপনের ক্ষেত্রে ব্যাংক বিএফআইইউ সার্কুলার নং-১০ তারিখঃ ২৮-১২-২০১৪ ইং এর নির্দেশনা এবং এফএটিএফ রিকমেন্ডেশন নং ৭ ও ১৮ অনুসরণ করতে হবে।

ক্রম	শিরোনাম	নীতি	পদ্ধতি
৮	পর্দানশীল মহিলা (অক্ষর জ্ঞান সম্পন্ন)	ব্যাংক প্রচলিত পদ্ধতি অনুসরণ করে পর্দানশীল মহিলার ব্যাংক হিসাব খুলতে পারবে।	হিসাব খোলার সময় শাখা ব্যবস্থাপক/দায়িত্ব প্রাপ্ত কর্মকর্তার সম্মুখে গ্রাহকের সশরীরে উপস্থিতি হবে এবং তার পরিচিতি নিশ্চিত করতে হবে।
৯	দৃষ্টিহীন ব্যক্তি	যে কোন দৃষ্টিহীন ব্যক্তি নিজের পছন্দের অন্য ব্যক্তির সহায়তায় প্রচলিত পদ্ধতি অনুসরণ করে ব্যাংক হিসাব খুলতে পারবে।	গ্রাহক এবং সহায়তাকারী উভয়ের কেওয়াইসি সম্পন্ন করতে হবে এবং অর্থ উত্তোলনের সময় উভয়কে স্বশরীরে উপস্থিত থাকতে হবে।
১০	সশরীরে অনুপস্থিত বা দূরবর্তী গ্রাহকের ক্ষেত্রে করণীয়	সশরীরে অনুপস্থিত বা দূরবর্তী গ্রাহককে সেবা প্রদানের ক্ষেত্রে মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়নের ঝুঁকি নিরূপণ ও ঝুঁকি নিরসনের নীতি ও পদ্ধতি অনুসরণ আবশ্যক।	সশরীরে অনুপস্থিত বা দূরবর্তী গ্রাহকের ক্ষেত্রে বিএফআইইউ সার্কুলার নং-১০ তারিখঃ ২৮-১২-২০১৪ ইং এর নির্দেশনা অনুসরণ করতে হবে।
১০	বিদ্যমান গ্রাহক	যদি কোন গ্রাহকের (ব্যক্তি/প্রতিষ্ঠান/গ্রুপ) হিসাব ব্যাংক সংরক্ষণ করে তবে তার অন্য হিসাবও ব্যাংক খুলতে পারবে।	এক্ষেত্রে গ্রাহকের পুনরায় কেওয়াইসি সম্পন্ন করার প্রয়োজন হবে না তবে কোন তথ্য পরিবর্তিত হলে তা হালনাগাদ করতে হবে। নতুন হিসাবের টিপি, অর্থের উৎস এবং ঝুঁকি ভিত্তিক গ্রাহক বিভাজন নিশ্চিত করতে হবে।
১১	প্রাতিষ্ঠানিক হিসাব	আইনগতভাবে প্রতিষ্ঠিত যে কোন প্রাতিষ্ঠান নিজ নামে ব্যাংক হিসাব পরিচালনা করতে পারবে। ব্যক্তি মালিকানাধীন প্রতিষ্ঠানের নামে ব্যাংক হিসাব পরিচালনা করতে পারবে।	প্রতিষ্ঠানটি একটি আইনগত স্বত্ত্বা হলে তার স্বপক্ষে দলিল এবং অন্যান্য ক্ষেত্রে ট্রেড লাইসেন্স/রেজিস্ট্রেশন সনদ বা সংশ্লিষ্ট কর্তৃপক্ষের অনুমতিপত্র সংগ্রহ করতে হবে। হিসাব পরিচালনার ক্ষেত্রে সিগনেটরিজের ক্ষমতা যথাযথভাবে নিশ্চিত হতে হবে। হিসাবের স্বার্থ সংশ্লিষ্ট সকলের কেওয়াইসি নিশ্চিত করতে হবে। হিসাবের টিপি, অর্থের উৎস এবং ঝুঁকি ভিত্তিক গ্রাহক বিভাজন নিশ্চিত করতে হবে। হিসাবের বেনিফিসিয়াল ওনার চিহ্নিত করতে হবে। সরকারী প্রতিষ্ঠানের বেলায় হিসাব পরিচালনার ক্ষেত্রে সিগনেটরিজের ক্ষমতা যথাযথভাবে নিশ্চিত হতে হবে এবং তার কেওয়াইসি সম্পন্ন করতে হবে।
১২	এন জি ও, ক্লাব, চ্যারিটি প্রতিষ্ঠান, সামাজিক সংগঠন	ব্যাংক নির্ধারিত পদ্ধতিতে যে কোন এনজিও, ক্লাব, চ্যারিটি প্রতিষ্ঠান ও সামাজিক সংগঠন এর হিসাব খুলতে পারবে।	এন জি ও, ক্লাব, চ্যারিটি প্রতিষ্ঠান, সামাজিক সংগঠন বিশেষভাবে যে সকল প্রতিষ্ঠান ধর্মীয় মূল্যবোধ, বিশেষ আদর্শ প্রতিষ্ঠা বা বিশেষ কালচার ও গোষ্ঠী নিয়ে কাজ করে, সে সকল ক্ষেত্রে হিসাব খোলা এবং পরিচালনার ক্ষেত্রে গ্রাহকদের সম্পর্কে সতর্ক থাকতে হবে এবং অধিকতর গুরুত্ব সহকারে নিয়মিত লেনদেন মনিটরিং করতে হবে।
১৩	Executors, Administrators, Trustee হিসাব	প্রচলিত নিয়ম অনুসরণ করে ব্যাংক Executors, Administrators এবং Trustee হিসাব খুলতে পারবে।	হিসাব পরিচালনার ক্ষেত্রে সিগনেটরিজের ক্ষমতা যথাযথভাবে নিশ্চিত হতে হবে। হিসাবের স্বার্থ সংশ্লিষ্ট সকলের কেওয়াইসি সম্পন্ন নিশ্চিত করতে হবে। হিসাবের টিপি, অর্থের উৎস এবং ঝুঁকি ভিত্তিক গ্রাহক বিভাজন নিশ্চিত করতে হবে। হিসাবের বেনিফিসিয়াল ওনার চিহ্নিত করতে হবে।

"গ্রাহক নির্বাচনে অনুসরণীয় নীতিমালা (Customer Acceptance Policy)"

যে সকল হিসাব খোলা যাবেনা

ক্রম	শিরোনাম	নীতি	মন্তব্য
১৪	ছদ্মনামে ও নম্বরযুক্ত হিসাব	বেনামে বা ছদ্মনামে বা শুধুমাত্র নম্বরযুক্ত কোন গ্রাহকের হিসাব খোলা যাবে না।	-
১৫	Shell Bank and others	Shell Bank এর সাথে কোন ধরণের ব্যাংকিং সম্পর্ক স্থাপন করা যাবে না। যে সকল রেসপন্ডেন্ট ব্যাংক Shell Bank এর সাথে করেসপন্ডেন্ট ব্যাংকিং সম্পর্ক স্থাপন করে তাদের সাথে কোন ব্যাংকিং সম্পর্ক স্থাপন করা যাবে না। এক্ষেত্রে Shell Bank বলতে ঐসব ব্যাংককে বুঝাবে যারা যেদেশে নিবন্ধিত সেদেশে তাদের কোন শাখা বা কার্যক্রম নেই এবং কোন নিয়ন্ত্রিত আর্থিক গ্রুপ (Regulated Financial Group) এর অধিভুক্ত নয়।	-
		লাইসেন্সবিহীন কোন ব্যাংক/আর্থিক প্রতিষ্ঠান ও মানি চেঞ্জার এর কোন হিসাব খোলা যাবে না।	-
১৬	ML/FT সন্দেহভাজন	গ্রাহক মানি লন্ডারিং বা সন্ত্রাসী কার্যে অর্থ যোগানে জড়িত, ব্যাংক যদি তা জানে বা জোড়ালোভাবে সন্দেহ করার কারণ থাকে তবে ব্যাংক গ্রাহকের হিসাব খুলবে না।	-
১৭	Online হিসাব	বাংলাদেশ ব্যাংক হতে পরবর্তী কোন নির্দেশনা না দেয়া পর্যন্ত গ্রাহকের সশরীরে উপস্থিতি ব্যতীত Online হিসাব খোলা যাবে না।	বিদেশে অবস্থিত বাংলাদেশী নাগরিকগণের কেওয়াইসি, টিপি, অর্থের উৎস এবং ঝুঁকি ভিত্তিক গ্রাহক বিভাজন নিশ্চিত করে বিদেশে অবস্থিত বাংলাদেশী দুতাবাসের মাধ্যমে অথবা নিজস্ব শাখা অথবা আইনগত প্রতিনিধির মাধ্যমে হিসাব খুলতে পারবে।
১৮	Sanctions List	UN Sanction list, OFAC Sanction List এবং বাংলাদেশ ব্যাংক নির্দেশিত/প্রেরিত অন্য যে কোন Sanction list ভুক্ত কোন ব্যক্তি বা প্রতিষ্ঠানের হিসাব ব্যাংক খুলবে না এবং পরিচালনা করবে না। জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলুশনের আওতায় সন্ত্রাস ও সন্ত্রাসীকার্যে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার কোন হিসাব খোলা যাবে না বা পরিচালনা করা যাবে না। জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলুশনের আওতায় তালিকাভুক্ত ব্যক্তি বা সত্তা বলতে সন্ত্রাস বিরোধী বিধিমালা, ২০১৩ এর ২ (ছ) নং বিধিতে সংজ্ঞায়িত রেজুলুশনের আওতায় তালিকাভুক্ত ব্যক্তি বা সত্তাকে বুঝাবে।	-

যে সকল হিসাব খোলা যাবেনা

ক্রম	শিরোনাম	নীতি	মন্তব্য
১৮		এই তালিকাসমূহ http://www.un.org/sc/committees/index.shtml বা http://www.bb.org.bd/aboutus/dept/bfiu/sanction_list.php ওয়েবলিংক হতে সংগ্রহ করা যাবে। বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তা বলতে সন্ত্রাস বিরোধী আইন, ২০০৯ এর ১৮ নম্বর ধারায় প্রদত্ত ক্ষমতাবলে বাংলাদেশ সরকার কর্তৃক সময়ে সময়ে সরকারি গেজেট প্রজ্ঞাপন দ্বারা তফসিলভুক্ত কোন ব্যক্তি বা সত্তাকে বুঝাবে।	-

অনুসরণীয় অন্যান্য নীতিমালা ঃ

১. হিসাব খোলা ও পরিচালনার সময় প্রচলিত আইন ও নিয়মের পাশাপাশি মানি লন্ডারিং প্রতিরোধ আইন ২০১২, সন্ত্রাস বিরোধী আইন ২০০৯, সন্ত্রাস বিরোধী আইন (সংশোধিত) ২০১২, সন্ত্রাস বিরোধী আইন (সংশোধিত) ২০১৩, মানি লন্ডারিং প্রতিরোধ বিধিমালা ২০১৩, সন্ত্রাস বিরোধী বিধিমালা ২০১৩ এবং মানি লন্ডারিং প্রতিরোধ সার্কুলার ও সার্কুলার লেটারসমূহের নির্দেশনা আবশ্যিকভাবে অনুসরণ করতে হবে। এ ছাড়াও ব্যাংকের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ পলিসি অনুসরণ করতে হবে।

২. হিসাব খোলার সময় অভিন্ন হিসাব খোলার ফরম যথাযথভাবে পুরণ করতে হবে।

৩. গ্রাহকের পরিচিতির স্বপক্ষে অবশ্যই সমর্থিত ডকুমেন্ট থাকতে হবে।

৪. প্রাসঙ্গিক অন্যান্য সকল ডকুমেন্ট ও তথ্য সংগ্রহ করতে হবে।

৫. গ্রাহকের লেনদেনের অর্থের উৎস সম্পর্কে নিশ্চিত হতে হবে।

৬. গ্রাহকের নিকট হতে লেনদেনের অনুমিত মাত্রা (টিপি) সংগ্রহ করতে হবে এবং তা অবশ্যই যৌক্তিক ও গ্রাহকের অন্যান্য তথ্যের সাথে সামঞ্জস্যপূর্ণ হতে হবে।

৭. সকল গ্রাহককে অবশ্যই ঝুঁকি ভিত্তিক বিভাজন করতে হবে। উচ্চঝুঁকি সম্পন্ন গ্রাহকদের হিসাব খোলার সময় উচ্চতর অনুমোদন গ্রহন করতে হবে, এই সম্পর্কে সতর্ক থাকতে হবে এবং অধিকতর গুরুত্ব সহকারে নিয়মিত লেনদেন মনিটরিং করতে হবে। নিম্ন ঝুঁকি সম্পন্ন গ্রাহকদের ক্ষেত্রে ন্যূনতম সাধারণ সতর্কতা অবলম্বন করতে হবে এবং নির্দিষ্ট বিরতিতে লেনদেন মনিটরিং করতে হবে।

দায়িত্বঃ

এই নীতিমালা বাস্তবায়নের দায়িত্ব প্রাথমিক ভাবে হিসাবখোলার সাথে সংশ্লিষ্ট কর্মকর্তা (হিসাব খোলার ফরমে স্বাক্ষরকারী কর্মকর্তাগণ), শাখা মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা ও শাখা ব্যবস্থাপকের উপর আরোপিত হবে। নীতিমালা বাস্তবায়নে সার্বিক দায়-দায়িত্ব ব্যাংকের উপর থাকবে।

Annexure- F

Social Islami Bank Limited
Anti Moneylaundering Unit
Corporate Office, Dhaka.

Framework of Central Compliance Unit (CCU) of Prevention of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction of Social Islami Bank Limited.

1.	Deputy Managing Director (Branches Control, General Banking & Marketing Division)	-	Head of Central Compliance Unit (CCU) & Chief Anti Money Laundering Compliance Officer (CAMLCO)
2.	Head of Branches Control, General Banking & Marketing Division	-	Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)
3.	Head of Financial Administration Division	-	Member
4.	Head of Investment Administration Division	-	Member
5.	Head of International Division	-	Member
6.	Head of Information Technology Division	-	Member
7.	Head of AML Unit	-	Member

Framework of Branch Compliance Unit (BCU) of Prevention of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction of Social Islami Bank Limited.

1.	Branch Manager	-	Incharge, Branch Compliance Unit (BCU)
2.	Operation Manager (Deputy Branch Manager)	-	Branch Anti Money Laundering Compliance Officer (BAMLCO)
3.	Head of General Banking Department	-	Member
4.	Head of Investment Department	-	Member
5.	Head of Foreign Exchange Department	-	Member
6.	Any other executive/officer (if required)	-	Member

Social Islami Bank Limited
Anti Moneylaundering Unit
Corporate Office, Dhaka.

AUTHORITIES AND RESPONSIBILITIES OF CAMLCO & BAMLCO of SIBL

For preventing ML, TF & PF in the branch, the **Chief Anti Money Laundering Compliance Officer (CAMLCO)** should perform the following authorities and responsibilities:

Authorities-

1. CAMLCO should be able to act on his own authority;
2. He/she should not consult or seek any permission from the MD or CEO before submission of STR/SAR and any document or information to BFIU;
3. He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
4. He/she must have access to any information of the bank;
5. He/she shall ensure his/her continuing competence.

Responsibilities-

1. CAMLCO must ensure overall AML&CFT compliance of the bank;
2. oversee the submission of STR/SAR or any document or information to BFIU in time;
3. maintain the day-to-day operation of the bank's AML&CFT compliance;
4. CAMLCO shall be liable to MD , CEO or BoD for proper functioning of CCU;
5. CAMLCO shall review and update ML & TF risk assessment of the bank;
6. ensure that corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.

For preventing ML, TF & PF in the branch, the **Branch Anti Money Laundering Compliance Officer (BAMLCO)** should perform the following responsibilities:

1. ensure that the KYC of all customers have been done properly and for the new customer KYC is being done properly;
2. ensure that the UN Security Council and domestic sanction list are checked properly before opening of account and while making any international transaction;
3. keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;
4. ensure regular transaction monitoring to find out any unusual transaction (In case of an automated bank, the bank should follow a triggering system against transaction profile or other suitable threshold. In case of a traditional bank, transaction should be examined at the end of day against transaction profile or other suitable threshold. Records of all transaction monitoring should be kept in the file);
5. review cash transaction to find out any structuring;
6. review CTR to find out STR/SAR;
7. ensure the checking of UN sanction list before making any foreign transaction;
8. ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
9. compile self-assessment of the branch regularly and arrange quarterly meeting regularly;
10. accumulate the training records of branch officials and take initiatives including reporting to CCU, HR and training academy;
11. ensure all the required information and document are submitted properly to CCU and any freeze order or stop payment order are implemented properly;
12. follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
13. ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements of chapter 5;
14. ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.