MONEY LAUNDERING & TERRORIST FINANCING RISK MANAGEMENT POLICY

December, 2024

AML & CFT Division

NRBC Bank PLC.

Head Office, Dhaka

Approved by Board of Directors of the Board on December 12, 2024

Focus Group on Money Laundering & Terrorist Financing Risk Management Policy

Coordinator:

Mohd. Humayun Kabir
Deputy Managing Director & CAMLCO
NRBC Bank PLC.
Head Office, Dhaka.

Members:

Md. Limon Sikder
DCAMLCO &
Head of AML & CFT Division
NRBC Bank PLC, Head Office, Dhaka.

Mahin Mursalat Synthia
AML & CFT Division
NRBC Bank PLC, Head Office, Dhaka.

Fabia Amin Promi
AML & CFT Division
NRBC Bank PLC, Head Office, Dhaka.

Table of Contents

Preamble

NRBC Bank PLC. is one of the Leading 4th Generation Commercial Bank in Bangladesh. From the inception of NRBCB, It is fully compliant and committed to oblige the rules and regulation of Bangladesh Financial Intelligence Unit (BFIU) on priority basis.

Anti-money Laundering and Combating Financing is the Global buzzword. To maintain stability and integrity of international financial system, Financial Action Task force (FATF), an inter-governmental body established by G-7 in 1989, has set recommendations for preventing money laundering and terrorist financing. All the recommendations by Financial Action Taskforce (FATF) are being implemented globally day by day.

In domestic level, Bangladesh Bank, as the major regulator of the financial system of the country plays a pivotal role to stabilize and enhance the efficiency of the financial system. To comply with the international requirement, BFIU has issued 'Money Laundering and Terrorist Financing Risk Assessment Guidelines' for banking sector on January, 2015 and instructed banks to assess their own ML & TF risk considering their customers, products, delivery channels and geographical positions. As per instruction The NRBC Bank submitted the Risk Assessment guidelines for vetting purposes.

Upon submission of the Risk Assessment guidelines of all the banks, BFIU has prepared a guideline for managing money laundering and terrorist financing risk. In light of the guideline provided by the BFIU, This ML & TF risk management policy outlines the operational, regulatory and legal framework of managing ML & TF risk within NRBC Bank. As instructed by BFIU, NRBC Bank PLC. Formatted this Money Laundering and Terrorist Financing Risk Management Policy.

Chapter 1: Money Laundering & Terrorist Financing at a Glance

1.1 Introduction:

Money Laundering is conducted by launderers worldwide to conceal the proceeds earned from criminal activities. It happens in almost every country in the world, and a single scheme typically involves transferring money through several countries in order to obscure its origins. And the rise of global financial markets makes money laundering easier than ever, making it possible to anonymously deposit proceeds of crime in one country and then have it transferred to any other country for use.

Money laundering has a major impact on a country's economy as a whole, impeding the social, economic, political, and cultural development of a society. Both money laundering and terrorist financing can weaken individual financial institution, and they are also threats to a country's overall financial sector reputation. Combating money laundering and terrorist financing is, therefore, a key element in promoting a strong, sound and stable financial sector.

1.2 Defining Money Laundering:

Money laundering can be defined in a number of ways. But the fundamental concept of money laundering is the process by which proceeds from a criminal activity is disguised to conceal their illicit origins.

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

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

ii. Smuggling money or property earned through legal or illegal means to a foreign country;
iii. knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or

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

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

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

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

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

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

1. Any person who commits or abets or conspires to commit the offence of money laundering, shall be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to

that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lacks, whichever is greater.

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

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

1.3 Stages of Money Laundering:

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

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

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

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

1.4 Why Money Laundering is done:

• First, money represents the lifeblood of the organization/person that engages in criminal conduct for financial gain because it covers operating expenses and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.
• Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.
• Third, the proceeds from crime often become the target of investigation and seizure.
• To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or, alternatively, make them look legitimate.

1.5 Penalties under Money Laundering Prevention Act, 2012 (Amendment, 2015)

i) Offence of Money Laundering and Punishment (Section 4):

a. According to section 4 (1), Money laundering is an offence.
b. According to section 4 (2), 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) lac, whichever is greater. However, in case of failure of the payment of the fine in due time, the court may issue an order of extra imprisonment considering the amount of the unpaid fine.

c. According to section 4 (3), In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved in or related with money laundering or any predicate offence.
d. According to section 4 (4), Any entity which commits or abets, assists or conspires to commit the offence of money laundering under this section, subject to the provisions of section 27, measures shall be taken as per sub-section (2) and punished with a fine of not less than twice the value of the property related to the money laundering or taka 20 (twenty) lacs, whichever is higher and in addition to this the registration of the said entity shall be liable to be cancelled. However, in case of failure in payment of the fine by the entity in due time, the court may, considering the amount of unpaid fine, issue an order of imprisonment to the entity's owner, chairman or director or by whatever name he is regarded.

ii) Punishment for violation of a freezing or attachment order (Section 5):

Any person who violates a freeze order or order of attachment issued pursuant to this Act shall be punishable with an imprisonment for a maximum period of 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or both.

iii) Punishment for divulging information (Section 6):

Whoever contravenes the provisions contained of this act shall be punishable by imprisonment of maximum period of 2 (two) years or a fine, not exceeding Tk. 50,000/- (fifty thousand) or both.

iv) Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information (Section 7):

Any person found guilty of an offence under this act shall be punishable by imprisonment of maximum period of 1 (one) year or with a fine not exceeding Tk. 25,000/- (twenty-five thousand) or with both.

v) Punishment for providing false information (Section 8):

Any person who violates the provisions contained of this act will be punishable by imprisonment of maximum period of 3 (three) years or a fine not exceeding Tk. 50,000/- (fifty thousand) or both.

1.6 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 (source: http://www.un.org/law/cod/finterr.htm); 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.

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

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

a) To carry out terrorist activity;

b) By a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.

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

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

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

1.7 The Relation between Money laundering & 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.

1.8 Why Combating against ML & TF is Crucial:

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

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

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

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

Chapter 2: AML & CFT Compliance Programme of NRBC Bank

2.1 Introduction:

National ML & TF risk assessment suggests that banking sector is one of the most vulnerable sectors for the ML & TF among the financial sectors due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership. To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU, NRBCB bank shall develop and maintain an AML and CFT compliance program. It covers senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

2.2 Components of AML & CFT Compliance Program:

The compliance program of NRBC bank shall be documented and communicated to all levels of the organization after getting approval by the Board of Directors. The program shall include-

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

2. Internal policies, procedure and controls, Bank's AML & CFT 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 Committee (CCC), 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's employees, member of the board of directors, owners and above all for the customers on AML & CFT issues.

2.3 Communication of Compliance Program:

The compliance program shall be communicated immediately after the approval from the board of directors to all employees, member of the board of the directors and other relevant stakeholders at home and abroad through our online circular archive and email. The information related to the compliance program shall be propagated through our bank's internal circulars, AML Policies etc.

2.4 Senior Management Role:

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

As part of our AML & CFT policy, Management of NRBC bank shall communicate clearly to all employees on annual basis by a statement from our honorable MD & CEO that clearly sets forth our policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities.

Statement of commitment of MD & CEO of our bank shall always include the followings-

- Bank's policy and strategy to prevent ML, TF & PF;
- Emphasize on effective implementation of bank's AML & CFT compliance program;
- 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 arise;
- Consequences of non-compliance as per human resources (HR) policy of the bank. Senior management shall ensure the adequacy of the personnel and other resources devoted to AML & CFT. Moreover, they shall ensure the autonomy of the designated officials related to AML & CFT. Senior management of our bank shall take the report from the Central Compliance Committee (CCC) 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.

2.5 Policies & Procedures:

AML & CFT policy of NRBCB shall be available through our online circular archive. Our AML & CFT shall policy includes the 4 (four) key elements; they are -

- High level summary of key controls;
- Objective of the policy;
- Scope of the policy; and
- Waivers and exceptions- procedures for obtaining exemptions from any aspects of the policy are carefully controlled; and Operational controls.

2.5.1 Written AML & CFT Compliance Policy:

The key contents of the AML & CFT policy of NRBC Bank are described as follows:

• The AML&CFT compliance policy shall establish clear responsibilities and accountabilities within our bank to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using our facilities for money laundering and the financing of terrorist activities, thus ensuring that we comply with our obligations under the law.

• The Policies shall be tailored to our bank's specific needs; taking into account factors such as its product & services we offer, branch location/Agent banking outlets, activities, delivery channels, and risks or vulnerabilities to money laundering and terrorist financing.

• It shall include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures addresses Know

Your Customer ("KYC") policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transactions

• It shall include HR aspects such as KYE (know your employee) and training employees and a separate audit or internal control function to regularly test the training program's effectiveness.

• It will also include a description of the roles the AML&CFT Compliance Officers(s) and Central Compliance Committee and other appropriate personnel (e.g. GB In charge) who will play in monitoring compliance with and effectiveness of AML&CFT policies and procedures.

• It shall outline the implementation of screening programs to ensure high standards when hiring employees. It shall also discuss implementation of standards for employees who consistently fail to perform in accordance with an AML & CFT framework.

The AML&CFT policies shall be reviewed and updated 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.

2.6 Customer Acceptance Policy:

NRBC bank has developed a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The customer acceptance policy is available in our online circular archive. The Customer Acceptance Policy ensures that explicit guidelines are in place to set-up any kind of business relationship with our bank. The Customer Acceptance Policy is very important because inadequate understanding of a customer's background and purpose for utilizing a bank account or any other banking product/service may expose the Bank to a number of risks. The primary objectives of the Customer Acceptance Policy are –

1. To manage any risk that the services provided by our Bank may be exposed to;
2. To prevent our 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.

Customer acceptance policy of our bank is based on but not limited to the following principles-

- 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.

Chapter 3: Compliance Structure of NRBC Bank

3.1 Introduction:

Compliance structure of a bank is an organizational setup that deals with AML & CFT compliance of the bank and the reporting procedure. In NRB Commercial bank AML & CFT structure includes following elements-

- Central Compliance Committee (CCC),
- Chief Anti-Money Laundering Compliance Officer (CAMLCO),
- Deputy Chief Anti-Money Laundering Compliance Officer (DCAMLCO),
- Branch Anti-Money Laundering Compliance Officer (BAMLCO).

3.2 Central Compliance Committee:

The Central Compliance Committee shall be headed by the CAMLCO of the bank. The authorities, responsibilities and appointment criterion are defined in this policy.

The Senior Management shall also nominate one deputy of the CAMLCO, who shall be known as the Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO). The designation/rank of the DCAMLCO shall not be less than SVP. Both the CAMLCO and DCAMLCO should have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML & TF. The committee shall report directly to MD & CEO.

The CCC shall arrange at least 4 (four) meetings in which the CCC shall assess the overall scenario of AML & CFT compliance of the bank, take related decisions and disseminate appropriate instructions.

The CCC shall issue instructions for the branches, which includes the use of transaction monitoring system, internal control system, policies and techniques to prevent Money Laundering and Terrorist Financing. The CCC shall report to BFIU immediately if any account/business relationship is 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 CCC shall also submit Suspicious Transaction Report (STR) or Suspicious Activity report (SAR) directly to BFIU in this regard.

3.2.1 Formation of Central Compliance Committee (CCC):

The Central Compliance Committee shall be established at the Head Office of NRBC bank which will completely separate from Internal Control Compliance Department. The Committee shall have at least 7 (seven) members and shall include CAMLCO, DCAMLCO as well as heads of various Divisions of the bank (i.e. Head of Human Resources Division, Credit Risk Management Division, Corporate banking Division, International Division, Information and Communication Technology Division etc.). However, The CCC shall not include any member from Internal Control and Compliance Division.

The members of the CCC should be well acquainted on national AML & CFT measures of Bangladesh including MLPA, ATA and rules and instructions issued by BFIU or Bangladesh Bank as well as all other related acts and laws

3.2.2 Authorities and Responsibilities of the CCC:

The CCC shall be responsible for the followings-

- Formulating bank's policy, procedure and strategies in preventing ML, TF & PF;
- Coordinating bank's AML & CFT compliance initiatives;
- Coordinating the ML & TF risk assessment of the bank and review;
- Preparing a report containing AML & CFT compliance status with recommendations half yearly basis. In addition to the compliance status, the report shall include the issues described in this policy as well as description of measures taken by BFIU regarding AML & CFT. The report shall be presented to the meeting of board of directors/management Committee including the instructions and recommendations from MD & CEO of the bank. A copy of the report shall be forwarded to BFIU within two months after the reporting period.
- Forwarding STR/SAR (if found) and CTR to BFIU in time and in proper manner;
- Reporting summary of self-assessment and independent testing procedure to BFIU in time and in proper manner;
- Conducting training, workshop, and seminar related to AML & CFT for the employee of the bank;
- Initiating required measures to submit related information, report or documents in time.

3.3 Chief Anti Money Laundering Compliance Officer (CAMLCO):

The duty of the CAMLCO shall be performed by a senior level executive appointed by the senior management. The designation of the CAMLCO shall not be less than SEVP. The CAMLCO shall report directly to MD & CEO of the bank. The CAMLCO shall be responsible for oversight of our bank's compliance with the regulatory requirements on systems and controls against money laundering and terrorist financing. The CAMLCO, directly or through the CCC, shall be central point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML&CFT program.

3.3.1 Authorities and Responsibilities of CAMLCO:

The CAMLCO has the following Authorities:

- He will not need to take any permission or consultation from/with the MD & CEO before submission of STR/SAR and any document or information to BFIU;
- He shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He shall have access to all information of the bank;

The CAMLCO has the following Responsibilities:

- The CAMLCO shall ensure overall AML & CFT compliance of the bank;
- The CAMLCO shall oversee the submission of STR/SAR or any document or information to BFIU in time;
- He shall oversee the day-to-day operation of the bank's AML&CFT compliance;
- CAMLCO shall be liable to MD & CEO for proper functioning of CCC;
- CAMLCO shall review and update ML & TF risk assessment of the bank;
- The CAMLCO shall initiate corrective actions has taken to address if there's any deficiency identified by the BFIU or BB.

3.4 Branch Anti Money Laundering Compliance Officer (BAMLCO):

The CCC shall nominate a BAMLCO for each branch. The recommended skills for a BAMLCO are as follows:

- Preferably Head of Branch or Manager Operations of the branch

• Senior official with extensive experience and knowledge in General Banking/ Foreign Exchange/ Credit operations.
• Detailed knowledge about act, rules and regulations, BFIU's instructions and bank's own policies on preventing money laundering

All the branches shall have a BAMLCO who is experienced in general banking. The BAMLCO of a branch shall be nominated by the CCC. Clear job descriptions and responsibilities of BAMLCO shall be made available in the job description

BAMLCO shall arrange AML & CFT meeting with other concerned important officials of the branch quarterly and 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,
- Implementation of local and International Sanction Lists (UNSCR)
- Self-assessment
- Record keeping,
- Training.

3.4.1 Authorities and Responsibilities of BAMLCO:

For preventing ML, TF & PF in the branch, the BAMLCO shall 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;
• Keep information of 'dormant accounts' and taking proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;
• Review cash transaction to find out any evidence of structuring;
• Review CTR to identify STR/SAR;
• 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;
• Accumulating the training records of branch officials and take initiatives including reporting to CCC, HR and NRBCB Training Academy;
• Ensure that all the required information and document are submitted properly to CCC and any freeze order or stop payment order are implemented properly;
• Keep an eye on 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 shall submits STR/SAR;
• Ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per BFIU requirements;
• Ensure that corrective actions have been taken by the branch to address the deficiency identified by the BFIU or BB.

3.5 Anti Money Laundering & Combating Financing of Terrorism Division:

AML & CFT Division shall work as a separate and independent division to tackle ML & CFT issues. AML & CFT Division shall be headed by the DCAMLCO of the bank. Sufficient human resource shall be ensured for smooth operation of the division. This division shall play the primary role for implementing AML & CFT Compliance program. The AML & CFT Division shall circulate instructions based on directions from the CCC

3.6 Internal Control and Compliance:

Internal Audit or Internal Control and Compliance Division (ICC) of NRBC bank plays an important role for ensuring proper implementation of bank's AML & CFT Compliance Program. ICCD shall be equipped with enough manpower and autonomy to look after the prevention of ML&TF. The ICCD shall oversee the implementation of the AML & CFT compliance program of the bank and review the 'Self-Assessment Report' received from the branches and execute the 'Independent Testing Procedure' appropriately. To mitigate ML & TF Risk, Our Internal Audit team shall do the followings:

- They shall 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;
- Use the report modules of our CBS to identify and aggregate large transactions;
- Communicate the findings to the senior management in a timely manner;
- Recommend corrective action to address the identified deficiencies;
- Track previously identified deficiencies and ensure 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;

3.7 External Auditor:

External auditor may also plays 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- focused 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.

Chapter 4: 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.

To implement adequate CDD measures considering the risks of money laundering and terrorist financing. Concerned officials shall focuses on the following criterions-

- Type of customers;
- Business relationship with the customer;
- Type of banking products; and
- Transaction carried out by the customer.

4.2 General Rules & Principles of CDD in NRBCB:

Completeness and Accuracy Concerned officials are required 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.

It is an obligation for our bank to maintain complete and accurate information of our customer and person acting on behalf of a customer. 'Complete' in this context 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. The following table contains various types of identification documentation and their verification procedure:

Sl.	Type of Identification Document/Information	Verification procedure
1	Photocopy of National ID Card	Verification by using EC Database
2	Photocopy of Passport	By seeing the original.
3	Photocopy of Birth Certificate	By seeing the original.
4	Present / Permanent address	Physical visit, Thanks letter.
5	Profession & Source of Fund	Job ID, Salary Certificate, Trade license, Financial Statements.

The detailed list of documentation required for various types of accounts are given in Annexure B.1. Verification is generally a cumulative process. The accuracy of the verification is subject to the satisfaction of the concerned official.

In case the branch 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, the branch shall not open the account, commence business relations or perform the transaction; or shall terminate the business relationship; and shall consider making a suspicious transactions report in relation to the customer.

4.2.1 Ongoing CDD measures (Review and update):

Ongoing CDD measures shall include the following responsibilities for the branches:

• General Banking Officials shall take necessary measures to review and update the KYC of the customers after a certain interval. This procedure shall be conducted in every 5 (Five years) in case of low risk customers. Furthermore, this procedure shall be conducted in every year in case of high risk customers.

• Officials shall update the changes in any information on the KYC as soon as the branch gets informed. Moreover, KYC shall be updated 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 by the concerned official.

• Any subsequent change to the customer's name, profession, business, ownership structure, transaction pattern address, or employment details of which the branch becomes aware shall be recorded as part of the CDD process. In addition branch shall consider relevant media reports as a part of ongoing CDD process

• If the violation of Transaction Profile occurs, the branch shall enquire and explanation from the customer and if necessary update the Transaction Profile.

• Branches shall collect the announcement of customer about the Transaction Profile of customer account in the specified form (Attached with our AOF). After six months of opening the account, the branch shall update the Transaction Profile based on type, profession, source of fund of customer and type of transaction without informing the customer or obtaining the customer's signature. However, if a significant level of deviation is observed between initially declared transaction profiles and actual transactions, the branch shall communicate and consult with customer before updating transaction profile. Branch may file STR/SAR in applicable cases if there's any reasonable ground for suspicion

• In case of foreign/Non Resident Bangladeshi customers, the branch shall follow instructions provided on Foreign Exchange Regulation Act, 1947 and related instructions provided from Bangladesh bank in this regard When to apply Enhanced CDD

The branches/concerned officials shall conduct Enhanced CDD measures, when necessary, in addition to normal CDD measures. The branch shall conduct Enhanced Due Diligence (EDD) under the following cases:

• Individuals or legal entities scored with high risk;
• Individuals who are identified as politically exposed persons (PEPs), Influential Persons and Chief Executives or top level officials of any international organization;
• Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes (See Annexure B.2);
• 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).

4.2.2 Enhanced CDD measures shall include:

• Obtaining additional information on the customer (Occupation, volume of assets, information available through public databases, internet, etc) from independent and reliable sources and updating more regularly the identification data of customer and beneficial owner (See Annexure B.1).
• Obtaining additional information on the intended nature of the business relationship (e.g. the product and services the business intends to avail now and in future).
• Obtaining information regarding the reason behind opening the account or availing banking services
• Obtaining information on the source of funds or source of wealth of the customer.
• Obtaining information on the reasons for intended or performed transactions (either by phone or face to face interview).
• Obtaining the approval of senior management or CAMLCO 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 (See Annexure B.2).
• Making aware the concerned bank officials about the risk level of the customer.

4.3 Timing of CDD:

The concerned officials shall apply CDD measures in following circumstances:

• Establishing a business relationship;
• Carrying out an occasional transaction with a value of Tk. 5 Lac or more by walk-in- customers
• Suspecting money laundering or terrorist financing; or
• Suspicion regarding the veracity of documents, data or information previously obtained for the purpose of identification or verification.
• If there is any reason to suspect that the customer may be tipped-off during standard CDD process, STR can be filed before implementing CDD measures

4.4 Transaction Monitoring:

The branches shall monitor the transactions of customer on a regular basis. The complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern is more emphasized during monitoring. The following table lists some example criterion and interval for monitoring:

Sl.	Transaction Category	Monitoring Interval
1	CTR of Branch	Every Month
2	TP Exceeding of Transaction	Immediately
3	Transaction list of the accounts that have the highest number of TP exceed	Weekly (list can be generated using CBS)
4	Transactions of High Risk Customers	Weekly
5	Transaction / Activities with High impact from Risk matrix (Annexure A)	On-going basis

4.4.1 Branch officials are also advised to follow the instructions provided below:

• Branches shall increase monitoring of daily transactions for identifying suspicious transactions by meticulously following the instructions provided on our AML Circulars
• Branches shall also scrutinize Cash Transaction Report at each month's end to identify possible red flags (list o possible red flags provided in Annexure B.2) and suspicious activities/ transactions
• Branches shall generate and analyze automated structuring detection report from our core banking system at every week and month's end to identify structuring attempts
• The BAMLCO of the branch shall closely oversee and guide the activities of the officer appointed for transaction monitoring as per our internal Circulars and instructions provided by the regulatory authorities
• All kind of transitions shall be monitored including foreign exchange transactions and transactions carried out through electronic channels
• The countries that either have failed to or have substantial gap in maintaining international standard in prevention of money laundering and terrorist financing and UN Sanction list shall be taken in consideration while monitoring transactions.

4.5 In Case where Conducting the CDD Measure is not Possible:

If conducting the CDD measure becomes impossible because of the non-cooperating behavior of the customer or if the collected information seemed to be unreliable, that is, the concerned official could not collect satisfactory information on customer identification and could not verify that, the concerned official may resort to the following measures:

• Will not carry out a transaction with or for the customer through an account;
• Will not establish a business relationship or open account or carry out an occasional transaction with the customer;
• Will terminate any existing business relationship or close the account with the customer;
• In case of terminating existing business relationship/ closing existing account, the branch shall obtain permission from HO and provide a notice to the customer with necessary explanations before closing the account
• Will consider whether it ought to be making a report to the BFIU through an STR.

4.6 Customer Identification:

Customer identification is an essential part of CDD measures. 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 branch becomes aware of any time that it lacks sufficient information about an existing customer; concerned official shall 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 shall 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 per BFIU requirements, and information shall be updated or reviewed as appropriate by the concerned official.

4.7 Verification of Source of Funds:

Officials shall collect and verify the document supporting source of fund of the person at the time of establishing any business relationship or while conducting CDD. The document may 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 officer. The concerned official shall request the person to produce E-TIN (Electronic Tax Identification No) certificate which declares taxable income.

4.8 Verification of Address:

Branch officials shall verify the address of the person at the time of establishing any business relationship or while conducting CDD. This shall be done through any or all of the following procedure:

• Physical verification by a branch official. In this case the branch official shall bring an acknowledgement from the customer.
• By standard mail or courier service correspondence.
• By collecting any other document (recent utility bill mentioning the name and address of the customer) as for satisfaction.

Where business is conducted face-to-face, the concerned official shall see originals of any documents involved in the verification.

4.9 Persons without Standard Identification Documentation:

It is important, 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 approaches and some flexibility considering risk profile of the prospective customers without compromising sufficiently rigorous anti-money laundering procedures is recommended. Some of the examples of such cases are listed in the following table:

SI	Customer Type	Identification Procedure
1	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.	A letter from the guardian or a similar professional as confirmation of a person's address. The Head of Branch may authorize the opening of a business relationship if he/she is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.
2	Students or other young people	Home address of parent(s), or by making enquiries of the applicant's educational institution
3	Minor	A family member or guardian who has an existing relationship with the institution concerned will introduce a minor. In cases where the person (legal guardian) opening the account is not already known, the identity of that person, and any other person who will have control of the account, will be verified.

4.10 Walk-In/ One off Customers:

The branch officials shall collect complete and correct information while serving Walk-in customer, i.e. a customer without having account. The concerned officials shall try to know the sources of fund and motive of transaction while issuing PO or sending/receiving remittance through third party service providers such as Western Union, Express Money, Ria, Placid etc.

Branch officials shall collect photocopies of NID or any other identification documents of any person other than customers who deposit or withdraw using on-line facilities. Additionally, in regards to on-line deposit banks will identify sources of funds as well.

4.11 Non Face To Face Customers:

'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". The concerned official shall assess money laundering and terrorist financing risks using the risk registrar provided in Annexure A.2 while providing service to non-face to face customers and will verify the identity of the customers by various measures such as visiting customer's address by a bank official.

4.12 Unique Customer Identification Code (UCIC):

The Core Banking System (CBS) of NRBC Bank automatically generates Unique Customer Identification Code (UCIC) for each of the customers which shall use to track customers, their accounts and their transactions. Such unique identification system Enables the bank to avoid redundancy, and saves time and resources.

4.13 Adoption of Technology based products and services:

Whenever the bank intends to introduce any new technology based products or services, ML & TF risk of that particular product shall be assessed. The risk assessment and preventive measures shall be added to the risk registrar before the launch of that particular product services. These shall also be applicable for technology based improvement and development of existing services

4.14 Correspondent Banking:

'Cross Border Correspondent banking' refers 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, and international wire transfer, drawing arrangement for demand draft or other similar services." Our bank shall ensure the following criterion when providing correspondent banking services:

• The nature of business of the foreign institution shall be verified by scrutinizing the annual statements, and other related policies of the institution. Moreover, information shall be collected through other independent sources such as Bankers Almanac and SWIFT KYC Registry

• AML policies and practices of the institution shall be verified by our AML & CFT Questioner for correspondent relationship, Wolfsburg Questioner, their AML policy and other related documents. Moreover, information shall be collected through other independent sources such as Bankers Almanac and SWIFT KYC Registry

• No correspondent relationship shall be established before it is reasonably ensured that the correspondent bank/ FI is actively and effectively supervised by their controlling and regulatory authority

• After collecting satisfactory information regarding the entity's nature of business and AML practices, CAMLCO's approval shall be sought before proceeding to provide correspondent services

• Our bank shall not establish relationship with shell banks or any other banks that maintains correspondent relationship with shell banks. The authenticity shall be verified by obtaining written commitment, checking both world ranking and country ranking of the institution through independent sources such as Bankers Almanac and SWIFT KYC Registry

• In case of the organizations belonging to the countries that either have failed to or have substantial gap in maintaining international standard in prevention of money laundering and terrorist financing , the bank shall apply enhanced due diligence (EDD) for establishing and maintaining correspondent relationships. Additional information shall be collected of their ultimate beneficial owner and ML & FT prevention policy

• In case of the respondent banks that provide 'Payable through Account" services, following measures should be taken

It shall be reasonably ensured that the respondent banks properly follow CDD procedure for their customer base

It shall be ensured that the respondent bank is capable of providing information related to CDD of their customers when required within reasonable time frame

• We shall check both the entity and owners/directors through screening mechanism system to make sure the institutions or its owners/top management is not sanction listed.

• The instructions mentioned above shall be applicable for both new correspondent relationships and review of existing correspondent relationships

• Detailed information about the ownership nature of the institutions shall be obtained.

• In addition to the instructions mentioned above, any other policy, procedure, procedure required by the regulatory authorities shall be applicable

4.15 Agent banking:

Following instructions shall be applicable for the agents:

• Agents shall use the same uniform account opening forms (prescribed by BFIU) that are used by the branches

• Agents should be aware of suspicious transaction detection and reporting

• Money Laundering & Terrorist financing prevention activities shall be added to agent banking related compliance program

• Trainings shall be arranged for agents to raise awareness regarding Prevention of Money laundering & Terrorist Financing

• Following measures shall take for appointing agents and monitoring their activities

Proper screening mechanism shall be followed and complete, accurate identification of the agents shall be collected while selecting and appointing agents

Each agent shall be classified into three risk categories (i.e. high, medium, low) based on their transaction volume and frequency, geographical location, business and nature of ownership and other relevant criteria. The risk based classification shall be used to monitor the agent's transactions and activities Risk classification of agents shall be done on ongoing basis

ICCD shall conduct comprehensive inspection of high risk agent points on yearly basis and send a copy of the reports to AML Division

ICCD shall conduct comprehensive inspection of low and medium risk agent points on every three years interval and send a copy of the reports to AML Division

Up to date list of agents shall be posted on the bank's website. In addition, list of canceled agent due to complaints and irregularities shall be posted on company website.

4.16 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.

4.16.1 Cross-Border Wire Transfers:

The officials shall follow the procedures described below for Cross-Border Wire transfer services:

• Under general or special permission, in case of threshold cross-border wire transfers of 1000 (one thousand) or above USD or equivalent foreign currency, complete and accurate information of the originator shall be collected and preserved electronically in

Our CBS and shall be sent to intermediary/beneficiary bank on demand.

• For cross-border wire transfers, below the threshold full and meaningful originator information shall preserved by the concerned official so that the originator can be identified later

• For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information shall be preserved.

• In case of cross border wire transfers where a single originator initiates transfer bundled in a batch file in favor of more than one beneficiary, Complete and accurate information of both originator and beneficiary shall be included in the batch file.

4.16.2 Domestic Wire Transfers (BEFTN/RTGS/Debit Card/Credit Card):

The officials shall follow the procedures described below for Domestic-Border Wire transfer services:

• For domestic wire transfers, usual CDD measures described in this policy shall be applicable for collecting and verifying Originator/ Beneficiary information

• In case of wire transfer by using debit or credit card (except for buying goods and services), similar information described as above shall be preserved.

• In case of domestic wire transfer in favor of government, semi government and autonomous institutions, the procedures described in above is not mandatory

4.16.3 Other instructions related to wire transfer:

• All related instructions, circulars circulated by regulatory authorities and relevant laws/ acts shall be duly followed while dealing with wire transfers

• In addition, instructions described in section 2.6 and Chapter 8 shall be complied while dealing with international/ domestic wire transfers

4.16.4 Responsibilities while acting as ordering bank:

• Applicant's complete and accurate information shall be collected and preserved.

Meaningful information of the beneficiary shall be collected and preserved so that the beneficiary can be traced back later

4.16.5 Responsibilities while acting as Intermediary bank:

• For both domestic and cross border wire transfers where the bank acts as an intermediary of an ordering and an intermediary bank, both applicant and beneficiary information shall be collected and preserved. Moreover, the bank shall undertake necessary steps to identify whether the information provided is sufficient

• The bank shall follow a risk based approach to carry on/halt/reject wire transfers and proceed with necessary follow ups based on the sufficiency of originator/ beneficiary information

4.16.6 Responsibilities while acting as Beneficiary bank:

• The bank shall follow a risk based approach to assess the sufficiency of originator/ beneficiary information while acting as a beneficiary bank. If deemed necessary, the bank shall south necessary information by mutual communication of relevant parties or any other sources. Complete and accurate information of beneficiary shall be collected and preserved at the time of payment

• The bank shall follow a risk based approach to carry on/halt/reject wire transfers and proceed with necessary follow ups based on the sufficiency of originator/ beneficiary information

4.17 Simplified CDD measures:

The concerned officials may apply simplified CDD measures in following circumstances:

• In case of carrying out transactions with a value of Tk. 50,000.00 (Taka Fifty Thousand or less) by walk-in-customers, only name and address of both sender/applicant, receiver/beneficiary and phone number of sender applicant should be obtained

• In case of carrying out transactions with a value of between Tk. 50,000.00 (Taka Fifty Thousand) and Tk. 5,00,000.00 (Tk. Five lac) by walk-in-customers, Photo ID (Preferably NID/ Passport) of sender/applicant/depositor/ withdrawer should be obtained in addition to Name , address and phone number

• Braches may take less strict CDD measures for accounts with low risk that are opened to facilitate financial inclusion (i.e Student, farmers accounts or other o frill accounts)

4.18 Reliance on Third Party:

The branches/Concerned may sometimes 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.

Chapter 5: Politically Exposed Persons (PEPs)

5.1 Definition:

PEPs (as well as their family members and persons known to be close associates) are required to be subject to undertake enhanced due diligence by NRBC Bank in general. This is because international standards issued by the FATF recognize that PEP may be in a position to abuse their public office, political power for private gains and PEP may use the financial system to launder the illicit gains. As FATF says „these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatizing PEPs as such being involved in criminal activity. The FATF has categorized PEPs into 3 (three) criteria which include:

- Foreign PEPs;
- Domestic PEPs (known as Influential Persons: IPs in Bangladesh) and
- Chief or similar high-ranking positions in an international organization.

It is important to note that only foreign PEPs automatically should be treated as high risk and therefore bank should conduct Enhanced Due Diligence (EDD) in this scenario. However, EDD should be undertaken in case of domestic PEPs (Influential Persons: IPs) and PEPs of the international organization when such customer relationship is identified as higher risk.

A politically exposed person (PEP) is defined by the FATF as an individual who is or has been entrusted with a prominent public functions which include individuals in foreign country and domestic level. So, PEPs as per the FATF Standards and IPs as per Bangladeshi regulations, are the following individuals but not limited to-

- Heads of state or government, ministers and deputy or state ministers;
- Members of parliament or of similar legislative bodies;
- Members of the governing bodies of political parties (generally only apply to the national governing bodies where a member has significant executive power, eg. over the selection of candidates or distribution of significant party funds);
- Senior politicians
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, Charges d' affairs and high-ranking officers in the armed forces;
- Head or the senior executives or members of the administrative, management or supervisory bodies or State-owned enterprises;
- Chief, directors, deputy directors and members of the board or equivalent function of an international organizations.

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 board or equivalent functions.

The definition of PEPs is not intend to cover middle ranking and more junior individuals.

5.2 Family members of a PEPs:

Family members of a PEP shall include:

- Spouse, or civil partner
- Children and their spouses or civil partner
- Parents

However, this is not an exhaustive list. We should take a proportionate and risk- based approach to the treatment of family members who do not fall into this definition. A corrupt PEP may use members of his/her wider family to launder the proceeds of corruption on his/her behalf.

It may be appropriate to include a wider circle of family members (such as aunts and uncles) in cases where bank assessed a PEP to pose a higher risk. This would not apply in relation to lower risk PEPs. In low-risk situations, we should not apply any EDD measures to someone who is not within the definition above and should apply normal customer due diligence measures. A family member of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

5.3 Close associates of PEPs:

A `known close associate' of a PEPs is defined as:

- An individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a PEP
- An individual who has sole beneficial ownership of a legal entity or a legal arrangement that is known to have been set up for the benefit of a PEP

A 'known close associate' of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

5.4 Various scenarios related with PEPs/IPs:

A PEP/IP must be treated as a PEP/IP after he or she leaves office for at least 12 months, depending on the risk. This does not apply to family members, who should be treated as ordinary customers, subject to normal CDD obligations from the point that the PEP/IP leaves office. A family member of a former PEP/IP should not be subject to enhanced due diligence measures unless this is justified by the bank's assessment of other risks posed by that customer.

If a person who is a PEP/IP is no longer entrusted with a prominent public function, that person should continue to be subject to risk-based enhanced due diligence for a period of at least 12 months after the date they ceased to be entrusted with that public function. We may apply measures for a longer period to address risks of money laundering or terrorist financing in relation to that person, but the BFIU consider this will only be necessary in the cases of PEPs/IPs where a reporting organization has assessed that PEP/IP is posing a higher risk.

5.5 PEPs Risk:

No–the risk of corruption will differ between PEPs. Bank has to take appropriate approach that considers the risks an individual PEP poses based on an assessment of:

- The prominent public functions the PEP holds
- The nature of the proposed business relationship
- The potential for the product to be misused for the purposes of corruption
- Any other relevant factors the reporting organization has considered in its risk assessment.

We discusses on how bank may differentiate between PEPs. The terms lower risk and higher risk are used to recognize that banks are required to apply Enhanced Due Diligence on a risk-sensitive basis. An overall risk assessment will consider all risk factors that a customer may present and come to a holistic view of what measures should be taken to comply. Not only risk factor means a customer should automatically be treated as posing a higher risk; it is necessary to consider all features of the customer.

5.5.1 Lower Risk PEPs:

The following indicators suggest a PEP poses a lower risk:

- If he/she is seeking access to a product bank has assessed to pose a lower risk.
- If he/she is from an area where ML/TF risks is lower
- If he/she does not have executive decision making responsibilities (e.g. an opposition Member of the Parliament)

A family member or close associates of a politically exposed person may pose a lower risk if the PEP himself/herself poses a lower risk.

5.5.2 Higher Risk PEP:

The following indicators suggest a PEP poses a higher risk:

5.5.2 (a) Product:

Banks risk assessment finds the product or relationship a PEP is seeking for may be misused to launder the proceeds of large-scale corruption.

5.5.2 (b) Geographical:

A PEP may pose a greater risk if he/she is entrusted with a prominent public function in a country that is considered as a higher risk for corruption. To draw this conclusion, we should have regard to whether, based on information available, the country has the following characteristics:

- Associated with high levels of corruption
- Political instability
- Weak state institutions
- Weak anti-money laundering defense
- Armed conflict
- Non-democratic forms of government
- Widespread organized criminality
- A political economy dominated by a small number of people/entities with close links to the state
- Lacking a free press and where legal or other measures constrain journalistic investigation
- A criminal justice system vulnerable to political interference
- Lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector
- Law and culture antagonistic to the interests of whistleblowers
- Weaknesses in the transparency of registries of ownership for companies, land and equities
- Human rights abuses

5.5.2 (c) Personal and Professional:

The following characteristics might suggest PEP poses higher risk:

- personal wealth or lifestyle is inconsistent with known legitimate sources of income or wealth; if a country has laws that do not generally permit the holding of a foreign bank account, a bank should satisfy itself that the customer has authority to do so before opening an account
- Credible allegations of financial misconduct (eg facilitated, made, or accepted bribes)
- responsibility for, or able to influence, large public procurement exercises, particularly where procurement is not subject to competitive tender, or otherwise lacks transparency
- Responsible for, or able to influence, allocation of scarce government licenses such as mineral extraction concessions or permission for significant construction projects.

5.5.2.3 Higher risk of a PEPs family member or close associates:

The following characteristics might suggest a family member or close associates of a politically exposed person poses a higher risk:

- Wealth derived from the granting of government licenses (such as mineral extraction concessions, license to act as a monopoly provider of services, or permission for significant construction projects)
- Wealth derived from preferential access to the privatization of former state assets
- wealth derived from commerce in industry sectors associated with high-barriers to entry or a lack of competition, particularly where these barriers stem from law, regulation or other government policy
- Wealth or lifestyle inconsistent with known legitimate sources of income or wealth
- Credible allegations of financial misconduct (e.g. facilitated, made, or accepted bribes)
- Appointment to a public office that appears inconsistent with personal merit

5.6 Banks' Obligations:

The Regulations require banks to have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is a PEP (or a family member or a known close associate of a PEP) and to manage the risks arising from our relationship with those customers. This includes where a PEP, family member or close associate is operating via an intermediary or introducer (this may include others in the regulated sector such as banking staff, lawyers, estate agents etc.). There are many legitimate reasons for doing so (e.g. a solicitor acting in a property transaction). In these situations, and in line with FATF guidance, BFIU expects us to understand as part of their due diligence why a PEP, family member or close associate is using such an arrangement and use that as part of their assessment of risk.

The Regulations state that in determining whether these systems and procedures are appropriate, we should refer to:

- Its own risk assessment of the money laundering/terrorist financing risks;
- An assessment of the extent to which the risk would be increased by a business relationship with a PEP, family member or close associate. BFIU would expect that this is a case-by-case assessment and not an automatic assessment that a relationship creates a high risk of money laundering; and
- Any information provided by the BFIU. This will include the BFIU's publication, thematic reviews, speeches on financial crime issues, BFIU's annual report.

Where bank has identified that a customer (or beneficial owner of a customer) does meet the definition of a PEP (or a family member or known close associate of a PEP), we must assess the level of risk associated with that customer and, as a result of that assessment, the extent to which enhanced due diligence measures need to be carried out. The risk factors set out in this guidance will help us to consider relevant factors when meeting these obligations. Banks assessment and its decision to apply relevant enhanced due diligence measures need to be clearly documented.

BFIU expects banks to make use of information that is reasonably available to them in identifying PEPs, family members or known close associates. This could include the following:

- Public domain information such as websites of the governments, reliable news sources and work by reputable pressure groups focused on corruption risk. We should use a variety of sources where possible.
- In line with the nature and size of the bank, it may choose, but is not required, to use commercial databases that contain lists of PEPs, family members and known close associates. Bank choosing to use such lists would need to understand how such databases are populated and will need to ensure that those flagged by the system fall within the definition of a PEP, family member or close associate as set out in the Regulations and this guidance.

BFIU expects that bank will not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or a family member of a PEP or known close associate of a PEP). Bank may, after collecting appropriate information and completing its assessment, conclude the risks posed by a customer are higher than they can effectively mitigate; only in such cases it will be appropriate to decline or close that relationship.

If, having assessed the risk associated with the customer and decided on an appropriate level of enhanced due diligence measures in line with this guidance, bank is unable to apply those measures, we needs to comply with the requirement not to establish, or to terminate, a business relationship.

5.7 Measures of a foreign PEPs:

The following measures should be taken where a customer meets the definition of a foreign PEP, IPs/Chief of International Organization posing higher risk or a family member or known close associate of a foreign PEP, IPs/Chief of International Organization posing higher risk:

- Obtain senior management approval for establishing or continuing business relationships with such persons
- Take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons
- Conduct enhanced, ongoing monitoring of those business relationships

The nature and extent of this due diligence should be appropriate to the risk bank has assessed in relation to the customer. We should apply more extensive measures for relationships assessed as high risk and less extensive measures for lower risk customers.

5.8 Measures of a Domestic PEPs (IPs):

Domestic PEP's will be treated as IP's as per BFIU Guidance notes on politically Exposed Persons; Section 2. In case of Domestic PEP's, NRBC Bank shall conduct Enhanced Due Diligence which combines the following measures:

1) Additional Know Your Customer (KYC) information will be collected from independent and reliable sources;

2) Enhanced measures will be observed to know the purpose and source of fund of the respective Accounts;
3) Conducting on-going transaction monitoring of the respective Accounts;
4) Obtaining permission from CAMLCO if required.

5.9 Measures taken in lower risk situations:

In lower risk situations bank may take the following measures:

• Conduct enquiries about a PEPs family or known close associates in a flexible manner except those required to establish whether such a relationship does exist.

• Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP. It is necessary to seek source of wealth information but in all lower risk cases, especially when dealing with products that carry a lower risk of laundering the proceeds of corruption we should minimize the amount of information they collect and how they verify the information provided (for example, via information sources it has available).

• Oversight and approval of the relationship takes place at a lower level of senior management.
• A business relationship with a PEP or a PEPs family and close associates is subject to less frequent formal review than it was considered high risk.

5.10 Measures taken in higher risk situations:

In higher risk situations bank may take the following measures:

• Take more intrusive and exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP
• Oversight and approval of the relationship takes place at a senior level of management
• A business relationship with a PEP (or a PEPs family and close associates) is subject to more frequent and thorough formal review as to whether the business relationship should be maintained.

5.11 Long-term insurance contracts:

In relation to life insurance policies, bank should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiaries, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, we should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

5.11.1 Beneficial owners of legal entities who are PEPs:

Bank should identify when a PEP is a beneficial owner of a customer. It does not require that a legal entity should be treated as a PEP just because a PEP might be a beneficial owner.

Once a bank is satisfied that a PEP is a beneficial owner then, in line with the risk-based approach, it should assess the risks posed by the involvement of that PEP and, after making this assessment, we should apply appropriate measures in accordance with this guidance. These could range from applying customer due diligence measures in cases where the PEP is just a figurehead for an organization (this will vary according to the circumstances of each entity but could be the case even if they sit on the board, including as a non-executive director) through to applying

EDD measures, according to the risk assessed in line with this guidance where it is apparent that the PEP has significant control or the ability to use their own funds in relation to the entity. Where a PEP is a beneficial owner of a corporate customer, then a bank should not automatically treat other beneficial owners/shareholders of the customer as a PEP or known close associate under the regulations, but may do so having assessed the relationship based on information available to bank.

Chapter 6: Beneficial Owner

6.1 Definition:

The definition of beneficial owner means the individual who–

a) Has effective control of a customer; or
b) Owns a prescribed threshold, 20% as per Bangladeshi regulation of the company or legal arrangements.

As per 2(4) of MLPR 2019 beneficial owner means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercises ultimate effective control over a legal person or arrangement or holds 20% or more share of a company. Here "ultimately owns or controls" and "ultimate effective controls" refers to situation in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

6.2 Identifying the Beneficial Owner:

Identifying the beneficial ownership of a customer one must apply three elements. Any one element or any combination of these three elements satisfies beneficial ownership. These elements are:

a. Who owns 20 or more percent of a company or legal arrangements b. who has effective control of the customer
c. The person on whose behalf a transaction is conducted.

Effective control, ownership and persons on whose behalf a transaction is conducted are not mutually exclusive. The beneficial owner must be a natural person and cannot be a company, an organization or a legal arrangement.

It is crucial to know who the beneficial owner(s) are so that one can make appropriate decisions about the level of money laundering and terrorist financing risk associated with customer. Some criminal enterprises deliberately try to hide the true owners and controllers of their business and its assets.

Acting on behalf of a customer is not part of the beneficial ownership definition. However, the reporting entities should identify and verify those persons. Information on 'acting on behalf' is included to help reporting entities understand the distinction between a beneficial owner and a person acting on behalf of a customer.

A risk-based approach will allow some flexibility in the measures to verify the identity of the customer's beneficial owners. Generally, simplified customer due diligence relates to customers that are already subject to transparency and public disclosure. Thus, simplified customer due diligence, which in effect means there is no requirement to check beneficial ownership.

6.3 Importance of identify the Beneficial Owner:

Corporate entities such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements conduct a wide variety of commercial and entrepreneurial activities. However, despite the essential and legitimate role that corporate entities play in the economy, under certain conditions, they have been misused for illicit purposes, including money laundering (ML), bribery and corruption, insider dealings, tax fraud, terrorist financing (TF), and other unlawful activities. This is because, for criminals trying to circumvent anti-money laundering (AML) and countering the financing of terrorism (CFT) measures, corporate entities provide an attractive avenue to disguise the ownership and hide the illicit origin.

Various studies conducted by Financial Action Task Force (FATF), World Bank, United Nations Office on Drugs and Crime (UNODC) have explored the misuse of corporate entities for illicit purposes, including for ML/TF. In general, the lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising:

a) The identity of known or suspected criminals,

b) The true purpose of an account or property held by a corporate entities, and/or

c) The source or use of funds or property associated with a corporate entity.

6.4 Ways of beneficial ownership information can be hidden/obscured:

Beneficial ownership information can be obscured through various ways, including but not limited to;

a) Use of shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions,

b) Complex ownership and control structures involving many layers of ownership, sometimes in the name of other legal persons and sometimes using a chain of ownership that is spread across several jurisdictions,

c) Bearer shares and bearer share warrants, d) Use of legal persons as directors,

e) Formal nominee shareholders and directors where the identity of the nominator is undisclosed,

f) Informal nominee shareholders and directors, such as close associates and family,

g) Trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,

h) Use of intermediaries in forming legal persons2, including professional intermediaries such as accountants, lawyers, notaries, trust and company service providers.

6.5 Ownership:

The reporting entities should understand the ownership and control structure of the customers. The threshold for controlling interest owns 20% or more of the customer. The ownership can be simple and complex in nature.

As per MLPR 2019 Legal person means any entity other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundation, installations, partnerships or associations and other relevantly similar entities,

An individual who has a control over a portion of equity directly or via family relationship or via nominee or close associate (whether disclosed or undisclosed) can be considered as a beneficial owner.

Ownership can be spread over a large number of individuals with no individual owning more than 20 percent. For example, a co-operative that has a large number of members is likely to have no individual(s) owning more than 20 percent. In such instance, the effective control element is more likely to determine the beneficial owner(s).

6.6 Effective Control:

It is essential to understand the customer's governance structure as an aid in identifying those persons that exercise effective control over the customer. In deciding the effective controller(s) in relation to a customer, reporting entities should consider:

a. A person who can hire or terminate a member of senior level management;
b. A person who can appoint or dismiss Directors;
c. Senior managers who have control over daily/regular operations of the person/arrangement (e.g. a CEO, CFO or a Managing Director).

Natural persons may also control the legal person through other means such as:

a) Personal connections to persons in positions such as Executive Directors/ CEOs/ Managing Director or that possess ownership;

b) Significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person;

c) Control without ownership by participating in the financing of the enterprise, or because of close family relationships, historical or contractual associations, or if a company defaults on certain payments;

d) Use, enjoyment or benefiting from the assets owned by the legal person even if control is never exercised.

When a reporting entity identifies a customer, it should identify the beneficial owner(s) and take all reasonable steps to verify his identity:

(a) Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.

(b) Where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to 20 or more percent of capital or profits of the partnership.

(c) Where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to 20 or more of the property or capital or profits of the unincorporated association or body of individuals.

(d) Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(e) Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The beneficial owner must also be noted in the case of non-profit associations, although earning profit is not the goal of any of them. According to the definition of beneficial owner, the person(s) under whose control the company is opening are indicated in such a case. Usually, they are member of the management board. Exceptions are possible, e.g. if the founders or members of a non-profit association are legal entities, the beneficial owners are defined in the same way as in the case of companies. The same principle applies here, i.e. nothing the chairman of the management board is enough is enough if the management board has more than four members. If a person is noted as the beneficial owner due to their position as a member of a managing body, this does not mean that they receive monetary income from the company or that the company operates in their personal interests.

In the event of a limited partnership fund, civil law partnership, community or other association of persons that does not have the status of a legal entity, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or via other means and who is the association's:

- Founder or person who has handed over property to the asset pool;
- Trustee or manager or possessor of the property;
- Person ensuring and controlling the preservation of property, where such person has been appointed, or
- The beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates

In the case of a foundation, the person noted as the beneficial owner is the person who may make payouts from the assets of the foundation, where such person(s) have been specified by name in the articles of association of the foundation. If such persons have not been specified by name in the articles of association, the members of the management board and supervisory board are noted as the beneficial owners.

6.7 Person on behalf of Transaction:

Another part of the definition of beneficial owner is a person on whose behalf a transaction is conducted. This may be the individual who is an underlying client of the customer. This concept is important when considering the relationship between managing intermediaries and their underlying clients. There are various scenarios, many of which are complicated.

An example is, if a reporting entity knows that someone (person A) is conducting an occasional transaction on behalf of another person (person B), then person A and person B should be identified and verified along with any other beneficial owners.

6.8 Beneficial owner of Legal Arrangements:

Legal arrangement includes an express trust, a fiduciary account or a nominee.

All trusts have the common characteristic of causing a separation between legal ownership and beneficial ownership. Legal ownership always rests with the trustee. Beneficial ownership can rest with the author of trust, trustees or beneficiaries, jointly or individually.

Reporting entities should identify and take reasonable measures to verify information about a trust, including, the identities of the author of the trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including those who control through the chain of control or ownership).

Reporting entities are required to obtain trust documents (e.g. deed of trust, instrument of trust, trust declaration, etc.) and the provisions of the trust document must be fully understood within the context of the laws of the governing jurisdiction. The Reporting entities should take reasonable measures to verify trust document through independent means (e.g. Registry of Trust, Notary)

Example: Person 'B' is the author of a trust for the benefit of his child. The trustee seeks to establish a relationship with a financial institution to help manage the assets of the trust. Even though the trustee is the controller of the assets of the trust he may not be the ultimate beneficial owner and the main focus of CDD should include person 'B'" as well.

6.9 Applying a Risk-Based Approach:

A risk-based approach refers how the beneficial ownership of a customer will be verified. Identifying beneficial ownership of a customer is an obligation that must be satisfied, regardless of the level of risk associated with that customer. However, when deciding what reasonable steps should be taken to satisfy that the customer's identity and information is correct, one may vary approach depending on the risk assessment of the customer. The process for assessing customer risk and deciding how to identify and verify beneficial ownership should be set out into the AML/CFT programme.

One should apply enhanced customer due diligence and make a suspicious transaction report to the BFIU where there are reasonable grounds for suspicion of money laundering or terrorist financing,

A risk-based approach allows some flexibility in obligation to use data, documents or information obtained from a reliable and independent source to verify the identity of the beneficial owner(s) of customer.

The risk assessment will set out what to do to verify different types of customers. If the customer is higher risk, one may apply enhanced customer due diligence, in which case one must obtain information relating to the source of funds or wealth of the customer. Verification of the identity of the beneficial owner(s) is the last step in the process. To verify the beneficial owner(s) appropriate documentations must be obtained so that it is known who the beneficial owner is.

It is appropriate for beneficial ownership identification process to include measures to ensure that make consistent decisions about customers. This process should be in line with risk assessment. If the customer is associated with higher risk factors, internal controls in AML/CFT programme should set out when to escalate decisions to a higher level.

6.10 Due Diligence of Beneficial Owner:

The obligation is to determine the individual(s) who are the beneficial owner(s). A beneficial owner is an individual (a natural person). Therefore the beneficial owner can only be an individual, not a company or organization. There may be more than one beneficial owner associated with customers. The task is to identify and verify the identity of all the beneficial owners of the customers.

If the customer is an individual to treat that person as the beneficial owner unless there are reasonable grounds to make the suspect that are acting on behalf of another. If the customer is acting on behalf of another person, anyone will need to establish that person's identity, the beneficial ownership of the customer and any other beneficial owners.

6.11 Record Keeping:

It is a good practice to keep detailed records of all decisions and retain customer due diligence and relevant records in a readily auditable manner. It is important to record the rationale behind any decision is made. Anyone reading the notes years later should be able to understand why such a risk-based decision is taken.

6.12 Some Queries:

6.12.1. Required to submit data to the reporting entity in supporting beneficial ownership

- A private limited company
- General partnership
- Limited partnership
- Commercial association
- Foundation
- Non-profit association
- Economic Interest Grouping

6.12.2 Not obliged to submit data of the beneficial owner:

- Apartment association;
- Building association;
- A company listed on the regulated market to which disclosure rules complying with Bangladeshi law or similar international standards are applied, which ensure the sufficient transparency of the data of owners;
- A foundation the goal of whose economic activities is safekeeping or collecting assets in the interests of the beneficiaries or group of persons specified in the articles of association and that has no other economic activity.
- As gardening associations are ordinary non-profit associations within the legal meaning, then the obligation to submit the data of the beneficial owner applies to them.

The data of the beneficial owner are not submitted in the case of the branch of a foreign company, because the branch is not a legal. A foreign company is responsible for the activities of its branch and enters the data of the beneficial owner in its respective register of beneficial owners.

Companies listed on the stock exchange do not have to submit the data of beneficial owners, but the subsidiaries belonging to their groups of companies must do it. The same principles that apply to ordinary companies apply here as well: if there are no natural persons among the shareholders of a listed company whose shareholding in the company exceeds 20%, the members of the controlling body of the listed company, i.e. the management board and the supervisory board, are noted as the beneficial owners.

6.13. Beneficial owner of a state-owned company or foundation, or non-profit association established by a local government (city, town or municipality):

State-owned companies are ordinary private legal entities. The beneficial owner of a state-owned company is the minister responsible for the area, which represents the state in the company and appoints the members of the supervisory boards of the companies in their area of government, the chairman of the supervisory

board/management board of the company and the members of both bodies. For example, the finance minister as the representative of the state, the chairman and members of the supervisory board and the chairman and members of the management board can be considered beneficial owners.

In the case of foundations established by the state where the rights of a founder are exercised by ministries and foundations with state participation, the minister of the respective area, the chairman/members of the supervisory board and the chairman/members of the management board can be considered the beneficial owners. The members of the supervisory board are appointed and the other rights of a founder or shareholder of a foundation of a municipality, town or city, whose sole founder is the municipality, town or city, as well as of a private limited company or public limited company, whose sole shareholder is a municipality, town or city, are exercised by the government of the municipality, town or city, so the mayor of the municipality, town or city or the members of the government of the municipality, town or city can be considered the beneficial owners. The principle applied here is the same: noting the chairman of a body is enough if the body consists of more than four persons. If an association has been established with the state and a local government or several local governments together, none of which have dominant influence over the association, the chairmen or members of the management board or supervisory board of the association are noted as the beneficial owners.

Chapter 7: e-KYC

7.1 Definition:

E-KYC is a combination of paperless customer onboarding, promptly identifying and verifying customer identity, maintaining KYC profile in a digital form and determining customer risk grading through digital means. It is a faster process of doing KYC of customer verifying his/her identity document or bio-metric data.

The e-KYC module can be divided into following two types based on the customer's risk exposures:

(a) Simplified e-KYC: Where a customer can be on boarded and verifying customer identity electronically using simplified digital KYC form in case of proven lower risk scenario. No risk grading will be required while onboarding of customer. However, sanction screening should be undertaken and KYC review shall be done every five years; and

(b) Regular e-KYC: Where a customer can be on boarded and verifying customer identity electronically, a prescribed digital KYC required to be filled in and stored as well as a risk grading exercise required to be documented. However, based on the risk grading exercise where customer rated as high risk or some specific scenarios (for example. PEPs), some Enhanced Customer Due Diligence (EDD) required to be undertaken as per provided sample.

7.2 Objectives:

The key objective of promoting e-KYC is that it can provide an ample scope of quick onboarding of customer by verifying customer identity through digital means which can leverage saving of time and provide ease both for the client and service providers. Additionally, e-KYC can save institutional cost as well as foster growth of customer base compare to the traditional growth. Therefore, the basic objectives of implementing e-KYC are as follows:

- Establish good governance within the financial industry;
- Enhancing the growth of financial inclusion;
- Protect financial sector from abuse of criminal activities;
- Ensure integrity and stability of the financial sector;
- Manage ML/TF risks;
- Reduction of cost related to customer on boarding and managing CDD;
- Promote fintech services; and
- Participate in the national level well-being.

7.3 e-KYC Process:

The traditional KYC process requires to be filled in the KYC form and collect photo ID and signature of the customers along with required documents. All the way it's a manual process. However, e-KYC is a digital process where financial institutions can open a customer account by filling

1. This guideline suggested two types of biometrics i.e. fingerprint and face matching, however, if the infrastructure permit Financial Institution can introduce other type of biometric for example iris.

2. The EDD measures should include collection of additional information, monitoring of account activity and approval from Chief AML/CFT Compliance officer up a digital form, taking photograph on the spot, and authenticate the customer's identification data (ID No., biometric information, address proof) instantaneously. Such bio metric

information or digital signatures or electronic signatures may be used for transaction authentication as well. The customer onboarding process may undertake via followings means:

(a) Assisted customer onboarding: Where a financial institution or its nominated agent or third-party visit customer or customer visit financial institution or its nominated agent or third party's premises and open account with the direct assistance of financial institution or its nominated agent or third party; and

(b) Self check- in: Where customer can on board at his own by using kiosk, smart phone, computer or other digital means abiding by the norms of this e-KYC Guidelines. Self-check in shall be allowed for face matching model only as described in this Guideline.

7.4 Applicability:

e-KYC shall only be applicable for natural person who have valid NID document. Natural person without NID and a legal entity or arrangement has to follow the KYC norms as prescribed by the BFIU from time to time. Therefore, 'simplified' and 'regular' e-KYC norms shall be applicable based on threshold and risk mentioned in this Guideline. The threshold mentioned in this Guideline may be changed from time to time by the BFIU. The financial institutions shall conduct paper based customer onboarding and simplified or regular KYC and CDD measures if any customer unable to onboard with this e-KYC mechanism.

7.5 Customer Onboarding-Simplified:

7.5.1 Customer onboarding models:

The financial institutions' are allowed to follow customer boarding under this Guidance which is based on national identification document, information stored within a specific NID plus any one of the bio-metric verification out of fingerprint matching, face matching, voice matching and iris matching5. The customer onboarding should also be covered self-check- in, check in with assistance of service providers and other relevant means as required necessary.

An electronic customer onboarding involves multiple activities. An efficient customer onboarding starts from clients' identity information and can be segmented into following steps:

a) Data capture and generation;
b) Identity verification;
c) Sanction and other screening;
d) Account opening;
e) Customer profiling (e-KYC Profile); and
f) Customer risk grading (as applicable).

For the purpose of undertaking e-KYC, this guideline suggests initially following two bio-metric based models of customer onboarding which are as follows:

(a) Customer onboarding by using fingerprint; and
(b) Customer onboarding by matching face.

However, other two models i.e. voice matching and iris matching can also be used if there are sufficient infrastructural and logistics facilities available. Moreover, we can also introduce other innovative models using biometric beyond these four models having prior approval from BFIU.

7.5.2 Customer onboarding by using fingerprint:

The customer onboarding by using fingerprint matching is one of the commonly used methods where customer fingerprint will be used as a main identifier of a person's identity. The minimum generic approach for this model will be as follows:

(a) Step-one

NID Number:.....

Date of Birth: (DD/MM/YYYY).....

Biometric verification..... Next

In this step, a customer approaches to a bank or its agent approaches to a customer for account opening or BO account opening or policy opening process using e-KYC. Then, the customer will provide his or her NID. Bank or its agent inserts NID number and Date of Birth (DOB) into the specified template and also collects fingerprint, then press Next button. Once bank or its agent presses Next button the information of NID number, DOB and fingerprint data will be matched with NID database, if the data is matched, then next template will be appeared.

(b) Step-two

Applicant's Name: .....

Mother's Name: .....

Father's Name: .....

Spouse Name: .....

Gender (M/F/T): ……...

Profession: ……

Mobile Phone Number: ……..

Present Address: .....

Permanent Address: .....

Nominee: …… Relation: …… Photograph: ……Next

In step two, bank or its agent will insert or punch customer's personal information data as far as possible. It is encouraged that bank use the technology that enable data fetching from the NID and wherever required insert rest other information manually. On completion of personal information, the bank or agent will press Next option.

(c) Step-Three

Photograph: .....Next

In step three, bank or its agent or client will capture or upload customer's photograph. However, when there is self-check in occurs, then live selfie with proper light and camera frame is required; then press Next option.

(d) Step-Four

Client wet signature or electronic signature or digital signature or PIN…….. Next

In step four, customer wet signature (signature using pen) or customer electronic signatures (signature using devices) or digital signature or personal identification number (PIN) is required to be preserved for future reference.

(e) Step-Five

Account Opening Notification

In step five, after completion of all the processes, system will generate a notification of account opening in process. After completion of necessary sanction and other screening, account opening confirmation notification should be sent to the customer.

The simplified customer onboarding process will be completed once the client gets notification from the bank. However, at any point of relationship, the financial institution may ask for additional information from customer and will preserved it in the digital KYC profile of customer.

In case of joint customer (more than one) onboarding the similar process need to be followed. All the field mentioned in step- two is the minimum requirement, however, banks may add few fields where necessary.

7.5.3 Required technology:

The electronic customer onboarding and e-KYC process requires technology platform. Therefore, based on the simplified e-KYC model at a minimum, following technology and instruments may be used to complete the process;

(a) Software/App/Program compatible to the above process;
(b) Internet connection;
(c) Online connection to the NID verification server;
(d) Fingerprint capturing devices;
(e) Electronic signature capturing devices (where necessary) etc.

7.5.4 Customer onboarding by using face matching:

The financial institution may adopt customer onboarding using face matching model where customer face biometrics will be used as a main identifier of a person's identity along with the national ID number. Following steps will be required for onboarding of a customer by using face matching model:

(a) Step-one

- Taking picture of customer NID (original copy)-front page
- Taking picture of customer NID (original copy)-back page ……Next

In this step, a customer approaches to a bank or its agent approaches to a customer or customer engaged in self check-in for account opening, or BO account opening or insurance policy opening process by using e-KYC procedures. Then, it requires to capture photograph or scanning front page of the customer NID followed by the back page. An optical character recognition (OCR) should be used to capture the NID data both in Bangla and English. In the back end all NID data will be preserved within specific format.

(b) Step-two

- Taking picture of customer face……Next

In step two, bank or its agent or client will take an appropriate photograph of the customer's face by using high resolution camera or webcam. While taking picture agent or client required to be tactful enough to take the face only of the customer as well as visible quality of the photograph.

(c) Step-Three

Applicant's Name: .....

Mother's Name: .....

Father's Name: .....

Spouse Name: .....

Gender (M/F/T): ……...

Profession: ……

Mobile Phone Number: ……..

Present Address: .....

Permanent Address: .....

Nominee: …… Relation: …… Photograph: ……Next

In step three, all necessary information will be fetched up in the above digital format. Furthermore, additional input may be punched to fulfill the whole template.

(d) Step-Four

Client wet signature or electronic signature or digital signature or PIN……Next

In step four, customer wet signature (signature using pen) or customer electronic signatures (signature using devices) or digital signature or personal identification number (PIN) is required to be preserved for future reference.

(e) Step-Five

Account Opening Notification ……Next

In step five, after completion of all the processes, system will generate a notification of account opening in process. After completion of necessary sanctions and other screening, account opening confirmation notification should be sent to the customer.

The simplified customer onboarding process will be completed once the client gets notification from the financial institution. However, at any point of relationship, the financial institution may ask for additional information from customer and will preserve it in the digital KYC profile of customer.

In case of joint customer (more than one) onboarding, the similar process required to be followed. All the field mentioned in step- two is the minimum requirement, however, banks may add few fields where necessary. On the other hand, the capital market intermediaries and the insurance companies may add necessary relevant fields as per CDBL requirement and policy proposal form respectively.

7.6 Required technology (same for Regular Measures):

At a minimum, the customer onboarding via face matching model requires to use the following technology to complete the whole customer onboarding process;

(a) Software/App/Program compatible to the above process; (b) Internet connection;
(c) Smart phone or desktop computer with high resolution webcam;
(d) Online connection to the NID verification server15;
(e) Electronic signature capturing devices (where necessary) etc.

7.6.1 Sanctions and other screening:

The full-fledged account procedures will be completed by completion of sanction and other necessary screening which includes as follows:

(a) UNSCRs screening;
(b) Adverse media screening (where necessary); and
(c) Internal or external exit list (where necessary).

7.6.2 Audit trail of customer profile:

To maintain an audit trail a bank or their nominated third parties are required to preserve a digital KYC profile and relevant logbook, even for low risk or financial inclusion products, which should include the followings:

(a) Customer details (name, contact, address, etc) with photograph;
(b) Customer ID image (both side);
(c) Customer signature (where necessary);

(d) Customer risk review process (once in 5 years);
(e) Transaction pattern etc; and
(f) Others information as deemed necessary to complete customer KYC.

The financial institution should maintain a digital log for all successful and unsuccessful clients onboarding, matching parameters etc. for further use and audit trail. All the technology data should be preserved and stored digitally for further both internal and external audit purposes. The sample e- KYC profile, at a minimum, should be look like as per annex -1.

7.7 Customer onboarding- Regular measure:

Bank encouraged to use electronic onboarding and e- KYC procedures for the products and services which are not fall under proven low risk or limited risks as well. This means electronic onboarding and e- KYC procedures are also applicable for any sorts of financial products.

Both the technology-based model i.e. fingerprints and faces matching technologies are applicable for regular onboarding and managing KYC. Similarly, such onboarding process only applicable for natural person who have valid NID.

Initially onboarding process for the regular e-KYC is similar, however, it requires few modes of additional information and conduct additional customer due diligence compared to the simplified method. The reporting entities are required to create digital customer KYC profile and risk grading exercise digitally during the regular e-KYC. This means similar step by step17 procedures have to be followed in case of different models (fingerprint and face matching) as discussed above to complete the regular e-KYC procedures.

Therefore, the component of regular e-KYC includes the following elements:

a) A digital template with more information compared to simplified e-KYC;
b) A more stringent KYC profile of the customer;
c) Screening of customer other than UN Sanctions (for example: PEPs/IPs, Beneficial Owner, Adverse Media, Internal External list checking etc.); and
d) Risk grading exercise.

The digital information template at a minimum required for regular e-KYC would be as follows:

Account Name…… Account Type……

Account Number…….....Unique Account Number…….....

Applicant's Name: .....

Mother's Name: .....

Father's Name: .....

Spouse Name :.....

Gender (M/F/T)…….. Date of Birth……

Profession…… Monthly income…… Sources of Fund…….

Mobile Phone Number:……

Present Address: ..... Nationality……

Permanent Address: .....

Nominee:……Date of Birth…….. Relation…… Photograph……

NB: a) Incorporate 'add' button of similar field if there is more than one applicant;

b) Incorporate 'add' button of similar field if there is more than one nominee;

c) If applicant is minor then they should proceed for traditional methods of account opening;

d) Incorporate 'add' the following field if nominee is 'Minor'

i) Name of minor nominee… ii) Name of Guardian… iii) Address…. iv) Relation…. v) NID of Guardian……. vi) Photograph of Guardian…….

The customer onboarding process and instructions as discussed above for the simplified measures will be similar for regular e-KYC. After opening account financial institution may collect additional information and customer wet signature to create full digital profile of the client.

7.7.1 Sanctions and other Screening:

The screening mechanism for regular e-KYC is quite stringent compare to the simplified one. The full-fledged account procedures will be completed by completion of sanctions and other necessary screening which includes as follows:

(a) UNSCRs screening;
(b) PEPs/IPs Screening;
(c) Identification of beneficial ownership (if any);
(d) Adverse media screening;
(e) Risk grading of customer;
(f) Customer Due Diligence template;
(g) Enhanced Due Diligence (if needed).

7.7.2 Audit trail of customer Profile:

To maintain an audit trail we and our nominated third parties are required to preserve a digital KYC profile and relevant log book or data which should include the followings:

(a) Customer details (Name, contact, address, etc) with photograph;
(b) Customer ID image (both side);
(c) Customer signature (where necessary);
(d) Risk grading of customer (where necessary);
(e) Customer Due Diligence template (where necessary)

(f) Customer transaction pattern; and
(g) Others information as deemed necessary to complete customer KYC.

We should maintain a digital log for all successful and unsuccessful e-KYC onboarding process for further work and audit trail. All the technology data should be preserved and stored digitally for further audit purposes.

7.8 Matching parameters:

Required Technology and the same technologies and the similar matching parameters mentioned in the simplified e-KYC will be applicable for regular e-KYC.

7.9 Security measures:

NRBC Bank may use additional security measures in the customer onboarding process which may contains checking the phone number by generating pin codes and other measures as deemed necessary. Additionally, security of the data recorded and preserved under this e-KYC should be maintained properly by us so that no customer data to be hacked or compromised. This Guideline also suggest to preserved customer data locally hosted server or cloud sever and put in place necessary data protection and data security measures as prescribed by the prudential and self-regulators and/or by the government of Bangladesh.

7.10 Other relevant issues:

7.10.1 Record Keeping:

Bank should maintain all sorts of digital data and log until five years after the closure of the account or business relationship. The digital data shall contain customer onboarding, customer identity verification, KYC profile, risk grading exercise; transaction related data and their analysis; all sorts of correspondence with customer; data collected later for CDD purposes; and all other relevant files.

Digital footprint and log should contain but not limited to information collected during clients' identity verifications and other relevant information related to the screening measures also required to be preserved. We also may collect other complementary data (such as, geo location, IP addresses, etc.) which could also support ongoing due diligence.

7.10.2 Reliance on third Parties:

To implement the e-KYC, bank may rely on the third- party technology providers either full or part to implement e-KYC. Though a bank may be engaged with third party, the ultimate responsibility still lies with them. This means we may rely on another entity or technology providers that satisfies the criteria described above to conduct customer due diligence which covers (i) customer identification and verification data from independent and reliable sources; (ii) identify and understand who the beneficial owner(s) is; and (iii) identify the purpose and intended nature of business and relevant CDD measures in a digital manner. Yet, the bank itself should ensure the reliability and authenticity of the data collected. The following condition may apply while engaging with any third party for the bank:

• Immediately obtain the necessary information concerning the identity of the customer as mentioned in (i) –(iii) in the above.

• Take adequate steps to satisfy itself that the third party will make available copies of identity evidence or other appropriate forms of access to the data or digital log as mentioned (i) –(iii) in the above and in this Guideline without delay.

• The activities of the third party shall be regulated under this e-KYC Guidance and will be monitored by bank.

• Third party shall ensure customer and financial institutions' data protection according to the IT security policy of Bangladesh Government and the respective prudential and self-regulators.

• Both the third party and the bank covered under this guidance shall ensure the customer data collected under this guidance shall not digitally transmitted or transferred outside Bangladesh without prior approval of the prudential regulators and/or BFIU. In this case, BFIU Circular No. 26 dated 16/06/2020 will be applicable.

7.11 Risk Assessment:

Bank shall have to conduct a risk assessment of new technology based electronic KYC mechanism to understand how it may be abused and put in place appropriate measures to prevent such abuse as per the circulars and Guidance issued by BFIU. Bank also required to conduct customer risk assessment.

7.12 Transformation of Existing Clients CDD:

Bank may transform their existing clients CDD related documents into digital form following above mentioned procedures where applicable.

Chapter 8: Trade Based Money Laundering Controls, Risk Assessment & Mitigation Mechanism

8.1 Introduction:

Adequate risk based controls are essential to address trade based money laundering risks. This chapter shall introduce TBML risk assessment methodologies and mitigating control measures. This chapter shall also introduce how the risk assessment procedure shall be documented, reviewed from time to time and updated accordingly.

8.2 TBML Risk Assessment & Mitigation Mechanism:

Trade based Money Laundering risk may arise and affect due to inadequate infrastructure of the bank, inaccurate assessment of the customer before on board, poor identification and handling of TBML alert while conducting trade transaction by the officials concerned and; overall for failure of the bank to address the risk at the enterprise or institute level. To ensure proper compliance, TBML risk assessment and mitigation control measures must be implemented at following levels:

- Infrastructure level
- Customer level
- Transaction level
- Enterprise level

First comes infrastructure risk assessment and mitigation as it is impossible to implement mitigation measures without adequate infrastructure.

Secondly, high risk customers with dubious trade transaction give birth to trade fraud. Hence knowing and assessing customer before on board for trade transaction shall be of great use to combating TBML

Thirdly, TBML risk assessment and mitigation at the transaction level is the most important and vital for combating this offense as it is at this level that the TBML takes place. And finally a holistic approach by the entire institution can be effectively implemented through senior management engagement in TBML risk assessment and mitigation at enterprise level. Details are described below.

8.2.1 Infrastructure Level Risk Assessment:

The following infrastructures shall be established and maintained for risk assessment and prompt mitigation:

• Standard Sanction screening process: Sanction screening process shall be fully automated and real time. In case where real time solution cannot be deployed, appropriate controls and standards should be outlined

• Standard for manual screening: Screening procedures for on demand and manual screening shall be thoroughly documented preferably as a part of KYC procedure.

• Own data base based on transactions: The data base shall be integrated with our CBS and also other MIS portals

- Subscription for publically available online commodity pricing website
- Vessel tracking system

8.2.2 Customer Level TBML Risk Assessment and Mitigation Mechanism:

(a) General ML/TF Risk Assessment and Mitigation: The customer level risk assessment starts with the establishment of customer relationship. While establishing business relationship/account opening with the trade customer, general ML/TF risk assessment and mitigation measures as outlined in relevant BFIU circular and ML & TF risk management Guidelines issued for banks by BFIU as well as instructions provided in our ML & TFP Risk Management Policy shall be followed.

(b) Risk Assessment related to Trade: As in most cases there are some products and commodities, various delivery channels and jurisdictions through which TBML occurs, it is quite convenient to have a risk based approach. Risk assessment shall be done by the model given in Annexure C.3. The standard format provided in Annexure C.1 shall be used to collect the required information for the risk assessment model. For fresh/new customers the assessment may be done on the projection submitted in the format by the customers and for the existing and old customers historical data may be chosen. It is also recommended that branches ensure independent evaluation/assessment of importers and exporters by officials and ensure/examine, to the extent practicable, the relationship between importers and exporters through third parties. Customer level risk assessment for newly onboarded trade customer is to be done before initiation of trade transactions. For existing trade customers, customer level risk assessment should be done as early as possible but should not be later than next periodic review of KYC in pursuance with BFIU circular

General steps for customer risk assessment and alert escalation is as follows:

1. General ML/TF Risk Assessment and Mitigation while establishing relationship/account.

2. Risk Assessment: risk assessment through RBA model, then trade related

CDD/EDD before Trade Transaction (Annexure C.1)

3. If risk is acceptable continue trade transaction through three level review system

4. If risk is high forward to level 3 for decision

5. If the transaction is permitted by level 3, conduct EDD and continue else halt the transaction and submit STR/SAR

In all the steps all the records of escalation shall preserved with proper documentation.

(c) Trade related CDD/EDD: If a customer's risk level is found low or medium, branch will conduct CDD for the trade customers before trade transaction takes place. However, if a customer is assessed as high risk, this should be escalated to Level 3 for further scrutiny and verification. If Level 3 is satisfied, they may approve the customer for transaction after conducting EDD. If Level 3 is not satisfied considering the magnitude of risk, bank's risk appetite and internal policy, they may reject the customer for trade transaction. After completion of CDD/EDD, the customer will be allowed to go for trade transaction.

(d) Trade Transaction through 3 Level Review Systems: When a customer is allowed for trade transaction, trade transaction will take place following Three Level Review System

(e) Maintaining a database of escalations with proper documentation: A database shall be established with customers assessed as high risk to facilitate yearly customer wise review and assessment. The DB shall be integrated with our CBS and other MIS systems.

(f) Review and Assessment of Customers: For high risk customers review and assessment frequency shall be one year, for medium risk customers this frequency shall be every three years and for low risk customers it shall be 5 years. This review system will facilitate input for the enterprise wide risk assessment and assist banks to update TBML trend and typology and devise appropriate policy and strategy at the enterprise level.

8.2.2.1 Customer Level Risk Assessment:

The customer level risk assessment shall be done using the framework described in Annexure C.3.

Relevant data such as on jurisdiction, products, services, value & number of trade transactions shall be obtained from TTP.

8.2.2.2 Trade Related CDD Requirements:

In addition to the general CDD measures conducted at the time customer on boarding/ account opening, concerned officials shall also conduct additional trade related CDD before initiating trade transactions. For this purpose, KYC form provided in Annexure C.1 shall be used. In addition to filling up the form, the following documentation/ information shall also be collected in line with the risk based framework:

1. Collection of required documents & information such as:

i. Nature of business including major goods, services and jurisdictions the customer deals with;

ii. Usual delivery / transportation mode for goods or services;

iii. Major suppliers and buyers;

iv. Products and services to be utilized from the bank;

v. Existing/anticipated account activities;

vi. Usual methods and terms of payment and settlement;

vii. Any observations/ratings on the customer by concerned departments of the bank;

viii. Any previous suspicious transaction/activity reports to BFIU;

ix. Other information from the relevant staff; and

x. Trade Transaction Profile.

2. Verification of the documents & information mentioned in 1 above through reliable and independent sources.

3. Ascertaining and verifying the identity of the beneficial owners of the trade customer.

4. Conducting enhance due diligence if required.

5. Record Keeping.

6. Understanding business, production capacity, end-use of goods, the principal counterparties, the countries where the counterparties are located and the goods or services that are exchanged, as well as the expected annual transaction volumes and flows to conduct Customer Due Diligence (CDD) for trade customers.

7. Updating CDD information in accordance with BFIU Circulars and our ML & TF Risk Management Policy.

8. Maintaining customer wise trade transaction profile (TTP) including items of goods, value, volume, nature of business, and principal counterparty country etc. TTP format is given at Annexure C.2. TTP shall be made available to Level 1, 2 & 3 so that they can easily check that a transaction is within the agreed profile of the customer. Until TTP is integrated within core banking system, it may remain offline outside of the core banking system. Level 2 shall conduct TTP review and decide on certain transactions escalated by Level 1. If necessary Level 3 may also consult TTP while taking ultimate decision on transactions escalated by Level 2. Post facto review of TTP against trade transactions shall be conducted at least annually to identify TBML Alerts. Also, TTP may be updated based on trigger events

9. The CDD processes are expected to include "feed-back loops" where a trigger event in a transaction or normal review process leads to new information or questions about a relationship. Objective behind updating of the CDD profile is to ensure that the information in the CDD profile is current. The reviews may also lead to the status of the relationship with the customer being escalated for decisions related to additional controls being applied or the exit of the customer

8.2.2.3 Screening System:

1) Sanction screening shall be conducted on individual, entity, banks, insurer, NGO/NPO, country, port, flag, vessel etc. The screening shall also be conducted on all the parties involved in the transaction and geographic location to the transaction, such as seller of the goods, the shipping company, any agents or third parties, countries or ports etc. that appear in the transactions.

2) For sanction screening it is important to ensure that there is no "risk based approach" –i.e. only screening certain transaction or parties. All parties (known to the bank) related to the transactions at the time and additional parties that come into the picture as the transaction progresses are required to be screened.

3) Vessel tracking (origin port, transshipment, destination port) and its voyage history shall be tracked to determine whether it has docked at embargoed countries during its previous voyage and dealt with sanctioned entities or embargoed goods. It should be borne in mind that vessels may change their names but cannot change their IMO number; hence cross-checking IMO number through a reliable source is recommended.

4) Care should also be taken to PEPs/IPs screening, adverse media screening, High Risk Country screening.

Additional database shall be used for PEP/IP screening.

5) A combination of automated and manual controls will be employed in the context of AML and counter- terrorist financing (CTF) efforts.

Typically the following elements to be, but not limited to, checked via automated /manual procedure:

i. Unit prices

ii. Number of items shipped iii. Shipping marks

iv. Trade term – often an Inco terms rule followed by a place

v. Commercial contract

vi. The documentary credit applications vii. The guarantee applications

viii. The documents presented under import documentary credits

ix. The documents presented under export documentary credits

x. The documents presented under import documentary collections xi. The documents presented under export documentary collections xii. Guarantee demands

xiii. All incoming and outgoing non-SWIFT messages etc.

8.2.2.4 Price Verification:

Prices shall be verified using both internal historical transactional database as well as third party verification sites. Price verification shall be done initially by level 1 officer be escalated further if necessary. Assessment for the threshold shall be done centrally by International Division which shall be disseminated through our central circular archive. Acceptable level of price variances shall be determined by the senior management and be communicated time to time using our circular archive.

8.2.2.5 TBML Alerts:

KYC process is the foundation on which the individual transaction should be evaluated/ examined for TBML Alerts. However, compliance checks carried out on the trade finance transactions are, to a large degree, Manual. This requires a structured risk-based approach to identify, escalate and examine unusual/suspicious activities. One such approach is to work with "TBML Alerts."

A non exhaustive list of "TBML Alerts" indicators is provided in the Annexure B1 & B2. However, the TBML Alerts shall regularly be updated and will be communicated through our circular archive. Also the scenarios shall gradually be added in automated transaction monitoring systems.

8.2.3 Enterprise/Institute Wide TBML Risk Assessment and Mitigation:

Enterprise level TBML risk assessment shall be a part of overall Enterprise Wise Risk Assessment and management of ML & TF risks. The assessment shall later be used to review and update existing policies. The key focus shall be on reviewing new trend and typologies and taking into account gaps found out through annual EWRA. The TBML risk management framework shall use inputs from three primary sources:

- Input from External environment/Factors: Identify emerging risks by reviewing new trends and typologies.
- Input from internal sources: Review the existing own trade based money laundering guidelines:

1. Review the data base of Level 3 escalations and STRs without using identity of the customer.

2. Consolidate overall no. of Alerts raised to level 3 and how they were addressed.

3. Consider inclusion or deletion of high risk country and why.

4. Review, to the extent practicable, TBML alerted counterpart [for import: Beneficiary/Exporter, for

Export: Applicant/importer]

5. Revisit the existing Alerts (along with input from The Model in 5.2.2) based on previous year operation and knowledge of any recent techniques used by trade based money launderers.

6. Revise policy, if and when required. Review customers' risk assessment as per RBA model.

- Input from regulatory changes: Review domestic and international regulatory changes.

Input from all three sources shall be gathered and analyzed. The insights shall be reviewed and analyzed by the CCC. The team may then propose new strategy and policy to combat TBML risk based on the existing insights and gap analysis. The policies and strategies shall later be incorporated in our ML & TF Risk Management Guidelines.

8.3 Few More Notes on Trade Controls:

a) All relevant staff and officials of the bank should be made aware and remain updated of trade controls.

Dissemination through regular correspondence shall be done using various tools such as our central circular archive, online meetings, trainings, webinar etc.

b) To assess the effectiveness and adequacy of the trade controls, independent review shall be done from time to time. Frequency of review shall be yearly unless emergence of any particular or special need arising out of changes in regulatory instructions etc.

c) Trade Controls shall address all possible difficulties that relevant officials may face in combating TBML.

d) Trade Controls should ensure clear division of roles and responsibilities and ownership of risks relating to critical functions.

e) Trade Controls should require decisions relating to trade transactions, work flow procedures and TBML Alerts to be documented appropriately for audit trail purposes, having regard to the record keeping standards as mentioned in MLPA, 2012, GFET, 2018 and ML & TF Risk Management Guidelines. They should also include mechanism to ensure that customer information including applicable trade processes and relevant updates is captured in the relevant bank's customer database, in order to facilitate the assessment and ongoing monitoring of customer activities.

f) Apart from the yearly review of strategy and policy by senior management, they must also be involved in planning and implementation of Trade Controls. The review shall take place yearly through MANCOM meetings.

g) The trade transactions conducted through any IT or Technological Platform will be governed under the directives of Bangladesh Bank issued from time to time.

h) Relevant senior officials having awareness of contemporary intelligence & knowledge on geopolitics and other cross border regulatory restrictions which are not as much stringent as that of Sanction but may lead to regulatory

and legal hassle should guide the transaction level officials on due diligence measures to be exercised in such situations.

i) Trade Controls should be readily identifiable by and made known to all relevant officials engaged in trade related activities.

8.4 Suspicious Transaction/Activity Report Regarding TBML:

a) STR/SAR reporting should be done in accordance with the procedure detailed in the section 10.4. Before submission of STR/SAR, DCAMLCO (if not level 3) and CAMLCO shall only ensure compliance with instructions of relevant BFIU circular. Risk of tipping off should also be managed.

b) Branches should always file an STR/SAR when required to do so under MLPA, ATA and relevant BFIU Circulars. In complex situations banks may seek opinion from BFIU.

8.5 Training on Trade Based Money Laundering:

a) BFIU Circular 26 and our ML & TF Risk Management Policy provide guidance on AML & CFT training.

Through training it shall be ensured that concerned officials understand the trade based money laundering

in both national and international context, bank's exposure to TBML and own Trade Controls.

b) Training need assessment shall be conducted on preventing TBML. For level 1, 2, 3 officials training is essential. Training should be designed in such a way that the trainees are able to provide, or contribute to, training depending on their background, role and experience.

c) For officials involved in day to day trade processes role based training should also be included. Objective behind such training should be to impart training to them on TBML specific risks and responsibilities.

d) Trade based money laundering training should form a core part of a bank's training calendar or training plan. Training records should also be retained properly.

Chapter 9: Credit Backed / Based Money Laundering

9.1 Definition & Process:

Credit backed method of money laundering involves cleaning of money obtained from criminal activities such as insider trading, extortion, illegal gambling, and drug trafficking to appear to have been derived from legal activities in order for financial institutions to deal with it without any suspicion. Money can be laundered using various methods which vary in terms of sophistication and complexity. Investments and mortgages are usually taken as a cover to launder money proceedings, and lump sum cash repayments are used to repay the investments or mortgages.

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

Most often, the money launderer establishes an apparent legal origin of money through fabrication of transactions like agreements, book keeping, and invoices, deeds, reports, and spoken/written statements. The common methods used to justify money laundering is fabricating a credit, also referred to as back-to-back or credit - back. The most popular credit - back form of laundering money is when criminals borrow their own criminal money. This is usually done through the creation of a credit agreement between the criminal and a third party. Most used third parties are offshore corporations who are controlled by the criminals. Although back-to-back loan/credit are the common ways that money can be washed.

9.2 Money laundering through Real Estate Sector:

The real-estate sector may be one of the many vehicles used by criminal organizations to launder their illicitly obtained money. The emerging markets seem to be more vulnerable to misuse of the real estate sector. Due to the worldwide market growth of real estate-backed securities and the development of property investment funds, the range of options for real estate investments has also grown. This effect has not gone without notice in emerging markets. Money laundering transactions can be easily camouflaged in genuine commercial transactions among the huge number of real estate transactions taking place. Complicating matter is the fact that often these less developed economies do not have an average market price for real estate, but rather prices varying across sectors and districts. To complete real estate transactions in some stage of the process involvement of legal expert is inevitable.

The real estate sector merits closer consideration given the large scope of monetarytransactions, its significant social impact, and because of the number of cases in which money laundering, and in limited circumstances terrorist financing and tax fraud schemes, have been detected. Abuse in this

sector also has the undesirable effect of political, institutional and economic destabilization. Moreover, due to the international nature of the real-estate market, it is often extremely difficult to identify real estate transactions associated with money launderingor terrorist financing.

In order to misuse the real-estate sector, a number of methods, techniques, mechanisms, and instruments are available. Many of these methods are in and of themselves illegal acts; however, certain of them might be considered perfectly legal if they were not associated with a money laundering or terrorist financing scheme.

A series of the more common or basic methods is used which are mentioned as under:

a) Use of complex investments or credit finance.
b) Use of non-financial professionals.
c) Use of corporate vehicles.
d) Manipulation of the appraisal or valuation of a property.
e) Use of monetary instruments.
f) Use of mortgage schemes.
g) Use of investment schemes and financial institutions.
h) Use of properties to conceal money generated by illegal activities.

9.3 Assistance in the Purchase or Sale of Property:

Non-financial professionals such as notaries, registrars, real-estate agents, etc., are sometimes used by suspected criminals on account of their central role in carrying out real-estate transactions. Their professional roles often involve them in a range of tasks that place them in an ideal position to detect signs of money laundering or terrorist financing.

The role of non-financial professionals in detecting illegal activity can also be significant in this area. There have been examples of notaries and registrars detecting irregularities in the signing of the property transfer documents (for example, using different names or insisting on paying a substantial part of the cost of the transaction in cash). Other examples include buying land designated as residential through a legal person and then reclassifying it a short time later for commercial development. Professionals working with the real-estate sector are therefore in a position to be key players in the detection of schemes that use the sector to conceal the true source, ownership, location or control of funds generated illegally, as well as the companies involved in such transactions.

9.4 Corporate Vehicles:

Corporate vehicles – that is, legal persons of all types and various legal arrangements (trusts, for example) – have often been found to be misused in order to hide the ownership, purpose, activities and financing related to criminal activity. Indeed, that practice is so common that it almost appears to be ubiquitous in money laundering cases. The misuse of these entities seems to be most acute in

tax havens, free-trade areas and jurisdictions with a strong reputation for banking secrecy; however, it may occur wherever the opacity of corporate vehicles can be exploited.

Apart from obscuring the identities of the beneficial owners of an asset or the origin and destination of funds, these corporate vehicles are also sometimes used in criminal schemes as a source of legal income. In addition to shell companies, there are other specialized companies that carry out perfectly legitimate business relating to real estate, which have sometimes been misused for money laundering purposes. This aspect is illustrated by the use, for example, of property management or construction companies. The use of corporate vehicles is further facilitated if the company is entirely controlled or owned by criminals.

9.5 Shell Companies:

A shell company is a company that is formed but which has no significant assets or operations, or it is a legal person that has no activity or operations in the jurisdiction where it is registered. Shell companies may be set up in many jurisdictions, including in certain offshore financial centers and tax havens. In addition, their ownership structures may occur in a variety of forms. Shares may be held by a natural person or legal entity, and they may be in nominative or bearer form. Some shell companies may be set up for a single purpose or hold just one asset.

Others may be set up for a variety of purposes or manage multiple assets, which facilitates the co-mingling of legal and illicit assets.

The potential for anonymity is a critical factor in the use of shell companies. They may be used to hide the identity of the natural persons who are the true owners or who control the company. In particular, permissive practices regarding the form of the shares, whether corporate, nominative or bearer, together with the lack of co-operation on the collection of information, represent a significant challenge when seeking to determine the ultimate beneficial owner.

9.6 Manipulation of the Appraisal or Valuation of a Property:

Manipulation of the real value of properties in relation to real estate involves the overvaluing or undervaluing of a property followed by a succession of sales and purchases. A property's value may be difficult to estimate, especially in the case of properties that might be considered a typical, such as hotel complexes, golf courses, convention centers, shopping centers and holiday homes. This difficulty further facilitates the manipulation when such property is involved.

9.7 Over-valuation or Under-valuation:

This technique consists of buying or selling a property at a price above or below its market value. This process should raise suspicions, as should the successive sale or purchase of properties with unusual profit margins and purchases by apparently related participants. An often-used structure is, for example, the setting up of shell companies to buy real estate. Shortly after acquiring the

properties, the companies are voluntarily wound up, and the criminals then repurchase the property at a price considerably above the original purchase price. This enables them to insert a sum of money into the financial system equal to the original purchase price plus the capital gain, thereby allowing them to conceal the origin of their funds.

9.8 Investment in Hotel Complexes, Restaurants and Similar Developments:

Real estate is commonly acquired in what is known as the integration or final phase of money laundering. Buying property offers criminals an opportunity to make an investment while giving it the appearance of financial stability. Buying a hotel, a restaurant or other similar investment offers further advantages, as it brings with it a business activity in which there is extensive use of cash.

9.9 Personal Loan/Car Loan/Home Loan:

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

9.10 Money laundering through Credit Cards:

Criminals and terrorist groups are finding new and complex methods to conceal the illegal profits they earn via an online environment. Now a days, an extensive range of payment systems has become available such as PayPal, Google Pay, Amazon Pay, Apple pay etc. This, along with the progressively increasing amounts of e-commerce activities happening online, causes difficulties when it comes to detecting fraudulent financial transactions and money laundering through credit cards, payment service providers and banks.

As a prominent payment method, credit cards have been used as a vehicle to conduct money laundering. Therefore, detection and prevention of transaction laundering or credit card money laundering is a pressing concern for financial services. They need to develop rigorous anti money laundering (AML) policies to act on credit card money laundering red flags and mitigate credit card money laundering risk.

Transaction laundering or electronic money laundering is an extension of money laundering. Itis a streamlined form of money laundering used to secretly processed credit card or other digital payment forms. Transaction Laundering happens when one approved merchant/vendor uses payment credentials to process payments for another undisclosed store often selling illegalproducts and services.

Structured credit card money laundering schemes help illegal merchandise sellers hide their transactions by entering sales receipts into payment system and washing the dirty money. While these illegal sellers can be a bricks and mortar store, they are primarily set up as web stores in modern days. The largest amount of credit card money laundering is committed by those who sell counterfeit merchandise, drugs, sex services and online casino operators and who operate without a license. Even when the goods and services are sold legally, representing the nature of credit card payment falsely violates the processing merchant's agreement with its acquiring bank. By benefitting from a scheme such as this, the criminals are violating number of state, FIU and AML laws, depending on the nature of the transactions.

Credit card money laundering or transaction laundering is also known as "factoring" and un-authorization aggregation. This takes place when one business (often a website) processes payment for another website. This allows the sellers for illicit products (goods & services) to hide their transactions and wash their illegal money by illicitly entering their sales receipt into official and legal payment system. For example, a fashion e-commerce website can help process payment made from illegal drug networks.

In order to target the system, supporting drug businesses, the U.S. Food and drug administration (FDA) set out a series of investigations that were focused on credit card processors involved in the credit card money laundering or transaction laundering arrangements. This operation was a notable example to show the payment industry why transaction laundering monitoring is so important. It also witnessed how law enforcement agencies perceive the role of credit card processors in the network of illegal business.

Chapter 10: Record Keeping

10.1 Records to Be Kept:

The types of records that shall be kept will include but not limited to the following:

Customer information. This will include:

- All kinds of information, documentations or any other reports derived while Conducting CDD/ KYC Measures at any point of business relationships
- Transaction related information/ documentation of walk in customers
- Transactional data, documentation and other evidences (Domestic and Cross border transactions)
- Suspicion reports
- All Reports from AMLD/CCC/CAMLCO
- Training and compliance monitoring
- Information and records related to workshops, meeting, training, audit/inspection and special inspections
- Information about the effectiveness of trainings
- Any other information, documentation, report or evidences that are generated in the course of due diligence or monitoring process
- Any other information, documentation, report or evidences required to be preserved by the regulatory authorities

In addition to the categories mentioned here. The concerned officials may preserve additional records if deemed necessary. Detailed instructions for the each category of records are outlined in subsequent sections.

10.2 Length of Record Keeping Period:

All records shall be kept at least for five (5) years period after end of business relationship with respective customer

10.3 Customer Information:

Customer information in this context will refer to information regarding customer identity and description. Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. /The branches and concerned divisions shall preserve customer information in the format mentioned as follows:

10.3.1 Deposit Product Customers:

Branches shall preserve account opening forms and other related documents depending on the type of account. List of required document for various type of accounts are given in Annexure B.1. Any of the following documents may be preserved during CDD for customer Identification:

- Photocopy of NID. Or,
- Photocopy of Passport. Or,
- Photocopy of Birth Certificate with an additional Photo ID.

Additional documentation such as driving license, E-TIN, Organizational ID may be obtained for the satisfaction of the account opening officer.

10.3.2 Money Transfer Services:

In case of delivering services through money transfer services (e.g. Western Union, Xpress Money, Ria), branches shall preserve TRM forms containing detailed remitter and beneficiary information. Detailed instructions are provided in via our instructions circulars

10.4 Transactions:

All transactions carried out on behalf of or with a customer in the course of relevant business shall be recorded within the bank's records. These records shall be retained in physical or electronic form (i.e. recorded in our CBS). Transaction records in support of entries in the accounts, in whatever form they are used, e.g. Cheques, Deposit Vouchers, specimen signature and other related transaction vouchers shall be maintained in hardcopy/printed form in a sorted way at the branches so that those could easily be retrieved when needed. However, In case of transactions where physical copies transaction records are not available, System generated reports/vouchers shall be used on demand. 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.

10.5 Internal & External Reports:

The following categories of reports shall be preserved:

SI	Report Name	Preservation Format
1	Monthly STR	Hard copy at the branch premise & a scanned copy send to AML & CFT Division, HO
2	Monthly CTR	Hard copy at the branch premise & a scanned copy send to AML & CFT Division, HO
3	Quarterly BAMLCO Meeting Minutes	Hard copy at the branch premise & a scanned copy send to AML & CFT Division, HO
4	Half Yearly Self Assessment	Hard copy at the branch premise & a scanned copy send to AML & CFT Division, HO

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

10.6 AML & CFT Training Information:

The following records shall be preserved regarding AML & CFT Training:

• Date, Course Content & name of resource persons shall be preserved both by AML& CFTD & NRBCB Training Institute.
• List of staff who received the training shall be preserved both by AML& CFTD & NRBCB Training Institute.
• Test results shall be preserved by NRBCB training institute.

10.7 Formats & Retrieval of Records:

In addition to the physical reports, all customer information, transactional data shall be inserted into our CBS for record keeping and retrieval in future. The retrieval methods for various types of records are as follows:

Sl	Information Category	Retrieval Method
1	Customer Information	AOF, NID Photocopy, Passport photocopy etc from branch premises. Through CBS reporting modules from any Branches/HO.
2	Transactional Data	Transaction records in support of entries (Cheque, deposit slip, debit instructions, specimen signatures etc). Through CBS reporting modules from any Branches/HO.
3	Reports for regulatory authorities	Physical copies from respective branch/division.
4	Training Information	Physical records kept in AML & CFTD & NRBCB Training Institute

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. Records preserved in databases of our CBS can deliver required information instantly. However, searching through physical records poses certain challenges regarding time constraint. That's why it is imperative that all the branches and concerned division shall follow an organized method for preserving hardcopies so that the required information can be retrieved with minimal delay.

Chapter 11: Reporting to BFIU (Suspicious Transaction/Activity Report & Others Reporting)

The final output of all compliance programs is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the risk for bank. So it is necessary for the safety and soundness of the bank.

11.1 Definition of STR/SAR:

Generally STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seems to be usual manner. Such report is to be submitted by financial institutions to the competent authorities.

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

(1) the property is the proceeds of an offence,

(2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;

(3) 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.

11.2 Obligations Of Such Report:

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

11.3 Reasons For Reporting Of STR/SAR:

As discussed above, STR/SAR is very crucial for the safety and soundness of the financial institutions. The financial institutions should submit STR/SAR considering the followings:

- It is a legal requirement in Bangladesh;
- It helps protect the reputation of banks
- It helps to protect banks from unfounded allegations of assisting criminals, including terrorists;
- It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

11.4 Identification And Evaluation of STR/ SAR:

Identification of STR/SAR is very crucial for banks to mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place by the banks. Such suspicion may not only at the time of transaction but also at the time of doing KYC and attempt to transaction.

Identification of STR/ SAR:

Identification of STR/SAR may be started identifying unusual transaction and activity. Such unusual transaction may be unusual in terms 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 valid reasonable explanation.
- ✓ By monitoring customer transactions.
- ✓ By using red flag indicator.

Simply, if any transaction/activity is consistent with the provided information by the customer can be treated as

normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.

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

a) Identification:

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

b) Evaluation:

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

c) Disclosure:

This is the final stage and bank should submit STR/SAR to BFIU. After checking the sufficiency of the required documents, CCC/ ML and TFP Div. shall submit a suspicious transaction/activity report to BFIU without delay by using goAML web as per instruction mentioned in goAML Manual. Every stages of evaluation bank should keep records with proper manner.

CCC/ ML and TFP Div. shall submit suspicious transaction/activity report to BFIU if it identifies any transaction or activity as suspicious even though the concerned branch did not identified as suspicious.

11.5 Risk-Based Approach:

An integrated risk-based system depends mainly on a proper assessment of the relevant risk sectors, products, services, and clients and on the implementation of appropriate risk-focused due diligence and record-keeping. These in turn become the foundation for monitoring and compliance mechanisms that allow rigorous screening of high-risk areas and accounts. Without sufficient due diligence and risk profiling of a customer, adequate monitoring for suspicious activity would be impossible. According to the Wolfsburg Group guidelines, a risk-based monitoring system for financial institutions clients should:

- ✓ compare the client's account/transaction history to the client's specific profile information and a relevant peer group, and/or examine the clients account/transaction history against established money-laundering criteria/scenarios, in order to identify patterns of suspicious activity or anomalies;
- ✓ establish a process to compare customer or transaction-specific data against risk-scoring models;
- ✓ be capable of recognizing patterns and of "learning" which transactions are normal for a client, rather than designating certain transactions as unusual (for example, not all large transaction are unusual and

may easily be explained);

- ✓ issue alerts if unusual transactions are identified;
- ✓ track alerts in order to ensure they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required; and
- ✓ Maintain an audit trail for inspection by the institution's audit function and by financial institutions supervisors.

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

Questions that a financial Institution must consider when determining whether an established customer's transaction must be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?

Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

11.6 Internal Reporting Procedures and Records:

a) Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the CAMLCO. This ensures speed, confidentiality and accessibility to the CAMLCO. However, in line with accepted practice, some financial sector businesses may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting to the CAMLCO or an appointed deputy through the branch/unit level AMLCO.

b) Supervisors should also be aware of their own legal obligations. An additional fact which the supervisor supplies may negate the suspicion in the mind of the person making the initial report, but not in the mind of the supervisor. The supervisor then has a legal obligation to report to the BAMLCO.

c) All suspicions reported to the CAMLCO should be documented (in urgent cases this may follow an initial discussion by telephone). In some cases it may be possible for the person with the suspicion to discuss it with the BAMLCO.

d) The CAMLCO should acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. "tipping off". All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should 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

e) On-going communication between the CAMLCO and the reporting person/department is important. The institution may wish to consider advising the reporting person, department or branch of the CAMLCO's decision, particularly if the report is believed to be invalid. Likewise, at the end of an investigation, consideration should be given to advising all members of staff concerned of the outcome. It is particularly important that the CAMLCO is informed of all communication between the investigating officer and the branch/unit concerned at all stages of the investigation.

f) Records of suspicions, which were raised internally with the CAMLCO but not disclosed to BFIU, should be retained for five years from the date of the transaction. Records of suspicions which the BFIU has advised are of no interest should be retained for a similar period. Records of suspicions that assist with investigations should be retained until the bank is informed by the BFIU that they are no longer needed.

Officers of the Bank will not divulge any information pertaining to STR submitted to BFIU in any circumstances to the customer or other for which investigation is hampered or impact adversely.

11.7 STR Reporting Procedures :

Institutions enlisted as per MLPA, 2012 and ATA, 2009 (as amended in 2012) are obligated to submit STR/SAR to BFIU, Bangladesh Bank. Such report must come to the BFIU from AMLD of the bank by using specified format/instruction given by the BFIU.

SUSPICIOUS TRANSACTION TO BE REPORTED IMMEDIATELY ON DETECTION AS PER CIRCULAR NO. AML-19/008 DATED AUGUST 14,2008 ANNEXURE-A

STR to be submitted in the prescribe format directly by the CAMLCO to:

Director, Bangladesh Financial Intelligence Unit (BFIU)

Bangladesh Bank, Head Office, Dhaka. Email: goAML Portal: fiuportal.bb.org.bd/

The use of a standard format in the reporting of suspicious activities is important and bank is required to use the unusual/suspicious transactions reporting form as per Annexure KA of the AML Circular No.19 dated 14th August, 2008. Suspicious activity reports should be typed whenever possible or, if the standard layout is followed, generated on word-processing software. Further information and advice can be obtained from the Bangladesh Financial Intelligence Unit of Bangladesh Bank.

Sufficient information should be disclosed on the suspicious transaction, including the reason for the suspicion, Suspicious Activity/ information and transaction detail with counter parties detail to enable the investigating officer to conduct appropriate enquiries. If a particular offence is suspected, this should be stated so that the report may be passed to the appropriate investigation team with the minimum of delay. However, it is not necessary to complete all sections of the suspicious activity report form and its submission should not be delayed if particular details are not available.

Where additional relevant evidence is held which could be made available to the investigating officer, this should be noted on the form.

Following the submission of a suspicious activity report, bank is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal commercial reasons. It must not alert the customer to the fact of the disclosure as to do so would constitute a "tipping-off" offence. Close liaison with BFIU, Bangladesh Bank and the investigating officer is encouraged in such circumstances so that the interests of all parties may be fully considered.

11.8 Tipping Off:

Section 6 of MLPA 2012 and FATF Recommendation 21 prohibits bank, its directors, officers and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the bank is seeking to perform its CDD obligation in those circumstances. If there is any chance of Tipping off while doing CDD for a suspicious client, STR should be reported without doing CDD of the same. The customer's awareness of a possible STR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation.

11.9 Penalties of Tipping Off:

Under section 6 of MLPA, 2012, if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of

employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

11.10 "Safe Harbor" Provisions For Reporting:

Safe harbor laws encourage bank to report all suspicious transactions by protecting banks, employees and its board of directors from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. In section (28) of MLPA, 2012 provides the safe harbor for reporting.

11.11 Red Flags or Indicators of STR/SAR:

11.11.1 Moving Customers: A customers who moves every month, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal, could be suspicious.

11.11.2 Out of Market Windfalls: If you think a customer who just appeared at the bank sounds too good to be true, you might be right. Pay attention to one whose address is far from your branch, especially if there is no special reason why you were given the business. Isn't there any branch closer to home that could provide the service? If the customer is a business, the distance to its operations may be an attempt to prevent you from verifying there is no business after all. Don't be bullied by the sales personnel who follow the "no question asked" philosophy of taking in new business.

11.11.3 Suspicious Customer Behavior:

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses the record-keeping or reporting duties with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be recorded.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.
- Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.
- Customer who is a student uncharacteristically transfers/exchanges large sums of money.
- Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

11.11.4 Suspicious Customer Identification Circumstances:

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information when opening an account.
- Customer's permanent address is outside the branch's service area.
- Customer asks many questions about how the bank disseminates information about the identification of a customer.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.
- Customer is not interested to disclose any other bank account's information.

11.11.5 Suspicious Cash Transactions:

- Customer opens several accounts in one or more names, then makes several cash deposits under the reporting threshold.
- Customer conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf.
- Corporate account has deposits and withdrawals primarily in cash than cheques.

11.11.6 Suspicious Non-Cash Deposits:

- Customer deposits large numbers of consecutively numbered money orders or round figure amounts.
- Customer deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business.
- Funds out of the accounts are not consistent with normal business or personal items of the account holder
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

11.11.7 Suspicious Activity in Credit Transactions:

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

11.11.8 Suspicious Commercial Account Activity:

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.
- TT or other remittances to or from the border areas without any reasonable ground.
- Remittances from any High Risk or drug producing/transit countries
- Under/Over invoicing in import or export business.
- Mis-declaration of goods in import or export business.
- Maintain different accounts in different names

11.11.9 Suspicious Employee Activity:

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires.
- Employee frequently is involved in unresolved exceptions or recurring exceptions on exception reports.
- Employee lives a lavish lifestyle that could not be supported by his/her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.

11.11.10 Suspicious Activity in a bank Setting:

- Request of early encashment.
- A DPS (or whatever) calling for the periodic payments in large amounts.
- Lack of concern for significant tax or other penalties assessed when cancelling a deposit.

11.12 Cash Transaction Report (CTR):

As per Bangladesh bank directives Bank shall submit CTR centrally for deposit and withdrawal of cash for such amount as determined by Bangladesh Bank from time to time. CTR of one month should be reported by AML Division to BFIU by 21st day of the following month through goAML Web if in a particular month no CTR transaction is made by any Branch, Branch shall report to AML Division as "No CTR transaction has been occurred for the month of "YYY" and AML Division shall report a list of such Branches through goAML Message Board while submitting the CTR where no CTR transactions have been occurred for the reporting month. Inter Bank or Inter Branch transactions will not be reported. Only cash withdrawal transactions will be reported for Govt. accounts, Govt. owned entities, Semi Govt. owned entities and/or Autonomous organizations. At present CTR threshold amount is BDT10, 00,000.00 (Ten Lac) and above or equivalent either by single entry or multiple transaction in a day.

11.13 Structuring of Cash Transaction:

As per Money Laundering prevention Act, structuring (unnecessary transaction) is an offence. If a customer intends to conduct such transactions to avoid reporting requirements, under the MLP Act, it is called structuring. Branch official should be vigilant to detect structuring and report to AMLD as STR. CTR should be analyzed before submitting by Branches and if any suspicious transaction found, Branch shall report it immediately to AML Division. If no suspicious transaction found, Branch shall report to AML & CFT Division as "No suspicious Transaction Found".

11.14. Half Yearly Report to be submitted to the MD & CEO/ Board :

As per Bangladesh Bank directives in BFIU Circular No. 26 dated: 16/06/2020, AML & CFTD will submit a report on Half Yearly basis on the implementation Status/Steps taken to Combating Money Laundering and other related AML issues to the MD & CEO/Board on regular basis.

11.15 Self-Assessment Process:

Bank should establish a half-yearly self-assessment process that will assess how effectively the bank's anti-money laundering procedures enable management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment should conclude with a report documenting the work performed, who performed it, how it was controlled and supervised and the resulting findings, conclusions and recommendations. The self-assessment should advise management whether the internal procedures and statutory obligations of the bank have been properly discharged. The report should provide conclusions to three key questions:

- Is anti-money laundering procedures in place?
- Is anti-money laundering procedures being adhered to?
- Do anti-money laundering procedures comply with all policies, controls and statutory requirements?

Branch shall assess their performance on half-yearly basis according to AML circular 19 dated 17-09-2018, of BFIU, Bangladesh Bank. The shortcomings identified to be overcome and complied with in next half year and AML & CFT Division will prepare an appraisal report on half yearly basis and to be place to the CEO with a copy to BFIU, Bangladesh bank.

As per the format given in BFIU Circular No 26 dated 16/06/2020, issued by BFIU an Independent Testing Procedures should be conducted for the branches by the ICCD. While conducting the same they should look into whether the policy and directives on AML issues are followed meticulously by the Branches and appraise the performance of the branch with grading and submit report to AML & CFT Division. On receiving the Independent Testing Procedure report, AML & CFT Division will prepare a report on branch grading and marks on half yearly basis and that should be placed to the CEO for his review and comment. A copy should be forwarded to BFIU, Bangladesh Bank.

Chapter 12: Recruitment, Training & Awareness

12.1 Employee Screening:

Bank is subject to ML & TF risk from its customers as well as from its employee in absence of proper risk mitigating measures. ML & TF risks that arise from customers and its mitigating measures have been discussed in several chapters of this guideline. To mitigate ML & TF risks that arise by or through the bank's employees, our bank shall follow a fair recruitment procedure. This fair recruitment procedure shall not only includes implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, our bank shall implement the following:

- 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, the HRD shall examine the consistency and capability of the employee and ensure that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

12.2 Know Your Employee (KYE):

Know-your-customer, an essential precaution, shall 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 for this purpose is defined by the bank's HR Policy which is available in our online circular archive.

12.3 Training for Employee:

Almost every employee our bank shall have at least basic AML & CFT training that cover all the aspects of AML & CFT measures in Bangladesh. Basic AML & CFT trainings shall be provided through our In house training institute which will have evaluation module of the trainees. Relevant provision of Acts, rules and circulars, guidelines, regulatory requirements, suspicious transaction or activity reporting shall be covered in basic AML & CFT training course. Lectures shall be conducted by our in-house and external (BFIU) resource persons.

Besides basic and refresher AML & CFT training, we shall arrange job specific training or focused training e.g., 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. BAMLCO/ DCAMLCO and other related employees shall be given specialized training/enrolled in specialized certification programs to enhance their skill set.

12.4 Awareness of Senior Management:

Without proper concern and awareness of senior management of a bank, it is difficult to have effective implementation of AML & CFT measures in the bank. So our bank shall 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 management committee of our bank.

12.5 Customer Awareness & Awareness of Mass People:

The following measures shall be taken to raise the awareness of customers and mass people:

• Each new customer shall receive a handbill/leaflet regarding AML & CFT awareness along with each account opening forms.

• Our bank shall take necessary measures to broadcast awareness building advertisement/content through various media such as television, social media post, billboard, poster etc.

• The branch officials shall provide advices and suggestions when dealing with a customer face to face.

• Branches shall place a poster regarding the AML & CFT awareness in an easily observable place in branch premises.

Chapter 13: Combat Terrorist Financing and Financing Proliferation of Weapons of Mass Destruction.

13.1 Introduction:

Terrorist Financing (TF) and Financing of Proliferation (PF) are so intriguing in nature that individuals and entities involved frequently change their strategy to serve their purpose. This guidance outlines legal provisions in place to combat TF and PF a summary of non-exhaustive steps and best practices to be adopted by bank when dealing with TF and PF threat.

13.2 Terrorist activity:

As per Anti-Terrorism Act, 2009 Offences are described as under. Terrorist activities. - (1) If any person, entity or foreigner

(a) for the purposes of threatening the unity, integration, public security or sovereignty of Bangladesh by creating panic among the public or a section of the public with a view to compelling the Government or any entity or any person to do any act or preventing them from doing any act,–

(i) Kills, causes grievous hurt to, confines or kidnaps any person or attempts to do the same;

(ii) Conspires, abets or instigates any person to kill, injure seriously, confine or kidnap any person; or

(iii) Damages or tries to damage the property of any other person, entity or the Republic; or

(iv) Conspires or abets or instigates to damage the property of any other person, entity or the Republic; or

(v) Uses or keeps in possession any explosive substance, inflammable substance and arms for the purposes of sub-clauses (i), (ii), (iii) or (iv);

(b) With an intent to disrupt security of or to cause damage to the property of any foreign State, commits or attempts to commit or instigates or conspires or abets to commit an offence similar to the offences mentioned in sub-clauses (i), (ii), (iii), (iv) or (v) of clause (a);

(c) With a view to compelling any international organization to do any act or preventing it from doing any act, commits or attempts to commit or instigates or conspires or abets to commit an offence similar to the offences mentioned in sub-clauses (i), (ii), (iii), (iv) or (v) of clause (a);

(d) Knowingly uses or possesses any terrorist property;

(e) Abets, instigates, conspires to do or commits or attempts to commit an offence described in the United Nations conventions included in the Schedule 1 of this Act;

(f) Commits any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an 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 any act; the person, entity or foreigner shall be deemed to have committed the offence of “terrorist activities”;

13.3 Punishment for the offence of Terrorist Activity:

As mentioned in Anti Terrorism Act 2009: If any person or foreigner commits and offence the person shall be punished almost for a term not exceeding 14 years but not less than 04 years and with fine.

Other punishments are-

(a) With death or imprisonment for life and in addition to that a fine may also be imposed;

(b) If the offence is punishable with death, be punished with imprisonment for life or rigorous imprisonment

(c) With imprisonment for life or rigorous imprisonment

(d) With rigorous imprisonment

(e) With imprisonment for life or rigorous imprisonment

(f) With imprisonment for life or rigorous imprisonment

13.4 Terrorist Financing:

As per Ant-Terrorism Act, 2009 –

(1) 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.

(2) 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.

13.5 Punishment for the offence of Terrorist Financing under ATA, 2009:

If any person is convicted of any of the offences the person shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or taka 10(ten) lac, whichever is greater, may be imposed.

13.5.1 If any entity commits the offence of Terrorist Activities and Terrorist Financing, then

(a) Steps may be taken against the entity that a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is greater, may be imposed; and

(b) The head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20 (twenty) lac, whichever is greater, may be imposed unless he 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.

13.6 Other offences as per ATA, 2009:

Supporting any proscribed entity, criminal conspiracy of committing an offence, attempt of committing an offence, aid and abetment of an offence, participating as an accomplice, organizing or directing others; or contributing, instigating terrorist activities, harboring an offender are also punishable offence under this Act.

13.7 Punishment for the offence of violating United Nations Security Council Resolutions as mentioned in Anti Terrorism Act 2009-

a) If any person or entity violates a freezing or attachment order issued under this section, the person or the concerned person of the entity shall be punished with imprisonment for a term not exceeding 04(four) years or with a fine equivalent to twice the value of the property subject to freeze or attachment, or with both.

b) If any reporting agency fails to comply with the directions issued by BFIU under this section, or fails to take immediate freezing action required under this section, the said reporting agency shall be liable to pay a fine, determined and directed by BFIU, not exceeding taka 25 (twenty five) lac but not less than 05 (five) lac or twice the value of the suspected fund, whichever is greater, and Bangladesh Bank may also suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

13.8 Requirements for the Sanction Regime:

Sanctions regimes narrowly require a specific legal base and/or course of actions for the followings:

- Trade embargos;
- Travel bans;
- Freezing of Assets; and
- Economic sanctions.

Trade embargos and freezing of assets are directly related with the Banks. We must ensure that they are not maintaining or continuing business relationship with sanctioned/designated person and not engaged in the trade activities with sanctioned individual, entity or territories. Beneficial ownership issues should be consider very carefully and critically while complying with the sanction regime, as money launderer of sanctioned individual or entities always try to hide them from front person or legal entity.

13.8.1 Mechanisms should be established by bank to comply with the Sanction Regime:

- Put in place a comprehensive policy approved by the Board of Directors;
- Ensure all relevant sanctions lists (updated) are used electronically to detect the existence of the sanctioned individuals, entities, or territories;

• Ensure that existing arrangements of customer screening are able to detect the relevant lists of named terrorist and sanctioned entities.
• Ensure that existing arrangements of customer screening are able to detect the relevant lists of trade embargos;
• Conduct real-time transaction screening on all cross-border payments, SWIFT and other modes of payments in relation to relevant lists of named terrorist and sanctioned entities, or embargos;
• Freeze the accounts and the relevant transaction in relation to relevant lists of named terrorist and sanctioned entities, or embargos immediately;
• Report to the detected incidents to the BFIU without delay;
• Keep records or audit trail for all sorts of monitoring mechanism including the false positives;
• Take necessary training and awareness building arrangements; and
• Review the existing policies with any additional requirements of sanction regime.

13.8.2 As per MLPR Bank should do the followings:

- Maintain and update the listed individuals and entities in electronic form;
- Regularly run a check at the website of United Nations for updated list;
- Run regular check on the given parameters, including transactional review, to verify;
- In case of a match found the ROs shall immediately stop payment or transaction of funds, financial assets or economic resources;
- Report to the BFIU within the next working day with full particulars.

13.8.3 Red Flags pointing to Financing of Terrorism as mentioned in ML & TF Risk:

13.8.3 (a) 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.

13.8.3 (b) 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.

13.9 Elements of Proliferation Financing:

(a) Indicators of possible proliferation financing as mentioned in Annex 1 to the 2008 FATF Typologies Report on Proliferation Financing (with updated order)49

(i) Transaction involves person or entity in foreign country of proliferation concern.

(ii) Transaction involves person or entity in foreign country of diversion concern.

(iii) The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.

(iv) Customer activity does not match business profile, or end-user information does not match end-user's business profile.

(v) A freight forwarding firm is listed as the product's final destination.

(vi) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.

(vii) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).

(viii) Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).

(ix) Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.

(x) Circuitous route of shipment (if available) and/or circuitous route of financial transaction.

(xi) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.

(xii) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.

(xiii) Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).

(xiv) Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.

(xv) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.

(xvi) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.

(xvii) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

(xviii) Customer vague/incomplete on information it provides, resistant to providing additional information when queried.

(xix) New customer requests letter of credit transaction awaiting approval of new account.

(xx) Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.

13.9.1 Additional potential indicators of sanctions evasion activity mentioned in third-party reports:

(i) Involvement of items controlled under WMD export control regimes or national control regimes.

(ii) Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.

(iii) Use of cash or precious metals (e.g. gold) in transactions for industrial items.

(iv) Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.

(v) Involvement of a customer or counter-party, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.

(vi) Transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions.

(vii) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).

(viii) Involvement of a university in a country of proliferation concern. (ix) Description of goods on trade or financial documentation is non-specific, innocuous or misleading.

(x) Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.

(xi) Use of personal account to purchase industrial items.

Annexure A

Annexure A.1

Risk Taxonomies

This section describes the operational definitions and describes control tools and methodologies used

Risk Categories:

Risk can be defined as the combination of the probability of an event and its consequences. In simple term, risks can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur. The major risk criterions of NRBC Bank are separated into two broad categories. The categories and their subcategories are listed as follows:

Business Risk

Business risk is the risk that our business may be used for ML&TF. Our bank shall assess the following risks in particular:

- Customers.
- Product & Services.
- Business Practices/ Delivery Channels.
- Countries in which NRBC Bank operates and/or have correspondence relationship.

Regulatory Risk

Regulatory risk is associated with not meeting all obligations of banks under the Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two acts and instructions issued by BFIU.

Risk Likelihood

The chance of the risk happening is measured in a three point scale in this context. The implication of each level of frequency is given below:

- **Unlikely** The event is unlikely to happen, but not impossible.
- **Likely** High probability the event will happen once a year.
- **Very likely** The event is almost certain to happen in banking context. It will probably occur several times a year.

Impact Scale

An impact scale refers to the severity of the damage (or otherwise) which could occur should the event (risk) happen. Three levels of impacts are categorized in this context. These three risk levels are described as follows:

- **Minor** The risk is likely to cause minor or negligible consequences or effects.
- **Medium** The risk is expected to cause Moderate level of money laundering or terrorism financing impact.
- **Major** The risk is expected to cause huge consequences – major damage or effect, serious terrorist act or large-scale money laundering.

Risk Matrix

To properly manage and mitigate prevailing risks, we need to follow a structured and methodical approach to determine how and when to address the various risk categories. This task can be accomplished by assigning risk scores to the risk categories to determine their severity of damage and likeliness to occur. We combined the risk likelihood and impact scale (discussed in previous sections) to obtain risk matrix shown in the following table:

	Impact		
	Minor	Moderate	major
Very Likely	Medium	High	Extreme
Likely	Low	Medium	High
Unlikely	Low	Low	Medium
Likelihood			

The risk matrix gives us four levels of risk scores (Extreme, High, Medium and Low). The general rule of thumb to address each of the risk scores is described as follows:

- **Extreme** This type of risk is almost sure to happen and/or to have very serious consequences. General treatment is to not allow transaction to occur or reduce the risk to acceptable level.

- **High** This type of risk is likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.

- **Medium** Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.

- **Low** Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

Besides the general treatment, detailed control and mitigation approach is described in Appendix A.2, Which shows the detailed list of possibly risky events, their likelihood, impact and corresponding control measures and mitigation techniques.

Annexure A.2

Risk Register

The following tables enlist risk events according to risk group i.e. Customers, Product & Services, Business Practices/Delivery Channels and Countries in which NRBC Bank operates and/or have correspondence relationship.

Customers:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer	Likely	Moderate	Medium	a) Perform Standard CDD b) Identify the purpose of opening account c) Complete KYC properly d) Check sanction list under UNSCR before opening account Conduct Sanction Screening and adverse media screening. e) Check whether the nature of business and source of fund commensurate with estimated TP furnished by customer
Walk-in customer (beneficiary is government/semi government/autonomous body/ bank & NBFI)	Likely	Minor	Low	a) Obtain the purpose of transaction and source of fund b) Obtain complete and accurate information of applicant c) Complete short KYC
Walk-in customer (beneficiary is other than government/semi government/autonomous body/ bank & NBFI)	Likely	Moderate	Medium	a) Obtain the purpose of transaction and source of fund b) Complete simplified KYC if the transaction amount is below BFIU declared threshold. Else conduct regular KYC. c) Obtain complete and accurate information of applicant and beneficiary
Non-resident customer (Bangladeshi)	Unlikely	Moderate	Low	a) Perform CDD b) Complete KYC of the bank agent/ exchange house who marketed the account c) Follow Foreign Exchange guideline where applicable

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold)	Likely	Major	High	a) Apply CDD b) Obtain documents in support of source of fund c) Cross-check the income with occupation/ nature of business
A customer making series of transactions to the same individual or entity	Likely	Moderate	Medium	a) Generate statement/ report from system and review transactions b) Making sure that Transaction Profiles (TP) provided by the customers are proportionate with their respective professions and sources of funds supported by necessary documents c) Monitoring the on-line transactions exceeding the limits declared in their TPs d) Obtain justification from the customer regarding the transactions
Customer involved in outsourcing business	Unlikely	Moderate	Low	a) Perform CDD b) Keep the transaction under monitoring c) Obtain information about customer's customers (KYCC)
Customer appears to do structuring to avoid reporting threshold	Likely	Major	High	a) Make sure that Transaction Profiles (TP) provided by the customers are proportionate with their respective professions and sources of funds supported by necessary documents b) Generate structuring report and CTR of last three months from system and check & compare the transaction pattern to identify whether structuring occurred c) Obtain justification from the customer regarding transaction otherwise submit STR
Customer appears to have accounts with several financial institutions in the same area	Likely	Major	High	a) Obtain justification from the customer regarding maintenance of several accounts b) Monitor the transaction pattern c) Obtain information about sources of funds transacted d) If the justification is not satisfactory/ source of fund is not clarified, raise STR

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Unlikely	Major	Medium	a) Check the source of fund b) Keep the transactions under monitoring
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	Unlikely	Major	Medium	a) Review customer's KYC b) Keep the transactions under close monitoring c) Keep CCC/ senior management informed about the transaction
Negative news about the customers' activities/ business in media or from other reliable sources	Unlikely	Major	Medium	a) Check the TP and transaction pattern b) Inform CCC/ senior management immediately c) If found suspicious, raise STR d) Keep transactions under monitoring
Customer is secretive and reluctant to meet in person	Unlikely	Major	Medium	a) Visit the customer's place and meet customer in person keep a call report b) Keep the transaction under monitoring c) If found suspicious, raise STR
Customer is a mandate who is operating account on behalf of another person/ company.	Likely	Moderate	Medium	a) Conduct CDD of mandate b) Complete KYC of mandate c) Keep transaction under monitoring
Large deposits in the account of customer with low income	Unlikely	Major	Medium	a) Obtain declaration from customer about the particular large transaction with supporting documents b) If customer fails to provide supporting documents, raise STR.
Often large amount credited in a single account from abroad	Unlikely	Medium	High	a) Perform EDD b) Obtain documents in support of source of fund c) Transaction Monitor
Customers about whom BFIU seeks information (individual)	Unlikely	Major	Medium	a) Update customer information and KYC b) Check whether there is any negative information about the customer in media/ other reliable sources c) Keep their transaction under close

				monitoring

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A customer whose identification is difficult to check	Very Likely	Major	Extreme	a) Verify the identity of the customer (CPV) through third party b) If not satisfied, do not open account. In case of existing account, close account with prior notice to customer
Significant and unexplained geographic distance between the bank and the location of the customer	Likely	Major	High	a) Complete CDD b) Obtain justification from customer regarding the purpose of opening account c) Keep transactions (especially on-line) under monitoring
Customer is a foreigner	Likely	Major	High	a) Apply Enhanced Due Diligence b) Obtain reason for opening account in Bangladesh c) Follow foreign exchange guideline and circulars of FEPD
Customer is a minor	Likely	Moderate	Medium	a) Perform CDD for minor, guardian and beneficial owner (BO). b) Birth certificate should be obtained as identity proof c) Obtain source of fund with supporting document
Customer is Housewife	Likely	Moderate	Medium	a) Perform CDD for both customer and beneficial owner b) Obtain purpose of opening account c) Obtain source of fund with supporting documents
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	Very Likely	Major	Extreme	a) Conduct Enhanced Due Diligence b) Obtain approval from CCC before establishing relationship c) Keep transaction under monitoring d) Follow foreign exchange guideline and FEPD circulars e) Check whether the source of fund commensurate with the designation

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Very Likely	Major	Extreme	a) Identify beneficial owner(s) of the account and obtain their complete & accurate information b) Obtain documents in support of source of fund c) Monitor the transactions
Customers doing significant volume of transactions with higher-risk geographic locations.	Likely	Major	High	a) Generate report on on-line transaction from system and review transactions b) Make sure that Transaction Profiles (TP) provided by the customer commensurate with the profession and source(s) of fund supported by necessary documents c) Obtain written justification supported by documents (if any) from the customer regarding the transactions
A customer who brings in large amounts of used notes and/or small denominations	Likely	Moderate	Medium	a) Check whether the nature of business justifies the condition and small denominations of notes b) Obtain written justification from the customer regarding the condition and small denominations of notes c) Update KYC of the customer (if necessary)
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)	Unlikely	Major	Medium	a) Identify the source of fund with supporting document b) Obtain information about the customer's business (KYCB) and customer's customer (KYCC) c) Obtain the membership certificate issued from relevant trade body (i.e. membership of REHAB for real estate, Jewellery Association in case of jewellery business)
Customer is a money changer/courier service agent/travel agent	Likely	Moderate	Medium	a) Identify the source of fund with supporting documents b) Obtain information about the customer from available sources e.g. media, peer group c) Obtain license issued from competent authority

				d) Keep transactions under monitoring e) Follow foreign exchange guideline and FEPD circulars (if applicable)

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
Customer is outsourcing business	Very Likely	Moderate	High	a) Perform CDD b) Keep the transaction under monitoring c) Obtain information about customer's customers (KYCC) d) Identify the source of fund with supporting document
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Likely	Major	High	a) Perform CDD b) Identify the source of fund with supporting documents c) Obtain information about the customer from public media/ reliable source etc. d) Check certification or membership from concerned authority e) Keep transactions under monitoring
Customer is involved in Manpower Export Business	Likely	Major	High	a) Identify the source of fund with supporting document b) Obtain information about the customer from public media/ reliable source and screen against UNSCR sanction list c) Check license issued by Ministry of Expatriates' Welfare and Overseas Employment and membership certificate by BAIRA d) Keep the transactions under monitoring
Privilege Customer				
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold)	Likely	Major	High	a) Apply EDD b) Obtain documents in support of source of fund c) Cross-check the income with occupation/ nature of business

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Privilege Customer				
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	Very Likely	Major	Extreme	a) Conduct Enhanced Due Diligence b) Obtain approval from CCC before establishing relationship c) Keep transaction under monitoring d) Follow foreign exchange guideline and FEPD circulars e) Check whether the source of fund commensurate with the designation
Customer opens account in the name of his/her family member who intends to credit large amount of deposits	Unlikely	Major	Medium	a) Identify beneficial owner(s) of the account and obtain their complete & accurate information b) Obtain documents in support of source of fund c) Monitor the transactions
SME Banking Customers				
Customers with complex accounting and huge transaction Receipt of donor fund, fund from foreign source (MFI)	Likely	Moderate	Medium	a) Obtain documents in support of income and accounting (i.e. balance sheet, sales register etc.) b) Monitor transactions and check whether it commensurate with source of fund
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	Likely	Moderate	Medium	a) Complete KYC of the customer b) Obtain written declaration whether the customer follows MLP Act 2012 and respective guideline as a reporting organization
Wholesale Banking Customer				
Entity customer having operations in multiple locations	Likely	Minor	Low	a) Obtain justification from customer regarding operations in various locations b) Analyze the annual report/ balance sheet c) Keep transactions (especially on-line transactions) under monitoring
Customers about whom BFIU seeks information (large	Likely	Moderate	Medium	a) Update customer information and KYC b) Check whether there is any negative information about the customer in media/ other

corporate)				reliable sources c) Keep their transaction under close monitoring

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Wholesale Banking Customer				
Owner of the entity that are Influential Persons (IPs) and their family members and close associates	Likely	Moderate	Medium	a) Conduct Enhanced Due Diligence b) Obtain approval from CCC before establishing relationship c) Keep transaction under monitoring d) Check whether the source of fund commensurate with the designation/ profession
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	Likely	Major	High	a) Perform CDD by obtaining necessary documents in support of identity apart from Trade License, Partnership Deed, Memorandum of Association, Articles of Association, Certificate of Incorporation, Board Resolution, Form XII, by laws and source(s) of fund. b) Identify the beneficial owner and obtain complete & accurate information of beneficial owner c) Check whether TP of customer commensurate with the nature of business and transaction pattern. d) Check cash flow statement (audited/unaudited), sales register and previous bank statement e) Visit the client's business premises, prepare call report and visit web-site
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Likely	Moderate	Medium	a) Generate statement/ report from system and review transactions b) Making sure that Transaction Profiles (TP) provided by the customer is proportionate with the nature of business and sources of funds supported by necessary documents c) Monitoring the on-line transactions exceeding the limits declared in the TP d) Obtain justification from the customer regarding the transactions e) Obtain the purpose of transaction

A customer whose identification is difficult to check.	Likely	Moderate	Medium	a) Verify the identity of the customer (CPV) through third party or physical verification by bank official with call report b) If not satisfied, do not open account. In case of existing account, close account with prior notice to customer c) Obtain information about the customer from public media or other reliable sources or peer group

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Wholesale Banking Customer				
Owner of the entity that are Politically Exposed Persons (PEPs) or chief /senior officials of International Organizations and their family members and close associates	Likely	Major	High	a) Conduct Enhanced Due Diligence b) Obtain approval from CCC before establishing relationship c) Keep transaction under monitoring d) Follow foreign exchange guideline and FEPD circulars e) Check whether the source of fund commensurate with the designation
Charities or NPOs (especially operating in less privileged areas).	Likely	Moderate	Medium	a) Perform CDD b) Identify beneficial owner of the account c) Obtain documents in support of source of fund d) Obtain the permission/ license received by customer from competent authority e) Obtain information about the customer from media, peer group and other reliable sources f) Keep transactions under monitoring
Credit Card Customer				
Customer who changes static data frequently	Unlikely	Major	Medium	a) Address & contact number verification (CPV) through third party b) Obtain documents in support of changed information c) Customer acknowledgement obtain by sending letter to old and new addresses d) Keep transactions under monitoring

Credit Card customer	Likely	Moderate	Medium	a) Collect required documents as per Product Program Guideline (PPG) and bank's policy b) Complete KYC c) Collect & check CIB report d) Address & contact number verification (CPV) through third party e) UNSCR sanction list check f) Check whether customer is already availing credit card g) Keep transactions under monitoring

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Credit Card Customer				
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	Likely	Moderate	Medium	a) Compare transactions with customer's income b) Keep transactions under monitoring c) If suspicious, raise STR
Prepaid Card customer	Very Likely	Minor	Medium	a) Collect required documents as per Product Program Guideline (PPG) and bank's policy b) Complete KYC c) Collect & check CIB report d) Address & contact number verification. e) UNSCR sanction list check f) Check whether customer is already availing card g) Keep transactions under monitoring
International Trade Customer				
A new customer (Outward remittance-through SWIFT)	Likely	Minor	Low	a) Perform CDD b) Perform UNSCR sanction screening c) Ensure the purpose of the remittance with supporting documents d) Follow foreign exchange guideline and FEPD circulars
A new customer	Likely	Moderate	Medium	a) Conduct CDD

(Import/ Export)				b) In case of old customer of other bank obtain certificate from previous bank on " no overdue or outstanding bill of entry" c) In case of new customer: confirm that respective IRC issued mentioning d) Follow foreign exchange guideline and FEPD circulars

Risk	Likelihood	Impact	Risk Score	Treatment/Action
International Trade Customer				
A new customer (Inward remittance-through SWIFT)	Likely	Minor	Low	a) Perform CDD of the beneficiary b) Obtain C form where applicable c) Perform UNSCR sanction screening d) Ensure the purpose of the remittance with supporting documents e) Follow foreign exchange guideline and FEPD circulars
A new customer who wants to carry out a large transaction (Import/ Export)	Likely	Moderate	Medium	a) Conduct CDD b) Old customer of other bank: obtain certificate from previous bank on " no overdue or outstanding bill of entry" c) New Customer: confirm that respective IRC issued mentioning d) Follow foreign exchange guideline and FEPD circulars
A new customer who wants to carry out a large transaction (Inward/outward remittance)	Likely	Moderate	Medium	a) Perform CDD b) Check whether the transaction pattern matches with the nature of business c) Follow foreign exchange guideline and FEPD circulars
A customer wants to conduct business beyond its line of business (import/ export/ remittance)	Unlikely	Moderate	Low	a) Perform CDD b) Check the business diversification c) Obtain justification from the customer regarding diversification of business
Owner/director/shareholder of the customer is influential person(s) or their family members or	Likely	Major	High	a) Conduct Enhanced Due Diligence b) Obtain approval from CCC before establishing relationship

close associates				c) Keep transaction under monitoring d) Check whether the source of fund commensurate with the designation/ position

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Correspondent Banks	Likely	Minor	Low	a) Follow BFIU Circular No. 26 while establishing relationship b) Gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. c) Ascertain publicly available information d) Review KYC periodically
Money services businesses (remittance houses, exchange houses)	Likely	Moderate	Medium	a) Follow BFIU Circular No. 26 while establishing relationship b) Gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. c) Ascertain publicly available information d) Review KYC periodically

Product and services:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)	Unlikely	Major	Medium	a) Perform CDD for student, guardian (if minor) and beneficial owner (BO). Birth certificate should be obtained as identity proof (for minor) b) Obtain documents in support of source of fund c) Obtain justification from the customer regarding large transactions d) Make sure that Transaction Profile (TP) provided by the customer commensurate with the sources of fund
Foreign currency endorsement in Passport	Likely	Minor	Low	a) Endorse as per foreign exchange guideline and FEPD circulars b) Complete TM form

Large transaction in the account of under privileged people	Unlikely	Moderate	Low	a) Conduct CDD b) Obtain documents in support of source of fund c) Obtain justification from customer regarding the purpose of transaction
FDR (less than 2 million)	Likely	Minor	Low	a) Perform CDD b) Obtain documents in support of source of fund
FDR (2 million and above)	Likely	Moderate	Medium	a) Perform CDD b) Check whether the customer is maintaining multiple FDRs with ….. c) Obtain documents in support of source of fund. If source of fund is not justified, raise STR.
Special scheme deposit accounts opened with big installment and small tenure	Likely	Moderate	Medium	a) Obtain document in support of source of fund b) Complete short KYC c) Check other relationship of the customer with bank

Risk	**Likelihood**	**Impact**	**Risk Score**	**Treatment/Action**
Retail Banking Product				
Loan	Likely	Moderate	Medium	a) Obtain accurate and complete information of the customer b) Arrange face to face interview with loan customer c) Record the purpose of loan d) Verify information obtained from other financial institutions e) Obtain corroboration of information in employer letters, references, pay slips or credit card(s)
Multiple deposit scheme accounts opened by same customer in a branch	Likely	Moderate	Medium	a) Obtain document in support of source of fund b) Complete short KYC
Multiple deposit scheme accounts opened by same customer from different	Likely	Major	High	a) Obtain document in support of source of fund b) Obtain written justification from the

location				customer regarding opening scheme deposit in multiple location c) Complete short KYC d) Checking other relationship of the customer with bank e) Monitor on-line transactions f) Checking whether there is frequent transfer of funds between the accounts.
Open DPS in the name of a family member Or Installments paid from a account other than the customer's account	Very Likely	Moderate	High	a) Identify beneficial owner and obtain complete & accurate information b) Obtain written justification from the customer regarding the purpose of opening deposit scheme in the name of family member c) Checking other relationship of the customer with bank and keep the transaction under monitoring.
Stand alone DPS	Very Likely	Minor	Medium	a) Perform CDD of customer b) Obtain document in support of source of fund

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Early encashment of FDR, special scheme etc.	Very Likely	Minor	Medium	a) Obtain declaration of specific reason of early encashment
Retail Privilege Facilities				
Pre-Approved Credit Card with BDT 300K limit.	Unlikely	Minor	Low	a) Perform CDD b) Obtain document in support of source of fund
Enhanced ATM cash withdrawal Limit BDT 100K	Unlikely	Minor	Low	a) Obtain document in support of source of fund b) Complete KYC c) Obtain written justification from the customer regarding the purpose of requesting high withdrawal limit from ATM.
Islamic Banking Product				
Want to open Mudaraba Term Deposit account where the source of fund is not clear	Likely	Moderate	Medium	a) Perform CDD b) Obtain document in support of source of fund, if not satisfied do not open FDR

Early encashment of MTDR	Likely	Minor	Low	a) Obtain declaration of specific reason of early encashment
Multiple Mudaraba deposit accounts opened by different persons who are inter-linked	Unlikely	Medium	High	a) Identify beneficial owner and obtain complete & accurate information b) Obtain written justification from the customer regarding the purpose of opening deposit scheme c) Checking other relationship of the customer with bank and keep the transaction under monitoring.
Often large amount credited in a single account from abroad	Unlikely	Medium	High	a) Perform EDD b) Obtain documents in support of source of fund c) Transaction Monitor
Frequent inward remittance in account without any proper source (e.g. wages)	Unlikely	Medium	Low	a) Perform EDD b) Obtain documents in support of source of fund of remitter c) Monitor Transactions

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Fund transfer to in small chunks to accounts in banks/ branches located in border area	Unlikely	Moderate		a) Perform EDD b) Collect Source of Fund c) Understand the end use of Fund
SME Banking Product				
Want to open FDR where source of fund is not clear	Likely	Moderate	Medium	a) Obtain document in support of source of fund, if not satisfied, do not open FDR b) Perform CDD
Early encashment of FDR	Likely	Minor	Low	a) Obtain declaration of specific reason of early encashment
Repayment of loan EMI from source that is not clear	Likely	Moderate	Medium	a) Monitor transaction and check whether it commensurate with source of fund b) Obtain source of fund of repayment
Repayment of full loan amount before maturity	Likely	Moderate	Medium	a) Ensure source of fund of repayment before early adjustment of loan b) Obtain the reason behind early adjustment in writing
Loan amount utilized in	Likely	Major	High	a) Monitor the utilization of loan

sector other than the sector specified during availing the loan				b) If found suspicious, raise STR
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	Unlikely	Major	Medium	a) Ensure source of fund of repayment b) If found suspicious, raise STR
Source of fund used as security not clear at the time of availing loan	Likely	Moderate	Medium	a) Ensure source of fund of FDR keeping as security before sanctioning loan
Micro Credit Banking Product				
Repayment of loan/ investment before maturity	Unlikely	Moderate	Low	a) Perform EDD b) Obtain document in support of source of fund c) If found suspicious, raise STR

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Micro Credit Banking Product				
If the amount is used for other purpose apart from usual cause	Likely	Moderate	Medium	a) Perform EDD b) Monitor c) Understand the end use of Fund
Related parties applying for loans frequently	Unlikely	Moderate	Medium	a) Perform EDD b) Understand the end use of Fund c) Raise STR if necessary
Wholesale Banking Product				
Development of new product & service of	Likely	Moderate	Medium	a) Identify ML & TF risk of the product, assess the risk and devise action plan to treat the risk b) Obtain (by the concerned department) vetting from CCC
Payment received from unrelated third parties	Likely	Moderate	Medium	a) Receive payment only from the distributors, agents and suppliers of the customer b) Obtain information about the relationship of the parties c) Complete short KYC of depositor/withdrawer d) Monitor the transaction report regularly

High Value FDR	Very Likely	Moderate	High	a) Perform CDD b) Obtain documents in support of source of fund
Term loan, SOD(FO), SOD(work order), SOD(PO), Loan General, Lease finance, Packing Credit, BTB L/C	Very Likely	Moderate	High	a) Perform CDD b) Prepare comprehensive credit memo and analyze customer's creditworthiness c) Visit customer's office, factory and mortgaged properties d) Monitor end use of fund
BG (bid bond), BG (PG), BG (APG)	Likely	Moderate	Medium	a) Perform CDD b) Verify the work order from concerned authority c) Ensure assignment of bill from concerned authority d) Obtain margin e) Obtain sufficient collateral

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Micro Credit Banking Product				
L/C subsequent term loan, DP L/C	Very Likely	Major	Extreme	a) Ensure proper verification of the price of the imported items from market b) Obtain certificate from the respective country's chamber of commerce c) Obtain undertaking from the customer regarding the fair price.
C.C (H)	Very Likely	Moderate	High	a) Keep transactions under monitoring b) Ensure physical verification of sales register and stock report c) Verify the creditworthiness of the customer d) Verify other sources of income
Syndication Financing	Likely	Moderate	Medium	a) Perform EDD b) Verify the value of plant & machinery and imported items c) Obtain certificate from the respective

				chamber of commerce d) Take undertaking from the customer regarding the price
Credit Card				
Supplementary Credit Card Issue	Likely	Minor	Low	a) Collect required documents as per bank's policy b) Collect relationship of supplementary cardholder with customer c) Complete KYC d) Collect & check CIB report e) UNSCR sanction list check f) Check whether customer is already availing credit card g) Keep transactions under monitoring
Frequent use of Card Cheque	Likely	Minor	Low	a) Obtain the purpose of transaction b) Obtain relationship with the account holder, the account where the fund is transferred c) Keep transactions under monitoring

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Credit Card				
BFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)	Likely	Moderate	Medium	a) Allow the facility only to renowned and selected merchants b) Conduct CDD
Credit card issuance against ERQ and RFCD accounts	Likely	Minor	Low	a) Collect required documents as per bank's policy b) Collect relationship of supplementary cardholder with customer c) Complete KYC d) Collect & check CIB report e) UNSCR sanction list check f) Check whether customer is already availing credit card g) Ensure that transactions are conducted as per Foreign Exchange guideline and FEPD circulars

International Trade				
Line of business mismatch import/export/remittance)	Unlikely	Moderate	Low	a) Check the business diversification b) Perform EDD c) If found suspicious, raise STR
Under/Over invoicing (import/export/remittance)	Likely	Major	High	a) Check the unit price of the product intended for import and export with the present market price b) Perform EDD c) If found suspicious, raise STR
Retirement of import bills in cash (import/export/remittance)	Likely	Minor	Low	a) Check the size of the transaction with customer's cash flow b) Perform EDD
Wire transfer	Unlikely	Minor	Low	a) Obtain information of applicant and beneficiary as per BFIU Circular No. 26
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)	Likely	Moderate	Medium	a) Confirm the purpose of remittance with supporting documents b) Obtain information of applicant and beneficiary as per BFIU Circular No. 26 c) If found suspicious, raise STR

Business practices/delivery methods or channels

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Online (multiple small transaction through different branch)	Likely	Moderate	Medium	a) Obtain KYC of bearer as per BFIU Circular No. 10 b) Generate report on on-line transaction and monitor c) Obtain justification from customer regarding the transaction pattern, if not satisfied, raise STR
BEFTN	Likely	Minor	Low	a) Obtain relationship with customer & beneficiary and purpose of fund transfer b) Ensure that customer executes transaction as per agreement c) Monitor transaction pattern, update TP and keep track of deposit volume
IDBP	Very Likely	Moderate	High	a) Check the genuineness of the LC and acceptance from BB dashboard.

				b) Perform CDD
Credit Card				
New Merchant sign up	Likely	Moderate	Medium	a) Collect all documents as per PPG and bank's policy b) Complete Merchant KYC and visit merchant physically and conduct feasibility analysis
High volume transaction through POS	Likely	Major	High	a) Check merchant product & price and match with POS transactions b) Check Transaction Profile of merchant c) Obtain justification from merchant regarding any unusual transaction
Alternate Delivery Channel				
Transaction amount exceeding BDT 100,000 for Simplified E-KYC	Likely	Medium	High	a) Conduct CDD as per BFIU Circular No. 26 before conducting transactions b) Monitor Transaction c) Obtain source of fund

Risk	Likelihood	Impact	Risk Score	Treatment/Action
In case of Regular E-KYC, Transaction not with TP	Likely	Moderate	Medium	a) Conduct CDD as per BFIU Circular No. 26 b) Generate report on on-line transaction and monitor c) Obtain justification from customer regarding the transaction pattern, if not satisfied, raise STR
Multiple demand deposit opened in self mode by same customer	Unlikely	Medium		a) Perform EDD b) Monitor Transactions
Customer on-boarded through self on-boarding is requesting to increase transaction limit, however reluctant to visit branch	Likely	Moderate		a) Perform CDD b) Collect additional information using other available channels.
Large amount withdrawn/ Frequent withdrawal from ATMs	Likely	Major	High	a) Generate report on high value ATM transactions from the system and monitor the transactions b) Apply transaction restriction policy (transaction limit)

				c) Inform issuer bank if possible d) Follow Central Bank and International Payment Association ML rules e) Inform the cards payment Association (ie Visa, Master Card).
Larger amount transaction from different location and different time(mid night) through ATM	Likely	Major	High	a) Generate report on high value ATM transactions along with time from the system and monitor the transactions, if any irregularities found, inform relevant branch or department b) Obtain justification from the customer regarding the timing of transaction c) If found suspicious, raise STR
Large amount of cash deposit in CDM	Likely	Moderate	Medium	a) Branch to ask the customer about the authenticity of the deposit before giving input in CBS b) Keep transactions under monitoring

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Huge fund transfer through internet	Unlikely	Major	Medium	a) Ensure dual registration (both online and branch) at the time of taking internet banking facility b) Apply transaction restriction policy (transaction limit in terms of number and amount, session time limit) c) Generate report on high value transactions through internet from the system and monitor the transactions d) Communicate (IB administrator) with customer if customer transaction reaches the highest level every time
Transaction Profile updated through Internet Banking	Unlikely	Moderate	Low	a) Ensure dual registration (both online and branch) at the time of taking internet banking facility b) Check customer transaction profile on monthly basis c) Ensure that TP update request is received only from registered e-mail address d) Share the updated TP with concerned branch and branch will update the TP in CBS after proper verification

Customer to business transaction-Online Payment Gateway – Internet Banking	Likely	Moderate	Medium	a) Allow transaction with business houses that are listed under payment processors (e-commerce merchant) approved by Bangladesh Bank only b) Arrange AML & CFT training for payment processors and obtain KYC of business houses c) Conduct Enhanced Due Diligence
International Trade				
Customer sending remittance hrough SWIFT under single customer credit transfer (fin-103)	Likely	Minor	Low	a) Check whether the transaction meets the central Bank guide line/ circular. b) Obtain purpose of the remittance from the customer (documents if required). c) Obtain information as per BFIU Circular No. 26 d) UNSCR sanction list screening for all the parties involved in the transaction

Risk	Likelihood	Impact	Risk Score	Treatment/Action
International Trade				
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103)	Likely	Moderate	Medium	a) Take C form (if necessary) before release of remittance b) Obtain any other document as and when required.

.

Country/jurisdiction

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Import and export form/to sanction country	Likely	Major	High	a) Perform sanction screening b) Inform CCC immediately c) Have procedure in place to treat such situation
Transshipments, container, flag vessel etc. under global sanction	Likely	Moderate	Medium	a) Perform sanction screening b) Inform CCC immediately c) Have procedure in place to treat such situation
Establishing	Unlikely	Moderate	Medium	a) Perform sanction screening

correspondent relationship with sanction bank and/or country				b) Inform CCC immediately c) Have procedure in place to treat such situation d) Perform EDD
Establishing correspondent relationship with poor AML practice country	Likely	Major	High	a) Obtain KYC from the correspondent bank b) Ensure the specific purpose for establishing correspondent relationship c) Perform EDD
Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas	Likely	Major	High	a) Obtain KYC from the correspondent bank b) Ensure the specific purpose for establishing correspondent relationship c) Perform EDD

Risk	Likelihood	Impact	Risk Score	Treatment/Action
International Trade				
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.	Likely	Major	High	a) Obtain KYC from the correspondent bank b) Ensure the specific purpose for establishing correspondent relationship c) Perform EDD
Customer belongs to High Risk ranking countries of the Basel AML index.	Unlikely	Major	Medium	a) Obtain KYC from the entity/ bank b) Ensure the specific purpose for establishing relationship c) Perform EDD
Customer belongs to the countries identified by the bank as higher-risk because of its prior experiences or other factors.	Likely	Moderate	Medium	a) Perform EDD b) Ensure the specific purpose for transaction

3.3.2.2.1 Regulatory risk : Regulatory risk is associated with not meeting all obligations of banks under the Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two acts and instructions issued by BFIU. Following are some of ML&TF risk the bank may face in terms of non compliance of regulations and the possible ways to reduce and manage those risks.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML/CFT guideline.	Unlikely	Major	Medium	a) Develop bank's own AML/CFT guideline b) Update the guideline from time to time
Not forming a Central Compliance Committee (CCC)	Unlikely	Moderate	Low	a) Incorporate formation and TOR of CCC in guideline b) Constitution CCC as per the requirement of BFIU
Not having Branch Anti Money Laundering Compliance Officer	Unlikely	Major	Medium	Nominate and devise TOR for Branch Anti Money Laundering Compliance Officer (BAMLCO) as per BFIU instruction.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having an AML&CFT program	Unlikely	Major	Medium	Develop AML&CFT program and review from time to time
No senior management commitment to comply with MLP and ATA	Unlikely	Major	Medium	a) Provision of commitment of senior management to be included in the AML & CFT policy guideline b) Communicate the senior management commitment with all bank officials at least on yearly basis
Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	Unlikely	Major	Medium	Follow the AMLD/BFIU circular, circular letter, instructions issued from time to time
Unique account opening form not followed while opening account	Likely	Minor	Low	Develop/ revise account opening form for the bank in line with the unique account opening form prescribed by BFIU
Non screening of new and existing customers against UNSCR Sanction and OFAC lists	Likely	Major	High	Ensure that business units screen all new and existing customers against UNSCR Sanction lists
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Unlikely	Major	Medium	Ensure that bank follows the Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts
Complete and accurate information of customer not obtained	Likely	Moderate	Medium	a) Obtain complete and accurate information of customer as per BFIU Circular No. 26 b) Develop control mechanism to check whether business units are collecting complete

				and accurate information of customer and review & update the same from time to time c) If fails, close the account with prior notice to customer
Failure to verify the identity proof document and address of the customer	Likely	Moderate	Medium	a) Verify (business unit) the identity proof document and address of the customer b) Develop control mechanism to check whether business units are • Verify the identity proof document with the support of database from concerned authority • Verify address by sending thanks letter or conduct CPV or physical verification by bank official and receive, record supporting document with AOF

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Beneficial owner identification and verification not done properly	Unlikely	Moderate	Low	a) Identify beneficial owner and obtain information as per BFIU Circular No. 10 b) Check whether business units identify beneficial owner of the account and obtain complete and accurate information of them
Customer Due Diligence (CDD) not practiced properly	Unlikely	Moderate	Low	a) Perform CDD as per BFIU Circular No. 26 b) Develop control mechanism to check whether business units are performing Conduct Customer Due Diligence (CDD) as per BFIU instruction
Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPS and influential person and senior official of international organization.)	Unlikely	Major	Medium	a) Perform EDD for high risk customers without fail b) Check whether business units are obtaining Senior Management approval before opening such account c) Check whether business units are conducting both CDD & EDD for high risk customers as per BFIU instruction
Failure to complete KYC of customer including walk in customer	Unlikely	Moderate	Low	a) Complete KYC of customer including walk-in customer as per BFIU Circular No. 26
Failure to update TP and KYC of customer	Likely	Moderate	Medium	a) Update TP & KYC as per BFIU Circular No. 26 b) Develop control mechanism to check whether business units are updating TP &

				KYC as per the instruction of BFIU
Keep the legacy accounts operative without completing KYC	Unlikely	Moderate	Low	a) Update KYC of legacy account else keeping those as dormant b) Ensure off-site monitoring of legacy account from CCC
Failure to assess the ML & TF risk of a product or service before launching	Unlikely	Moderate	Low	a) Assess the ML & TF risk of a product or service, devise action plan to manage the same before launching the product or service b) Check whether all the PPGs approved by CCC before launching
Failure to complete the KYC of Correspondent Bank	Unlikely	Moderate	Low	a) Complete the KYC of Correspondent Bank reciprocally b) Obtain updated KYC of Correspondent Bank from time to time

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Senior Management approval not obtained before entering into a Correspondent Banking relationship	Unlikely	Moderate	Low	Obtain Senior Management approval before entering into a Correspondent Banking relationship
Failure to keep record properly	Unlikely	Major	Medium	a) Keep records as per BFIU instruction b) Check compliance status during audit/inspection
Failure to report complete and accurate CTR on time	Unlikely	Moderate	Low	a) Rectify the limitation of information in CBS b) Ensure uniformity of CTR submitted through goAML web and CD media (FIU software) c) Submit complete and accurate CTR on time
Failure to review CTR	Unlikely	Moderate	Low	a) Generate CTR from system b) Monitor the transactions reported in CTR by both branch & CCC on monthly basis and identify whether there is any suspicious transaction
Failure to identify and monitor structuring	Unlikely	Moderate	Low	a) Generate structuring report from system b) Identify and monitor structuring on monthly basis
Failure to provide sufficient controls and monitoring systems for the timely detection and	Unlikely	Major	Medium	a) Devise system to generate report that facilitate identifying STR b) Generate high value transaction report, TP

reporting of suspicious activity				exceed report, structuring report from the system to analyze and detect STR
Failure to conduct quarterly meeting properly	Unlikely	Minor	Low	a) Conduct quarterly meeting at branch in line with the agenda and instruction of BFIU Circular No. 26 b) Send the meeting minutes to CCC
Failure to report suspicious transactions (STR)	Unlikely	Major	Medium	a) Monitor account transaction and customer activity and report when find suspicious b) Monitor the transactions reported in CTR by both branch & CCC on monthly basis and identify whether there is any suspicious transaction

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Failure to conduct self assessment properly	Unlikely	Moderate	Low	a) Conduct self assessment properly b) Portray the actual strength, weakness and position of the branch in self assessment c) Cross check (CCC) the self assessment report with independent testing report and inspection report.
Failure to submit statement/ report to BFIU on time	Unlikely	Moderate	Low	a) Submit statement/report to BFIU timely b) Check submission status during audit/inspection
Submit erroneous statement/ report to BFIU	Unlikely	Moderate	Low	a) Check minutely the statements before submitting the same to BFIU
Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Unlikely	Major	Medium	a) Comply with the order for freezing or suspension of transaction issued by BFIU or BB instantly b) Check the compliance of freezing order by CCC
Not submitting accurate information or statement sought by BFIU or BB.	Unlikely	Major	Medium	Provide accurate information to BFIU on time
Not submitting required report to senior management regularly	Unlikely	Moderate	Low	Submit all the report to Senior Management timely
Failure to rectify the objections raised by BFIU or inspection	Unlikely	Moderate	Low	a) Regularize the objections raised by BFIU or inspection teams on time and submit

teams on time				compliance report b) CCC to follow up to rectify or regularize the irregularities
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Unlikely	Minor	Low	Comply with the responsibilities of ordering, intermediary and beneficiary bank as per BFIU instruction
Failure to scrutinize staff properly	Unlikely	Moderate	Low	a) HR to screen the applicant's details before recruitment b) Conduct reference check
Failure to circulate BFIU guidelines and circulars to branches	Unlikely	Moderate	Low	a) Update the branches on circulars/circular letters/ instructions received from BFIU b) Issue instruction circulars as required

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Inadequate training/ workshop arranged on AML & CFT	Unlikely	Moderate	Low	a) Arrange workshop on MLP & CFT for employees to build up awareness and conduct evaluation test b) Check whether all the employees of the bank has received training on AML & CFT c) Keep MIS on training
No independent audit function to test the AML program	Unlikely	Major	Medium	ICC to test the AML program and conduct independent testing procedure.

Annexure B

Annexure B.1

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 the HOB may feel necessary. 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. That certificate must include a photo which is duly attested by the signing renowned person. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.	• Salary Certificate (for salaried person). • Employed ID (for ascertaining level of employment). • Self declaration acceptable to the bank. (commensurate with declared occupation) • Documents in support of beneficial owner's income (income of house wife, students etc.) • Trade License if the customer declared to be a business person • TIN (if any) • Documents of property sale. (if any) • Other Bank statement (if any) • Document of FDR encashment (if any) • Document of foreign remittance (if any fund comes from outside the country) • Document of retirement benefit. • Bank loan.	• Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency.

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

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
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 commerce, market association, trade association i.e.; hardware, cloth merchant, hawker's association etc.	• Trade License. • TIN • Self declaration acceptable to the bank. (commensurate with declared occupation). • 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. • Personal borrowings (if any)	• Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency.

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
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 commerce, market association, trade association i.e.; hardware, cloth merchant, hawker's association etc. • Any other documents that is satisfactory to the bank.	• Trade License. • TIN • Self declaration acceptable to the bank. (commensurate with declared occupation) • 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. • Personal borrowings (if any)	• Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Third party verification report. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name. • Residential address appearing on an official document prepared by a Government Agency.

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

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
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 company's business • Expected monthly turnover Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee, officer or director of the company.	• A copy of last available financial statements duly certified by a professional accountant • Other Bank statement (if any) • Trade License • TIN • Cash flow statement • VAT registration • Bank loan • Any other genuine source	
Government-Owned entities	• Statue of formation of the entity • Resolution of the board to open an account and identification of those who have authority to operate the account. • Passport of the operator (s) • National ID Card of the operator (s)		

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
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 Grand	
Charities or Religious Organizations	• National Id Card of the operator (s) • Passport of the operator (s) • Resolution of the Executive • Committee to open an account and identification of those who have authority to operate the account. • Documents of nature of the organizations • 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	

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
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 organizations • 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 (if registered) • Other Bank statement •Certificate of Grant/ Aid/ subscription. • If unregistered declaration of authorized person/body.	
Trusts, Foundations or similar entities	• National Id Card of the trustee(s) Passport of the trustee (s) • Resolution of the Managing body of the Foundation/Association to open an account and identification of those who have authority to operate the account. • Certified true copy of the Trust • Deed • Bye-laws (certified) • Power of attorney allowing transaction in the account.	• A copy of last available financial statements duly certified by a professional (if registered) • Other Bank statement • Donation	

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Financial Institutions (NBFI)	• Passport of all the directors • National Id Card of all the directors • Certificate of incorporation • Memorandum and Articles of association • Certificate of commencement of business • List of directors in FORM -XII • Resolution of the board of directors to open an account and identification of those who have authority to operate the account. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Nature of the company's business • Expected monthly turnover identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee, officer or director of the company	• A copy of last available financial statements duly certified by a professional accountant. • Other Bank statement • Trade License • TIN • VAT registration • Cash flow statement	
Embassies	• Valid Passport with visa of the authorized official • Clearance of the foreign ministry • Other relevant documents in support of opening account		

Annexure B.2

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 thecommodity'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 C.1

Customer Information

1. Basic Information	
1.1 Name of Customer/ Organization	:
1.2 New trade Customer (First Trade Service)	: [ ] Yes [ ] No
1.3 Nature of Ownership	[ ] Individual [ ] Proprietorship [ ] Partnership [ ] Limited Company [ ] Co-operative Society [ ] Other:
1.4 Account number	:
1.5 Branch	:
1.6 Unique Customer Identification Customer Code (Org/Individual)	:
1.7 IRC No.	
1.8 ERC No.	
1.9 BEPZA/EZ permission no:	
1.10 BIN No.	
1.11 Vat reg. No.	
1.12 TIN	
2. Business Details	
2.1 Nature of Business:	
2.2 Major Goods/ Services (Add extra page if necessary):	
Sl. Product/Service Name HS Code (If applicable)	
2.3 Production/ Service Capacity:	
2.4 End use of Goods:	
2.5 Main Jurisdictions Customer Deals with:	
2.6 Is any of jurisdictions mentioned in 2.5 in high risk or monitored or sanction listed?: [ ] Yes [ ] No Remarks:	

2.7 Usual delivery / transportation mode for goods or services:

2.8 List of Major suppliers /buyers/ Counterparties (attach pages if necessary):

Sl.	**Name of Supplier/ Buyer/ Counterparty**	**Country/ Jurisdiction**

2.9 Is any of the supplier/ buyer/ counterparty located in High Risk or Monitored or sanction listed Jurisdictions?:

[ ] Yes [ ] No

Remarks:

2.10 Is any of the supplier/buyer/counterparty match with sanction listed entries? (e.g. BB, UN, OFAC, EU):

[ ] Yes [ ] No

If match found:

[ ] False Positive

[ ] True Positive

(Attach detailed sanction screening report)

Remarks

2.11 Products and services to be utilized from the bank:

Existing/anticipated account activities	
Usual methods and terms of payment and settlement	:
Any observations/ratings on the customer by concerned departments of the bank	
Any previous suspicious transaction/activity reports to BFIU	
TTP	

2.12 Beneficial Owner identified?:

[ ] Yes [ ] No

* if there's any beneficial owner, Same KYC procedure shall be conducted for each of the beneficial owner

3. Risk Assessment	
3.1 Last Review Date	:
3.2 Risk Status according to last review	: [ ] High [ ] Moderate [ ] Low Remarks:
3.3 Current Risk Score	Score: [ ] High [ ] Moderate [ ] Low Remarks:
3.3.1 If risk score is high: Please describe the EDD measures	:

Annexure C.2

Trade Transaction Profile

Customer Name & Address	
IRC number	
ERC number	
BEPZA/EZ permission no	
BIN No.	
Vat reg. No	
TIN No	

Particulars of Business	**Details**
Type of Business (Commercial/Industrial/Others)	
Nature of Business (RMG/Textile/	
Pharmaceuticals/Trading/Agro etc.)	
Import items [including service/performance]	
Export items [including service/performance]	
Types of Trade Loan from bank and other FIs	
Types of Guarantee/Standby LC	
Importing Countries	
Exporting Countries	

Details of Transactions	**Monthly Average Volume of Transactions**		**Monthly Average Value of transactions in Million USD**	
Details	Minimum	Maximum	Minimum	Maximum
Import LC Issuance				
Import through Collection/Contract				
Import payments				
Export LC/Contract				
Export Proceeds realization				
Other invisible receipt (inward remittances)				

Other invisible payment (outward remittance)				
Guarantee/Standby LC				
Import Loan (EDF/UPAS/LATR/MPI/MIB/Bai Muazzal/ etc)				
Import Under Aid/Barter/or any other special arrangements				
Import payment through FC account				
Term Loan for Machinery Import				
Export Loan foreign (Discounting/ Purchase/Bai As sarf/)				
Local Export Loan (Discounting/ Purchase/Musharaka Documentary Bills etc.)				
Others				

I/We the undersigned hereby confirm that the anticipated transaction amount and frequency are my/company's normal transactions. I/We further confirm that if necessary, I/we will revise our transaction profile from time to time.

Signature…….
.

Name……
…..

Designation……

Date……
….

Signature…….
.

Name……
…..

Designation……

Date……
….

For Bank's Use Only

The Trade Transaction Profile (TTP) of the client has been reviewed in accordance with the instructions of Bangladesh Financial Intelligence Unit (BFIU).

Designated bank official's name (with seal), signature and date

Annexure C.3

Customer Risk Assessment

SL	Risk Components		Risk Parameters	Risk Score		Composite Risk Level
				Obtained score	**Max Score**	
	Trade Customer Demographic		Business History		3	
			Payment Behavior		3	
			Adverse Media Report		3	
			Law suits Filed (Existing or Previous)		3	
			Others (If any)		3	
Sub Total						
	Geographic Locations of Trade Transactions		Jurisdiction 1 _____		3	
			Jurisdiction 2 _____		3	
			Jurisdiction 3 _____		3	
			Jurisdiction 4 _____		3	
			Jurisdiction 5 _____		3	
			Jurisdiction 6 _____		3	
Sub Total						
	Products Services		Food Grain		3	
			Industrial Raw Materials		3	

			Capital Machinery		3	
			Trading Goods		3	
			Service Import or Service Export		3	
			Defense Goods		3	
			Dual Use Goods		3	
			Other Products (If any)		3	
			Multiple Products		3	
Sub Total						
	Transaction Trend/History		Value of Trade Transaction		3	
			Number of Trade Transaction		3	
			Number of Escalated TBML Alerts		3	
			Number of STR		3	
Sub Total						
Grand Total						

Comprehensive Risk Level	Threshold in %	Actual Risk Level
High Risk	75 % and above	
Medium Risk	50 % and above but below 75 %	
Low Risk	Below 50%	

Annexure D.1

TBML Alerts Based on Categories

TBML Alert, a warning sign, is not in itself an indication that something is wrong but that given the nature of the client's business and the nature of the underlying transaction, the TBML Alert merits further review.

The TBML Alerts may be sub-divided into the following categories, i.e.

a) The transactions

b) The goods and size of shipment

c) Transport

d) Payment

e) Country

f) Party/parties

g) Discrepancies

h) Unusual documentation

Concerned officials should take into consideration the TBML Alerts described below while conducting trade operations:

TBML Alert No.	Alert Description	Purpose/Rationale with example
Applicant/Beneficiary		
1.	Importer and exporter are related parties and there is common interest.	In most cases of illegally transferred fund, applicant and beneficiary are related or connected parties or there are some common interests between them. So bank needs to be aware of whether the applicant and beneficiary of a trade transaction are in any way related to some common interests. In this context, bank should also follow instructions contained in para 2 of Chapter 7 and para 7(b)(iv) & para 7(c) of Chapter 8 of GFET, 2018.
2.	Transacting parties appear to be affiliated, conduct business out of a residential address or provide only a registered agent's address.	Party 'A' enters into a contract with Party 'B' for import of goods through documentary credit. The contact address of party 'B' appears C/O: legal representative name and its address details, or prior to opening of LC, credit report of party 'B' revels that party 'B's line of business is not consistent with underlying goods. In both instances, the exporter may try to hide the true beneficial owner of the transaction.

TBML Alert No.	Alert Description	Purpose/Rationale with example
3.	Customer Behavior	The behavior of customer may give rise to TBLM alerts. For example, the customer

		suddenly becomes anxious and puts pressure on the bank, or offers bribery, threatens to terminate business relationship to execute the transaction.
4.	Any of LC/Contract/ Guarantee parties are known to be owned and controlled by Politically Exposed Persons (PEPs) or Influential Persons (IPs).	PEPs and IPs may exert undue influence to conduct trade transaction in their favor. As such banks need to have an effective mechanism to identify PEPs involvement in the trade transactions as applicant or beneficiary or any other party.
3rd Parties		
5.	Involvement of the parties in the trade transaction cannot be explained.	It has been seen that applicant and beneficiary are not willing to explain the rational of involvement of intermediaries in the transaction. At this back drop, though banks may not be able to know all the parties involved in the transaction, they should understand why they are involved and involved parties with no apparent logical role in the transaction should be examined further.
Illustration	Party 'A' approaches bank 'B' to open an LC favoring beneficiary of country 'C'. Party 'A' requests bank to advise the LC in any bank in country 'D' instead of country 'C'. However there is no information in proforma invoice on the basis of which the reason of such demand by the beneficiary can be ascertained. In addition to that the beneficiary further demands credit available in another country not related to beneficiary's country. This type of scenario needs further analysis in order to understand different parties' involvement in the transaction.	

TBML Alert No.	Alert Description	Purpose/Rationale with example
6.	Too many intermediaries making transaction overly complex.	An applicant or beneficiary may approach a bank for a trade transaction with too many intermediaries involved in the transaction with an ill motive of executing transaction through creating complexity. As part of due diligence, bank should understand the justification of the involvement of intermediaries within the trade cycle. Contact from unexplained parties may be an indicator of a transaction that is more complex than it appears or an indication of unusual activity.
The Transactions		
7.	Transaction structure appears unnecessarily complex or unusual and designed to obscure the true nature of the transaction.	Though financially solvent, the applicant may avail trade finance facility from the bank in order to disguise the true nature of the transaction. He may use unusual trade term; involve many countries & intermediaries in the transactions.

		Hence, as part of process banks should review the structure and complexity of an L/C contract. Banks should analyze financial products and transaction structures and determine if they are intended to obscure the true nature of the transaction. For example, it is clear from the transaction structure that giving an undertaking to the beneficiary was not the purpose behind issuing the documentary credit.

TBML Alert No.	Alert Description	Purpose/Rationale with example
Illustration	Transaction structure appears unnecessarily complex: Party 'A' enters into the contract with party 'B' for import of goods through documentary credits. The underlying agreement is that Party 'B' (the beneficiary) will send some regulatory documents directly to the applicant. Documentary credit only requires that all regulatory documents like: fumigation certificate, phyto-sanitary certificate, quarantine certificate etc to be sent directly to the applicant by the beneficiary. The credit also requires being transferable. Bank 'X' opens a transferable LC with the above condition which is subsequently transferred to 2nd beneficiary. The issuing bank has received presentation from the transferring bank which indicates that the 2nd beneficiary assigned its proceeds to the third parties and requests the issuing bank to pay directly to the third party. Considering the above case, there are few elements that may be considered as alerts. i.e. 1. The beneficiary sends few regulatory documents directly to the applicant: By doing this, the beneficiary is able to keep the required regulatory documents outside the bank's operational purview. 2. The LC is transferable: Under general circumstance, there is no harm in making the LC transferable. But the issuing bank should understand the reasonable ground for transfer. In some situations, the beneficiary sometimes insists on the condition to gain tax benefits and to create gateway to transfer fund from one country to another. Moreover, the issuing bank should have prior knowledge of the prospective 2nd beneficiaries and if possible restrict transfer within the beneficiaries. By doing this, issuing bank has prior knowledge of those with whom they are dealing. Furthermore, the issuing bank should also understand whether it will restrict the transfer within the first beneficiary country or give authority to the transferring bank to make the transferred credit available in 2nd beneficiary's' country. The issuing bank should have prior knowledge about the 2nd beneficiary's country with whom the issuing bank intends to deal. 3. Assignment of proceeds: Even though it is not possible to have prior knowledge about request for assignment of proceeds until receipt of notice of assignments or indication in covering schedule, it is quite unusual to receive assignment of proceeds notice under transferable LC. Even in regular irrevocable LC, if the issuing banks receive assignment of proceeds notice, it indicates that the issuing bank is requested to deal with third parties other than the beneficiary. Assignment of proceeds under UCP 600 is always subject to applicable law and it will not be enforceable to the issuing bank until it acknowledges the assignment of proceeds. The issuing bank should conduct proper due diligence before	

	crediting the documentary credit third parties. The above is only one example of how a documentary credit can become unnecessarily complex. The Bank should consider every unusual request beyond its regular standard practice under the purview of trade based money laundering perspective. In fact opening Transferable LCs should be restricted to 2nd and 3rd.

TBML Alert No.	Alert Description	Purpose/Rationale with example
8.	The customer engages in transactions that are inconsistent with the customer's business strategy or profile. (Transaction is not in line with the customers' line of business or with his/her TTP.)	Any trade transaction that deviates from the customer's existing line of business may have ill-motive to transact against criminal proceeds or may simply move money rather than goods through accommodation of bill etc.
Illustration	Company 'X' imports garlic, cardamom etc through Bank 'A' regularly. Suddenly he approaches bank to import 10,000 MT of rice, inconsistent with his regular import items. The underlying purpose may be to facilitate hiding the true beneficial owner of the transaction. This may also be applicable where the customer approaches bank to open LC for larger quantity than his regular import volume without having any reasonable ground or any business expansion. Company 'Y' generally imports metals but suddenly opened an LC to import some electronics which are unusual and prices are unknown to the market. In this way value can be transferred using such new items of goods. It may be that both the importer and the exporter are sister concern managed by the shareholders. As there may not be any physical movement of the goods, the respective transaction has no economic value other than transfer of money from the importer to exporter in the guise of trade.	
9.	The Trade Finance transaction contains non-standard terminology and/or non-standard clauses. Documentary credits often stipulate very standard clauses as documents requirement, which is by its nature very traditional. If a bank receives an export LC or the customer approaches bank to open an import LC with non- standard terminology or clauses, it may be an indication that the counterpart is trying to convince bank of the creditworthiness of the party and legitimacy of the underlying transaction. Examples: Non-standard Terminologies in documentary credit: • Assignable • Divisible • Unconditional • Unconditional revolving etc. Non-standard Clauses in documentary credit: • 'Ready, willing and able' • "Letter of interest" • "Proof of Conduct" • "The funds are good, clean and cleared of non-criminal origin" • "This is a bearer instrument of letter of credit" • "To be advised between applicant and beneficiary." • "A prime bank guarantee issued by one of the top 50 or 100 world banks or a cash wire transfer etc."	

	The above mentioned indications on a documentary credit are very unusual. In such cases banks should further scrutiny.

TBML Alert No.	Alert Description	Purpose/Rationale with example
10.	Frequent amendment/ extension/ cancellation pattern.	An LC that has been repeatedly amended should be treated carefully. After an excessive number of amendments, the parties should be required to have a new LC issued. Correction of a slight misspelling of a beneficiary name or of the company designation (i.e. "LLP" vs. "Corp") should be handled as a transfer rather than an amendment.
11.	The transaction appears to involve the use of front or shell companies for the purpose of hiding the true parties involved.	Banks should look at the geographic location and addresses of the parties to a transaction paying special attention to those countries or areas where front and shell companies are known to operate. If a bank suspects that a party could be a front or shell company, it should take adequate steps to determine the identity of the suspect entity and whether the entity is designed to hide the true nature of the participants to the transactions.
12.	Guarantee/ Standby LC fails to reference underlying project or contract.	When a bank issues guarantee, or receives counter guarantee ultimately to issue guarantee, it may fail to incorporate all the required information including reference of underlying projects. Hence, banks need to ensure the apparent authenticity of the underlying contract, bid etc. based on which the guarantee is being issued. If beneficiary of the guarantee is a government entity, then it could be easily verified via their website. In case of private beneficiary extra due diligence should be applied for the underlying contract e.g. copy of the contract, copy of paper announcement etc.

TBML Alert No.	Alert Description	Purpose/Rationale with example
13.	Fake underlying transactions against a guarantee/SBLC/LC	Banks need to ensure the identity of the applicant, beneficiary and the underlying documents in order to avoid conflict of interest. Guarantee might be fake if both applicant and beneficiary are related entities and there is no such underlying transactions/performance. It can be executed through KYC for the parties in order to confirm that no same parties or related/common interest parties are

		involved in them.
Value/Price		
14.	The price is unusual e.g. very high or low.	Buyer and seller negotiates the price and the pricing is based on quality and costs of the goods, packaging, freight, customs duties, documentation preparation fees, inspection fees, insurance and many other factors. Therefore, it may not be easy for banks to ascertain the market price for all the components and circumstances that go into the price of a product. Bank officials should take adequate measures to try to identify any blatant or obvious pricing irregularities that may indicate the inconsistencies of pricing of the goods being shipped. Also note para 20 of chapter 7 of GFET, 2018.

Illustration	Typology 1: Company 'X' approaches Bank 'B' to open LC to import mobile phone or car. The price that is revealed in the proforma invoice is very low as compared to local market price. Moreover, the customs authority fixes certain amount or percentage of duty based on per piece etc. to prevent duty or tax evasion. The reason for quoting unit price very low may be for adjustment of debt which arises out of conducting transaction through informal or alternate remittance system. Typology 2: Company 'X' approaches Bank 'C' to open LC to import certain goods. Bank 'B' faces difficulties in knowing the exact unit price due to the nature of goods like capital machinery or chemical mixture etc. In some cases, local duty or tax is very nominal as the underlying goods have correlation with the economic development of the country. Typology 3: Company 'X' approaches Bank 'D' to open LC for import of rice or onion. The importer made certain percentage of advance payment through informal channel and opened LC up to the value where customs authority has reference value for custom valuation. But the actual price is higher than that of reference value. By doing so, the exporter is able to avoid customs duty and taxes for the advance payment made. Similarly, excess amount of freight and other charges may also be taken into consideration.	
TBML Alert No.	Alert Description	Purpose/Rationale with example
15.	Under Invoicing (against market price).	Invoicing goods at a price below the fair market price, the exporter can transfer value to the importer. Here the importer receives high value goods at a lower price. After re-selling the goods importer receives full value and thus additional value is received by the importer from the exporter through under-invoicing. Importer is also able to pay less

		customs duty/tax by under- invoicing. Trade processors should follow the mechanism and guidelines to be established by their own banks in pursuance with these guidelines.
16.	Over Invoicing (against market price).	Invoicing goods at a price above the fair market price value can be transferred from importer to exporter. Bank should frame appropriate policy in this regard and trade processors should follow the same.

TBML Alert No.	Alert Description	Purpose/Rationale with example
17.	Invoice showing significant amount of misc. charges e.g. handling charges.	Money can also be transferred from one party/country to other party/country showing significant amount of misc charges/handling charges/ unidentified charges/in the invoices of goods /services for laundering purpose. Bank should know the justification behind such unusual charges and act accordingly to prevent TBML
18.	There are indications of double invoicing/ Multiple Invoicing.	Double Invoicing: This is very much relevant for local trade transaction. Double invoicing is where a subsidiary purchases goods from a parent at too high a price, or a parent purchases from a subsidiary at too low a price. Multiple Invoicing: This is also very much relevant for local trade transaction. More than one invoice for the same international trade transaction, which enables a money launderer or terrorist financier to justify multiple payments for the same shipment. Though with the establishment of DX dashboard, multiple invoicing is very hard to do onshore, reasonable care should be taken in case of offshore.
Payment		

TBML Alert No.	Alert Description	Purpose/Rationale with example
19.	The payment terms appear inconsistent with the transaction.	An importer or exporter may default willfully and launder money if payment terms of the financing is made without due consideration to the nature and/or conversion cycle of the underlying goods. For example, if an importer is financed for 365 days to import perishable goods like onion etc. when his business is to sell fish, he may abuse the facility and launder money through different ways (send money abroad through over invoicing with banks finance, or may go willful default and use the money to launder or finance terrorism etc.). Hence, taking into consideration the market practice and business of the buyer and seller banks should determine whether payment terms are consistent with the nature and asset conversion cycle of the goods being shipped and act accordingly.
20.	The transaction involves the receipt of payments from third party entities that have no apparent connection with the transaction.	As third party payment arrangements can be used to disguise the identity of the true payer and true source of funds, they may expose to the risk of money laundering and/or unwanted sanctions evasions. Banks need to know and be satisfied with the underlying arrangement with the 3rd party who pay or receive the payments of the trade transaction.
Illustration	Bank 'I' issues an LC for raw cotton from Uzbekistan and LC available with any bank in UAE with an advising bank in UAE. After making shipment, while the beneficiary is trying to make presentation, UAE bank refuses to handle the transaction. Later on the beneficiary makes direct presentation to the issuing bank. Bank 'I' makes an attempt to make the payment through MT 103, which its foreign correspondent bank refuses to process. Much later, the beneficiary makes the presentation through his bank in Latvia, where the beneficiary maintains business account and Bank 'I' effects payment accordingly.	

TBML Alert No.	Alert Description	Purpose/Rationale with example
21.	Changing the place of payment i.e. payment is to be made to beneficiary's account held in another country other than beneficiary's stated location.	Banks should take into account that in some instances, beneficiary under an LC directly sends documents to the issuing bank within instruction to effect payment to a third country. This situation may arise either the beneficiary is not able to route trade document through banking channel due to possible sanction hits or trying to park the proceeds in relatively lax jurisdiction.

22.	Payment instruction changes in the last minute without any reason.	It should be borne in mind that last minute changes to payment instructions, inconsistent with the terms of the trade instrument, or instructions to effect payment to a third party or account unrelated to the trade instrument could indicate unusual activity.
23.	Applicant (customer) controls the payment.	The trade finance transaction includes a feature by which the buyer effectively controls the payment. This could indicate that the seller and buyer are colluding in a non-competitive manner and that they have an underlying relationship outside an expected trading relationship which is not known to the banks. Applicant (customer) controls the payment:
	Applicant (customer) controls the payment. Bank 'X' issues sight LC with a condition that payment will be effected upon receipt of applicant's acceptance regarding receipt of goods in good order. This type of clause enables applicant to control payment. Providing such condition, the applicant can actually delay the payment though inconsistent with its nature of goods or local regulations. In other word, there might be collaboration between the buyer and seller beyond the knowledge of the bank. Bank that issues LC with applicant control documents should be aware about requirement of applicant control and underlying transaction. Such as: import of capital machinery maybe done with provision of split presentation as under: -15% advance payment -70% upon presentation and - The rest 15% after proper installation of the capital machinery supported by applicant certificate. For import of capital machinery, the above split payment is customary. But split presentation or shifting payment obligation from beneficiary's presentation to applicant control document for trading items or industrial raw materials import may need further analysis.	

TBML Alert No.	Alert Description	Purpose/Rationale with example
24.	Claimed/lodged shortly while guaranty validity is a long tenor.	Long tenor guarantee is normally issued against a long term contract/project/performance (i.e. 24 months period). The guarantee claim is supposed to be placed after a reasonable long period of time when applicant fails to execute that long term project/contract. If situation arises that a claim is lodged within a short time after the guarantee is issued, e.g. one month, the guarantee issuing bank should take it as an alert and should perform proper due diligence by confirming the genuineness of the claim from the beneficiary office.
25.	Issuance of fraudulent Letter of Undertaking (LoU).	Bank should have independent policy in place to operate SWIFT system which includes checker and maker system and periodic

		auditing, both by internal and external auditors. In addition, SWIFT system should be integrated with their core banking system (CBS).
Illustration	Two employees of 'XYZ Bank' send unauthorized Letters of Undertakings (LoUs), essentially bank guarantees, to foreign banks on behalf of their customer M/s 'ABC Gems Ltd.' Owned by "Mr. X". The LoUs were undertaken to make payment in favor of foreign beneficiary for imports if on maturity, importer fails to pay, 'XYZ Bank' would make the payment. On receipt of guarantee foreign bank provides loan to the importer. The tenure of this loan varies from ninety days up to even five years for capital goods. The money gets used to settle the payment for imports. The money raised through this guarantee is not used to make payments for imports rather used to settle loans taken earlier. In fact, every time a firm related to Mr. 'X' asks for a bank guarantee, it is to settle an older loan taken through a previous bank guarantee. Thus the amounts go up to around BDT. 11,4000 million. LoUs were issued without any collateral or any usual process of the bank through colluding two bank officials of 'XYZ Bank' and the 'XYZ Bank' sends these guarantees in the absence of credit limits and collateral security. Secondly, he does not make an entry in the bank's Core Banking Software (CBS). In some cases, a corresponding entry is made in the core banking system, but for lower amounts. Every regular audit may not find it. Banks reconciliation department also could not find out the mismatch. It is revealed that in the said Bank, there is no SWIFT operating procedure in place, SWIFT is not integrated with the Bank's CBS and the SWIFT operation of that is not centralized and absence of proper auditing system i.e. IT audits did not take place. On this pretext, the ill motive customer was able to complete the evil scheme with the support of colluding employees of the Bank. Using such valid tools, dishonest officials of the bank in collusion can launder money.	

The goods and size of shipment		
TBML Alert No.	Alert Description	Purpose/Rationale with example
26.	There are no goods (phantom shipment).	Banks could be aware that under these circumstances the beneficiary or applicant refuses to provide documents to prove shipment of goods (possible phantom shipping or multiple invoicing). For example, LC or bank guarantee purportedly covers the movement of goods but fails to call for presentation of transport documents. LC covers steel shipment but allows a forwarders cargo receipt (FCR).
27	No goods description mentioned in documents/ Descriptions of the goods/ services are not clear or are coded or disguised.	Not having goods description is itself an alert. Bank should know the goods or services of underlying transaction from the related trade documents, such as LC, BL, invoice etc.

Illustration for alerts 26 & 27	As we know from documentary credit operation that Banks deal with documents not with underlying goods, service or performance, issuance of LC without asking for transfer document or allowing copy of transport document to be presented may facilitate phantom shipment. In addition to that documentary credit containing a condition "document acceptable as presented" or "all discrepancy accepted except value and quantity" may also have similar implication. Client may approach for issuance of local LC with above clause or without mentioning description of the goods. The inherent agenda in such cases may be to avail loan from the bank under the banner of trade finance.	
28.	The customer deviates significantly from it's historically pattern of trade activity (in terms of markets, monetary value, frequency of transaction, volume, or merchandise).	Banks need to understand the customer's traditional business patterns as part of the trade specific customer due diligence process that reviews and examines the customer's business activity, such as the frequency of shipments, the value, volume, types of products and/or services in which the customer typically deals. Banks should have processes that that will identify significant variations in these trading patterns.

TBML Alert No.	Alert Description	Purpose/Rationale with example
29.	Transaction involves obvious dual use goods.	Dual use items are goods, software, technology, documents and diagrams, which may have both civil and military applications. Identification of dual use goods is difficult given their possible complex and technical culture. While banks may be in a position to identify obvious dual use of goods, corporate clients should be best suited for making this determination. Each bank should refer to its own policies and procedures on how to appropriately identify and address the identification and handling of such goods.
Illustration	Though most of the banks are aware of obvious sanctioned country under UNSCR lists and generally do not open LCs where shipment is made from sanctioned port, company 'X' opened LC for import of bitumen from UAE mentioning any port of UAE and the respective transport document i.e. Bill of Lading also mentions shipment from Jebel Ali, a UAE port inconsistent with the LC terms. But later on upon analysis of shipment routing, it is revealed that the ship indeed started its journey from the Jebel Ali but instead of moving toward Chittagong, it went to Bandar Abbas (an Iranian port) then came back to Jebel Ali and then started journey towards Chittagong. Moreover, Bank should also be careful in importing goods from certain country where underlying goods is not within the exportable basket of the exporting.	
30.	Different HS Code is used.	In trade documents (i.e. LC, Invoice, EXP etc.) different HS code may be used to avoid high rate of customs duty. Bank should identify the goods description with appropriate HS code as per customs first Schedule of

		Bangladesh.
31.	Quantity of goods exceeds the known capacity of the shipping containers or tanker capacity or abnormal weights for goods are suspected.	Under shipment, over shipment, no shipment might occur when quantity of mentioned goods exceeds the capacity of the shipping containers/ tanker. Bank should try to know apparent capacity of the container, tanker etc.

TBML Alert No.	Alert Description	Purpose/Rationale with example
32.	High risk goods/ services are involved.	Goods/ services are assigned as high risk when those particular items of goods/ services are used for illicit purposes. Bank management should make relevant officials aware of the high risk goods and services from time to time.
Transport		
33.	Transportation route/ information is inconsistent with underlying transaction.	Commercial banks should take into consideration whether the transport route appearing in documents is usual or inconsistent. It may be that the transport route does not make sense for the purpose of the customer/goods shipped. It may also be that the actual transport route is inconsistent with the expected and documented transport route.
34.	Transshipment through a country for no apparent reason	Nature of goods, applicant & beneficiary country distance/location does not justify transshipment or transshipment from a country which is geographically absurd. For example, Shipment of raw cotton from Singapore, which is unusual?
35.	The mode or method of shipping is unclear or the shipping route is unclear.	If the mode of shipment and shipping is not clear or kept hidden, there might be involvement of some sanctioned/embargoed country/ port/location/entities. Banks should perform due diligence to identify the mode and route of the shipment.
36	Goods to be shipped from one country/place but supplier/beneficiary is located in another country/place.	Bank should check the valid reason for the shipment from a third country where beneficiary is not located. There might be underlying illicit arrangement between the beneficiary and the party in third country from where shipment is made.

TBML Alert No.	Alert Description	Purpose/Rationale with example
37.	Vessel/Container number cannot be tracked through web search.	Container number consists of an internationally standard format. The number includes four letters and seven digits, with the last digit (i.e. XXXU1234567). It is used for documentation purposes, including invoice, consular statement, bill of lading and others. Vessels can also be tracked through web link. Banks should check the vessel tracking/ container tracking through web link to ensure that the vessel/ container number appearing in the documents is valid.
38.	The bill of lading describes containerized but without container numbers or with sequential container numbers.	If bill of lading/shipping document does not contain the container number while the goods are shipped through containerized cargo, banks need to further scrutinize and ensure that the shipments appearing in the documents is valid.
Country/ Jurisdiction/Geographical Location/Sanction		
39.	Customer shipping items to, through, or from higher money laundering risk jurisdictions including countries identified by FATF as stated in FATF Public document.	Banks should understand where the customer undertakes business and on what basis as part of trade specific customer due diligence activities. As some countries, entities and individuals present heightened risk of financial crimes, care should be exercised to understand the rationale for the customer conducting, business in higher risk jurisdictions.
40.	Transaction involves high risk jurisdiction/country	To the extent possible, banks should determine if there is a valid reason, and if the business is within their risk parameters.
41.	Transaction involves sanctioned entities/countries/individuals.	Banks should maintain a list of jurisdictions identified by relevant bodies (e.g. FATF) that present high risk in terms of money laundering, terrorist financing or other financial crimes. Transaction with UN sanctioned countries, individuals and entities should be avoided. All the lists should be made available to the trade operations area and updated as necessary.

Discrepancies		
TBML Alert No.	Alert Description	Purpose/Rationale with example
42.	Good's description in the documentary credit.	Examples: There are significant discrepancies between the description of the goods on the bill of lading (or invoice) and the documentary credit, i.e. it is apparent that they are not the same type of goods.
43.	Clauses in the documentary credit.	If clauses in the documentary credit are not examined and addressed carefully by the bank, colluding parties may abuse trade and perpetrate TBLM.
Illustration	Clauses in the documentary credit: Bank 'I' issued LC for or on behalf of the customer 'X' in favor of the beneficiary 'Y' for import of raisin. After issuance of LC, the customer remitted 15% of actual goods value through informal channel. As soon as the beneficiary 'Y' received funds, the beneficiary 'Y' demanded an amendment for addition of clause "document acceptable as presented" or "all discrepancy acceptable except value and quantity". Bank 'I' issued the amendment reluctantly. Later on, the beneficiary made presentation except pre-shipment inspection certificate and phytosanitry certificate. Upon analysis, it was revealed that the quality of the shipped goods was inferior and not fit for human consumption but the fact is that the presentation was complying due to the amendment.	
44.	Essential documents presented in copy forms or not presented.	Essential documents such as invoices or transport documents are missing or presented in copy form.
45.	Waivers: amount significantly overdrawn, advance waivers provided etc.	The documentary credit/guarantee is significantly overdrawn; i.e. the drawing under the documentary credit/ guarantee is significantly above the outstanding amount of the documentary credit/ guarantee.

TBML Alert No.	Alert Description	Purpose/Rationale with example
Illustration 44 & 45.	44 & 45 Essentials documents presented in copy form or not presented: Waivers: Amount significantly overdrawn, advance waivers provided etc: Bank 'I' issued LC favoring the beneficiary 'Y' for its new customer 'X' under 50% margin. The beneficiary made presentation of copy of bill of lading instead of original. The customer approached banks to waive the discrepancies, which later on agreed after depositing 100% margin. Bank 'I' effected payment accordingly. After a few days, the bank received another presentation under documentary collection with payment instruction to deliver documents against payment for different customer of Bank 'I'. After checking documents, it was found that the original bill of lading of the earlier LC related documents had been presented. Moreover, the beneficiary was also different from the LC. In the meantime, the new customer also disappeared. Bank should take into consideration the type of discrepancy they are given waiver and should have an understanding of its after effect.	

	Sometimes, it is also seen in local documentary credit practice that bankers generally allow 10% excess payment on the plea of 10% tolerance level with or without LC conditions. While affecting such type of payment, bank should take due care of nature of goods, applicability of tolerance, and change in unit price etc.	
46.	The customer is overly keen to waive discrepancies.	Banks need to understand the motive behind the customer's keenness to accept the discrepancies and the gravity of the discrepancies. Although this is not related to trade rules, additional responsibility in respect of KYC (Know Your Customer), DD (Due Diligence), and EDD (Enhanced Due Diligence) have been vested on the bankers. When acceptance is provided by the importer, to the discrepant documents, the banker should verify the kind of discrepancy accepted and whether this may pose money laundering risk.
Unusual Documents		

TBML Alert No.	Alert Description	Purpose/Rationale with example
47.	Documents required or presented is unusual to related trade transaction.	Banks should be cautious if documents appear to have been altered, fraudulent, are inconsistent or illogical, or when documentary presentations do not include required transport documents, as this could be an indication of unusual activity.
48.	There are indications that documents have been reused. .	Although the failure of documents to appear on their face to comply with the terms and conditions of an LC may be routine discrepancies, certain unusual discrepancies may require additional due diligence. Examples include the presentation of documents showing a place of origin, loading, transshipment or destination entirely inconsistent with what is expected, the presentation of documents showing goods description entirely inconsistent with the expected goods, and the presentation of documents showing much higher or lower values or costs than expected.

Annexure D.2

Product wise TBML Alerts, Some Relevant Lists and Examples

Some of the important Products specific TBML alerts are given below. They do not eliminate the alerts mentioned in Annexure D.1

TBML Alerts common to almost all the products below and therefore should be guarded against are:

i. Under Invoicing (against market price)

ii. Over Invoicing (against market price)

iii. Underlying goods is not in line with the customer's line of business.

iv. Descriptions of the goods are not clear or are coded or disguised.

v. The method of payment appears inconsistent with the risk characteristics of the transaction.

vi. The transaction involves sanctioned entities.

1. Issuance of LC/LCAF

Price, Quantity and descriptions of Goods:

a) High risk goods or high risk jurisdiction/country is involved.

b) Transaction involves restricted or banned items of goods.

c) Different HS Code is used

Mode and Location of Shipment:

- Goods to be shipped from one country/place but supplier/beneficiary are located in another country/place and payment to be made to a different 3rd country/place.
- The mode or method of shipping is unclear or shipping route is unclear.

Payment Method:

a) Changing the LC beneficiary or collection payee name and address just before payment is to be made. Including requests for assignment of proceeds or transfer at the time documents are presented.

b) LC transfer or assignment of proceeds request names a transferee or assignee in an offshore financial haven. Request for transfer assignment or other financing under an LC which has expired or not in effect.

c) The customer offers to pay unusually high fees to the Bank.

Applicant, Beneficiary and other Parties/Entities Involved:

a) Supplier's credit report is not available.

b) Supplier's line of business is not in congruence with the goods imported.

c) Transaction is not in line with the customer's TTP (Trade Transaction Profile) or when an exporter steps outside normal business activities.

d) Any of LC parties are known to be owned or controlled by senior public figure. Transaction involves an unusual

intermediary (e.g. middleman is travel agency handling shipment of machine parts) or too many intermediaries making transaction overly complex.

LC Clauses and Required Documents:

a) Unusual/non-standard clause is inserted in the LC.

b) LC without regulatory required documents.

c) Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Import Bill (Scrutiny/Acceptance/Payment/Financing) & Export Bill (Scrutiny/ Financing/ Payment)
Price, Quantity and Descriptions of Goods:

- Under Shipment (in terms of quantity)
- Over Shipment (in terms of quantity)
- Discrepancies in Goods description, quantity and shipment locations.
- Where the quantity of goods exceeds the known capacity of the shipping containers or tanker capacity. Or where abnormal weights for goods are suspected.

Invoice:

- There are indications of double invoicing.
- Invoice showing significant amount of misc. charges e.g. handling charges.
- The documentation appears illogical, fraudulent and/ or improperly modified from its original content, or certain documentation is absent that would be expected given the nature of transaction.

Transport & other Documents:

i. The bill of lading describes containerized cargo but without container numbers or with sequential container numbers.
ii. Phantom shipment - where no goods are shipped at all and the documentation is completely falsified
iii. The mode or method of shipment is unclear or the shipping route is unclear.
iv. Vessel / Container number cannot be tracked through web search.
v. There are indications that documents have been re-used.
vi. There are dubious unauthorized alterations or amendments to the documents.

Payment Methods:

a) Payment is to be made to beneficiary's account held in another country other than the Beneficiary's stated location.

b) Payment is to be made to personal A/C of beneficiary instead of company A/C.

Others:

a) The customer is overly keen to waive discrepancies.

b) Transaction involves an unusual intermediary (e.g. middleman is travel agency handling shipment of machine parts) or too many intermediaries making transaction overly complex.

Export LC Advising

- High risk goods or high risk jurisdiction/country is involved
- Transaction involves restricted or banned items of goods.

Export LC/Contract Lien and Pre-shipment financing (B2B facility/Packing Credit/Working Capital Loan):
Price, Quantity and descriptions of Goods:

- High risk goods or high risk jurisdiction/country is involved.
- Transaction involves restricted or banned items of goods.

Mode and Location of Shipment:

- Goods to be shipped from one country/place but supplier/beneficiary are located in another country/place and payment to be made to a different 3rd country/place.
- The mode or method of shipment is unclear or the shipping route is unclear.

Payment Method:

Applicant, Beneficiary and Other Parties/Entities Involved:

- Bonafides of buyer is not known.
- Buyer's line of business is not in congruence with the underlying goods.
- Transaction is not in line with the customer's TTP (Trade Transaction Profile) or when an exporter steps outside normal business activities.
- Any of LC parties are known to be owned or controlled by senior public figure.
- Transaction involves an unusual intermediary (e.g. middleman is travel agency handling shipment of machine parts) or too many intermediaries making transaction overly complex.

LC Clauses and Required Documents:

- Unusual/non-standard clause is inserted in the LC.
- LC without regulatory required documents.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment

Shipping Guarantee

IDO/Shipping Guarantee is just copy document endorsement by bank and in addition bank issues a shipping guarantee favoring shipping company. While issuing IDO/Shipping Guarantee, TBML alerts relevant to IDO/Shipping guarantee mentioned below should be taken into consideration:

Price, Quantity and Descriptions of Goods:

i. Under Shipment (in terms of quantity)
ii. Over shipment (in terms of quantity)

iii. Discrepancies in Goods' description, quantity and shipment locations.

iv. Where the quantity of goods exceeds the known capacity of the shipping containers or tanker capacity. Or where abnormal weights for goods are suspected.

Invoice:

i. There are indications of double invoicing.

ii. Invoice showing significant amount of misc. charges e.g. handling charges.

iii. The documentation appears illogical, fraudulent and/or improperly modified from its original content, or certain documentation is absent that would be expected given the nature of the transaction.

Transport & other Documents:

i. Original import documents against the LC are already in the bank.

ii. There are indications that documents have been re-used.

iii. Transport document is not endorsed to the order of the bank as per LC terms.

Guarantee/Standby Letter of Credit (SBLC)

i. Guarantee/Standby LC fails to reference underlying project or contract (except for insurance related LCs, where the LC calls for a draft only. This is an acceptable practice).

ii. Applicant and beneficiary are related party and there is common interest.

iii. Claimed/lodged shortly whilst guaranty validity is a long tenor.

iv. Fake underlying transactions.

v. In case of transfer, there is a possibility to effect payment to a sanctioned or AML related party.

Service Export

a) Swift message does not mention any purpose of the transaction.

b) The reference number of underlying service contract/LC/Invoice is not mentioned in the Swift payment message.

c) Importer and exporter are related parties. d) Description of service is not clear.

e) Exporter and importer line of business do not support the services.

f) Exporter is not capable of providing those underlying services.

g) Payment received from a third party not mentioned in underlying contract. h) Price of service unusually high or low.