MANAGING CORES RISK IN BANKING - MONEY LAUNDERING & TERRORIST FINANCING (ML/TF) RISK MANAGEMENT GUIDELINES.

Prime Bank

AML & CFT Divsion, Prime Bank PLC. Head Office

MANAGING CORE RISK IN BANKING

Money Laundering & Terrorist Financing Risk Management Guidelines

January 2026

AML & CFT Division
Prime Bank PLC., Head Office

Prime Bank

Contents

AML & CFT POLICY STATEMENT OF PRIME BANK

ML & TF RISK MANAGEMENT GUIDELINE:

The primary purpose of ML & TF Risk Management Guidelines is to instruct the development of an AML/CFT control framework that is appropriate and proportionate to ML & TF risk that Prime Bank as a reporting entity may reasonably face. This implies that the ML/TF risk assessment identify and includes all known risks considering the size, range of activities, the complexity of operations, customer types, product and service, distribution channel and jurisdiction perspective as well as the policy and strategy to mitigate and prevent those risks. The resulting risk ratings influence the manner in which and the degree to which should be mitigated and managed.

POLICY ISSUES AND INTRODUCTORY:

In line with the embedding Core Risk Management culture across the banking sector, Prime Bank's first AML guidelines named "General Guidelines on Anti-Money Laundering Program for Prime Bank." was approved in its 189th meeting of the board of directors held on December 14, 2003.

The guidelines were revised in December 2012. The guideline was named "Guidelines on Prevention of Money Laundering & Terrorist Financing for Prime Bank." which was approved in its 390th meeting of the board of directors held on December 13, 2012.

In September 2016, a comprehensive revision of the guidelines was initiated based on BFIU Master Circular 10/2014 & BFIU "Money Laundering and Terrorist Financing Risk management guidelines"-2015. The guidelines were named "Money Laundering & Terrorist Financing Risk Management Guideline for Prime Bank." approved in its 453rd meeting of the board of directors held on September 25, 2016.

In May 2019, another revision of the guidelines was initiated based on BFIU Master Circular 19/2017 & BFIU "Money Laundering and Terrorist Financing Risk management guidelines"-2015. The guidelines were renamed as "PRIME BANK Money Laundering & Terrorist Financing Risk Management Guideline" and approved in its 490th meeting of the board of directors held on September 05, 2019.

In November 2022, the guideline have been reviewed and updated to accommodate the regulatory changes [BFIU Master Circular No. 26; BFIU guidance notes, directives & circulars; BFIU Guidelines on e-KYC]. The guidelines was approved in its 534th meeting of the board of directors held on November 01, 2022 and circulated among all employees of the bank.

The periodic review of the guidelines was initiated in 2025 to incorporate recent industry changes. This latest version was approved at the 588th meeting of the Board of Directors held on January 29, 2026.

OBJECTIVE OF THIS GUIDELINES:

Broad Objective:

To ensure that a system is established within the financial institution through which Money Laundering and Terrorist Financing control is managed and implemented through stringent and appropriate procedures in order to discharge our legal and moral duties.

Specific Objective:

Apart from this broad objective, the specific objectives are:

a. To Prevent Money Laundering, Terrorist Financing & Proliferation Financing through banking channels.

b. To Ensure the implementation of required provisions of Acts, Rules and Instruction & Directives of BFIU;

c. To prevent the PRIME BANK's products or services from being used as a channel for Money Laundering and Financing of Terrorism;

d. To build awareness on the importance of AML & CFT among all employees, members of the Board of Directors, owners and customers of PRIME BANK.

e. To prevent damage to the PRIME BANK's name and reputation by associating with money launderers or terrorist financers or proliferation financer of weapon of mass destruction;

f. To assist regulators/law enforcement agencies in their efforts to investigate and track money launderers & terrorist financers.

SCOPE OF THIS GUIDELINES:

This policy sets out:

a. The obligations of Prime Bank with respect to the requirements imposed under the MLP Act-2012 (including all amendments in 2015), ATA-2009 (including all amendments -2012 & 2013), MLP Rules-2019, BFIU ML & TF Risk Management Guidelines-2015, BFIU Guidelines for Prevention of Trade Based Money Laundering-2019, BFIU Guidance notes on PEPs, Beneficial Owner, Reporting of STR, E-KYC Guidelines, BFIU Master Circular-26 along with other active circulars, instructions & directives of BFIU;

b. Requirements imposed on implementing a comprehensive risk-based approach in managing ML/TF risks; and

c. Roles & Responsibilities of the Board of Directors, Senior Management, CAMLCO, CCC members, Deputy CAMLCO, BAMLCO /DAMLCO, Head Office & Branch Officials in putting in place the relevant AML/CFT measures.

BENEFITS OF THIS GUIDELINES:

a. Will enable PRIME BANK to increase awareness on anti-money laundering & combating financing of terrorism among all the employees.

b. Explain our duties and responsibilities under Money Laundering Prevention Act 2012 (amended in 2015) and Anti-Terrorism Act 2009 (amended in 2012 & 2013).

c. Help us to meet the regulatory requirements and international standards.

d. Introduce and continuing AML & CFT compliance program of the Bank, monitoring & reporting system.

e. Understand the consequences of non-compliance.

f. Answer our queries regarding the AML/ KYC/CDD procedures of the Bank.

COMPLIANCE POLICY STATEMENTS:

a. That In order to protect Bank's reputation and to meet its legal and regulatory obligations, it is essential that PRIME BANK shall minimize the risk of being used by Money Launderers & terrorist financiers. With that end in view, it will be an obligatory responsibility for all employees and management of the Bank to realize and combat the situation on these critical risk issues of ML, TF & PF.

b. That Keeping the AML&CFT issues in mind, PRIME BANK has developed a written AML & CFT compliance program duly approved by the Board of Directors that ensures and monitors compliance with the Acts, Rules & BFIU directives including record keeping and reporting requirements;

c. That the written AML&CFT compliance program establish clear line of responsibilities, accountabilities & reporting within the organization 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;

d. That the program is tailored to our bank and are based upon an assessment of the money laundering and terrorist financing risks, taking into account the bank's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering and terrorist financing;

e. That it includes standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse; addresses our '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, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness;

f. That it also includes a description of the roles the AML&CFT Compliance Officers(s)/ Unit and other appropriate personnel who will play significant roles in monitoring compliance with and effectiveness of AML&CFT policies and procedures.

g. That it develops and implements screening programs to ensure high standards when hiring employees; implements standards for employees who consistently fail to perform in accordance with an AML&CFT framework; incorporates AML&CFT compliance into job descriptions and performance evaluations of appropriate personnel; and has the arrangements for program continuity despite changes in management or employee composition or structure;

h. Formulation and review of this policy will be initiated by CCC as and when required, while period between successive reviews shall not exceed three years.

i. That it is the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers and officials will be held responsible for non-compliance with the applicable laws and the institution's policy including the criminal, civil and disciplinary penalties and reputational harm that may result from any bank with money laundering and terrorist financing activity.

j. That it is the responsibility of the every individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations is no excuse for non-compliance.

k. That PRIME BANK will support government, law enforcement agencies and BFIU in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal purposes.

AML & CFT POLICY MANAGEMENT:

a. CAMLCO is the authority to explain sense and sentiment of the policy. In case any ambiguity developed due to English version of the BFIU Circulars, original Bangla text to be considered. Laws of the land are to be considered superior to any policy and process of any bank and that of central bank. However, in case of any unintentional contradiction prevails or developed in future, international standards and laws and regulations adopted by the Government of Bangladesh and all relevant laws of land in force of Bangladesh, directives & guidelines of Bangladesh Financial Intelligence Unit (BFIU) shall prevail.

b. CAMLCO shall be the custodian of the policy. AML & CFT Division will coordinate the review and up gradation process of policy in conjunction with Central Compliance Committee (CCC).

c. This policy shall be applicable across PRIME BANK & its' both local and foreign branches and subsidiaries. Bank will ensure the comply of all the rules and regulations stipulated in MLPA-2012 (including all amendments in 2015), ATA-2009 (including all amendments in 2012 & 2013) by its foreign branches and subsidiaries. In case of any failure and inability of complying such rules and regulations, foreign branches and subsidiaries should inform to CCC or AML & CFT Division according to BFIU Circular No. 23 dated 31-01-2019.

d. As per instruction & directives of BFIU, PRIME BANK has prepared its own guidelines approved by the Board of Directors to prevent money laundering and terrorist financing.

Accordingly, change of guidelines is to be approved by the Board of Directors of PRIME BANK. MD's approval suffices the changes of guidelines as recommended by CAMLCO/CCC, which to be ratified by Board of PRIME BANK within 180 days of such approval.

e. Formulation and review of this guidelines based on legal/regulatory or business/operational changes should be reviewed & updated at a reasonable time or time-to-time which will be initiated by CCC, otherwise, the period between successive reviews shall not exceed 3 (three) years.

Chapter 01

AN OVERVIEW ON ML, TF & PF RISKS AND INTERNATIONAL & NATIONAL INITIATIVES

1.1 Introduction

Financial integrity is essential for economic and social development. Countries' financial systems must be transparent, must be inclusive and must function with integrity to ensure economic development and to promote good governance. Transnational organized criminal activity, corruption, the illegal trade in natural resources and the laundering of the proceeds of crime generate illicit flows that undermine good governance, financial sector stability, and economic development.

Money is laundered 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.

The process of money laundering and terrorist financing (ML/TF) is very dynamic and ever evolving. The money launderers and terrorist financiers are inventing more and more complicated and sophisticated procedures and using new technology for money laundering and terrorist financing. To address these emerging challenges, the global community has taken various initiatives against ML & TF. In accordance with international initiatives, Bangladesh has also acted on many fronts.

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. Most countries adopted to the following definition which was delineated in the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

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

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

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

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

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

Money laundering' means —

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

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

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

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

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

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

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

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

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

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

1.3 Predicate Offences

"predicate offence" means the offences mentioned below, by committing which within or outside the country, the money or property derived from is laundered or attempt to be laundered, namely: -

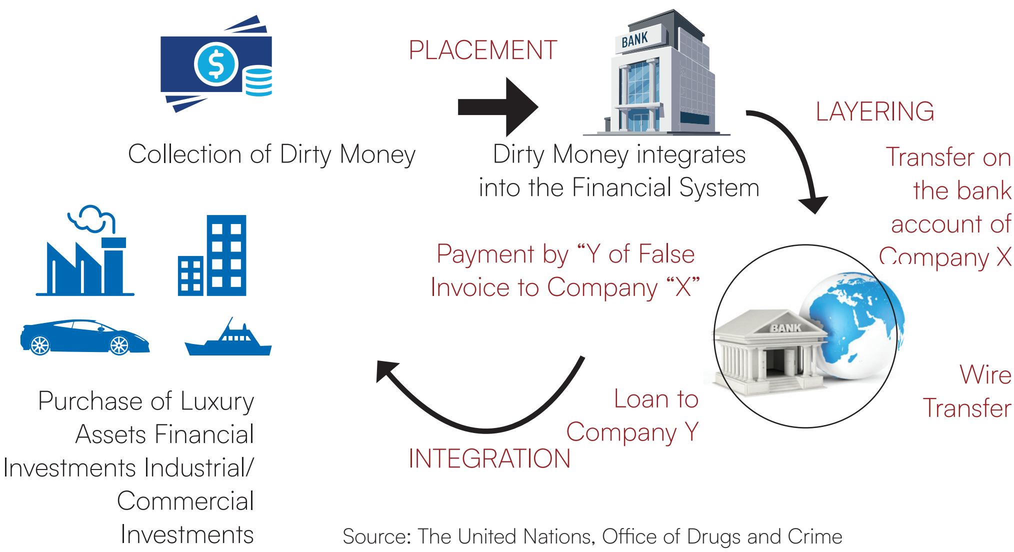
1. Corruption & bribery.
2. Counterfeiting currency.
3. Counterfeiting documents.
4. Extortion.
5. Fraud.
6. Forgery.
7. Illegal trade of firearms.
8. Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication.
9. Illegal trade in stolen and other goods.
10. Kidnapping, illegal restrain and hostage taking.
11. Murder, grievous physical injury.
12. Trafficking of women and children.
13. Black marketing.
14. Smuggling of domestic and foreign currency.
15. Theft or robbery or dacoity or piracy or hijacking of aircraft.
16. Human trafficking or receive or/and attempt to receive any amount of money or any valuable goods from any person by giving false commitment of foreign employment.
17. Dowry.
18. Smuggling and offences related to customs and excise duties.
19. Tax related offences.
20. Infringement of intellectual property rights.
21. Terrorism or financing in terrorist activities.
22. Adulteration or the manufacture of goods through infringement of title.
23. Offences relating to the environment.
24. Sexual exploitation.
25. Insider trading and market manipulation using price sensitive information relating to the capital market in share transactions before it is published for general information to take advantage of the market and attempting to manipulate the market for personal or institutional gain.
26. Organized crime and participation in organized criminal groups.
27. Racketeering.

28. Cyber Crime.
29. Pornography.
30. Any other offence declared as predicate offence by BFIU, with the approval of Govt. by Notification in the official Gazette, for the purpose of this Act.

1.4 How Money Laundering is done?

Money laundering often involves a complex series of transactions that are difficult to separate. However, it is common to think of money laundering as occurring in three stages:

Stages of Money Laundering



Source: The United Nations, Office of Drugs and Crime

Stage One: Placement — The physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions and other legitimate businesses, both domestic and international.

Examples of placement transactions include:

- Blending of funds: Comingling of illegitimate funds with legitimate funds such as placing
- the cash from illegal narcotics sales into cash-intensive locally owned restaurant
- Foreign exchange: Purchasing of foreign exchange with illegal funds

- Breaking up amounts: Placing cash in small amounts and depositing them into numerous
- bank accounts in an attempt to evade reporting requirements
- Currency smuggling: Cross-border physical movement of cash or monetary instruments
- Loans: Repayment of legitimate loans using laundered cash

Stage Two: Layering — The separation of illicit proceeds from their source by layering of financial transactions intended to conceal the origin of the proceeds.

This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds.

Examples of layering transactions include:

- Moving funds from one financial institution to another or within accounts at the same Institution
- Moving funds into advanced financial options and or markets
- Converting the cash placed into monetary instruments
- Reselling high value goods and prepaid access/stored value products
- Investing in real estate and other legitimate businesses
- Placing money in stocks, bonds or life insurance products
- Using shell companies to obscure the ultimate beneficial owner and assets

Stage Three: Integration — Supply apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.

This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets.

Examples of integration transactions include:

- Purchasing luxury assets like property, artwork, jewelry or high-end automobiles
- Getting into financial arrangements or other ventures where investments can be made in business enterprises

1.5 The Economic and Social Consequences of Money Laundering

Increased Exposure to Organized Crime and Corruption: Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government, and citizens to criminals. Furthermore, the sheer magnitude of the economic power that accrues to criminals from money laundering has a corrupting effect on all elements of society.

Undermining the Legitimate Private Sector: 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.

Economic Distortion and Instability: Money launderers are not primarily interested in profit generation from their investments, but rather, in protecting their proceeds and hiding the illegal origin of the funds. 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.

Loss of Tax Revenue: 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.

Weakening Financial Institutions: Money laundering and terrorist financing can harm the soundness, financial strength, stability of financial institutions and thus weaken the country's financial sector.

Loss of Control of or Mistakes in, Decisions Regarding Economic Policy: Due to the large amounts of money involved in the money laundering process, in some emerging market countries, these illicit proceeds may dwarf government budgets and thus country faces challenges to formulate strong economic policy.

Risks to Privatization Efforts: Money laundering threatens the efforts of privatization of state-owned properties such as land, resources, or enterprises.

Social Costs: The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. Bribing of government officials undermines the moral fabric in society, and, by weakening collective ethical standards, corrupts our democratic institutions. When money laundering goes unchecked, it encourages the underlying criminal activity from which such money is generated.

Reputation Risk for the Country: A reputation as a money laundering or terrorist financing haven can harm development and economic growth in a country.

Risk of International Sanctions: In order to protect the financial system from money laundering and terrorist financing, the United States, the United Nations, the European Union, and other governing bodies may impose sanctions against foreign countries, entities or individuals, terrorists and terrorist groups, drug traffickers, and other security threats.

The adverse consequences of money laundering are reputational, operational, legal and concentration risks and include:

Reputational Risk: The potential that adverse publicity regarding an organization's business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organization. As an example, reputational risk for a bank represents the potential that borrowers, depositors and investors might stop doing business with the bank because of a money laundering scandal.

The loss of high-quality borrowers reduces profitable loans and increases the risk of the overall loan portfolio. Depositors may withdraw their funds. Moreover, funds placed on deposit with a bank may not be a reliable as a source of funding once depositors learn that the bank may not be stable. Depositors may be more willing to incur large penalties rather than leaving their funds in a questionable bank, resulting in unanticipated withdrawals, causing potential liquidity problems.

Operational Risk: The potential for loss resulting from inadequate internal processes, personnel or systems or from external events. Such losses can occur when institutions incur reduced or terminated inter-bank or correspondent banking services or an increased cost for these services. Increased borrowing or funding costs are also a component of operational risk.

Legal Risk: The potential for lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an organization, or even the closure of the organization. For instance, legitimate customers may become victims of a financial crime, lose money and sue the financial institution for reimbursement. There may be investigations conducted by regulators and/or law enforcement authorities, resulting in increased costs, as well as fines and other penalties. Also, certain contracts may be unenforceable due to fraud on the part of the criminal customer.

Concentration Risk: The potential for loss resulting from too much credit or loan exposure to one borrower or group of borrowers. Regulations usually restrict a bank's exposure to a single borrower or group of related borrowers. Lack of knowledge about a particular customer or who is behind the customer, or what the customer's relationship is to other borrowers, can place a bank at risk in this regard. This is particularly a concern where there are related counter-parties, connected borrowers, and a common source of income or assets for repayment. Loan losses can also result, of course, from unenforceable contracts and contracts made with fictitious persons.

Considering above risks, international bodies have issued statements such as the Basel Committee on Banking Supervision's 2014 guidelines on the Sound Management of Risks Related to Money Laundering and Financing of Terrorism and FATF's International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

1.6 Offence of Money Laundering and Punishment:

Punishment against Accused Reporting Organization as per provision of MLP Act, 2012

Clause No.	Nature of Offense	Punishment
23.3	Failing to submit required information within stipulated time	a) Penalty of Tk. 10,000/= per day up to maximum Tk. 5.00 lac, b) If such penalty is imposed more than 3 times in a financial year, license of the concerned Branch/ Booth/Agent can be cancelled.
23.4	Furnishing false statements	a) Penalty of minimum Tk. 20,000/= and maximum Tk. 5.00 lac, b) If such penalty is imposed more than 3 times in a financial year, license of the concerned Branch/ Booth/Agent can be cancelled.
23.5	Failing to comply with any instruction given by BFIU under the act	a) Penalty of Tk. 10,000/= per day up to maximum Tk. 5.00 lac for particular non-compliance issue, b) If such penalty is imposed more than 3 times in a financial year, license of the concerned Branch/ Booth/Agent can be cancelled.
23.6	Failing to comply with the instruction of section 23(1)(Ga) regarding Account Freezing or Suspend Order by BFIU.	Minimum Penalty of that Account Balance which will not more than double of balance as per instruction circulation date
23.7	Failing to pay the penalty as per section 23 & 25 of MLPA, 2012	Realize the amount by debiting self-named account of related person/entity/reporting agency with any Bank/Financial Institution/Bangladesh Bank and if any amount remains unpaid, suit will be filed for recovery of the same by the order of Court.
23.8	Penalty have been imposed to Owner, Director and employees under payroll or contract service of any reporting agency for noncompliance of AML & CFT instruction	Individual penalty of minimum Tk. 10,000/= and maximum Tk. 5.00 lac along with administrative disciplinary action.

Clause No.	Nature of Offense	Punishment
25.2	Any reporting organization failed to discharge their responsibility as per Article 25 (1) of the MLP Act, 2012 like preserving customers proper and full information, record keeping for Closed A/C for minimum 5 (five) years, failure of submission return/ sending STR to BFIU.	a) Penalty of minimum Tk. 50,000/= and maximum Tk. 25.00 lac. b) Additionally, license will be cancelled of that organization or branch, service center, booth of that organization.

Punishment against Accused Person or Entity as per provision of MLP Act, 2012

Clause No.	Nature of Offense	Punishment
4.2	Attempt, assist and make conspiracy for Money Laundering by any person.	Minimum 4 years and maximum 12 years of imprisonment with seizure of double the property acquired through ML or Tk. 10 (ten) lac which one is higher. Additionally, Court can order to forfeit the property acquired through ML or Predicate Offences of that person
4.4	Attempt, assist and make conspiracy by any entity.	Penalty of double the value of property acquired or Tk. 20 (Twenty) lac which one is higher with cancellation of registration/approval.
5	Defying attachment order for moveable properties.	Imprisonment up to 3 years or penalty to the value of attached property/properties or both.
6.3	Disclosure of information.	Imprisonment up to 2 years or penalty of maximum Tk. 50,000/= or both.
7.3	Obstructing or non-cooperating in enquiry process.	Imprisonment up to 01 year or penalty of maximum Tk. 25,000/=or both.
8.2	Providing false statements.	Imprisonment up to 3 years or penalty of maximum Tk. 50,000/= or both.

1.7 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 Anti-Terrorism Act, 2009 (including all amendments in 2012 & 2013).

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

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

Bangladesh has ratified this convention and criminalized terrorism or terrorist activities under section 6(1) of Anti-Terrorism Act, 2009 (including all amendments in 2012 & 2013) in line with the requirement set out in 9 (nine) conventions and protocols that were annexed in the convention.

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

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

   a. to carry out terrorist activity;

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

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

Terrorist activities — 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, confines or kidnaps any person or attempts to do the same, or damages or attempts to damage any property of any person, entity or the State;

   II. abets or instigates any person to murder, injure seriously, confine or kidnap any person, or abets or instigates to damage any property of any person or entity or the State; or

III. damages or tries to damage the property of any other person, entity or the state; or

IV. conspires or abets or instigates to damage the property of any other person, entity or the state; or

V. uses or keeps in possession any explosive substance, inflammable substance and arms for the purposes of sub clauses (i), (ii), (iii) and (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 an offence mentioned under section (a) sub-section (i), (ii), (iii), (iv) or (v);

c. for creating panic among the public or a section of the public with a view to compelling any international

d. organization to do any act or preventing them from doing any act, commit or attempts to commit or instigates or conspires or abets to commit an offence mentioned under section 6(1) (a) sub-section (i), (ii) & (iii);

e. knowingly uses or possesses any terrorist property;

f. abets, instigates, conspires to do or commits or attempts to commit an offence described in the UN conventions included in the Schedule-1 of Anti-Terrorism Act, 2009 (including all amendments in 2012 & 2013);

g. 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;

1.8 The Link between Money Laundering and Terrorist Financing

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

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

1.9 Targeted Financial Sanctions

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

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

b. **TFS related to Proliferation -**FATF recommendation 7 requires 'Countries' should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations'.

1.10 Powers and Responsibilities of BFIU in Preventing Money Laundering

In restraining and preventing the offence of money laundering:

a. For the purposes of the MLP Act, BFIU shall have the following powers and responsibilities, namely:

    i. to analyze or review information related to cash transactions and suspicious transactions received from any reporting organization and to collect additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data on the same and, as the case may be, provide with the said information to the relevant law enforcement agencies for taking necessary actions;

    ii. ask for any information or obtain a report from reporting organizations with regard to any transaction in which there are reasonable grounds to believe that the transaction involves in money laundering or a predicate offence;

    iii. issue an order to any reporting organization to suspend or freeze transactions of any account for a period not exceeding 30 (thirty) days if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing any offence: Provided that such order may be extended for additional period of a maximum of 6 (six) months by 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account;

iv. issue, from time to time, any directions necessary for the prevention of money laundering to the reporting organizations;

v. monitor whether the reporting organizations have properly submitted information and reports requested by BFIU and whether they have duly complied with the directions issued by it, and where necessary, carry out on-site inspections of the reporting organizations to ascertain the same;

vi. arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by BFIU;

vii. Carry out any other functions necessary for the purposes of this Act.

b. If any investigation agency makes a request to provide it with any information in any investigation relating to money laundering or suspicious transaction, then BFIU shall provide with such information where there is no obligation for it under any existing law or for any other reason.

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

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

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

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

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

h. If any reporting organization is imposed fine under this Act, BFIU may also impose a fine not less than taka 10 (ten) thousand but not exceeding taka 5 (five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

1.11 Responsibilities of Reporting Organizations in Preventing Money Laundering:

As a reporting organization PRIME BANK has the following responsibilities in the prevention of money laundering, (Section 25/1-4 of MLPA-2012) namely:

i. to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;

ii. if any account of a customer is closed, to preserve previous records of transactions of such account for at least 5(five) years from the date of such closure;

iii. to provide with the information maintained under paragraphs 1.11(i) and 1.11(ii) to BFIU from time to time, on its demand;

iv. if any doubtful transaction or attempt of such transaction as defined under clause (n) of section 2 is observed, to report the matter as suspicious transaction report to the BFIU immediately on its own accord.

1.12 International Initiatives towards AML/CFT:

In response to the growing concern about money laundering and terrorist activities, the initiatives taken by international community has acted on many fronts. This part of this Guidelines mentions names of the various international organizations and their initiatives relating to anti-money laundering (AML) and combating the financing of terrorism (CFT). These organizations have developed various documents, practices and instruments which can be useful in building awareness & knowledge on and combating the ML, FT&PF.

United Nations	The Financial Action Task Force	The Basel Committee on Banking Supervision	Other Organizations
• The Vienna Convention • The Palermo Convention • International Convention for the Suppression of the Financing of Terrorism • Security Council Resolution 1267 & Successors • Security Council Resolution 1373 • The Counter-Terrorism Committee • Global Program against Money Laundering	• FATF 40 Recommendations • FATF New Standards • Monitoring Members Progress • The NCCT List • ICRG	• Statement of Principles on Money Laundering • Basel Core Principles for Banking • Customer Due Diligence	• International Organization of Securities Commissions • The Egmont Group of Financial Intelligence Units • Asia Pacific Group on Money Laundering (APG)

1.13 National Initiatives on ML & TF:

In line with international efforts, Bangladesh has also taken many initiatives to prevent money laundering and combating financing of terrorism and proliferation of weapons of mass destructions considering their severe effects on the country.

National initiatives in AML/CFT aspect are as follows:

Legal Frame work	National Vigilance	Cooridantion with International Level	Others Inititives
• MLP Rules-2019 • MLPA 2012 & Amedment 2015 • ATA 2009, (Amend. 2012 & 2013) • BFIU-26, 25,24,23,22 and Guidance Notes on PEPs, STR, BO & PF, TBML prevention guidelines • Mutual Legal Assistane in Criminal Matters Act 2012 • Mutual Legal Assistane in Criminal Matters Rules 2012	• Central and Regional Taskforce • Bangladesh Financial Intelligence Unit (BFIU) • Inetligence Management • National Coordination Committee and Working Committee • Conference for CEO & CAMLCO on AML & CFT	• Founding Member of APG & CO-CHAIRS • Egmont Group Memberships • MoU Between BFIU with National & International parties • Coordination on the Implementaion of the UNSCR • Implementtion of recommenda-tions mentioned in the Mutual Evaluation Report	• New Risk Grading & KYC Profile Form • Implementation of goAML Software and CTR & STR/SAR reporting • Risk Based Supervision • Complaints/ Information Exchange and Dissemination with Domestic Authority • Implementation of eKYC , Agent Banking and AML & CFT Compliance.

Chapter 02

RISK BASED APPROACH (RBA)

2.1 What is the RBA?

According to FATF:

a. A RBA to AML/CFT means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

b. When assessing ML/TF risk, countries, competent authorities, and financial institutions should analyze and seek to understand how the ML/TF risks they identify may affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CFT risks, but it is still used for ML or TF purposes.

c. A RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low.

2.2 Obligation for ML&TF Risk Assessment and Management

a. According to "ML/TF Risk Assessment Guidelines for Banking Sector" issued by BFIU, bank will determine the ML and TF risk at regular definite time interval. In determining the risk, bank will consider bank's size/nature, product/services, customer, country/jurisdiction/geography. The risk assessment report will be used in preventing bank's ML and TF.

b. Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on anti-money laundering (AML) and combating terrorist financing (CTF) states that countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

c. Section 10 of MLP Rules-2019 states that every Reporting Organization-Financial Institution (RO-FI) shall conduct periodic risk assessment considering the Customer, Product, Delivery Channel & Geographical Location.

d. Money Laundering Prevention Act, 2012 empowers BFIU sufficiently to establish a sound and efficient AML&CFT regime. Every reporting agency has to comply with the instructions issued by BFIU under the power of Money Laundering Prevention Act (MLPA), 2012 and Anti-Terrorism Act (ATA), 2009 (including all amendments).

2.3 What is Risk assessment and Management?

Risk assessment and management is a systematic process and approach for identifying risks and developing methods to both minimize and manage those risks. This requires the development of a method to identify, prioritize, treat (deal with), control and monitor risk exposures. In risk management, a process is followed where the risks are assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

2.4 Which Risk do PRIME BANK Needs to Manage (identifying risks)

2.4.1 Risk Identification

The first step is to identify what ML&TF risks exist in PRIME BANK when providing designated services. Some examples of ML&TF risks associated with different banking activities are as follows:

a. **Retail banking:** provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services.

b. **Corporate banking:** where PRIME BANK provide corporate finance and corporate banking products and investment services to corporations, governments and institutions

c. **Wealth management:** culture of confidentiality, difficulty or ambiguity to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.

d. **Investment banking:** layering and integration transfer of assets between parties in exchange for cash or other assets, global nature of markets.

e. **Correspondent banking:** high value transactions, limited information about the remitter and beneficiary, source of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

f. **Trade services:** Price mis-invoicing (Over invoicing/under invoicing), unsatisfactory credit report of beneficiary/applicant, high-risk countries, sanctioned port/vessel/owner of vessel etc.

2.4.2 For the ML&TF aspects, BFIU expects from PRIME BANK risk management practices to address two main risks: business risk and regulatory risk.

a. **Business risk:** PRIME BANK must consider the risk posed by any element or any combination of the elements listed below:

- **Customers:** followings are some indicators (but not limited to) to identify ML&TF risk arises from customers of a bank:
  - ✓ a new customer;
  - ✓ a new customer who wants to carry out a large transaction;
  - ✓ a customer or a group of customers making lots of transactions to the same individual or group;
  - ✓ a customer who has a business which involves large amounts of cash;
  - ✓ a customer whose identification is difficult to check;

- ✓ a customer who brings in large amounts of used notes and/or small denominations;
- ✓ customers conducting their business relationship or transactions in unusual circumstances, such as: significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations;
- ✓ a non- resident customer;
- ✓ a corporate customer whose ownership structure is unusual and excessively complex;
- ✓ customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates;
- ✓ customers submits account documentation showing an unclear ownership structure;
- ✓ customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income.

- **Products and services:**
  - ✓ private banking i.e., prioritized or privileged banking;
  - ✓ credit card;
  - ✓ prepaid card;
  - ✓ anonymous transaction;
  - ✓ non face to face business relationship or transaction;
  - ✓ payment received from unknown or unrelated third parties;
  - ✓ any new product & service developed;
  - ✓ service to walk-in customers;
  - ✓ agent banking transactions;
  - ✓ mobile banking;
  - ✓ Internet banking/digital channel

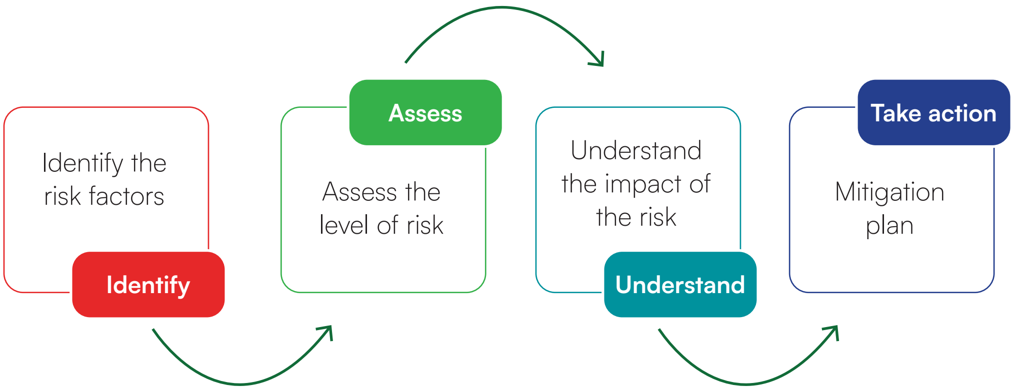
- **Business practices/delivery methods:**
  - ✓ direct to the customer;
  - ✓ online/internet;
  - ✓ phone;
  - ✓ Fax;
  - ✓ Email;
  - ✓ third-party agent or broker.
- **Channels /Countries it does business in/with (jurisdictions):**
  - ✓ any country which is identified by credible sources as having significant level of corruption and criminal activity;
  - ✓ any country subject to economic or trade sanctions;
  - ✓ any country known to be a tax haven and identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country;
  - ✓ any country identified by FATF or FSRBs as not having adequate AML&CFT system;
  - ✓ any country identified as destination of illicit financial flow.

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

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

- not submitting accurate information or statement requested by BFIU or BB.

2.5 Risk Management Process of PRIME BANK



2.5.1 Risk Assessment and Evaluation

a. Having identified the risks involved, they need to be assessed or measured in terms of the chance (likelihood) they may occur and the severity or amount of loss or damage (impact) which may result if they do occur. The risk associated with an event is a combination of the chance (likelihood) that the event may occur and the seriousness of the damage (impact) it may do. Therefore, each risk element can be rated by:

- the chance of the risk happening — 'likelihood' ; and
- the amount of loss or damage if the risk happened — 'impact' (consequence).

To help assess the risks identified in the first stage of this process, we can apply the risk rating scales for likelihood and impact and from these get a level of risk or risk score using the risk matrix.

LIKELIHOOD X IMPACT = RISK LEVEL/SCORE

b. **Likelihood Scale:** A likelihood scale refers to the potential of an ML&TF risk occurring in the business for the particular risk being assessed. Three levels of likelihood of an ML & TF risk are shown by BFIU, but the bank can have as many as they believe are necessary:

- **Very likely-** Almost certain, it will probably occur several times a year;
- **Likely-** High probability it will happen once a year ;
- **Unlikely-** Unlikely, but not impossible.

c. **Impact Scale:** An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen. Three levels of impact of an ML & TF risk are shown by BFIU, but the bank can have as many as they believe are necessary.

- **Major**-huge consequences, major damage or effect. Serious terrorist act or large-scale money laundering.

- **Moderate**-moderate level of money laundering or terrorism financing impact.

- **Minor**- minor or negligible consequences or effects.

d. **Risk Matrix and Risk Score:** Risk matrix can be used to combine LIKELIHOOD and IMPACT to obtain a risk score. The risks core may be used to aid decision making and help in deciding what action to take in view of the overall risk. Four levels of risk score of an ML & TF risk are shown by BFIU, but the bank can have as many as they believe are necessary:

LIKELIHOOD

Very Likely	**Medium 2**	**High 3**	**Extreme 4**
Likely	**Low 1**	**Medium 2**	**High 3**
Unlikely	**Low 1**	**Low 1**	**Medium 2**
	Minor	Moderate	Major

What is the chance it will happen?

How serious is the risk?

IMPACT

- **4 Extreme** - risks almost sure to happen and/or to have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level.

- **3 High-** risks likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.

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

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

e. **Risk Assessment and Management Exercise:** From the above discussion, PRIME BANK will have a strategy to calculate risk score by blending likelihood and impact, the risk matrix and risk score can assess the risks of individual customer, product/service, delivery channel and risks related to geographic region by implementing the simplified risk management worksheet. It can also fix up its necessary actions against the particular's outcomes of risks. All the exercises done by the banks would be called together "Risk Register" given in Annexure-A.

2.5.2 Monitoring and Review

It is essential for PRIME BANK to Keep records and regular evaluation of the risk management process and AML&CFT program. The risk management process and AML&CFT program cannot remain static as risks change over time; for example, changes to customer base, products and services, business practices and the law.

2.6 Ongoing Risk Monitoring

Ongoing monitoring of its risk management procedures and controls may also alert PRIME BANK to any potential failures including (but not limited to):

- failure to include all mandatory legislative components;
- failure to gain board and/or executive approval of the AML&CFT program;
- insufficient or inappropriate employee due diligence;
- frequency and level of risk awareness training not aligned with potential exposure to ML&TF risk(s);
- changes in business functions which are not reflected in the AML&CFT program (for example, the introduction of a new product or distribution channel);
- failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML&CFT program;
- legislation incorrectly interpreted and applied in relation to a customer identification procedure;
- customer identification and monitoring systems, policies and procedures that fail to:
- prompt, if appropriate, for further identification and/or verification when the ML&TF risk posed by a customer increases;
    - ✓ detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;
    - ✓ take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;
    - ✓ take appropriate action where the identification document provided is neither an original nor a certified copy;
    - ✓ recognize foreign identification documentation issued by a high risk jurisdiction
    - ✓ record comprehensive details of identification documents, for example, the date of issue;
    - ✓ consult appropriate resources in order to identify high-risk customers;

    - ✓ identify when an expired or old identification document (for example, a driver's license) has been used;
    - ✓ collect any other name(s) by which the customer is known;
- lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers;
- lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:
    - ✓ customer identification policies, procedures and systems;
    - ✓ identifying potential ML&TF risks
- acceptance of documentation that may not be readily verifiable.

2.7 Higher Risk Scenario

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations include the following:

a. Customer risk factors:

- The business relationship has been conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer);
- Non-resident customers;
- Legal persons or arrangements that are personal asset-holding vehicles;
- Companies that have nominee shareholders or shares in bearer form;
- Business that are cash-intensive;
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

b. Country or geographic risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML&CFT systems;
- FATF published Jurisdictions under Increased Monitoring and High-Risk Jurisdictions subject to a Call for Action;
- Countries subject to sanctions, embargos or similar measures;

- Countries identified by credible sources as having significant levels of corruption or other criminal activity;
- 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.

c. Product, service, transaction or delivery channel risk factors:

- Private banking;
- Anonymous transactions (which may include cash);
- Prepaid and Credit Card;
- Non-face-to-face business relationships or transactions;
- Foreign Exchange transactions (as per TBML Guidelines);
- Wire transfer (cross border remittance from or to FATF High Risk Jurisdictions);
- Payment received from unknown or un-associated third parties.

2.8 Lower Risk Scenario

There are circumstances where the risk of money laundering or terrorist financing may be lower. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

a. Customer risk factors:

- Banks — where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements;
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- Public administrations or enterprises.

b. Product, service, transaction or delivery channel risk factors:

- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

c. Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML&CFT systems;

- Countries identified by credible sources as having a low level of corruption or other criminal activity. In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

d. Note that having a lower money laundering and terrorist financing risk for identification and verification purposes does not necessarily mean that the same customer poses lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

2.9 Risk Variables

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

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

2.10 Counter Measures for Risks

a. Enhanced due diligence measures:

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

- Obtaining and verifying additional information through independent, reliable sources on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;
- Obtaining and verifying additional information on the intended nature of the business relationship;
- Obtaining and verifying information on the source of funds or source of wealth of the customer;
- Obtaining and verifying information on the reasons for intended or performed transactions;

- Obtaining and verifying the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

b. Simplified CDD measures

Where the risks of money laundering or terrorist financing are lower, PRIME BANK is allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are as setout BFIU-26 Section [3.5]:

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

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

2.11 Ongoing Due Diligence

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

Chapter 03

AML & CFT COMPLIANCE STRUCTURE OF PRIME BANK

3.1 Introduction

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. Banks can play a vital role in preventing ML, TF & PF and in this regard their roles and responsibilities are delineated in MLPA, 2012, ATA, 2009 and rules and instructions issued under this legal framework by BFIU. To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU, PRIME BANK has developed and maintaining an effective AML and CFT compliance program.

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

1. senior management role including their commitment to prevent ML, TF & PF;
2. internal policies, procedure and controls- it should include Bank'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 banks employees, member of the board of directors, owners and above all for the customers on AML & CFT issues.

3.2 Roles and Responsibilities of Board of Directors

The Board of Directors (Board) has the following roles and responsibilities:

a. shall understand their roles and responsibilities in managing ML/TF risks faced by the bank as reporting institution;

b. must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services;

c. understand the AML/CFT measures required by the laws including the MLPA-2012 (including all amendments in 2015), ATA-2009 (including all amendments in 2012 & 2013) and the industry's standards and best practices as well as the importance of implementing AML/CFT measures to prevent the bank from being abused by money launderers and financiers of terrorism;

d. maintain accountability and oversight for establishing AML/CFT policies and minimum standards;

e. approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;

f. establish appropriate mechanism to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the bank's products and services, technology as well as trends in ML/TF;

g. establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the bank;

h. define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

i. ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;

j. assess the implementation of the approved AML/CFT policies through regular reporting and updates by the Senior Management and Audit Committee; and

k. establish MIS that is reflective of the nature of the bank's operations, size of business, complexity of business operations and structure, risk profiles of products and services of offered and geographical coverage.

3.3 Statement of Commitment of MD & CEO

As a part of Senior Management, the MD & CEO communicates clearly to all employees at least on an annual basis that clearly sets forth its policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement is evidence of the strong commitment of the bank and the tone of senior management to comply with all laws and regulations designed to combat money laundering and terrorist financing. Statement of commitment of MD & CEO includes the followings:-

- bank's policy or 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; and

- consequences of non-compliance as per human resources (HR) policy of the bank.

3.4 Roles and Responsibilities of Senior Management

For the purposes of preventing ML, TF & PF, senior management includes members of the board of directors of the bank and the Managing Director & Chief Executive Officer of the bank. The Senior Management has the following roles and responsibilities:

a. be aware of and understand the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;

b. formulate AML/CFT policies & guidelines to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the bank and its geographical coverage;

c. establish appropriate mechanisms and formulate procedures to effectively implement AML/CFT policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

d. undertake review and propose to the Board the necessary enhancements to the AML/CFT policies to reflect changes in the bank's risk profiles, institutional and business structure, delivery channels and geographical coverage;

e. provide timely periodic reporting to the Board on the level of ML/TF risks facing the bank, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which may have an impact on the bank;

f. convey a clear signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service;

g. communicate clearly to all employees on an annual basis by a statement from the MD & CEO that clearly sets forth its policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement should evidence the strong commitment of the bank to comply with all laws and regulations designed to combat money laundering and terrorist financing;

h. allocate adequate resources to effectively implement and administer AML/CFT compliance programs that are reflective of the size and complexity of the bank's operations and risk profiles;

i. appoint a chief anti-money laundering compliance officer (CAMLCO) at management level at Head Office and designate a compliance officer at management level at each branch or subsidiary;

j. provide appropriate level of AML/CFT training for its employees at all levels throughout the organization;

k. ensure that bank's HR Policy includes at least following issues for proper implementation of AML &CFT measures:

   i. proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;

   ii. proper weight should be given in the annual performance evaluation of employees for extra ordinary preventive action vis-a-vis for non-compliance;

   iii. written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;

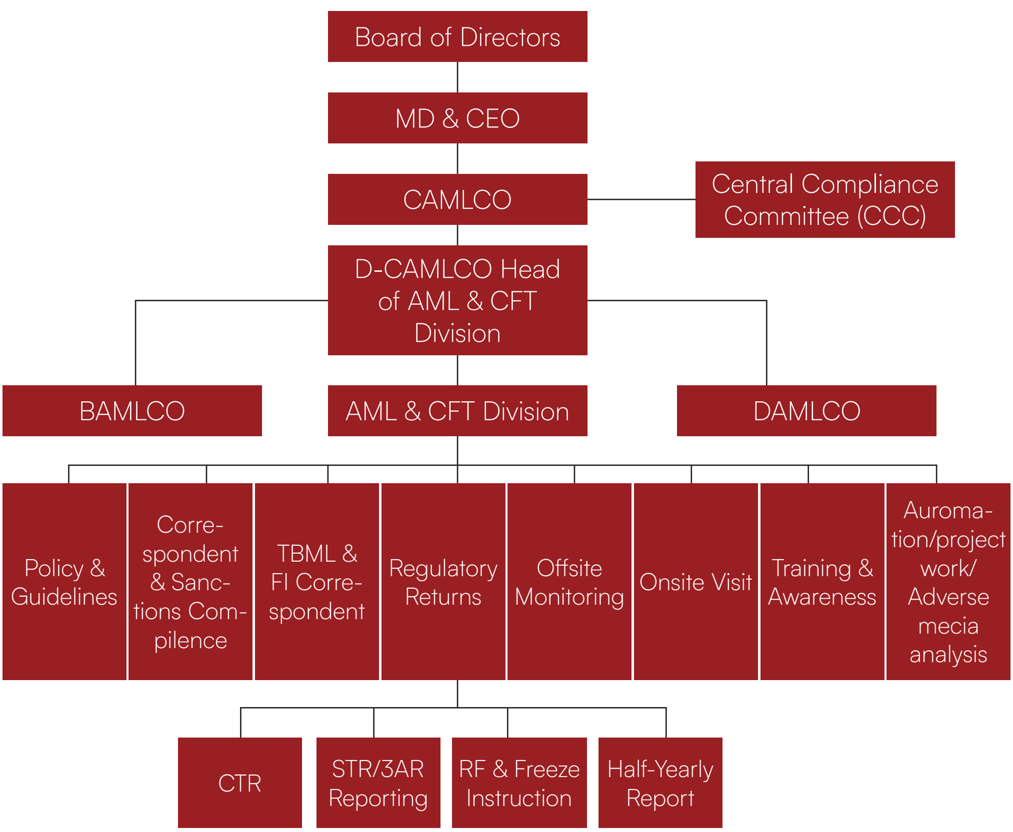
   iv. other measures that shall be taken in case of non-compliance by the bank;

l. ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees;

m. ensure that AML/CFT issues raised are addressed in a timely manner; and

n. ensure the integrity of its employees by establishing appropriate employee assessment system.

Organizational Structure for Implementation of AML & CFT Program



Adequate human resources and other logistic support shall be provided to AML & CFT Division based on the size and customer base of the bank and considering the complexity, sensitivity, introduction of new technology, increase efficiency.

3.6 Central Compliance Committee (CCC)

Obligations under BFIU Circular   Section 1.3 of BFIU Circular-26; dated- 16.06.2020

To keep the bank free from the risks related to Money Laundering & Terrorist Financing and for the effective/proper compliance of all existing acts, rules and instructions issued by BFIU time-to-time, PRIME BANK set up a Central Compliance Committee (CCC) that will be headed by CAMLCO and report to MD & CEO.

Formation of CCC:

- CCC shall be established in the head office of the bank as a permanent set-up with a specific organogram and headed by a high official who will be called as the 'Chief Anti Money Laundering Compliance Officer' (CAMLCO). In this case, 'High official' will be considered as an official up to 2 (two) steps below the managing director/ chief executive officer.

- PRIME BANK has to nominate one deputy of the CAMLCO, who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (D-CAMLCO). The D-CAMLCO will be at least in the rank of 'Senior Vice President' of the bank.

- It will be comprised of adequate number of members but not less than 7 (seven) members and will include senior management of the bank along with CAMLCO & D-CAMLCO. The other officials in the CCC, should be from several divisions like Human Resources, Operations Division, CniB, Emerging Market, Transaction Banking Division, Consumer Banking, MSME, CRM, CAD, Trade Services Division, International Division/FI, Risk Management Division, Card, IT and AML & CFT Division and none from Internal Audit Division/Department.

- Subject to approval of MD & CEO or CAMLCO or CCC, new member may be added in the Committee. However, regarding adoption of member on ad-hoc basis, CAMLCO's approval suffices. In line with the requirement of combating money laundering and terrorist financing, members can be selected from related divisions to participate subject to approval of CAMLCO. If any member of CCC absent more then 2 (two) meeting of CCC in a calendar year, CAMLCO or CCC may add/replace new/existing member of the Committee.

- The CAMLCO, D-CAMLCO and other members of the CCC must have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU or Bangladesh Bank from time to time and international standards on preventing ML, TF& PF.

- CCC shall be an independent committee/body and shall be completely separated from Internal Audit. To ensure this autonomy there shall not be any member from Internal Audit to CCC and vis-a-vis, but there shall have to be enough co-ordination and co-operation in performing their responsibility and information exchange.

- Based on the functional and operational requirement, CCC may form subcommittee for specific tenor. However, such tenor shall be limited to 360 days.
- Committee shall be operated under the direct supervision of CAMLCO and will report to MD & CEO or Board of Directors (if applicable) regarding Bank's AML & CFT Program.

Secretariat:

AML & CFT Division shall act as secretariat to the committee.

Operations:

Committee shall meet at least four (04) times at quarterly intervals; however, meetings preferably will be held within January- March, April- June, July-September and October—December. 55% of the members shall form quorum while standard decision-making process shall be adopted. Committee may request participation of related other divisions to attend on need basis and they shall do so. Meeting minutes of the Committee may be circulated in the CCC members and related divisions for information and necessary action.

Reporting:

This CCC will submit a half-yearly (January-June & June-December) report to MD & CEO for the information and guidance on the steps, progress and recommendation regarding AML & CFT. After review, guidance, comments and remarks of MD&CEO, the above half-yearly report will be submitted to the PRIME BANK Board of Directors and a copy of the report will be submitted to Bangladesh Financial Intelligence Unit (BFIU) on a half-yearly basis within 60 days after completion of the respective half year.

Authorities & Responsibilities of CCC:

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

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

For shouldering the responsibilities Senior Management of PRIME BANK has given the following authorities to CCC:

- appointment of BAMLCO and assign their specific job responsibilities at Branch and Sub-Branch.
- appointment of DAMLCO and assign their specific job responsibilities at selective divisions of Head Office.
- requisition of human resources and logistic supports for CCC / AML & CFT Division.
- make suggestion or administrative sanction for non-compliance by the employees.
- provide necessary instruction & directives to AML & CFT Division.
- Authorized to seek any kind of documents or data from Branches / Divisions / Offshore Banking Units /Foreign Subsidiaries.

3.7 Separation of CCC from Internal Audit Division

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

3.8 Chief Anti Money Laundering Compliance Officer (CAMLCO)

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

Authorities of CAMLCO:

CAMLCO must have sufficient authority to implement and enforce corporate wide AML policy, procedure & measure and shall report directly to the MD & CEO and the Board of Directors. The authorities must include at least the followings:

- CAMLCO shall exercise the authorities of the CCC as Head of the Committee.
- CAMLCO shall be able to act on his own authority.
- He/she shall not take any permission or consultation from/with the MD & CEO before submission of STR/SAR and any document or information to BFIU.
- He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU.
- He/she have access to any information of the bank.
- He/she shall ensure his/her continuing competence.
- Depending on the scale and nature of the bank the designated CAMLCO may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions.

Responsibilities of CAMLCO:

The CAMLCO is responsible for overall oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering, terrorist financing and proliferation financing. Few of the responsibilities are:

- CAMLCO must take all the responsibilities of CCC as Head of the Committee.
- CAMLCO must ensure overall AML&CFT compliance of the bank.
- He/she shall oversee the submission of STR/SAR or any document or information to BFIU in time.
- He/she shall maintain the day-to-day operation of the bank's AML&CFT compliance.
- CAMLCO shall be liable to MD & CEO or Board of Directors for proper functioning of CCC.
- CAMLCO shall review and update ML & TF risk assessment& management of the bank.
- He/she shall ensure that corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.
- He/she shall oversee all other issues that may arise from time to time regarding ML, TF & PF.

3.9 Authorities & Responsibilities of D-CAMLCO

- The authorities & responsibilities of D-CAMLCO shall be same as the authorities & responsibilities of CAMLCO but he/she must discharge his/her authorities and responsibilities under command, control & supervision of CAMLCO.

- D-CAMLCO shall exercise the authorities of the CCC as Head of AML & CFT Division.
- D-CAMLCO shall work as a member secretary of Central Compliance Committee (CCC).
- Analyzing & evaluating the self-assessment report and making recommendations.
- Analyzing & evaluating the independent testing procedure and making recommendations.
- Analyzing & evaluating the STRs for sufficiency of data & documents.
- Ensuring the CDD & EDD measures for PEPs, IPs, chief executives of international organizations, non-face-to-face customers and other high-risk customers; and monitoring the transactions of such accounts.
- Conducting inspection in the branches, sub-branches and/or subsidiaries and preparing reports there against for submission to CAMLCO.
- Designing, imparting & evaluating trainings, workshops and seminars related to AML & CFT for the employee of the bank.
- Ensuring the timely submission of required reports to BFIU.
- Ensuring the all record keeping requirements in-favor of CCC related to AML/CFT issues.
- Moreover, he/she will be act as Current Charge in absence of CAMLCO.

3.10 Roles & Responsibilities of AML & CFT Division

- Deputy CAMLCO shall lead the AML &CFT Division.
- AML & CFT Division shall work as secretariat of CCC.
- AML & CFT Division support CCC to implement the AML & CFT program of the PRIME BANK.
- Under Deputy CAMLCO, AML & CFT Division shall facilitate and enforce operational activity of ML/TF related issues.
- AML & CFT Division shall conduct the surprise visit, AML process development work, onsite/offsite monitoring, enhance AML status of branch/division based on Internal Audit Division ITP or Branch Self-Assessment report or offsite monitoring report.
- AML & CFT Division shall conduct the onsite/off-site visit on branches/divisions (as per AML annual approved work plan) & every foreign subsidiary of PRIME BANK at least once in every 2 years.
- Analyzing & evaluating the self-assessment report and communication with Branches.
- Analyzing & evaluating the independent testing procedure and informed to D-CAMLCO;
- Analyzing & evaluating the STRs/SARs for sufficiency of data & documents.

- Obtaining approval from CAMLCO/D-CAMLCO for PEPs, IPs, chief executives of international organizations of such accounts.
- Designing, imparting & evaluating trainings, workshops and seminars related to AML & CFT for the employee of the bank and provide certificate as well.
- Ensuring the timely submission of required reports to BFIU.
- Forward STR/SAR and CTR to BFIU in time and in proper manner.
- Ensuring the all record keeping requirements in-favor of CCC for AML/CFT issues.
- AML & CFT Division shall be liable to Deputy CAMLCO/CAMLCO/CCC.
- AML & CFT Division is authorized to seek any kind of documents or data from Branches / Divisions / Offshore Banking Unit /Foreign Subsidiaries related to AML & CFT issues.
- AML & CFT Division is authorized to communicate with BFIU officials directly as required time to time with regards to AML/CFT. Mode of communication may be over phone or mail or goAML or physical visitation etc;
- Communication between Division/Departments & Branches — AML & CFT Division may collect update/compliance report from the concerned Branches/divisions/ departments based on bank's Internal audit department inspection report (ITP, Other Special inspection related AML &CTF), regulators & external auditor inspection report.

3.11 Branch Anti Money Laundering Compliance Officer (BAMLCO)

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

The Head of Branch (HoB) or Branch Operation Manager (BoM) of the branch shall be nominated as the BAMLCO. In-charge of sub-branch will be will play the role of BAMLCO. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her office order as per this guideline. CCC has given the authority to Head of Branch to sign the BAMLCO Office Order. If HoB plays the role of BAMLCO in branch, the office order should be signed by Head of BDN. For sub-branch, the BAMLCO office order shall be signed by the HoB of mother branch. The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and bank's own policies on preventing Money Laundering and Terrorist Financing. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her office order.

Authorities of BAMLCO:

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

- Know Your Customer;
- Transaction monitoring;

- Identifying and reporting of Suspicious Transactions;
- Sanction Screening;
- Self-Assessment;
- Record keeping;
- Training.

Responsibilities of BAMLCO:

For preventing ML, TF & PF in the branch & sub-branch, the BAMLCO shall perform the following responsibilities:

- ensure proper implementation of PRIME BANK Customer Acceptance Policy (CAP) at Branch level before establishing any business relationship or while opening a new account;
- ensure that the KYC of all customers have done properly and for the new customer KYC is being done properly with proper identification;
- ensure that the Bank's approved Sanctions List & PEPs list checked properly before the opening of account and/or banking relationship and /or while making any international transaction;
- obtain approval from CAMLCO while opening any account related to Politically Exposed Persons (PEPs) or Influential Persons (IPs) & Chief or similar high-ranking positions in an international organization;
- Ensure accurate & complete information in Uniform Account Opening Form;
- Ensure proper Risk grading in KYC Profile Form & T24 for new customer, review risk grading score in case any changes of existing customer information or in the KYC process according to BFIU-26 section [3.6];
- Ensure EDD and proper monitoring for High Risk Account;
- Assess the Transaction Profile (TP) for new & existing customers and ensure the review process according to BFIU-26 section [3.6];
- keep information of 'legacy dormant accounts' or 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;
- ensure regular transaction monitoring to find out any unusual transaction;
- review cash transaction to find out any structuring;
- review of CTR to find out 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 on half yearly basis;
- arrange quarterly meetings on AML&CFT issues;
- accumulate the training records of branch officials and take initiatives including reporting to AML & CFT Division or HRTDC;
- ensure all the required information and document are submitted properly to CCC/AML & CFT Division and any freeze order or stop payment order are implemented properly;
- follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, illicit outflow / capital flight, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
- ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements of chapter 13 of this guidelines;
- ensure that corrective actions have been taken by the branch to address the deficiency identified by the BFIU or AML & CFT Division or Internal Audit Department or any external audit firm;

3.12 Roles & Responsibilities of Account Opening Officer/Teller/Customer Service/ Relationship Manager

- Perform due diligence on prospective clients' prior opening an account;
- Be diligent regarding the identification(s) of account holder and the transactions relating to the account;
- Ensure all required documentation is completed satisfactorily;
- Complete the KYC Profile Form for the new customer;
- Ongoing monitoring of customer 's KYC profile and transaction activity;
- Obtain documentary evidence of large cash deposits;
- Analyze fair or justified price and obtain sufficient document, in case of Trade;
- Escalate any suspicion to the BAMLCO/DAMLCO/ Supervisor.

3.13 Departmental/Divisional Anti Money Laundering Compliance Officer (DAMLCO)

- DAMLCO is the first point of contact in case of any AML & CFT issues of concerned department. They must familiar with the requirements of existing acts, rules and regulations, BFIU's instructions and bank's own policies to prevent Money Laundering and Terrorist Financing.
- CAMLCO/CCC/Head of Division shall appoint the DAMLCO from selective Divisions of Head Office;

- DAMLCO shall have sufficient operational knowledge on his/her Division;
- DAMLCO shall Understand ML/TF risk;
- DAMLCO shall have sufficient knowledge on PRIME BANK Sanctions Screening System;
- DAMLCO shall have sufficient knowledge on KYC/CDD
- Clear job descriptions and responsibilities of DAMLCO shall be mentioned in his/her JD according to associated task related to his/her division on AML & CFT;
- The role and responsibilities of DAMLCO shall be according to the job nature of respective Division;
- Escalate any suspicion to the AML & CFT Division through Head of Division;
- Create awareness among the officials of Divisions/Departments;

3.14 Roles & Responsibilities of Internal Audit Division

- Internal Audit Division of the bank shall play an important role for ensuring proper implementation of bank's AML & CFT Compliance Program. Bank shall ensure that Internal Audit Division is equipped with enough manpower and autonomy to look after the prevention of ML, TF& PF.
- The Internal Audit Division shall oversee the implementation of the AML & CFT compliance program of the bank and has to review the 'Self-Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.
- Internal Audit Division shall be well resourced and enjoy a degree of independence within the bank. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable, according to BFIU Circular-26 section 8.2[1]. In case of finding any High Risk issue related to ML & TF, should report it to CAMLCO immediately.
- Internal Audit Division shall conduct inspection at least 10% Branches of PRIME BANK, specially on AML & CFT according to BFIU Circular-26 section 8.2[2] .
- Internal Audit Division shall send the report containing AML & CFT audit/inspection rating of the branch to AML & CFT Division and Compliance Department of ICCD.
- For agent banking, Internal Audit Division shall conduct inspection at least 5% agents of bank on their AML & CFT activities and send the report to AML & CFT Division.

The internal audit must:

- understand ML & TF risk of the bank and check the adequacy of the mitigating measures;

- examine the overall integrity and effectiveness of the AML/CFT Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML & CFT Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU or Bangladesh Bank;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;

3.15 Compliance Department of ICCD

- Compliance management is an integral part of the operations of a bank. Compliance Department under ICCD of Head Office shall also play an important role in order to avoid Money Laundering & Terrorist Financing consequences of non-compliance by Branches/Divisions/Department of PRIME BANK.
- Communication between Division/Departments& Branches — Compliance division should collect update/compliance report from the concerned Branches/divisions/departments based on bank's Internal audit department inspection report (ITP, Other Special inspection related AML &CTF), regulatory & external auditor inspection report.
- Compliance Department must closely monitor non-compliance issues related to AML & CFT to ensure meticulous compliance.

Chapter 04

CUSTOMER ACCEPTANCE POLICY (CAP)

While stiff competition is forcing banks to pay more attention to satisfy customers' needs, it is also essential to ensure that an effective Customer Due Diligence is in place as part of bank's risk management policies. Although, customers are the focal point of bank activities sometimes they pose the risk of money laundering and financing of terrorism thereby putting the interest of the bank at stake. Know Your Customer (KYC) program to have sufficiently verified/ authenticated information about customers is vital and most effective defense against Money Laundering (ML) and Terrorism Financing (TF). As such, inadequacy in KYC standard can result in serious customer and counterparty risks, especially, reputational, operational, legal and compliance risks. Collecting sufficient information about the customers is the most effective defense against banks' being used as the medium to launder the proceeds of crimes and to finance the terrorist activities through accounts. As per regulatory requirement PRIME BANK needs to keep complete and accurate information of its customers. It is also the responsibility of PRIME BANK to identify suspicious transactions of their customers with due care and diligence. Pursuant to above legal requirement.

4.1 Objectives

PRIME BANK has developed this customer acceptance policy with a view to:

a. manage any risk that the services provided by the Bank may be exposed to;

b. prevent the Bank from being used, intentionally or unintentionally, for ML/TF purposes;

c. identify customers who are likely to pose a higher than average risk.

4.2 Who are Customers?

For the purposes of these guidelines, a customer includes:

a. a person or entity that maintains an account and/or has a business relationship with the bank.

b. one on whose behalf the account is maintained (i.e. the beneficial owner).

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

d. any person or entity connecting high value occasional transaction or a transaction which can pose significant reputational or other risks to the bank (i.e. occasional transaction means a transaction which is unusual considering customer occupation or profile).

4.3 Customer Acceptance Policy

4.3.1 General Requirements

Branch, Authorized Subsidiaries and/or concerned Division of Head Office shall ensure the following aspects while establishing relationship with a customer or providing any banking services or conducting transactions and considering the instruction of BFIU Circular No.26:

a. No account shall be opened or operated by violation of AML/CFT laws and rules of Bangladesh Government;

b. No account and/or banking relationship shall be opened or established in the name of any person or entity or country listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance adopted under Chapter VII of the Charter of UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government according to section 18 of ATA-2009 and associated with the entities those sanctioned by the agencies that the Bank refers to like, OFAC, EU, HMT, HKMA, MAS, domestic Sanctions list and PRIME BANK Own Negative list.

c. Bank shall not establish any correspondent relationship/s with the shell Bank and / or the Foreign Financial Institution/s that deal with shell Bank. Any identified business relationship/s with the financial institution/s that allow the transaction of shell bank, shall be discontinued.

d. Bank shall not establish any RMA with the Bank that delisted by SWIFT.

e. No account shall be opened in the name altering from the primary identity document, anonymous or fictitious (benami) name(s), blank names or numeric/alphanumeric characters.

f. Accounts shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identity document of the person/entity. Accounts may however be opened with different account titles identifying the nature/ use/purpose/type/ of account at the written request of the legal person/organization with appropriate control parameters.

g. No account or business relationship shall be opened or operated by PRIME BANK that are identified as Casinos, Gambling, Marijuana related entities, Red light business/ adult entertainment, Shell bank, shell company, unregulated charities, virtual asset service provider, Betting and deals with Bit Coin/Crypto currency or virtual currencies or same nature of business/enterprises.

h. Not to open an account where the staff/s designated to open new accounts, find sufficient ground/s that the identity of the prospective customer/s could not be verified and/or the prospective customer/s is not disclosing the required identity, the reason for opening account, transaction frequency and volume, etc. and any other such information/s deemed necessary for account opening. The refusal shall be documented properly and shall be communicated to the CAMLCO/D-CAMLCO/ AML & CFT Division Compliance Officer through BAMLCO.

i. Not to open an account or allow withdrawal of money or close an existing account where the bank is unable to apply appropriate customer due diligence measures, i.e., bank is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the branch. However, Branch should be careful to avoid harassment of customers.

j. No account or business relationship shall be opened or operated related to existing freeze accounts, those furnished by regulators.

k. Customers are to be categorized into low & high risks ones for identified risks in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc;

l. For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of CDD are to be met.

m. In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & jewelry and precious metal shall also be categorized as 'high risk' requiring enhanced due diligence. Other examples of high risk customers requiring enhanced due diligence include:

    i. Correspondent bank customer located in High Risk Jurisdiction & MSBs;

    ii. trusts, charities, NGOs, NPOs, MLM and religious organizations receiving donations;

    iii. account of arms dealer, atomic power extractive industries;

    iv. accounts of Embassy and consulate office;

    v. companies having shareholding or beneficial ownership with PEPs/IPs or their family members and/or close associates;

    vi. high net worth individuals;

    vii. firms with 'sleeping partners';

    viii. politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;

    ix. influential persons (IPs), customers who are close relatives of IPs and accounts of which a IP is the ultimate beneficial owner;

    x. chief executive or top level officials of any international organization, customers who are close relatives of chief executive or top level officials of any international organization and accounts of which a chief executive or top level officials of any international organization is the ultimate beneficial owner;

    xi. non-face to face customers (except SMF KYC as per e-KYC guidelines); and

    xii. those with dubious reputation as per public information available etc.

n. apply enhanced due diligence 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 terrorist financing (such as the countries and territories enlisted as High—Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force's Public Statement).

o. In addition to what has been indicated above, it is required to take steps to identify and assess their ML/TF risk for customers, products & services, transactions, delivery channels, countries and geographical areas; and effectively manage and mitigate their risk adopting a risk-based approach as indicated in these guidelines. As a corollary, it is also required to adopt enhanced measures for products, services and customers with a high risk rating.

p. In this regard, further guidance can be taken from MLPA-2012 (including all amendments -2015), ATA-2009 (including all amendments -2012 & 2013) & BFIU Master Circular no.26 dated 16-06-2020 & other Directives of BFIU from time to time. A risk register (annexure A) is added with these guidelines for guidance & meticulous compliance.

q. Unique customer identification code for any customer who maintains more than one account or availing more than one facilities shall be used. Such unique identification system shall facilitate banks to avoid redundancy, and saves time and resources. This mechanism also enables banks to monitor customer transactions effectively.

r. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of MLPA-2012 (including all amendments -2015), ATA-2009 (including all amendments -2012 & 2013) & BFIU Directives from time to time;

s. Decision by a branch to close an account should be taken from High Official/Line Management after giving due notice to the customer explaining the reasons for such a decision.

t. Circumstances, in which a customer is permitted to act on behalf of another person/ entity or when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity, must be in conformity with the established law and practice of banking and appropriate EDD to be applied;

u. Accounts for the non-resident Bangladesh citizens are to be opened subject to compliance of Foreign Exchange Regulation Act, 1947 and circulars issued by BFIU or Bangladesh Bank under it.

v. No account or business relationship shall be opened or operated with customers/staffs those are related/convicted with any fraud activities within PRIME BANK or customers in PRIME BANK own negative list.

The customer identification process does not end at the point of application. Once account relationship has been established, reasonable steps should be taken by the branch from time to time to ensure that descriptive information is kept updated at least on 5 years' intervals for low risk accounts and on annual intervals for high risk accounts.

In developing customer acceptance policy, the following important factors are required to be taken into consideration:

i) Customer's background

ii) Country of origin

iii) Public or high profile position

iv) Linked accounts

v) Volume of business activities

vi) Risks associated in the business of customers

vii) Basic requirements for Account Opening

viii) All information available for judging the creditworthiness of borrowers

ix) All information on walk-in customers as required in AML circular.

It is important to bear in mind that the implementation of this customer acceptance policy must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

CHAPTER 05

KYC, CDD, EDD & TRANSACTION MONITORING

5.1 Introduction

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources.

The CDD obligations on banks under legislation and regulation are designed to make it more difficult to abuse the banking industry for money laundering or terrorist financing. The CDD obligations compel banks to understand who their customers are to guard against the risk of committing offences under MLPA, 2012 (with amendments in 2015) including 'Predicate Offences' and the relevant offences under ATA, 2009 (with amendments in 2012 & 2013).

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

a. Risk in Product/Service;

b. Nature of on-boarding;

c. Geographical Risk;

d. Relationship Risk;

e. Transaction related Risk;

f. Transparency Risk;

g. Risk related to customer's business & profession;

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

5.1.1 Standard KYC Information

a. KYC procedures refer to knowing a customer physically and financially. This means to conduct an effective KYC, it is essential to accumulate complete and accurate information about the prospective customer. Complete refers to combination of all information for verifying the identity of the person or entity and accurate refers to such complete information that has been verified for accuracy.

b. Branches or authorized subsidiaries or concerned Head Office Divisions are required to collect complete & accurate KYC information of the customer before or during establishing business relationship or carrying out any occasional transaction as per bank's account opening form and/or any other applicable printed forms duly approved by the Bank and/or KYC forms.

c. Branches or authorized subsidiaries or concerned Head Office Divisions may collect additional information about the KYC & the purpose and intended nature of the business relationship in addition to paragraph 5.1.1(b) up to their satisfaction which are required to conduct appropriate due diligence considering the risk of the customer in the light of existing directions.

d. Branches or authorized subsidiaries or concerned Head Office Divisions are required to comply the requirements of customer acceptance policy as specified in the chapter 4(four) of this Guidelines.

e. Detail has been set out in Annexure-B (KYC Documentation).

5.2 What is Required for CDD?

Branches or authorized subsidiaries or concerned Head Office Divisions are required to:

a. identify the customer and verify that customer's identity using reliable, independent source documents, data or information, i.e., complete &accurate information of the customer;

b. verify that any person purporting to act on behalf of the customer is so authorized, and also verify the identity of that person i.e. complete & accurate information of the authorized person(s);

c. Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the branch or authorized subsidiary or concerned Head Office Division is satisfied that it knows who the beneficial owner is. It includes collection & preservation of:

    i. **Complete & accurate** information of the person(s) on whose behalf the customer operates the account;

    ii. complete & accurate information of the person(s) who control(s) the customer; and

    iii. in case of company, complete & accurate information of the shareholder who controls the company or has 20% or more shares of the company;

d. understand and, where relevant, obtain information on, the purpose and intended nature of the business relationship.

5.3 When CDD is Required (Timing of CDD)?

Branches or authorized subsidiaries or concerned Head Office Divisions are required to conduct CDD on the customer and the person conducting the transaction, when:

a. establishing business relationships including opening accounts;

b. providing wire transfer (remittance) services [e.g. BEFTN, EFT, RTGS & etc];

c. providing money or value transfer (remittance) services;

d. providing trade finance and trade service facilities;

e. while selling bank's own products, issuing credit cards, payment of dues of credit cards and reloading of prepaid/travel cards and any other product;

f. carrying out occasional transactions;

g. while reactivate a dormant account as per BB instructions;

h. while allowing mandate to operate an account;

i. it has any suspicion of ML/TF, regardless of amount; or

j. it has any doubt about the veracity or adequacy of previously obtained information.

5.4 Risk Grading and Applicable CDD

a. Branch or authorized subsidiary of concerned Head Office Division shall review the KYC & other information they have collected (paragraph 5.1.1) for each new customer, assess & evaluate the risk of the customer and categorize them into two groups: high risk customers & low risk customers.

b. The nature and extent of due diligence will depend on the risk perceived by the branch or authorized subsidiary or concerned Head Office Division. However, while preparing customer's risk category branch or authorized subsidiary of concerned Head Office Division should take care to seek only such information from the customer, which is relevant to the risk category.

c. For the purpose of risk categorization, branch or authorized subsidiary of concerned Head Office Division shall follow the instructions as specified in the chapter 2(two) of this Guidelines.

d. Branch or authorized subsidiary of concerned Head Office Division shall apply normal customer due diligence measures in case of individuals or legal entities or legal arrangements scored with low risk.

e. Branch or authorized subsidiary of concerned Head Office Division shall apply enhanced due diligence in case of individuals or legal entities or legal arrangements scored with high risk.

f. Branch or authorized subsidiary of concerned Head Office Division shall also apply enhanced due diligence in case of Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes.

g. The account of NGO, NPO, MLM Company, PEP, IP and their family members or close associates will be always treated as HIGH Risk on subjective judgement.

5.5 Simplified Customer Due Diligence

Simplified CDD never means an exemption from CDD measures. A simplified set of CDD measures may be basic and minimal according to BFIU Circular-26 Section [3.5]. In line with the RBA, it is the timing, intensity and the extent of customer information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level.

a. Branch official or official of authorized subsidiary of concerned Head Office Division shall obtain information of Applicant/Sender, Beneficiary/Receiver name & address and Applicant/Sender contact number for any transaction below BDT 50,000.00 by Walk-in Customer / non account holder/ bearer.

b. Branch official or official of authorized subsidiary of concerned Head Office Division shall obtain Standard information with attested photo ID of Depositor/Withdrawer/ Applicant/Sender / Beneficiary/Receiver for any transaction amount from BDT 50,000.00 to BDT 5,00,000.00 by Walk-in Customer / non account holder/ bearer.

c. Branch official or official of authorized subsidiary of concerned Head Office Division shall obtain complete KYC of Depositor/Withdrawer/ Applicant/Sender / Beneficiary/ Receiver for any transaction amount BDT 5,00,000.00 & above by Walk-in Customer / non account holder/ bearer.

d. Simplified CDD also enforced for the purpose of financial inclusion opening of low risk account of student, farmer and other No-Frill.

5.6 Customer Due Diligence Process and Digital Financial Inclusion (according to BFIU Circular-26 Section [3.16])

a. Digital financial inclusion refers broadly to the use of digital financial products and services to advance financial inclusion. It involves the deployment of digital means to reach financially excluded and underserved populations with a range of regulated financial services tailored to their needs, delivered responsibly at a cost affordable to customers and sustainable for providers. “Digital financial services” covers financial products and services, including payments, transfers, savings, credit, insurance, securities, financial planning and account statements. They are delivered via digital/ electronic technology such as e-money (initiated either online or on a mobile phone), payment cards and regular bank accounts.

b. Increasingly, digital financial inclusion also includes the use of digital identity products and services to provide individuals with proof of identity for CDD purposes (though conventional and other alternative means of identifying customers and verifying identity may also be used). It also increasingly involves technological solutions like NID verification through Bangladesh Election Commission NID database or future API.

c. Branch official or official of authorized subsidiary of concerned Head Office Division shall follow BFIU Circular No. 25 & 20.

5.7 Ongoing CDD Measures (Review and Update- according to BFIU Circular-26 Section [3.6.4])

a. Branch or authorized subsidiary or concerned Head Office Division shall take necessary measures to review and update the KYC of the low risk customers in every five (05) years & high risk customers in every year.

b. Branch or authorized subsidiary or concerned Head Office Division shall update the changes in any information on the KYC as soon as they get to be informed. Moreover, they should update KYC information anytime if there is any particular necessity realized.

c. Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay.

d. Any subsequent change to the customer's name, address, or employment details of which the branch or authorized subsidiary or concerned Head Office Division becomes aware shall be recorded as part of the CDD process.

e. Reviewing the nature of the customer, the source of money in the account and the nature of transactions from 6 to 12 months of establishing business relation and assessing the effectiveness with a logical consideration, branch or authorized subsidiary or concerned Head Office Division shall again collect the Transaction Profile along with the amendments in it from the customer.

f. Information in Core Banking Solution (TEMENOS T24) & AOF — Branches or Concern Division/Department of Head Office should ensure data input/update.

g. Branches or Concern Division/Department of Head Office should ensure proper Risk Grading of Customer's Account.

h. KYC Profile/Digital KYC Profile with Risk Grading and total risk score should be preserved in System (digitally).

5.8 Enhanced CDD measures

Branches or authorized subsidiaries or concerned Head Office Divisions are required to apply enhanced due diligence measures where required as identified in the paragraph 5.4 or in any high risk scenario in addition to performing normal CDD measures as indicated in the paragraph 5.2 of this guidelines. Enhanced Due Diligence (EDD) should be conducted under the following circumstances:

a. Individuals or legal entities scored with high risk;

b. Individuals who are identified as politically exposed persons (peps), influential persons and chief executives or top level officials of any international organization;

c. Customer / Account marked as High Risk based on subjective judgement(i.e. NGOs, NPO, Trust, MLM Business, Atomic & Arms Business, Correspondent Banking, MSBs, precious metals business, charities & etc);

d. Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes;

e. While establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering and terrorism financing (such as the countries and territories enlisted as High —Risk and Non- Cooperative Jurisdictions in the Financial Action Task Force's Public Statement).

Enhanced CDD measures includes:

- Obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet, etc) and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management of Head Office to commence or continue the business relationship when applicable.
- In case of PEPs/IPs data/remarks should input properly in Core Banking Solution (TEMENOS T24) and AOF as well.
- Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- Making aware the concerned officials about the risk level of the customer.

5.9 CDD Measures for Beneficial Owner

5.9.1 Who is Beneficial Owner

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.

1. 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.

2. 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 on the customer;

   c. the person on whose behalf a transaction is conducted

3. 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.

Branches or authorized subsidiaries of concerned Head Office Divisions should identify the beneficial owner(s) and take all reasonable steps to verify his/her 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 a joint venture, beneficial owners should be properly identified and EDD must be ensured for every party.

(d) 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.

(e) 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 (ex. CFO, MD, CEO etc.

(f) 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.

Detail has been set out in **Annexure-I .**

5.10 Specific CDD Measures

5.10.1 Individual & Entity

Detail has been set out in Annexure-B (KYC Documentation).

5.10.2 Verification of address or CPV:

The client's residential address and telephone number(s) must be recorded. Preferred means of validation of residence are as following:

a. Visit to residence documented by the preparation of a call report in which the dealing officer explains the basis upon which he/she concluded that the client uses the home visited as a place of residence.

b. Residential address appearing on an official document prepared by a Government Agency supported by online verification from trusted site.

c. Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). If the bill is not in the name of applicant, then option d or e has to be exercised.

d. Sending a registered (welcome) letter to the address through postal / courier service correspondence.

e. Contact Point Verification (CPV) through third party approved by Bank Management.

Proof of Address must match to any of the addresses (i.e. Present or Work address) stated in the Account Opening Form.

5.10.3 Verification of Source of Fund

a. Branches or authorized subsidiaries or concerned Head Office Divisions are required to ensure the collection and verification of the documents supporting source of fund of the person or entity at the time of establishing any business relationship or while conducting CDD.

b. The document related source of fund of a person or entity may include:

    i. present employment identity;

    ii. salary certificate/copy/advice;

    iii. pension book;

    iv. financial statement;

    v. income tax return;

    vi. business document or any other document that could satisfy the branch or authorized subsidiary or concerned Head Office Division.

c. The branch or authorized subsidiary or concerned Head Office Division shall request the person or entity to produce latest Income Tax Return copy (Acknowledgement Receipt) which declares the amount of customer's total income, paid tax and net assets.

5.10.4 Exception When Opening a Bank Account (Opening Account without Verification)

The branch or authorized subsidiary or concerned Head Office Division may verify the documents of account holder after opening the account, provided that there are adequate safeguards in place to ensure that, before verification has been completed, transaction is not carried out by or on behalf of the account holder (including any payment from the account to the account holder).

5.10.5 In Case Where Conducting the CDD Measure is not Possible

a. 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 branch or authorized subsidiary or concerned Head Office Division could not collect satisfactory information on customer identification and could not verify that, they should take the following measures:

    i. must not carry out a transaction with or for the customer through a bank account;

    ii. must not establish a business relationship or carry out an occasional transaction with the customer;

    iii. must terminate any existing business relationship with the customer;

    iv. must consider whether it ought to be making a report to CCC or AML & CFT Division for ultimate submission to the BFIU through an STR.

b. The branch or authorized subsidiary or concerned Head Office Division should always consider whether an inability to apply CDD measures is caused by the customer. In this case, they should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, they should consider whether there are any circumstances which give grounds for making a report to CCC for ultimate submission to BFIU.

c. If the branch or authorized subsidiary or concerned Head Office Division concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be sent to CCC or AML&CFT Division for ultimate submission to the BFIU. The branch or authorized subsidiary or concerned Head Office Division must then retain the funds until consent has been given to return the funds to the source from which they came.

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

5.10.6 Persons without Standard Identification Documents

It is to be realized that most of the people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, street children or people, students and minors shall not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approaches and some flexibility considering risk profile of the prospective customers without compromising sufficiently rigorous anti-money laundering procedures is recommended by BFIU.

a. The branch or authorized subsidiary or concerned Head Office Division advised to allow above considerations, and must find out alternative ways on how identity can be confirmed in these exceptional circumstances considering.

b. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address.

c. A manager or head of the division or subsidiary may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

d. For students or other young people, the normal identification procedures set out in the preceding paragraphs should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant's educational institution. Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

5.10.7 Walk-in/One Off Customers

a. Walk-in/one off customer means a customer who has no account in the bank.

b. Branch or authorized subsidiary or concerned Head Office Division shall collect& preserve following information while issuing DD/PO or serving for TT/MT for transferring fund at the request of Walk-in/one off customer:

    i. complete and accurate information of sender/originator/applicant;
    ii. complete information of beneficiary;
    iii. Purpose of the transfer of the fund/remittance and relationship; and
    iv. Source of fund.

c. Complete refers to combination of all information for verifying the identity of the person or entity such as sender's/applicant's & receiver's/beneficiary's name, present & permanent addresses, Passport/NID/Birth Certificate/acceptable any photo ID, phone/active mobile no. etc.; and accurate refers to such complete information that has been verified for accuracy.

d. A detail provisions in this regard are discussed in the chapter 6 for wire transfer & money or value transfer services of this Guidelines.

e. Branch or authorized subsidiary or concerned Head Office Division shall collect complete and accurate information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit banks should identify sources of funds as well.

f. Branch / Concern Division of Head office must use Form of Walk-in Customer (Annexure-D) to keep records for Walk-in Customer.

5.10.8 Non Face to Face Customers

a. '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".

b. Branches or authorized subsidiaries or concerned Head Office Divisions must collect KYC & other information of the customer as per paragraph 5.1.1 of this guidelines.

c. Branches or authorized subsidiaries or concerned Head Office Divisions shall conduct specific CDD measures on customer, authorized person(s) or professional representative and beneficial owner(s) as specified in Annexure-I of this guidelines;

d. Branches or authorized subsidiaries or concerned Head Office Divisions must categorize these accounts as high risks accounts and apply enhanced due diligence as specified in the paragraph 5.8 of this guidelines.

e. Branches or authorized subsidiaries or concerned Head Office Divisions are required to physically verify the residential & business addresses of such customers.

f. Branches or authorized subsidiaries or concerned Head Office Divisions shall obtain senior managements' approval before establishing such business relationship when applicable.

g. Branches or authorized subsidiaries or concerned Head Office Divisions must make a list of such accounts and apply applicable ongoing CDD measures as specified in the paragraph 5.7 of this guidelines.

h. Branches or authorized subsidiaries or concerned Head Office Divisions must monitor the transactions of such accounts as specified in the chapter 10 of this guidelines and generate STR report whenever there are any unusual or suspicious transactions as specified in the chapter 12 of this guidelines.

i. The above precaution measures are not applicable for the customer who onboarded through eKYC.

5.10.9 Corresponding Banking

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

b. Branches or authorized subsidiaries or concerned Head Office Divisions must collect KYC & other information of the customer as per paragraph 5.1.1 of this guidelines.

c. Branches or authorized subsidiaries or concerned Head Office Divisions shall conduct specific CDD measures on customer, authorized person(s) or professional representative and beneficial owner(s) as specified in the Annexure-B & I of this guidelines;

d. Branches or authorized subsidiaries or concerned Head Office Divisions must categorize these accounts as high risks accounts and apply enhanced due diligence as specified in the paragraph 5.8 of this guidelines.

e. The branch or authorized subsidiary or concerned Head Office Division shall establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank through collection of additional information as per Annexure-E as indicated in the BFIU master circular-26 dated 16 June, 2020.

f. The branch or authorized subsidiary or concerned Head Office Division shall also obtain approval from its senior management before establishing and continuing any correspondent relationship.

g. The branch or authorized subsidiary or concerned Head Office Division must be sure about the effective supervision of that foreign correspondent or respondent bank by the relevant regulatory authority before establishing and continuing any relationship.

h. The branch or authorized subsidiary or concerned Head Office Division shall not establish or maintain any correspondent relationship with any shell bank. Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

i. The branch or authorized subsidiary or concerned Head Office Division shall not establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank.

j. The branch or authorized subsidiary or concerned Head Office Division shall not establish or maintain any correspondent relationship with any institution which is listed an entity in TFS of UN or OFAC or PRIME BANK approved list and/or delisted by SWIFT. located in a sanctioned country and/or its' owner(s)/director(s), beneficial owner(s), senior management are listed in TFS of UN or OFAC or PRIME BANK approved list;

k. The branch or authorized subsidiary or concerned Head Office Division shall pay particular attention or conduct Enhanced Due Diligence while establishing or maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standards for the prevention of money laundering and terrorist financing (such as the countries and territories enlisted in High—Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force's Public Statement). Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained.

l. If any respondent bank allow direct transactions by their customers to transact business on their behalf (i.e. payable through account), the corresponding bank, i.e., the branch or authorized subsidiary or concerned Head Office Division must be sure about the followings:

   i. The respondent bank has conducted appropriate CDD of the customer; and

   ii. Upon request of the correspondent bank, the respondent bank shall be able to provide all CDD information of the respective customer it has to be ensured that collecting the information on CDD of the respective customer.

   Here, 'Payable through accounts' refers to "Corresponding accounts that are used directly by third parties to transact business on their behalf."

m. The branch or authorized subsidiary or concerned Head Office Division is required to screen the correspondent or respondent bank, owners/directors, beneficial owner(s) and authorized person(s), if any, for the sanctions as specified in the Chapter -9 of this Guidelines;

n. Branches or authorized subsidiaries or concerned Head Office Divisions must make a list of such accounts and apply applicable ongoing CDD measures as specified in the paragraph 5.7 of this guidelines.

o. Branches or authorized subsidiaries or concerned Head Office Divisions must monitor the transactions of such accounts as specified in the chapter 10 of this guidelines and generate STR report whenever there are any unusual or suspicious transactions as specified in the chapter 12 of this guidelines.

5.10.10 Politically Exposed Persons (PEPs), Influential Persons (IPs) & Chief or similar high-ranking positions in an international organization

.Politically Exposed Persons (PEPs):

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

Influential Persons (IPs):

Influential Person (IP) refer to "individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of states owned corporations, important political party officials."

So, PEPs as per the FATF Standards and IPs as per Bangladeshi regulations, includes 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

The definition of PEPs & IPs is not intending to cover middle ranking and more junior individuals.

Chief or similar high-ranking positions in an international organization

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.

Detail has been set out in **Annexure- I.**

General guidelines for maintaining accounts of PEPs, IPs & Chief or similar high-ranking positions in an international organization

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 that the Branches or authorized subsidiaries or concerned Head Office Divisions has assessed in relation to the customer. Branches or authorized subsidiaries or concerned Head Office Divisions should apply more extensive measures for relationships assessed as high risk and less extensive measures for lower risk customers.

Detail CDD procedure for maintaining accounts of PEPs, IPs & Chief or similar high-ranking positions in an international organization

a. Branches or authorized subsidiaries or concerned Head Office Divisions are required to adopt the Risk Based Approach & use the software called PRIME BANK Automated Sanction Screening System / DOW JONES Risk & Compliance to determine whether a customer or the ultimate beneficial owner of an account is PEP/IP/Chief or high official of an international organization.

b. If the real beneficial owner of an account is a PEP/IP/Chief or high official of an international organization, the account shall be treated as High Risk and EDD measures shall be applicable.

c. Branches or authorized subsidiaries or concerned Head Office Divisions must collect KYC & other information of the PEP/IP/Chief or high official of an international organization as per paragraph 5.1.1 of this guidelines.

d. Branches or authorized subsidiaries or concerned Head Office Divisions shall conduct specific CDD measures on PEP/IP/Chief or high official of an international organization customer, authorized person(s) or professional representative and beneficial owner(s) as specified in the paragraphs 5.10.1 to 5.10.9 of this guidelines;

e. Branches or authorized subsidiaries or concerned Head Office Divisions shall take reasonable measures to establish the source of fund of a PEP/IP/Chief or high official of an international organization account as specified in the paragraph 5.8 of this guidelines.

f. Branches or authorized subsidiaries or concerned Head Office Divisions must categorize these accounts as high risks accounts and apply enhanced due diligence as specified in the paragraph 5.8 of this guidelines.

g. Branches or authorized subsidiaries or concerned Head Office Divisions shall obtain senior managements' approval before establishing such business relationship.

h. Branches or authorized subsidiaries or concerned Head Office Divisions must make a list of such accounts and apply applicable ongoing CDD review measures as specified in the paragraph 5.7 of this guidelines.

i. Branches or authorized subsidiaries or concerned Head Office Divisions must monitor the transactions of such accounts in a regular basis as specified in the chapter 10 of this guidelines and generate STR report whenever there are any unusual or suspicious transactions as specified in the chapter 12 of this guidelines.

j. Branches or authorized subsidiaries or concerned Head Office Divisions must comply all provisions of Foreign Exchange Regulation Act, 1947 and issued circulars, rules and regulations by BFIU or Bangladesh Bank under this act while opening account of PEP/ Chief or high official of an international organization.

k. Same instruction to be followed for the family members of influential persons or their close associates;

5.10.11 Reliance on Third Party

a. Branches or authorized subsidiaries or concerned Head Office Divisions can rely on the third parties to perform the CDD measures with the prior permission of competent authority through Head Office which may includes:

   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.

b. Reliance on third party must be under the following criteria:

   i. A third party must immediately obtain necessary information related to paragraphs 5.10.11a(i), 5.10.11a(ii) and 5.10.11a(iii) as mentioned above;

   ii. All necessary data and documents held with the third party must be available for the branches or authorized subsidiaries or concerned Head Office Divisions without any delay;

   iii. Branches or authorized subsidiaries or concerned Head Office Divisions must be satisfied that third party is regulated, supervised and monitored for, and has taken appropriate measures in compliance with CDD and record keeping requirements set out in the AML & CFT Guidelines & circulars issued by BFIU. Branches or authorized subsidiaries or concerned Head Office Divisions must also take senior management approval from Head Office in this regard.

5.10.12 Management of Legacy Accounts

a. Legacy account refers to those accounts which were opened before 30 April, 2002 and are yet to update KYC procedures.

b. Branches or authorized subsidiaries or concerned Head Office Divisions are required to treat these legacy accounts as “Dormant”.

c. No withdrawal shall be permitted in those accounts; however, deposit can be permitted. These accounts will be fully functional only after conducting proper CDD measures.

d. Central Compliance Committee (CCC) /AML & CFT Division should preserve data of such accounts at their end.

5.10.13 High Risk Countries

a. Branches or authorized subsidiaries or concerned Head Office Divisions are required to conduct enhanced CDD and any other measures that have a similar effect in mitigating risks for business relationships and transactions with any person or entity from countries identified by the FATF or BFIU as having on-going or substantial ML/TF risks.

b. Where ML/TF risks are assessed as higher risk, branches or authorized subsidiaries or concerned Head Office Divisions are required to conduct enhanced CDD and any other measures that have a similar effect in mitigating risks for business relationships and transactions with any person or entity from countries identified by the FATF or BFIU as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

c. In addition to the enhanced CDD requirement under 5.8, branches or authorized subsidiaries or concerned Head Office Divisions are required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries listed as having on-going or substantial ML/TF risks, as follows:

   i. limiting business relationship or financial transactions with identified countries or persons located in the country concerned;

   ii. review and amend, or if necessary terminate, correspondent banking relationships with financial institutions in the country concerned;

   iii. conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the reporting institution or financial group, located in the country concerned;

   iv. submit a report with a summary of exposure to customers and beneficial owners from the country concerned to CCC for review and submission to BFIU (if necessary);

   v. conduct any other measures as may be specified by BFIU.

5.11 Periodic KYC Review

Periodic KYC review involves the simple procedure of submitting the latest identity, address, profession and source of fund related documents to the bank. There is regulatory guidance for doing periodic KYC review/update in every 5 (five) years for the low-risk accounts and 1(one) year for high-risk accounts [BFIU circular no. 26 dated 16th June, 2020 (section no 3.6.4)].

511.1 Customer Communication

a. Letter communication

- Respective Branch /Division/ Dedicated Team (Operations) to generate the letters centrally as per given format.
- Respective Branch /Division/ Dedicated Team (Operations) to distribute the letters through courier/GPO at the T24 registered addresses of the customers taken from a shared folder given by respective Division/ Unit / KYC Project Team.
- Respective Branch /Division/ Dedicated Team (Operations) to keep POD against the sent letters properly as a proof of letter communication.
- In case of remote branches/areas with very limited courier/GPO facilities, hand-to-hand letter delivery to the known addressed customers is accepted under exception but a customer signed photocopy of the letter to be preserved as POD.

b. Email Communication

Respective Branch /Division/ Dedicated Team (Operations) will take initiative to send given format email to the T24 registered email addresses of the customers with the assistance of IT Division/ADC in parallel to letter sending.

c. SMS Communication

Respective Branch /Division/ Dedicated Team (Operations) Team will take initiative to send SMS to the T24 registered mobile numbers of the customers by IT and ADC according desire text of respective Business Unit.

d. Call over phone/mobile

Respective Branch /Division/ Dedicated Team (Operations) Officials to call the customers over the phone, where KYC review is pending and keep the record (Date, caller name, call to, call from & call status).

e. KYC Review Pending Alert during OTC Cash/Fund Transfer

If required, Bank may arrange alerts through OTC cash/fund transfer transactions for Teller and Branch officials, where KYC review is pending against respective customer.

5.11.2 Standard KYC Review Procedure

Following procedure will be followed as standard KYC review procedure for Personal & Non-Personal Account, however following may be reviewed & updated at a reasonable time or time-to-time based on legal/regulatory or business/ operational changes which should be approved by CAMLCO & respective Business Unit. For ensuring proper KYC documentation Branch/RM should follow the Annexure-J of this guidelines.

Collection of documents & process

- Customers may provide/submit their updated documents to RM or at any of his/her nearest Prime Bank branch.
- RM/DAMLCO or BAMLCO must fill-up the KYC profile Form with a complete risk rating including Monthly Transaction Amount (TP).
- Personal Information Form (PIF) must be signed by the Customer, where there is any change in customer data (i.e. Passport, Address, Mobile, email & etc.).
- Any changes in Non-personal Account (i.e. Address, Mobile, email & etc) we should obtain the signature of customer or operators and/or directors based on customer types, where Branch/RM should use page 1&2 of Non-personal Account Opening Form.
- If there is no change found in the customer's personal information or entity's information, BAMLCO/RM will collect the updated documents of the Customer and BAMLCO/RM fill-up only KYC Profile Form with the declaration "No changes found".
- RM/DAMLCO of Head Office may upload documents through PrimeIntellect(PI).
- Operations/LOD should update the information in CBS with a proper KYC review date.
- In case of inadequate documents found, Operations/LOD may refuse or return the documents to Branch or RM with proper reason.
- Hard copies of KYC review documents should preserve in the customer file of the respective Branch.

Posting restriction:

- Posting restrictions such as "Post No Debit" shall impose to the accounts of non-response customers if there is no positive response from the account holder or unable to conduct proper CDD by Branch/RM/DAMLCO.
- Before impose posting restriction, the Operations/KYC project Team will provide the account list to Branches and Division.
- When an account requires a temporary unblock for valid reasons—such as bank charges, loan installments, or rate changes—the Relationship Manager (RM) shall submit a formal request to the Division or Branch Head. The Head will then seek approval from Operations, supported by the recommendation and consent of the

Head of BDN/Regional Head and the respective Business Segment Head. Once approved, the LOD/SD team will unblock the account and must immediately re-apply the block once the transaction is completed.

5.12 Transaction Monitoring

A well-designed transaction monitoring (TM) system is an important component of an effective anti-money laundering (AML) compliance program. It supports the efforts to combat money laundering and terrorist financing by helping financial institution to identify unusual or suspicious activity that must be reported to regulatory in tracking and prosecuting criminals involved in ML/TF.

An effective monitoring system comprises the following two key components: -

(i) Monitoring performed by staff who deal directly with customers (e.g. relationship managers) or process customer transactions (e.g. counter staff/front-line staff); and

(ii) Regular reviews of past transactions to detect unusual activities by BAMLCO/DAMLCO.

Branches/ concern Division/Department of Head Office needs to monitor the transactions of customer on a regular basis. The complex transaction - transactions that deviate from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized during monitoring.

5.12.1 Key requirement for setting Transaction Profile (TP)

Transaction Profile (TP) is an and likely the first effective tool for transaction monitoring (TM) system to identify unusual transactions.

Initial TP Limit-Setting

In this step, TP is set-up at the time of account opening based on the information provided by the customer such as nature of business/occupation, net worth/business turnover, monthly income/source of fund & etc.

Some examples of TP setting techniques:

1. While a house wife declared in the TP that her husband's income as her main source of funds then the responsible bank official should justify her husband's nature of business/profession, account activity, proof of the sources of funds and its true entity; etc. through proper scrutiny.

2. While a businessman declared that his/her business income is the main source of funds then the responsible bank official should justify the true entity, business turnover and its reality, nature of business, account activity and the entity's customers; etc. through proper scrutiny.

3. While a student declared that his/her parent's income as his/her main source of funds then the responsible bank official should justify his/her parent's nature of business/ profession, account activity, reality of the sources of funds and grounds for operating the account; etc. through proper scrutiny.

TP Limit Review/Modification:

According to section 3.6(3) of BFIU Circular No-26, every after 6(six) to 12(twelve) months from the establishment of relationship with customer, Bank shall take reasonable and appropriate measures to update/modify Transaction Profile (TP) of each customer. Customer notification/communication is not required for reducing the existing TP amount as an outcome of TP amount analysis against transactions.

5.12.2 Over-the-counter TP Breach Alert

- **Monitoring Action Parties**
  - Branches
- **Monitoring Actions**

Branch desk official to send the customer to account opening/review officer where account transaction records generated from PRIME BANK CBS/PrimeShield/Dashboard to be analyzed and customer to be questioned accordingly.

In case of TP Breach, TP updated with the availability of supporting document(s)/proof, if latest information varies significantly with the earlier provided information in bank records or seems suspicious by Branch or not get any co-operation from customer, respective official may report SAR/STR through the PrimeDefence.

LOD to maintain/update TP in T24 based on the information filled-up in KYC Profile Form / TP Form.

5.12.3 Regular Transaction Monitoring Activities

(a) TP Brach reports (High Risk, Low Risk and Newly opened accounts)

<u>Key Takeaways</u>

- Branch to generate TP breach reports by themselves from AML System (i.e. 'PrimeShield' or others system)
- Highly deviated transaction amount against the existing TP.
- Whether any SAR/STR/ISAR raised by Branch?

i. A common task will be issued from AML portal for all the branches and AML supervisor to follow-up his/her portfolio branches.

ii. Action time by branches: 1st to 15th day of the following month.

(b) Transaction structuring report

<u>Key Takeaways</u>

- Branch to generate reports by themselves from AML System (i.e. 'PrimeShield' or others system);

- Whether any SAR/STR/ISAR raised by Branch?

i. A common task will be issued from AML portal for all the branch to collect the monitoring reports with BAMLCO's comments.

ii. Action time by branches: 1st to 15th day of the following month.

(c) Cash Transaction Report (CTR)

Key Takeaways

- Are there any KYC lapses in CTR accounts?
- Whether KYC reviewed or pending?
- Whether sufficient documents or supporting paper collected against CTR transactions?
- Are there special findings against the accounts like as SB or Housewife / Students accounts and new accounts in CTR?
- Whether any SAR/STR/ISAR raised by Branch?
- Whether any STR detected by Branch from last month CTR?

i. Responsible AML Officer will ensure the data availability for the Branch.

ii. A common task will be issued from AML portal for all the branch and AML supervisor to follow up his/her portfolio branches.

iii. Action time by branches: within 21st day of the following month.

(d) Threshold / Channel based /Monthly High Amount Transaction Accounts

Branches/ concern Division/Department of Head Office should monitor the high-volume transaction from all types of transactions (i.e. Teller/Cash, ATM, Clearing (BACH), RTGS, EFT, iBANKING transactions) on a regular basis and keep record as well to identify unusual transactions.

Key Takeaways

- Are there any KYC lapses in High volume transacted accounts?
- Whether KYC reviewed or pending?
- Whether sufficient documents or supporting paper collected against High volume transactions?
- Whether any SAR/STR/ISAR raised by Branch?

i. Responsible AML officer will provide data to all AML Supervisor.

ii. Individual AML supervisor will issue a task from AML Portal and collect response from Branch.

iii. Action time by branches: 21st to 30th day of the following month.

(e) Online Transaction Analysis/Monitoring:

Branches/ concern Division/Department of Head Office should monitor the online transactions of customers on a regular basis and generate online transactions reports from PRIME BANK CBS/PrimeShield/Dashboard to detect suspicious transactions.

Key Notes: Find-out who perform this activity as a top & frequency.

Find where the transaction performed (i.e. geographical area).

Compare online transaction with customer Business area & activity.

Find out unusual deposit and followed by withdrawals.

(e) Transaction Monitoring on PEPs/IPs Customer:

Branches/ concern Division/Department of Head Office should monitor the transactions of PEPs/IPs customers on a regular basis and analyzed the reports to detect suspicious transactions.

Key Notes: Use of corporate vehicles without valid business reason

Transactions which do not commensurate with source of fund.

Transactions by usual third-party.

Compare transactions with customer Business area & activity.

Find out unusual deposit and followed by withdrawals.

(g) Trade Transaction Analysis to prevent TBML:
(As describe TBML Risk Management Guidelines)

CHAPTER 06

WIRE TRANSFERS & MONEY OR VALUE TRANSFER SERVICES

6.1 Wire Transfers

6.1.1 Wire Transfer Related Definitions

Accurate - is used to describe complete information that has been verified for accuracy.

Beneficiary - refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

Beneficiary Financial Institution - refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.

Cross-border wire transfer - refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

Complete — refers to combination of all information for verifying the identity of the person or entity. For example: name and detail address of beneficiary/applicant, account number (if any), passport/national ID card/ birth certificate accompanied by acceptable identification certificate with photo/any other acceptable photo ID, phone/active mobile number, etc.

Domestic wire transfers - refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country.

Intermediary financial institution - refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

Meaningful — refers to such complete information which are apparently seems to be correct but not verified for accuracy.

Ordering financial institution - refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

Originator/Applicant - refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

Wire transfer - refers to any transaction carried out on behalf of an originator 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, irrespective of whether the originator and the beneficiary are the same person.

Transaction Reference — each Cross-border wire transfer must have a Unique Transaction Reference Number [BFIU-26 dated June 16, 2020].

6.2 General Requirements

6.2.1 The requirements under this chapter are applicable to cross-border wire transfers, money or value transfer services (MVTS) and domestic wire transfers including serial payments, cover payments.

6.2.2 Where relevant, references to a "customer" in this chapter include originators, beneficiaries and beneficiary owners of wire transfers or fund transfers.

6.2.3 Branch or Authorized Subsidiary or concerned Head Office Divisions will ensure each Cross-border wire transfer must have a Unique Transaction Reference Number according to directives of BFIU-26 dated June 16, 2020. For batch file upload/ transactions Unique Transaction Reference Number should ensure also.

6.2.4 Branch or Authorized Subsidiary or concerned Head Office Divisions must conduct applicable appropriate CDD measures as specified in the chapter four (Customer Due Diligence) of this guideline before making payment of any inward remittance & executing any outward remittance.

6.2.5 Branches or Authorized Subsidiaries or concerned Head Office Divisions are required to conduct enhanced CDD specified in the paragraph 5.10 chapter five (Customer Due Diligence) of this guidelines for business relationships and transactions with any person or entity from countries identified by the FATF or BFIU as having on-going or substantial ML/TF risk (higher risk countries).

6.2.6 Branch or Authorized Subsidiary or concerned Head Office Division shall not execute the wire transfer or provide money or value transfer services (MVTS) if it does not comply with the requirements specified in this Chapter.

6.2.7 Branch or Authorized Subsidiary or concerned Head Office Division must comply the Bangladesh Bank Guidelines for Foreign Exchange Transactions; circulars issued by Bangladesh Bank & BFIU, & other applicable acts, rules & regulations for executing any cross border wire transfer.

6.2.8 Branches or Authorized Subsidiaries or concerned Head Office Divisions are required to screen/check the names of the originator(s), beneficiary (ies), beneficiary owner(s), ordering institution, intermediary institution(s) appearing in any wire transfer message or MVTS instruction against the names in the Targeted Financial Sanctions databases of UNSCR, OFAC & BFIU . If there is any name match, it is required to take reasonable and appropriate measures to verify and confirm the identity of name(s) match. Once confirmation has been obtained about the true matching, branches or authorized subsidiaries or concerned Head Office Divisions must immediately stop the payment or transfer of fund and report it to CCC so that CCC can report it to BFIU within next working day.

6.2.9 Branch or Subsidiary or concerned Head Office Division are required to maintain all originator and beneficiary information collected in accordance with record keeping requirements under Chapter Thirteen.

6.2.10 Branches or Authorized Subsidiaries or concerned Head Office Divisions shall not undertake any transactions without face-to-face contact with the customer unless the business relationship with the customer has been first established and CDD measures have duly been conducted as per chapter five of this guidelines.

6.3 Ordering Banks/Institutions (Banks/Institutions Conducting Outward Remittance)

Cross Border Wire Transfer according to [BFIU-26 dated June 16, 2020].

6.3.1 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all cross-border wire transfers involving an amount USD1000.00 and above or equivalent in any other foreign currency are accompanied by the following information before transmitting the same to Intermediary/Beneficiary Banks:

a. Collected & preserved the complete and accurate originator/applicant information such as:

   (i) name;

   (ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

   (iii) reason for transactions;

   (iv) residential or mailing address;

   (v) NID/Birth Registration/Any acceptable ID with Photo;

   (vi) Phone/Active Mobile No;

   (vii) Additional Documents related to Transaction (if required);

b. Collected & preserved the meaningful beneficiary information such as :

   (i) name;

   (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction; and

   (iii) Details Address.

6.3.2 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branch are required to ensure that the message or payment instruction for all cross-border wire transfers involving an amount below USD1000.00 or equivalent in any other foreign currency are accompanied by the following information before transmitting the same to Intermediary/Beneficiary Banks:

a. Collected & preserved the complete and meaningful originator/applicant information such as:

   (i) name;

   (ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

   (iii) residential or mailing address;

   (iv) NID/Passport/Birth Registration with any Photo ID;

   (v) Phone/Active Mobile No.

b. Collected & preserved the meaningful beneficiary information such as:

   (i) name;

   (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction; and

   (iii) Address in Details.

6.3.3 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain Complete and accurate originator information, and beneficiary information, that is fully traceable within the beneficiary country; and Branches or Authorized Subsidiaries or concerned Head Office Divisions are required to include the originator's account number or unique transaction reference number.

6.3.4 Where required information in the paragraphs 6.3.1 indicates "Accurate Information", Branches or Authorized Subsidiaries or concerned Head Office Divisions are required to verify that information to ascertain its' accuracy using reliable, independent source documents, data or information.

6.3.5 The meaningful information required under Paragraphs 6.3.1 & 6.3.2 need not be verified for accuracy except when there is a suspicion of ML/TF.

Domestic Wire Transfer according to [BFIU-26 dated June 16, 2020].

6.3.6 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all domestic wire transfers involving an amount USD1000.00 and above or equivalent in any other foreign currency are accompanied by the information as mentioned in the paragraph 6.3.1(a)(b) for Domestic wire transfer before transmitting the same to Intermediary Banks/Beneficiary Banks/Organizations.

6.3.7 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all domestic wire transfers involving an amount below USD1000.00 or equivalent in any other foreign currency are accompanied by the information as mentioned in the Section-9 of BFIU Circular No.26 for Domestic wire transfer before transmitting the same to Intermediary Banks/Beneficiary Banks/Organizations.

6.3.8 Where required information in the paragraphs 6.3.6 & 6.3.7 indicates "Accurate Information", Branches or Authorized Subsidiaries or concerned Head Office Divisions are required to verify that information to ascertain its' accuracy using reliable, independent source documents, data or information.

6.3.9 The meaningful information required under Paragraphs 6.3.6 & 6.3.7 need not be verified for accuracy except when there is a suspicion of ML/TF.

6.3.10 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branches are required to collect & preserve documents and information as per paragraphs 6.3.6 to 6.3.9 in addition to KYC format as supplied by Bangladesh Bank Payment System Department vide their circulars time to time.

6.3.11 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branches are required to collect & preserve documents & information as per paragraphs 6.3.6 to 6.3.9 in case of wire transfer using credit or debit or prepaid cards (except purchase of goods and/or service).

6.3.12 It is not compulsory to comply paragraphs 6.3.10 & 6.3.11 in case of wire transfers in favor of Government/Semi-government/Autonomous bodies/organizations. Besides these paragraphs are also no applicable for interbank transactions, i.e., where both the applicant and beneficiary are either banks or financial institutions.

6.4 Intermediary Banks/Institutions

6.4.1 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the intermediary banks/ institutions are required to ensure the followings:

a. For both cross-border wire transfers & domestic wire transfers, intermediary institutions are required to retain all originator and beneficiary information that accompanies a wire transfer.

b. Where the required originator or beneficiary information accompanying a cross-border wire transfer or domestic wire transfer cannot be transmitted due to technical limitations, intermediary banks/institutions are required to keep a record in accordance with record keeping requirements under chapter 13, for at least five years, of all information received from the ordering bank/institution or another intermediary bank/financial institution.

c. Intermediary banks/institutions are required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

d. Intermediary institutions are required to have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

6.5 Beneficiary Banks/Institutions (Banks/Institutions Conducting Inward Remittance)

6.5.1 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the beneficiary banks/Branches are required to ensure that the message or payment instruction for all cross-border wire transfers involving any amount are accompanied by the following information before disbursing the amount to beneficiaries:

a. Complete originator/applicant information such as:

(i) name;

(ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

(iii) residential or mailing address;

b. Complete and accurate beneficiary information such as :

(i) name;

(ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

(iii) reason for transactions;

(iv) residential or mailing address;

(v) NID/Birth Registration/Any acceptable ID with Photo;

(vi) Phone/Active Mobile No;

(vii) Additional Documents related to Transaction (if required);

6.5.2 Cross-border wire transfers or fund transfers with inadequate originator/applicant information, Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the beneficiary banks/Branches are required to contact the concerned parties for complete information or may collect complete information from any other reliable & acceptable sources.

6.5.3 Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the beneficiary banks/Branches are required to collect the above mentioned beneficiary information at the time of payment of any inward cross-border wire transfer or fund transfer & preserve the same information for at least five years in accordance with record keeping requirements under chapter 13.

6.5.4 Branches or Authorized Subsidiaries or concerned Head Office Divisions are required to verify the information collected in accordance with paragraph 6.5.1(b) to ascertain its' accuracy using reliable, independent source documents, data or information.

6.5.5 Beneficiary institutions are required to have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking the required originator or required beneficiary information; and (b) the appropriate follow-up action.

6.6 Money or Value Transfer Services (MVTS)

6.6.1 Money or Value Transfer Services Related Definitions

Money Value Transfer Service: Money or Value Transfer Services (MVTS) as defined by the FATF: "Money or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions."

MVTS provider/MSB: Any natural or legal person who is licensed or registered to provide MVTS as a business, by a competent authority, including through agents or a network of agents.

Agent: Any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.

6.6.2 Responsibilities of MVTS/MSB

Branches or Authorized Subsidiaries or concerned Head Office Divisions offering MVTS/MSB either directly or as an agent to MVTS operators or providers or sub-agent to an agent of MTVS operators or providers are required to comply with all of the relevant requirements under Paragraphs 6.2.1 to 6.5.5 of this chapter on Wire Transfer (Remittance) of this document in the countries in which they operate, directly or through their agents or sub-agents.

6.6.3 MVTS/MSB - Good Principal/ Agency practice:

Agent "on-boarding" — selecting and appointing an agent

- Sanction Screening test must be completed before appointing agent;
- Complete the CDD procedure according to the chapter 5(five);
- Access the honesty, integrity and reputation of the beneficial owner and managers of the agent;

Agent "Monitoring"

- Adopt and apply a written policy to assess the risk of potential agents;
- Document the assessment of each agent risk;
- Establish expected levels of transactions for each agent;
- Monitor the agent's transaction on regular basis;

Agent "Training"

- Train agents and all their staff who access the principal's systems, assessing agents and staff to ensure that training messages have been understood and applied to an appropriate standard;

System and IT security

- Operate a system to ensure that exclusive passwords are issued to and used by each agent and relevant staff on an individual basis.
- Ensure that access to network systems is only allowed during opening hours agreed with the principal.

Agent "De-listing"

- Principal/ Authorized Subsidiaries should circulate the name of the de-listed agents in their web sites due AML & CFT non-compliance or KYC/CDD issues;

6.6.4 Where the Branches or Authorized Subsidiaries or concerned Head Office Divisions offering MVTS/MSB control both the ordering and the beneficiary side of a wire transfer, the Branches or Authorized Subsidiaries or concerned Head Office Divisions are required to:

a. all Authorized Subsidiaries must ensure the implementation of directives of BFIU, Bangladesh in connection with MLPA-2012 (including all amendments -2015) and ATA-2009 (including all amendments -2012 & 2013), due to any conflict with the operating country law, the respective should informed to the Principal according to BFIU-23 date January 31,2019;

b. take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious transaction report has to be filed; and

c. file a suspicious transaction report (STR) when detected any suspicious wire transfer, and make relevant transaction information available to respective compliance division/ department/CCC for ultimate submission to Local/oversees concern regulatory body (i.e. BFIU, FCA/HMRC/NCA, MAS, Hong Kong Customs Authority & other competent authority).

CHAPTER 07

AGENT BANKING

Introduction:

The aim of Agent Banking is to provide limited scale banking and financial services to the underserved population of the country through engaged Agents under a legal agreement. With a view to ensuring the safety, security, and soundness of the banking system Bangladesh Bank has issued "Prudential Guidelines for Agent Banking Operation in Bangladesh" and all scheduled Banks are instructed to comply with the prevailing Anti-Money Laundering (AML) & Combating Financing of Terrorism (CFT) related laws, regulations and guidelines issued by Bangladesh Financial Intelligence Unit(BFIU) from time to time.

Committed to abide by the guidelines of Bangladesh Bank, Prime Bank PLC. has developed separate AML/CFT policies and procedures on Agent Banking to ensure the coverage of requirements, guidelines & circulars delivered by the concerned departments of Bangladesh Bank.

Agent Banking:

"Agent Banking" means providing limited-scale banking and financial services to the underserved population through agents under a valid agency agreement, rather than a teller or cashier. Agent Banking services through agents for the rural customer who does not have access to formal banking system even through Mobile Banking.

"Agent" means a person engaged in a commercial/business activity and has been contracted by a financial institution to provide the services of the financial institution on its behalf in a manner specified in these directives of Bangladesh Bank;

- **Permissible Activities of an Agent** (As per Prudential Guidelines for Agent Banking Operation in Bangladesh-2017 of Bangladesh Bank):
- **Prohibited Activities** (As per Prudential Guidelines for Agent Banking Operation in Bangladesh-2017 of Bangladesh Bank):

AML-CTF related regulatory requirements for Agent Banking:

AML-CTF related regulatory instructions for Agent Banking were described in Section 3.14 of BFIU Master circular No. 26 dated 16-06-2020. Key instructions are furnished below for information and meticulous compliance of all concerned (Agent Banking):

1) Both agent and bank shall ensure compliance of all AML & CFT related instructions;
2) Uniform Account opening form should be used for opening account of Agent and Customer;
3) To be alert regarding identification and reporting of Suspicious Transaction/Activity of Agent and Customer;
4) AML-CTF related activities should be included in Agent Banking Compliance program and training should be arranged for Agents;

5) Following initiatives to be taken for appointing agent and monitor their activities:

   a) Appropriate screening mechanism should be followed while selecting agents and obtaining complete and correct information should be ensured;

   b) Risk of agents should be assessed based on volume and number of transactions, geographic location, nature of business etc. and monitoring should be done considering the level of assessed risk of agents;

   c) Risk assessments should be done on-going basis;

   d) Agents' AML-CFT compliance status to be checked;

   e) Internal Audit Department should conduct inspection on Agent point in a regular interval based on Risk Based Approach (RBA) and a copy of the report to be sent to the CAMLCO;

   f) Agents' list to be updated (January-June based) in PRIME BANK web site;

Separate list of agents who were delisted due to complain/irregularity shall have to be updated in PRIME BANK web site.

Organization Structure for PRIME BANK Agent Banking:

As PRIME BANK has both the Mobile Financial Service and Agent Banking and PRIME BANK Management is committed to comply with the BFIU's instructions, for smooth operation of Agent Banking function a separate Department has been created in PRIME BANK in the name and style "Agent Banking Department (ABD)". ABD shall serve wide range of customers through Agent Banking Offices throughout the country by providing banking and financial services with the help of mobile telecommunication devices/ computer system/ using biometric technology or e-KYC. PRIME BANK ABD shall ensure compliance of all instructions/guidelines laid in this manual to prevent money laundering and terrorist financing.

Divisional Anti-Money Laundering Compliance Officer (DAMLCO) of Agent Banking Department:

Agent Banking Department (ABD) will nominate one official to act as DAMLCO. The responsibilities of an DAMLCO are as follows:

- The DAMLCO will act as a team leader of AB Office Compliance Unit and get related reports from the concerned Agent/Sub-Agent of the Office;
- Arrange Quarterly AML meeting and preserve the minutes of the same for record;
- Manage the transaction monitoring process;
- Maintain proper record of the regulatory instructions / HO instructions and dissemination of instructions/guidance note to all relevant officials.
- Collect reports from the Agent/Sub-Agent as —
  - o Sub-Agent (up gradation status of KYC, Transaction Profile, Risk Grading, Source

of Fund and other compliance issues);

  - o Ensure suspicious transactions identification and reporting by concerned Sub-Agent;
  - o Ensure monitoring of day to day cash transactions beyond the TP of account holder monitored by concerned Agent/Sub-Agent or mobile banking officials;

- Report any suspicious activity to AML & CFT Division, Head Office;
- Provide training to Agent/Sub-Agent;
- Communicate to all staff in case of any changes in national or Prime Bank policy;
- Submit all required returns to Head Office or Bangladesh Bank timely.

It is imperative to mention that the DAMLCO of Agent Banking Department (ABD) is ultimate responsible for all compliance issues of Agent Banking Office. He will monitor and supervise all activities of the ABD to safeguard the Bank.

Responsibilities of Agent Banking Department (ABD):

Agent Banking Department (ABD) is committed to ensure compliance of the Money Laundering Prevention Act, 2012 (Amendment in 2015) and ATA 2009 (Amendment in 2012 & 2013), all the AB Offices of PRIME BANK shall cooperate with DAMLCO to mitigate the Money Laundering (ML) / Terrorist Financing (TF) risk and also ensure proper monitoring and control mechanism. The DAMLCO will define concrete responsibility of the team members of ABD to identify suspicious transaction and risky accounts to report it to AML & CFT Division, Head Office.

Brief flow chart of the functions and responsibilities (not limited to these extend) of the Agent/Sub-

Agent:

Function	Role / Responsibilities
Agent/ Sub-Agent Responsibility for Account Opening	• Exercise due diligence while opening an account. • Be diligent regarding the correct identification of account holder. • Ensure all required documentation is completed & satisfactorily. • Complete the Personal Information Form & KYC Profile. • Complete the Transaction Profile according to profession, source of income and economic status of the customer. • Complete the Risk Grading properly and maintain a checklist for monitoring the transaction activity of High Risk Accounts. • Source of fund or nature of business must be mentioned accurately and obtain supporting documents.

Function	Role / Responsibilities
Staff Responsible for account opening	• Check Agent's due diligence while opening an account. • Check regarding the correct identification of account holder. • Check & ensure Complete the KYC Profile. • Ensure all required documentation is completed & satisfactorily. • Check & Complete the Transaction Profile according to economic status of the customer. • Complete the Risk Grading properly and maintain a checklist for monitoring the transaction activity of High Risk Accounts. • Source of fund or nature of business must be mentioned accurately and obtain supporting documents. • Ensure Screening through PRIME BANK Automated Sanction Screening Solutions or any third-party system. • Escalate any suspicion regarding the intending customer to the Supervisor. • Escalate any suspicion regarding the intending customer to the Supervisor DAMLCO, ABD and AML & CFT Division.
District/ Upazila Area Manager	• Counter check the account opening process to ensure that all vital information and documents have been obtained. • To ensure correctness about any information of the customer, interview the customer, if deemed necessary. • Support the Account Officer in accomplishing any of the above roles. • Ensure that all control points are put in place prior to transaction monitoring. • Be diligence about transaction trends of the clients. • Ensure correctness of the Transaction Profile. (Counter check or further investigate if any suspicion arises). • Follow the transaction profile and update it when deemed necessary. • Notify Agent Banking Department (ABD) about any suspicious activity or transaction of the customer as and when detected.

Function	Role / Responsibilities
Unit Head	• Ensure that the AML/CFT program is effective within the branch/agent unit. • Ensure all compliance issues of the branch/agent is done properly under his overall operational responsibilities of the branch/agent. • While approving opening of the account, Branch Manager must be satisfied about customer's identification, proper KYC, TP etc. • Take immediate necessary step to safeguard the bank from any unauthorized use of the banking facilities by any intending criminal. • Ensure that all staff gets proper training on AML/CFT issues. • Ensure that all staff are well aware of the developments of AML/CFT activities. • Take necessary steps if any suspicious transaction or activity is issues relating to AML/CFT activities.

Agent Due Diligence (ADD):

The Agent Due Diligence procedures shall at a minimum contain methods of identifying potential agents, initial due diligence and regular due diligence checks to be performed at specified intervals and a list of early warning signals and corrective actions to ensure proactive agent management.

Efficient and thorough Agent Due Diligence (ADD) procedures shall be put in place to mitigate risks.

Agent Banking Department (ABD) shall be responsible for having clear, well documented Agent Due Diligence policies and procedures. The Agent Due Diligence procedures shall clearly specify the roles and responsibilities of various functions in the institution with regard to agent management. Agent selection criteria set by Bangladesh Bank shall have to be followed accordingly. In assessing the due diligence of agents, ABD shall consider all relevant factors, including but not limited to:

i) the entity has an existing well established business/commercial activity and that the sources of funds of the agent have been ascertained;

ii) the entity possesses appropriate physical infrastructure and human resources to be able to provide services with the necessary degree of efficiency and security;

iii) the agent, as certified by police certificate from local police station or a self-declaration that he, has no criminal record in matters related to finance, fraud, honesty or integrity and has a good/acceptable reputation;

iv) audited financial statements at least for the last one year, where applicable;

v) liquidity position of the agent to entertain deposit and withdrawal request of customers; and

vi) any other matter that may negatively impact on the agent has been considered.

ADB shall ensure that agents are well established, enjoying good reputation and have the confidence of the populace in their areas of operation. ADB also ensures that proper AML/CFT monitoring processes exist for agent banking.

Customer Due Diligence:

PRIME BANK Agent Banking Department (ABD) shall carry out Customer Due Diligence (CDD) according to chapter 5 of PRIME BANK Money Laundering & Terrorist Financing Risk Management Guidelines. The factors to consider include;

a. Know Your Customer (KYC) requirements.

b. Transactional limits per day, month and year limits commensurate with customer's profile.

c. Maximum balance limits on debit and credit.

d. Minimum technological security requirements.

e. Two factor authentication (TFA) i.e., use of a photo ID, Personal identification Number (PIN) or any other secret code or message during transactions.

ABD shall comply with all applicable AML/CFT laws and requirements and must follow the customer acceptance policy described in **chapter 4 of PRIME BANK Money Laundering & Terrorist Financing Risk Management Guidelines.**

Transaction Threshold & Regulatory Obligation:

"Prudential Guidelines for Agent Banking Operation in Bangladesh"

- In general, the maximum number and volume of transactions for client at agent banking outlet should not exceed the limits specified in the following table:

Daily Number of Transactions and Amount Limit Amount in Lakh BDT

Nature of Accounts	Cash Deposit		Cash Withdrawal		Transfer/BEFTN/ Inter-bank/Intra-bank	
	No. of transactions	Total Volume	No. of transactions	Total Volume	No. of transactions	Total Volume
Current Account	4	6.00	2	5.00	4	15.00
Savings Account	2	4.00	2	3.00	2	5.00
Special Notice Deposit (SND)	4	6.00	2	3.00	4	10.00

- Transactions beyond the established limits may also be carried but this shall require at least 1 (one) working day prior notice to the bank through the agent.
- In special cases, when a client has need for regular banking transactions exceeding the limits of clause 27.6, banks may set an increased limit for that client with due approval from the Managing Director/Chief Executive Officer of the bank. The increase must be prudent, rational and must accord the merit of the account and client and transaction category based on customer due diligence, client needs and associated risks. Within 30 (thirty) days of such increase of transaction limit, the bank shall inform FID of Bangladesh Bank in writing along with the rationale of such increase with related information of client transactions of at least last 1 (one) month.

Segregation of Risk-based classified account (High/Low):

ABD shall also ensure segregation of AB accounts as Low Risk or High-risk category based on customer KYC, TP and other considerable issues. Classification of High Risk account as scored in KYC is not harmful for the Bank. Any potential account may be classified / segregated as High or Low Risk at any point of time on the basis of nature of business, transaction etc. However, to regular monitoring /review of such account is the vital for AB Office or ABD to mitigate the Risk.

If an account classified as “Low Risk” category, AB Office may exercise normal due diligence to monitor/review the account. But if an account marked as “High Risk” accounts or PEPs/IPs, ABD shall exercise extra precaution or Enhanced Due Diligence (EDD) measure set out in Chapter-5 of PRIME BANK Money Laundering & Terrorist Financing Risk Management Guidelines and nursing that account as well.

Monitoring:

Monitoring customers’ account transactions is an important element of effective AML/CFT Program. In accordance with the Guideline on Prevention of Money Laundering & Terrorist Financing, ABD shall ensure effective monitoring systems to enable them to identify and report suspicious transactions to discharge their legal and regulatory obligations in connection with AML/CFT program.

In addition to Monitoring activities, ABD may fix/set a specific threshold covering the following account activities to identify the client activities that do not appear commensurate with the client’s business activities:

- Large Cash transactions including cash deposits & withdrawals on any particular day.
- Large volume credit turnover or month-end credit balance of the same threshold.
- Remittance monitoring.

AB Office is to monitor on an ongoing basis the relevant activities in the course of the business relationship. Possible areas to monitor / focus should be:

- Transaction Type
- Transaction Frequency

- High Risk Account
- Unusually large amounts
- Geographical origin/destination
- Large Volume transaction
- Transaction inconsistent with the TP etc. (branches to check TP of AB customers, if required)

Monitoring System:

Monitoring system comprises the following two components: -

a. Monitoring performed by staff who deals directly with customers or processes customers transactions;

b. Regular reviews of past transactions to detect unusual activities;

Structuring of Transaction:

Structuring is a money laundering technique, which involves the splitting up of a large cash deposit into a number of smaller deposit (transaction below the CTR threshold/ limit) to evade the suspicious activity reporting requirement of the Bank. ABD shall also take precautionary measures to check "Structuring" (or smurfing) at the time of Cash Transaction Reporting.

Reporting:

Identification of Suspicious Activity may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, DAMLCO should conduct the following stages:

a) Identification

This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of Banks monitoring of unusual transactions may be automated, manually or both. Monitoring mechanisms should be more rigorous in high-risk areas of the branch 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 shall always be an ongoing activity. Considering the nature of business Banks must be vigilant in KYC and sources of funds of the customer to identify STR/SAR.

b) Evaluation and escalation process

After identification of suspicious transaction at Agent Point or AB Office, concerned officer or Agent should immediately report to the DAMLCO. After receiving such report ABBAMLCO will evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage, concerned DAMLCO must be tactful considering the tipping off provision of the acts. If DAMLCO is not satisfied, he/she should forward the report to the AML & CFT Division/CCC. After receiving report from ABD, AML & CFT Division will analyze and evaluate STR/SAR and will present for necessary approval from the CAMLCO. After obtaining necessary approval from the CAMLCO STR/SAR must be reported to BFIU through go AML web.

Audit/Inspection:

Internal Control and Compliance Division / Internal Audit Department of PRIME BANK shall audit 5% of its Agents annually to assess their AML/CFT compliance status and send a report to the AML & CFT Division.

Education and training for Agent banking Agent/Sub-Agent:

As per directive of BFIU, agent/sub-agent should be go under appropriate AML/CFT training program. In this regard, Agent Banking Department of PRIME BANK shall arrange AML/CFT training program or workshop for the Agent banking agent/sub-agent on regular basis. Bank will distribute leaflets among agent/sub-agent time to time to make them aware about prevention of money laundering and combating terrorist financing.

Education and Training for Customers:

Bank management/officials should respond to Agent Banking customers on different matters including KYC and would time to time distribute leaflets among customers to make them aware about money laundering and terrorist financing and arrange to stick posters in every branch at a visible place.

Record Keeping:

Obligations under MLPA, 2012 (including amendments in 2015): -

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

Obligations under MLP Rules, 2019 (including amendments in 2012 & 2013): -

The bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners, according to section 12 of BFIU Circular-26 dated 16/06/2020:

Agent Banking Department (ABD) shall ensure that customers correct and complete information is obtained during the opening of account and further due diligence process and all relevant documents including AB account opening form and transaction documents are preserved complying with the above Act, Rules & Circular.

The Agent Banking Department (ABD) must retain AML & CFT training record centrally. In case of transfer of any employee, AML/CFT training record of concerned officials must be sent to the AB Office where the employee has transferred for their information and record.

CHAPTER 08

NEW TECHNOLOGIES: CREDIT CARD, DEBIT CARD, PREPAID CARD, INTERNET BANKING AND ALTERNATIVE DELIVERY CHANNELS

8.1 New Technology

Technology-based innovations have radically changed the financial industry due to the emergence of new services and products, which has allowed the creation of opportunities for growth and efficiency, and at the same time, it improves the access and delivery of financial services and products to people, businesses and communities (customers/ occasional customers) excluded or unattended from the current financial system, promoting financial Inclusion.

It is important to prevent the misuse of the financial system through the new services and products that technology-based innovations offer to the public such as new tools and vehicles for the commission of money laundering and terrorist financing (ML/TF).

FATF Recommendation 15	New Technologies: identify and assess ML/TF risks relating to the development of new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and preexisting products.

Obligations under BFIU Circular-26 [section 3.16] dated : 16-06-2020	Every bank shall establish a procedure to identify and assess ML/ TF risks relating to introduce or development of new products, services and technologies and should have a mechanism to prevent ML/TF risk.

8.2 New Technology Related Definitions

Automated Teller Machine (ATM) - an automated teller machine (ATM) is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller.

Cash Deposit Machine (CDM) - the Cash Deposit Machine (CDM) is a self-service terminal that allows customers deposit cash & cheque directly in their account.

Credit Card — a Credit Card is a secured chip-based card issued as a payment instrument by a financial institution that allows its user to borrow pre-approved fund at the point of sale in order to complete a purchase or withdraw cash from ATM or counter of the financial institute.

Debit Card — a Debit Card is a secured chip-based card issued as a payment instrument by a financial institution that deducts money directly from a consumer's checking account for payment of a purchase or withdrawal of cash.

Internet Banking— Internet Banking is a system which allows customers to perform banking activities any time anywhere through the internet.

Mobile banking — Mobile Banking is a package of mobile financial services provided by a bank or other financial institution that allows its customers to conduct a range of financial transactions remotely using a mobile device such as a mobile phone or tablet, and using software, usually called an app, provided by the bank or financial institution for the purpose.

Prepaid Card - a Prepaid Card is a secured chip-based card issued as a payment instrument by a financial institution that is preloaded with funds which can be used for payment of a purchase or withdrawal of cash. The nature of a prepaid card is somewhat opposite of a normal credit card because instead of buying something with borrowed funds (through credit), customers buy things with funds that have already been deposited (prepaid) in the card.

Point of Sales (POS) - the Point of Sale (POS) is the time and place where a retail transaction is completed. It is the point at which a customer makes a payment to the merchant in exchange for goods or after provision of a service.

SMS Banking - Short Message Service (SMS) Banking is a service that allows customers to access their account information or make basic transactions via push-pull SMS services through mobile phones.

8.3 New Technology Related Products and Services & Their Vulnerabilities:

Credit cards are unlikely to be used in placement stage, but their use in the later stages of money laundering is unknown. Credit card accessed accounts in offshore banks create vulnerabilities to money laundering. Industry is giving focus on fraud and credit risk but not on money laundering. Acquirers use fraud and credit risk policies and controls that they believe address money laundering among merchants. Major card processors use fraud focused policies and programs to support clients AML efforts. Regulatory oversight of issuing and acquiring banks credit card operations is focused less on AML requirements because of lower perceived risk. Associations and third-party processors have not been subject to AML related requirements or oversight.

8.4 Challenges facing in handling Card Payment Systems:

- ***Challenges from Customers:*** Being a force sale product card is given on fund/ income particulars and it is difficult to access illegal source of fund if customer dose not disclose or willing to cooperate.

- ***Technological Challenges:*** CMS are well equipped with fraud monitoring tool and less focused on AML activities.

- ***Management and Operational Challenge:*** After placement and layering, it is difficult to find out suspicious activities from card payment system.

- ***Others:*** Lack of adequate training and course of actions.

8.5 The mitigation techniques to handle money laundering vulnerabilities in the Local , International Credit Card and other technology based products:

Branches or Authorized Subsidiaries or concerned Head Office Divisions who introduced the customer for technology based product of PRIME BANK, the following KYC process should be followed for both non account holder and account holder customers before providing technology based services:

(i) Complete sanction screen process and obtain report;

(ii) Legal agreement with customers for technology based product/services;

(iii) Assess the money laundering risk;

(iv) Complete the CDD process as set out in chapter 5;

(v) Complete the EDD process based on risk profile of the customer as set out in chapter 5;

(vi) Obtain approval from senior management in case of PEPs/IPS;

8.6 Transaction/Customer Monitoring:

Once the card or any other technology based product has been issued, Bank must establish an effective transaction monitoring framework as part of ongoing due diligence. We should seek the opportunity to develop and, where appropriate, integrate our AML monitoring scenarios with other systems.

Transaction Monitoring:

- Frequent and unusual use of the card or any other technology based product for withdrawing cash at ATM;
- Structuring payments/Overpayments: balances on card or any other technology based product may move into regular credit where customer pay too much or where merchants give credits to an account.
- Unusual cash advance activity and large cash payments: the monitoring of incoming cash is critical, as excessive cash payments are often an attribute of money laundering.
- Transactions from High Risk jurisdiction or frequent transactions from offshore Tax Haven;
- Unusual purchase of goods or services in countries regarded by an institution as posing a heightened risk for money laundering;
- Purchases at merchant on personal cards which are significantly out of pattern with historical spending behavior;

Customer Monitoring

- Abnormal customer contact behavior (e.g., frequent changes of address).

Card Account Settlement:

- Multiple and frequent cash payment or money orders; large, cross-border wire transfer payments;
- Settlements/partial settlements from unrelated third parties;

8.7 Closure of service/product & reporting of STR/SAR:

Based on the severity or Risk Appetite or frequency of suspicious activity, it may be appropriate, where legally permissible to exit a relationship. Prime Bank shall report STR/SAR or exit relationship after suspicious activity/transaction is detected and reported or after negative customer information is identified. PRIME BANK shall not asked/notify customer further information to avoid the risks of "tipping off". PRIME BANK Cards, ADC or other concern Division will proactively notify to CCC or AML & CFT Division for suspicious activity of customer.

8.8 Assessing ML/TF Risk before introducing new product/technology:

The concerned division should seek AML/CFT Division for ML/TF Risk assessment before introducing new product/technologies. According to the Risk Matrix AML division will provide the risk grading for the proposed product/services/technologies. The concerned division will ensure the risk mitigation as defined by AML before going live of the product/services/technologies.

CHAPTER 09

TERRORIST FINANCING AND PROLIFERATION FINANCING AND SANCTIONS SCREENING

9.1 Introduction

Bangladesh has criminalized terrorist financing in line with the International Convention for the Suppression of the Financing of Terrorism (1999). Section 16 of Anti-Terrorism Act-2009 (Amended in 2012 & 2013) states the responsibilities of the reporting agencies regarding funds, financial assets or economic resources or related services held in or through them.

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

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

9.2 Legal Obligations

Obligations under ATA, 2009 (Amended in 2012 & 2013)	Every Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 (Amended in 2012 & 2013) and if any suspicious transaction is identified, the agency shall spontaneously report it to BFIU without any delay. The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each bank should approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by BFIU under section 15 of ATA, 2009 (Amended in 2012 & 2013); which are applicable to the bank, have been complied with or not.

9.3 Obligations under Circular

Obligations under BFIU Circular-26; dated 16/06/2020	Every bank shall establish a procedure by approval of Board of Directors for detection and prevention of financing of terrorism and financing of proliferation of weapons of mass destruction, shall issue instructions about the duties of Bank officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.

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

9.4 Targeted Financial Sanction

To implement TFS in Bangladesh, the Government has issued Statutory Regulatory Order (SRO) under section 2 of the United Nations (Security Council) Act, 1948 (29 November, 2012) and amended the SRO to make it more comprehensive (June, 2013). To make the process enforceable, a separate section has been included in ATA, 2009 through amendment of ATA in 2012 & 2013. Section 20(A) of ATA, 2009 covers all the requirements under UNSCR's tool were taken and will be taken under chapter VII of the charter of UN. Before that BFIU used to issue circular letters for reporting organizations to implement UNSCR resolutions -1267 & 1373.

9.5 Prime Bank Sanctions Policy Statement

PRIME BANK is committed in complying with the sanctions laws and regulations of the Bangladesh Govt. United Nations (UN), the United States (US), the European Union (EU), United Kingdom(UK), Singapore & Hong Kong and, as well as all applicable sanctions laws and regulations in the jurisdictions in which we operate.

For effective implementation of TFS relating to TF & PF - PRIME BANK introduces automated sanctions screening mechanism that could prohibit any listed individuals or entities to enter into our banking channel.

Sanctions Policy and Sanctions Economic Standards that define the minimum standards in which PRIME BANK and its subsidiaries must comply with to meet the above obligations. This includes:

- Screening customers and transactions against the sanctions lists issued by the Bangladesh Govt., UN, OFAC, EU, HMT, MAS & HKMA and all applicable local regulatory sanctions lists in the jurisdictions in which PRIME BANK and its subsidiaries operate.
- While doing any cross-border transactions in foreign currency with any country, the sanctions list originated from the respective country must follow in addition to UN, OFAC, EU, HMT, MAS & HKMA and Bangladesh sanctions list.
- Prohibiting or restricting business activities, personal transactions, customer relationships or facilitating transactions, correspondent relationship that we believe:
  - o may violate the applicable sanctions laws, whether directly or indirectly.
  - o involve countries/jurisdictions, individuals, entities or vessels, owner of vessels

listed on an official sanctions list as below:

- UNSCR
- OFAC
- EC/EU
- HMT
- MAS
- HKMA
- Bangladesh Govt. Domestic Sanction List
- PRIME BANK Own Negative List &
- Any other Sanctions list approved by Prime Bank management from time-to-time

- Blocking or rejecting transactions where PRIME BANK is required to do so under applicable sanctions laws or regulations. Transactions may also be returned/rejected by Prime where they fall outside of Prime Bank's risk appetite.
- Reporting of breaching of sanctions laws to the relevant regulatory authority. This can include any attempt by a customer to evade sanctions laws.
- PRIME BANK Screening process also includes the list of Politically Exposed Persons (PEPs), Influential Persons (IPs)/Domestic PEPs and Heads of International Organizations to ensure proper EDD.
- Whitelists are maintained to reduce the False hit.

Data integrity / Data source for Sanction Screening:

PRIME BANK has developed its own Sanctions Screening System fueled by reliable data source (at present Dow Jones Risk & Compliance data) or global data providers or third party system, which will cover the following area:

a. Sanctions and Enforcements:

Global watch lists (UN,OFAC, EU, HMT,MAS,HKMA & Local Sanctions List etc.)

b. Politically Exposed Persons:

Individuals and their close associates/family members

c. Adverse Media:

Profiles linked to illicit activities worldwide related to ML & TF

d. State-Owned Enterprises:

Government-owned and government-linked entities

Manner, Timing, Frequency of Sanctions Screening & Thresholds limit

- Sanctions Screening process is mandatory for any international relationship or transaction;
- Sanctions Screening process is mandatory for establishing relationship domestically or opening any account or issuing any types of Card;
- Sanctions Screening process is mandatory for its customers, counterparties and Risk based approach (RBA) shall be followed for intermediaries;
- **Onboarding of Customer**
    - Automated process through Prime Intellect (PI) or any onboarding platform
    - Manual Screening through PRIME BANK Sanction Screening Solution
    - Manual Screening / EDD through DOW JONES Risk & Compliance portal
    - Spelling variation / Thresholds limit minimum 85%.
- **Periodical Screening of existing customers**
    - Daily basis screening on entire customer database of Prime Bank through automated process.
    - Spelling variation / Thresholds limit minimum 90% or approved by management time to time.
- **Screening of Remittance data**
    - Real-time Screening process
    - Spelling variation / Thresholds limit minimum 85% or approved by management time to time.
- **Screening of SWIFT messages or payment message screening**
    - Real-time Screening process
    - Spelling variation / Thresholds limit minimum 85% or approved by management time to time.

9.6 Automated Sanctions Screening Mechanism in PRIME BANK:

For effective implementation of TFS relating to TF & PF, PRIME BANK introduces automated sanctions screening mechanism that could prohibit any listed individuals or entities to enter into our banking channel. Branch/ Concern Division of Head Office should operate in such system to verify whether system could detect any listed individuals or entities prior to establish any relationship with them. In particular, branch needs to emphasize on account opening and any kind of foreign exchange transaction through our automated sanction screening mechanism so that any listed individuals or entities cannot use our formal financial channel. In a word, Branch/respective division have to ensure that our screening mechanism has done before-

- Any relationship or transaction both domestic and abroad;
- Opening any account or establishing relationship both domestic and abroad.

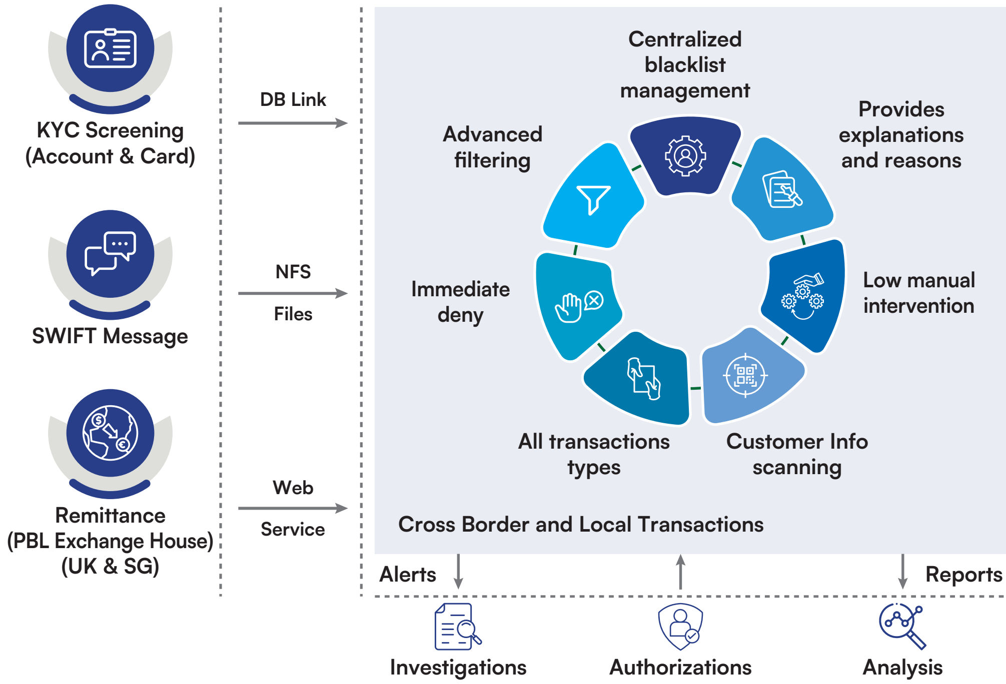
For proper implementation of UN, OFAC, EU, HMT, HKMA, MAS sanctions list and domestic sanctions list according to the section 18 of Anti-Terrorism Act-2009 (Amendment in 2012 & 2013), every bank official must have enough knowledge about-

- legal obligation and consequences of non-compliance;
- sources of information;
- what to do and how to do with sanction list;
- transactional review;
- how to deal with 'False Positives';
- how to deal with True Match;
- how to deal with 'aggrieved person or entity';
- how to exercise 'exemption' requirements;
- listing & de-listing process.

Bank's Practices - Screening Customers and Payments

- What needs to be screened?
    - o New customers
    - o Existing customers
    - o SWIFT Messages / Any Cross Border Transactions
    - o Inward NRB Remittances — Online, Foreign branches, Exchange House and other such partners.
    - o Trade Documents (i. e. Vessel/owner of vessel/Country of Trade/Buyer/Seller/ beneficiary/ counterparties/related parties etc.)

9.7 Technical Flow-chart for Sanction Screening by PRIME BANK



Sources of Sanction List (Third party like : DOW JONES or Open Source)

(a) UN Security council website
(http://www.un.org/sc/committees/list_compend.shtml)
(b) BFIU website (https://www.bb.org.bd/bfiu/index.php)
(c) Domestic sanction list from BFIU website
(d) Unilateral or Regional sanction list forwarded by BFIU
(e) OFAC SDN & Non-SDN Sanction List
(https://sdnsearch.ofac.treas.gov)

Run a regular check including transactional review-

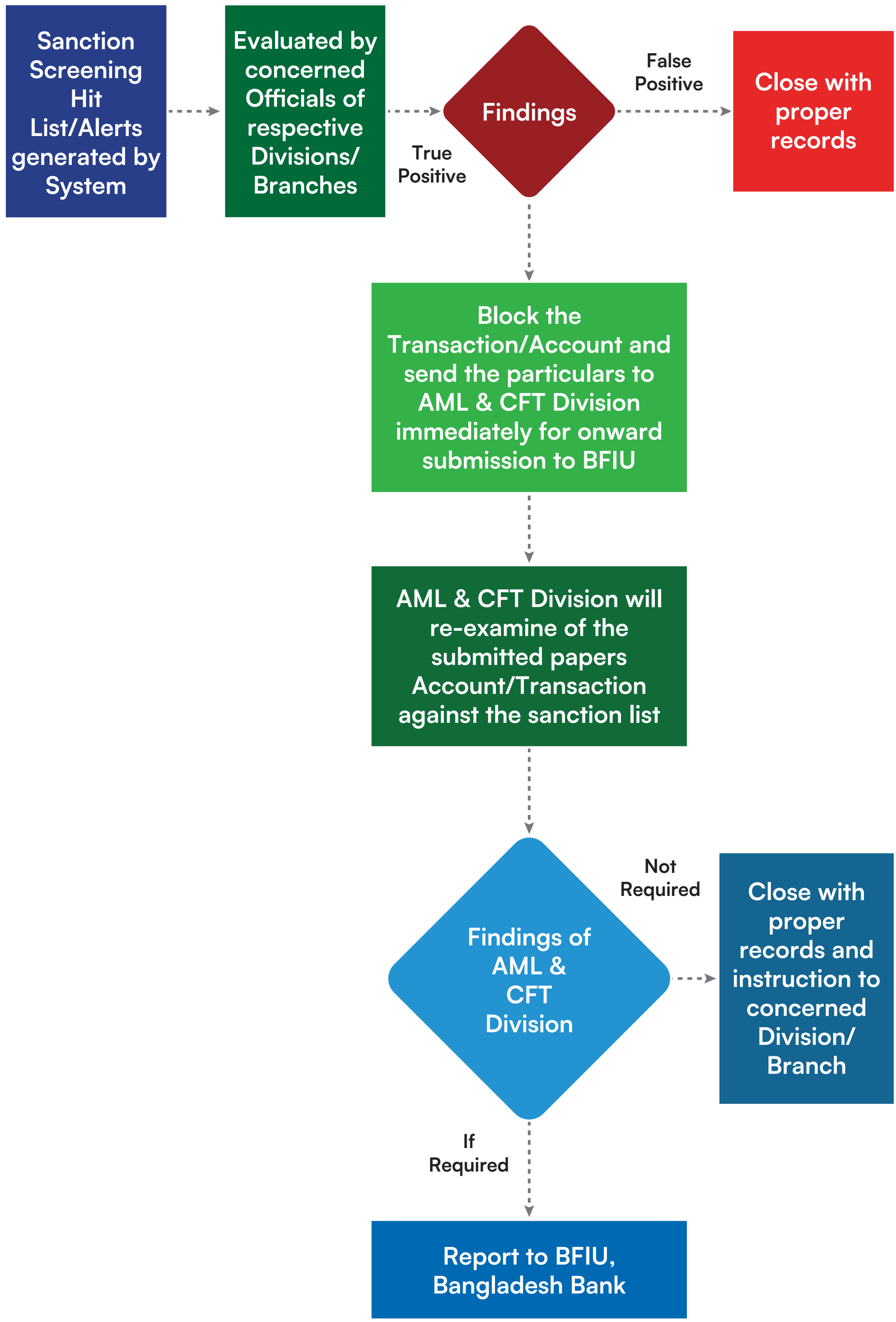
- before establish any relationship/ opening of any account
- check the existing accounts/customer
- before any foreign transaction through SWIFT
- before providing remittance service to the walk-in customer or over the counter
- screening on identified risk

If any match (True positive)

Report on the same day to AML&CFT Division

Report to BFIU (through PBL AML&CFT Division)

9.8 Screening Process business flow chart & action parties [SOP].



9.9 Screening Process for New/Walk-in Customer

a. Before opening any type of account, the concerned official of Branch/Division will check the name of applicant and beneficial owner in the system through Search Module.

b. In case of providing service to a walk-in customer name of Applicant/Beneficial Owner and Beneficiary shall have to be checked in the system.

c. If system does not find any 'True Match' the account can be opened, or service may be provided. Branch/Division has to retain the print copy of searching report duly signed by the Checker and Authorizer along with the Account Opening Form (AOF) or Customer Application Form.

d. In case of finding a 'True match' Branch will not open the account and not provide service to the customer and will submit the detail to AML & CFT Division within the same day. The report of 'True Match' has to be preserved in Branch/Division as a proof of rejection for future reference and send to AML/CFT Division for further analysis.

e. Head of Branch or Manger Operation/BAMLCO/DAMLCO will ensure that screening process has been duly followed for opening all type of accounts or providing service to walk-in customers.

9.9.1 Sanction Screen Process for existing Customers

PRIME BANK will conduct periodic rescreening of its entire customer base in a regular frequency to be determined by the Management from time to time. It's an auto process run by Head Office based on the updated UNSCR & OFAC, EU, HMT, HKMA, MAS, Bangladesh sanctions Data. Branch/concerned division Officials will check & verify the Alerts as well as preserve the False Positive Statement of existing Accounts list in the system. The process of handling alerts is described in brief in the section 9.9.7 of "Alerts Management Process".

9.9.2 Screening Process of Entities

Branch/Concerned Divisions need to check the entities name like: Correspondent/ Advising/negotiating Bank, LC Beneficiary/Importer/Exporter Company, Agent, Vessels & etc. through the Sanctions Screening System before establishing any relationship.

9.9.3 Remittance Screening Process

Remittance screening will include identify the receiver and sender of the Remittance who are in the published UNSCR & OFAC, EU, HMT, HKMA, MAS, Bangladesh sanction list. While doing any cross-border Remittance in foreign currency with any foreign country/ jurisdiction, the sanctions list issued by the respective country must follow in addition to UN and OFAC, EU, HMT, HKMA, MAS, Bangladesh sanctions list.

9.9.4 SWIFT Outgoing & Incoming Message Screening Process

The concerned branch/division should ensure sanctions screening of every SWIFT messages either manually or through automated system before executing. MT SWIFT messages (outgoing & incoming) must be screened centrally through Automated sanctions screening solution before it is transmitted or executed. The concerned division like Trade Services Division/CMO/FI/SWIFT Operations must check their respective SWIFT MT and if there is any True Match found, raise to AML/CFT Division for further analysis and resolve by defining TRUE or FALSE based on available documents and information.

9.9.5 Outgoing/Sending SWIFT Message

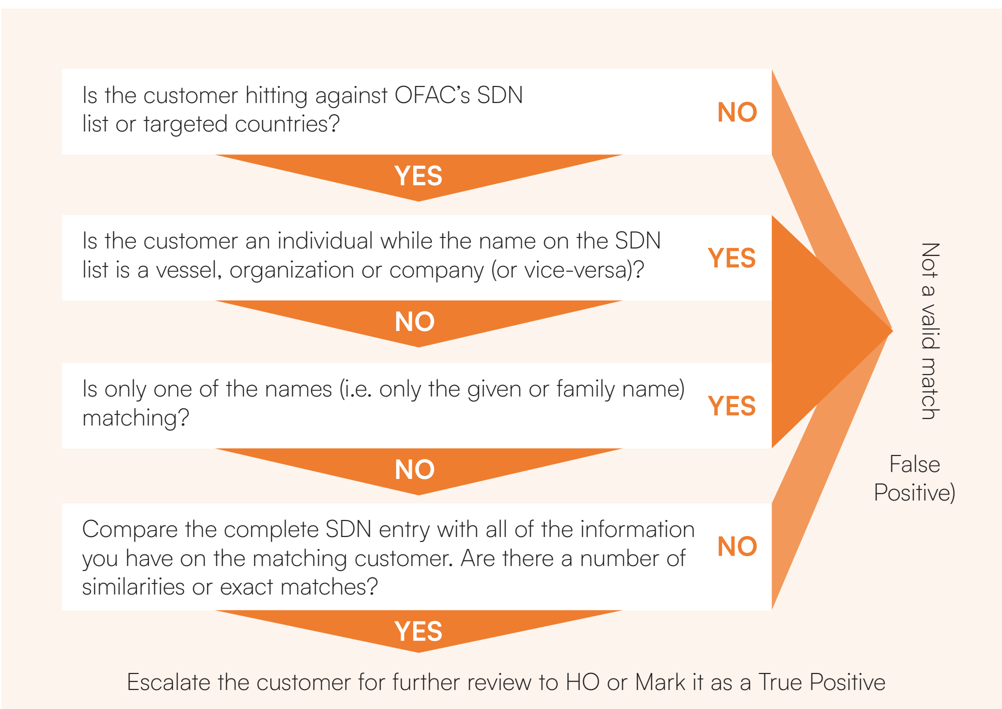
Messages are being generated automatically from our core banking solution TEMENOS T24 and then messages are transferred to Screening Server. Alerts (Hit List) are generated by the system automatically. The Sanctions Screening Users of respective Division (ex.: Trade Services Division/CMO/FI/SWIFT Operations) will review the Alerts.

9.9.6 Incoming/Receiving SWIFT Message

Bulk SWIFT Messages are being downloaded from our SWIFT system through AFT module. And Hit list generated by the system automatically. The Sanction Screening Users of respective Division (ex.: Trade Services Division/CMO/FI/SWIFT Operations) will review the Alerts.

9.9.7 Process of Managing Alerts generated by the Automated Sanction Screening Solution

Best practice or recommended process for name screening, which applies an assessment technique described as a process of elimination. OFAC is shown here as an example. It is applicable for any sanctions list.



1. System will generate alerts in following cases:
    i) At periodical screening of T24 accounts on daily basis,
    ii) At uploading Inward SWIFT messages in the screening system,
    iii) At generation of Outward SWIFT messages,
    iv) At uploading NRB Remittance File in the screening system,
    v) At uploading KYC information of Credit Card Holders for periodical screening.
2. In cases of generating alerts, system will forward the alerts to Checker of concerned Branch or Division of Head Office as per following schedule:
    i) In case of Periodical Screening of T24 Accounts, system will send the alerts to Checker of concerned Branch,
    ii) In case of screening of Inward SWIFT Messages, system will send the alerts to Checker of TSD/CMO/Treasury Operations etc. of Head Office.
    iii) In case of Screening Outward Messages, system will send the alerts to Checker of TSD/CMO/Treasury Operations etc. of Head Office and concerned AD Branches with a reference number.
    iv) In case of screening of NRB Remittances, system will send the alerts to Checker of NRB Operations/CMO, Head Office.
    v) In case of Screening of KYC information Card, system will send the alerts to Checker of Card Division/Card Operations, Head Office.
3. The parameters of generating alerts will be fixed by the admin user centrally as per approval of Management. At the initial stage system will generate alerts for 85% and above matches. The parameter may be changed in future as per approval of Management.
4. After generating alerts by login into the screening system Checker will show the alerts in the Home Screen/Dashboard.
5. Checker has to review the alerts considering the available information of the customer or applicant or the parties involved with the payment/message. The Checker has to manage the alerts by changing the status as follows:
    i) 'False Match' — if it is confirmed that it's a false match, which means that the customer/applicant/beneficiary is not the listed person/entity.
    ii) 'Pending Review'- if s/he can't take any decision and wants to forward it to her/his supervisor (Authorizer).
    iii) 'True Match'- if s/he finds satisfactory and justified matching in the information/ documents of the customer/applicant/beneficiary with the sanction list or there are enough reasons for suspicion.

iv) If AML/CFT Division finds satisfactory and justified matching in the information/ documents of the customer/applicant/beneficiary with the sanction list or there are enough reasons for suspicion, AML will submit to BFIU without delay/in the following day and block the account/business relationship.

6. System will forward all these alerts to Authorizer of concerned Branch or Division after changing the status by Checker.

7. The function of Authorizer is described below:

   i) 'Verify' — if Authorizer agrees with Checker s/he will select the option VERIFY.

   ii) 'Back to Checker'- if Authorizer does not agree with the decision of Checker, s/ he can send it back to Checker by selecting the option with necessary note in the field of comment.

   iii) In case of selecting 'Pending Review' by the Checker, Authorizer has to review the particulars of account or payment and will give her/his instruction in the field of comments to Checker for changing the status of the alerts.

8. In case of finding any 'True Match' the Authorized Officer of the Branch or Division has to block the account or transaction or payment immediately in CBS or respective system and has to submit all account or payment related papers to AML & CFT Division, Head Office, Dhaka within the same day for further analysis.

9. If any alert marked True/False wrongly, Authorizer of concern Branch/Division will review the related information and on his/her satisfaction a request has to be sent from his/her user to Admin User (AML & CFT Division, HO) through this solution (Sent to AML→ select the record in the field of "Sent for status rectification" → write a Review note→ Send to AML). Admin User of AMLD will reverse the alert at its initial stage and the Branch/Division has to manage the alert accordingly.

9.10 Sanctions Due Diligence for International Trade/Guarantee & Vessel Screening:

Sanctions due diligence is related to KYC and focuses on the risks specific to sanctions.

Divisions / TSD hubs/ Branches/ Foreign Subsidiaries/FI of PRIME BANK must check a customer or any instructing party involved in a trade finance transaction and enable the appropriate due diligence; checks on perceived 'high risk' customers; checks on Risk Based Approach (RBA) shall be applied.

The following shall be reviewed:

- Customers' trading partners (i.e. Country/Buyer/Seller/beneficiary/Shipper);
- Nature of the goods and their potential dual-use (military and civilian);
- Country of origin;
- Vessel name or IMO number;

- Details of vessels — such as owner of vessel, flag, journey history, name history;
- Beneficial ownership of the vessel and checks on the shipping company;
- Port of loading and discharge of the vessel;
- Ports of call of the vessel for the particular transaction flow (origin port, destination port);

9.11 Roles of Branches/Subsidiaries/Divisions of Head Office in preventing TF & PF

a. Branches or subsidiaries or concerned Head Office Divisions must comply established procedures as instructed by AML & CFT Division, Head Office for detection and prevention of financing of terrorism and financing in proliferation of weapons of mass destruction.

b. Branches or subsidiaries or concerned Head Office Divisions are required to conduct checks on the names of new customers, and regular checks on the names of existing customers or any other related individuals or entities in PRIME BANK Automated Sanctions Screening System. Once True Match found or confirmation has been obtained, they immediately must:

   i. stop payment or transaction of funds, financial assets or economic resources or any other services, if it is an existing customer;

   ii. reject the potential customer, if the transaction has not commenced;

   iii. report it to AML & CFT Division for ultimate submission to BFIU within the same day; and

   iv. AML will inform the relevant supervisory authorities within the next working day.

c. Branches or subsidiaries or concerned Head Office Divisions are required to ascertain potential matches with the Sanctions list to confirm whether they are true matches to eliminate “false positives”. The Branches or subsidiaries or concerned Head Office Divisions are required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.

d. Branch or Subsidiary or concerned Head Office Division is required to maintain all information & documents (electronic or paper) related to requirements & compliance of this chapter in accordance with record keeping requirements of BFIU Circular No. 26 dated 16.06.2020.

9.12 PRIME BANK Own Negative List:

Based on the severity or frequency of suspicious activity of customers or any false declaration of customer or fraud activities of customer, PRIME BANK has created its own negative list incorporating such persons to ensure not to open any account or any service in future by the bank.

Key Notes / Process:

a) Branch/Divisions/Department/Subsidiaries may provide name & other detail of customer to CCC/AML & CFT Division, which they want to put into the negative list.

b) Branch/Division/Department/Subsidiary and all other units of the bank MUST provide name and other details of the customer recommended to list in PRIME BANK Negative List along with supporting document (evidencing involvement of that customer in fraudulent/forgery/manufacturing document and ID etc.) to AML & CFT Division.

c) Negative lists may be circulated or displayed in PRIME BANK internal portal or incorporated in PRIME BANK automated sanctions screening system.

d) AML Division will review the proposal through proper scrutiny of the document and discussing with the proposing unit and seek approval from DCAMLCO and CAMLCO to add the customer in "Negative List". Upon obtaining approval from CCC/CAMLCO, they will incorporate the same in the sanctions screening solution. The same process is to be followed for delisting any customer from the list.

e) Delisting / Elimination process - the recommendation is required from respective Branches/Divisions /departments/Subsidiaries those who reported as a negative list.

f) Screening of PRIME BANK Negative List is mandatory prior establishing any account relationship.

9.13 Risk of Non-Compliance

In case of non-compliance BFIU can impose penalty on our Bank or can cancel license of the concerned Branch or Booth or can even instruct for taking administrative action against the concerned Officer(s)/Executive(s). If Bank faces any problem due to opening an account or conducting any transaction/payments to any listed person or entity without screening, the Checker and Authorizer of concerned Branch/Division will be held liable for that.

CHAPTER 10

E-KYC, KYC REVIEW & TRANSACTION MONITORING

10.1 e-KYC Background/Regulatory Guidance

In Bangladesh, Election Commission of Bangladesh holds the citizens (18 years and above) identity data with their biometrics has higher level of assurance and authenticity, where, the financial institutions' can have access to check the authenticity of customer provided identity data and bio-metrics by using this database. Therefore, BFIU has issued an e-KYC Guideline dated January 08, 2020 which is based on this national ID card and the bio-metrics data stored against each NID card.

This chapter contains a set of instructions for the financial institutions to enable them to conduct customer due diligence in a digital means.

10.2 Scope

This chapter shall be known as Electronic Know Your Customer (e-KYC) which deals with electronic customer onboarding, identification and verification of customer identity, creating of customer digital KYC profile as well as risk grading of customer in a digital means. The scope of this Guideline will be as follows:

(a) The provisions of this Guideline shall be applicable only for natural person;

(b) The requirements of this guideline shall be applicable based on the risk exposures of the customers of the financial institutions. For example, for an assessed low risk customer, financial institution shall be required to conduct simplified e-KYC which includes electronic customer onboarding, verify customer identity and preserve customer profile digitally, whereas, financial institution shall be required to conduct regular and enhanced e-KYC which includes electronic customer onboarding, verify customer identity, preserve KYC and risk grading in a digital manner for a customer with a regular and higher risks scenario;

(c) The e-KYC requirement of this Guideline is based on the biometric verification; therefore, a client whose status is legal person or legal arrangement excluded from the obligation of this Guideline. In this case, KYC and CDD norms for the legal person or legal arrangement shall be undertaken as per the provisions of the MLPA 2012, Anti-Terrorism Act (ATA), 2009, the MLP Rules, 2019, Anti-Terrorism (AT) Rules 2013; and instructions contained in the circulars and guidelines issued the BFIU time to time.

(d) Where e-KYC attempts failed due to any technical reason, the traditional KYC approach should be followed for the natural person.

10.3 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.

10.4 e-KYC Module based on Customer's Risk Exposures

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.

Simplified e-KYC limit

For Banking products

- Deposit or Withdrawal not exceeding BDT 1,00,000 per month in a checking account;
- Term Deposit upto BDT 10,00,000;
- Special deposit scheme with maturity value upto BDT 10,00,000;

For Agent Banking products:

Existing agent banking products within the transaction limits set by the Bangladesh Bank time to time;

(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/IPs), some Enhanced Customer Due Diligence (EDD) required to be undertaken.

Regular e-KYC limit

For Banking products: Other banking products except the banking products/limit mentioned in Simplified e-KYC limit.

For Agent Banking products: When agent banking customer performed transaction with the branch as a regular customer.

10.5 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 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 section 3.3 of the e-KYC Guideline.

10.5.1 e-KYC Procedure (Self Check-in)

Prime Bank has launched Self check-in e-KYC on June 09, 2021.

A. Simplified e-KYC

Person Responsible	Activities/ Tasks	Documents to be Used	Risk	Risk Mitigation
Customer (1-7)	1. Customer will visit E-KYC web URL or download mobile app 2. Enter self MSISDN/Mobile Number 3. Enter valid OTP 4. Select monthly transaction amount <has to be below or equal BDT 100,000 for simplified E-KYC as per BB guideline) 5. Upload NID image (both side) or take picture of NID image (both side) and take live selfie using web/app camera. 6. Select preferred product type (Savings-monthly basis or current account, currently these two product is available), enter other information like present and permanent address, nominee information, nominee NID/Birth Certificate/ Passport, Nominee photo (selfie or photo upload) and upload e-signature (not mandatory) and preferred branch, profession details 7. Customer select other information like FATCA and PEP/IP	• Customer NID • Live photo of customer • Nominee NID/ Passport/ Birth Certificate & photo • Digital Signature/ e-Signature (Optional)	• Customer try to open account using other person NID • Wrong nominee information & photo •	• Liveliness check and NID and photo verification with EC data • LOD will check manually before removing post no debit
Automated system (8-11)	8. Customer sanction screening 9. Customer duplication checking 10. Notify customer with newly generated a/c no. through SMS 11. Notify customer with proper message and request to contact with nearest branch in case of any decline scenario (due to dedupe, Sanctions, FATCA)	• Existing Server/ database data of customers	• Existing Customer can be created by creating new Customer ID instead of existing one • Customer try to open account by clicking FATCA yes	• LOD will check and adjust/shift customer to existing customer ID • System will stop and tell customer to visit nearest branch

Person Responsible	Activities/ Tasks	Documents to be Used	Risk	Risk Mitigation
LOD (12-14)	• Update customer account & TP related information in T24, also give necessary inputs for debit card and cheque book requisition (if any) as per existing process. Here customer will get only Master debit card and the printing name will be the Title of the account • Authorize the entries in T24 • In Exceptional cases LOD user can send it to tagged branch to notify customer regarding additional document/ information requirements	• NID, Live photo and signature of customer and nominee information uploaded by customer	• Negligence from LOD manpower can approve an account which should not be approved • Invalid card/ cheque application • Insufficient fund for Cheque Book	• Proper Due Diligence should be ensured at the time of account approval • Tell customer the proper reason or suggest them to visit nearest branch • System to create Demand for realization of Cheque Book fee post facto (in case of insufficient fund)
Branch (15-18)	• Identify Customer who opened A/C in e-KYC Platform by checking NID / Customer Photo from PI Archival • Serve customer regarding Signature Card Update or any other service request through Pi Servicing Workflow as an existing customer • Upload document / Customer Picture and send it to LOD • Follow up on completion of the service request	• valid documents (NID/ Photo ID) shared by customer.	• Lack of proper validation/ Identification of Customer • Validation of Provided Documents	• Proper Due Diligence should be ensured at the time of face to face customer serving by Sighting Original NID/ Document • Branch needs to check Pi Pending Flow/ Archival Workflow to identify customer & documents

B. Regular e-KYC

Person Responsible	Activities/ Tasks	Documents to be Used	Risk	Risk Mitigation
Customer (1-7)	1. Customer will visit e-KYC web URL or download mobile app 2. Enter self MSISDN/Mobile Number 3. Enter valid OTP 4. Select monthly transaction amount (has to be above BDT 100,000 for regular e-KYC as per BB guideline) 5. Upload NID image (both side) or take picture of NID image (both side) and take live selfie using web/app camera. 6. Select preferred product type (Savings-monthly basis or current account, currently these two product is available), enter other information like present and permanent address, nominee information, nominee NID/Birth Certificate/Passport, Nominee photo (selfie or photo upload) and upload e-signature (not mandatory), preferred branch, profession details 7. Customer select other information like FATCA and PEP/IP 8. Customer upload income proof document and address proof document 9. Customer upload e-signature	• Customer NID • Live photo of customer • Signature photo of customer • Nominee NID/ Passport/ Birth Certificate & photo • Address & Income Proof Documents • • Digital Signature/e-Signature (Optional)	• Customer try to open account using other person NID • Wrong nominee information & photo • Upload wrong address proof document and income proof document	• Liveliness check and NID and photo verification with EC data • LOD will check manually before removing post no debit
Automated system (10-13)	10. Do customer sanction screening 11. Do customer duplication checking 12. Notify customer with newly generated a/c no through SMS 13. Notify customer with proper message and request to contact with nearest branch in case of any decline scenario (due to dedupe, Sanction, FATCA)	• Existing Server/ database data of customers	• Existing Customer can be created by creating new Customer ID instead of existing one • Customer try to open account by clicking FATCA yes	• LOD will check and adjust/shift customer to existing customer ID • System will stop and tell customer to visit nearest branch

Person Responsible	Activities/ Tasks	Documents to be Used	Risk	Risk Mitigation
LOD **(14-20)**	14. Newly generated account validation 15. Check and decide whether debit restriction should be withdrawn 16. Update customer account & TP related information in T24, also give necessary inputs for debit card and cheque book requisition (if any) as per existing process. Here customer will get only Master debit card and the printing name will be the Title of the account 17. CPV (Contact Point Verification), check whether customer upload proper address proof document 18. Authorize the entries in T24 and remove debit instruction 19. Send it to tagged branch to notify customer regarding additional document/information requirements 20. Complete the request after all fulfilments	• NID • Live photo of customer • Signature photo of customer • Nominee NID & photo • Other relevant information & documents	• Negligence from LOD manpower can approve an account which should not be approved • Invalid card/ cheque approval • Proper CPV	• Proper Due Diligence should be ensured at the time of account approval
Branch (21-25)	21. Meet and communicate with customer regarding deficiency 22. Identify Customer who opened A/c in EKYC Platform by checking NID /Customer Photo from PI Archival 23. Issue resolution 24. Upload document (if required) and send it to LOD 25.Complete the request	• Rectified valid documents shared by customer	• Lack of proper validation of rectification of documents	• Proper Due Diligence should be ensured at the time of face to face customer serving by Sighting Original NID/ Document • Branch needs to check Pi Pending Flow/ Archival Workflow to identify customer & documents

10.6 Periodic KYC Review & Transaction Monitoring

Periodic KYC review involves the simple procedure of submitting the latest identity and address documents to the bank. There is regulatory guidance for doing periodic KYC review/update in every 5 (five) years for the low-risk accounts and 1(one) year for high-risk accounts [BFIU circular no. 26 dated 16th June, 2020 (section no 3.6.4)]. Transaction monitoring will be conducted by BAMLCO of respective Branch.

10.7 Threshold limit for Simplified e-KYC Account

In accordance with the Bangladesh Bank e-KYC Guidelines, Bank must implement a robust system to manage account thresholds, particularly for Simplified e-KYC accounts. Under these regulations, a Simplified e-KYC account—typically opened using only an NID is subject to Deposit or Withdrawal not exceeding BDT 1,00,000 (one lakh) per month in a checking account. To ensure regulatory compliance and risk mitigation, this threshold limit should be strictly incorporated into the bank's Core Banking System (CBS) to act as an automated hard block. Consequently, any customer who has opened an account through the simplified process must not be allowed to perform any transaction that exceeds this established limit. In the event a customer attempts a transaction above the simplified threshold, the system should trigger a real-time notification informing them that they must complete Regular KYC—which involves providing additional documentation such as proof of income and a full physical or digital due diligence—to enable regular, high-value transactions.

CHAPTER 11

HUMAN RESOURCE POLICY STATEMENT ON ANTI-MONEY LAUNDERING AND COMBATING FINANCING OF TERRORISM (AML & CFT)

11.1 Introduction:

It is our policy to operate all of our day-to-day business activities in an honest and ethical way. We took a zero-tolerance approach to money laundering, corruption or fraud-forgery and are committed to act professionally, fairly and with integrity in all our relationships and business dealings wherever we operate and to implementing and enforcing effective systems to counter corruption or fraud-forgery. Prime Bank has 'Employee Code of Ethics and Business Conduct' and Employees' Service Rules, 1995 (with up-to-date amendment) which works as framework of ethical and business behavior for employees. This provides guidelines on various issues, like, safeguarding customers' and Bank's confidential information, preventing money laundering or any fraudulent activity, complying with laws and regulations, etc. If any employee contravenes any provision of 'Employee Code of Ethics and Business Conduct', he/she shall be punished under Chapter — VIII & IX (General Code and Discipline & Disciplinary Action) of the said Service Rules.

Our honorable Board of Directors are well conversant with all the guidelines/policies and procedures regarding Anti-Money Laundering, Combating Terrorist Financing and Anti-Corruption. Prime Bank PLC. Family is consisting of nearly 3,200 Employees and 146 Branches in Bangladesh. The Concerned Division/Department regularly conveys the update circulars and instructions regarding AML & CFT to the Branches, Divisions and Departments as well.

As a part of communication with Customers/Business Partners the Branch Officials/Executives should displayed AML&CFT awareness banner/festoon in the branch premises and distribute leaflet at the time of opening account and on regular interval to create awareness among the customers.

Prime Bank PLC. is committed to prevent, detect and deter money laundering and terrorist financing. To that end, it is the responsibility of every employee (including contractual and part time employees) to comply with this program and all related acts i.e. Money Laundering Prevention Act-2012 (Amended in 2015), Anti-Terrorism Act-2009 (Amended in 2012 & 2013) etc. In accordance with these laws and regulations Bank must have an Anti-Money Laundering (AML) and Combating Financing of Terrorism (CTF) program that consists of following elements:

- Appointment & Qualification of CAMLCO;
- Appointment & Qualification of Deputy-CAMLCO;
- Appointment of a Branch Anti-Money Laundering Compliance Officer;
- Employee Screening Program;
- Administrative Action on Breaches and Non-Compliance;
- Training Program;
- Annual Performance Evaluation;
- AML & CFT Compliance Effectiveness Reviews;

11.2 Appointment, Qualification and Roles & Responsibilities of CAMLCO:

A Chief Anti-Money Laundering Compliance Officer (CAMLCO) is someone holding a management position (up to 2 (two) steps below the managing director/ chief executive officer) in the Bank that is appointed by Managing Director & CEO , and who is responsible for ensuring that the Bank complies with its obligations under the Anti-Money Laundering and Anti-terrorism related Acts & Rules.

(a) Appointment:

- The Managing Director & CEO shall appoint the CAMLCO at Head Office with sufficient authority to implement and enforce corporate wide AML & CFT policies, procedures and measures and who will report directly to MD & CEO;
- The designated CAMLCO, directly or through the CCC, shall be the central point of contact for communicating with the regulatory agencies regarding issues related to the Bank's AML & CFT program.
- As the CAMLCO is responsible for the oversight of all aspects of the Bank's AML & CFT activities and is the focal point for all activity within the Bank relating to ML & TF, his/her job description shall have to be clearly set out the extent of the responsibilities given to him/her.
- Before assigning the CAMLCO to other duties of the Bank, the Management has to be sure that the AML & CFT activities of the Bank will not be hampered; and
- If the CAMLCO is changed, it must be informed to Bangladesh Financial Intelligence Unit (BFIU) without delay.

(b) Authorities & Responsibilities:

- Please see section 3.8 of this guideline

11.3 Appointment, Qualification and Roles & Responsibilities of Deputy-CAMLCO :

Deputy-CAMLCO is someone who will be the head of the AML & CFT Division and to whom Branches/Divisions/Department will report their day-to-day AML & CFT activities.

a. Appointment:

- The Managing Director & CEO shall appoint the D-CAMLCO at Head Office to implement and enforce corporate wide AML & CFT policies, procedures and measures under supervision of CAMLCO;
- D-CAMLCO shall appoint as the Head of AML & CFT Division;
- The designated D-CAMLCO, through the CCC, shall be the central point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML&CFT program after CAMLCO.

- As the D-CAMLCO is responsible for the oversight of all aspects of the bank's AML & CFT activities and is the focal point for all activity within the bank relating to ML & TF after CAMLCO, his/her job description shall have to be clearly set out the extent of the responsibilities given to him/her under supervision of CAMLCO.
- Before assigning the D-CAMLCO to other duties of the bank, the management has to be sure that the AML & CFT activities of the bank will not be hampered; and
- If the D-CAMLCO is changed, it must be informed to BFIU without delay, if required.

b. Qualifications:

- D-CAMLCO shall be at least in the rank of 'Senior Vice President' of the bank.
- He/she shall be a sufficiently senior person having the authority to implement and enforce Anti-Money Laundering policies, procedures and measures and will report directly to CAMLCO.
- He/she will have vast knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML, TF & PF.
- He/she will also have vast knowledge & experience on general banking, investment, and foreign exchange business of the bank.

c. Authorities & Responsibilities of D-CAMLCO

- Please see the section 3.9 of this guidelines.

11.4 Appointment, Qualification and Roles & Responsibilities of BAMLCO

a. Appointment:

- This is the authority of Central Compliance Committee (CCC) to appointment of BAMLCO in every Branch and sub-branch.
- CCC has given the authority to Head of Branch to nominate BAMLCO as per Bank's AML policy. If HoB plays the role of BAMLCO in branch, the office order should be signed by Head of BDN. For sub-branch the BAMLCO Order will be signed by the HoB of mother branch.
- Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her appointment letter.

b. Qualifications:

- The Head of Branch (HoB) or Branch Operation Manager (BoM) shall be nominated as the BAMLCO of the branch. In sub-branch, the in-charge of sub-branch shall perform the role of BAMLCO.
- The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and bank's own policies & guidelines on preventing Money Laundering, Terrorist Financing & proliferation financing.

- He/she will also have vast knowledge & experience on general banking, investment and foreign exchange business of the bank.

c. Authorities & Responsibilities of BAMLCO:

- Please see section 3.11 of this guideline

11.5 Employee Screening Program:

As per Chapter—9, Clause no # 9.2 of Money Laundering & Terrorist Financing Risk Management Guidelines 2015 of BFIU, the Banks are advised to follow the following measures (at least one from below) to perform screening of applicants before appointment:

- Reference check;
- Background check;
- Screening through or clearance from Law Enforcement Agency;
- Personal interviewing;
- Personal guarantee etc.

According to Clause # 14 (Employee Screening) of the Recruitment & Selection Policy, in compliance with Money Laundering & Terrorist Financing Risk Management Guidelines of BFIU 2015, all selected candidates (fresh or lateral) for employment with Prime Bank shall go through the following verifications before issuance of Appointment Letter. The Bank will strive to comply with any three of the following background verifications either through internal resources or nominated 3rd Party Agency:

a. Previous employment check.

b. Academic and professional qualification verification.

c. Police Verification

d. Independent identity checks (Passport or NID).

e. Self-declaration on Credit history.

Any discrepancies in the information provided by the candidate will cancel the letter of offer/ appointment and may lead to termination.

As such, currently Human Resources Division of the Bank is conducting the following:

1. **Background verification:** Background and criminal history of the finally selected candidates are checked through Police verification.
2. **NID verification:** NID of finally selected candidates are verified from the web portal of Election Commission of Bangladesh Government.

3. **Academic certificate verification:** Academic certificates of the finally selected candidates are verified either through internal resources or nominated 3rd Party Agency. Please note that we have started the above verification from September 2017.

4. **Corporate Memory Management System (CMMS):** CMMS of Bangladesh Bank is used for checking disciplinary actions record of the entire job history of concerned candidates during recruitment.

5. Self-declaration by the finally selected candidates on (a) Relative Declaration, (b) Declaration of Accounts of Staff, (c) Personal and/or Individual Borrowing, (d) Outside Business Interest. Finally selected candidates undertake to take prior permission from the Bank in case he/she wants to involve in any outside business interest which includes (but not limited to) becoming a director/ beneficiary/ partner/ active participant/ sponsor/ volunteer for any organization outside Prime Bank PLC.. In the event if this declaration is found to be false at a later stage of employment with Prime Bank PLC., appropriate disciplinary action(s), up to separation from service, may be taken by the Competent Authority of the Bank.

11.6 Administrative Action on Breaches and Non-Compliance:

If any Non-Compliance found or Complaints is associated under Predicate offences under Money Laundering Prevention Act (MLPA) - 2012(amendment -2015), HR Division will follow the procedure as set out in the Policy "Disciplinary Action Policy Against Money Laundering and Terrorist Financing Activities".

11.7 Training Program:

Obligation Under; "Money Laundering & Terrorist Financing Risk Management Guidelines" -2015	As per section 9.4 of "Money Laundering & Terrorist Financing Risk Management Guidelines" issued by BFIU, every employee should have at least day long basic AML & CFT training. Before assigning an employee in a particular job or desk, banks shall examine the consistency and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

As a part of the Prime Bank's AML & CFT Compliance program, all Employees are expected to be fully aware of the Prime Bank's AML & CFT policy and procedures. Each Employee is required to read and comply with this Compliance policy and procedures, address concerns to the Compliance Officer and ensure that he/she has read and understands Prime Bank's AML & CFT policy and procedures. All Employees are required:

- To undertake training programs on AML & CFT policy and procedures.

- To get trained in how to recognize and deal with transactions which may be related to money laundering. To timely escalate and report the matter to the Compliance Officer.

- To get themselves acquainted with Anti Money Laundering Rules & Regulations.

- To comply with the requirements of Rules & Regulations.

- **Customer contact staff/RM/Front desk officials:** This is the front line of defense against money laundering; the ones who need the deepest practical understanding of why anti money laundering efforts are important and what they need to do to be vigilant against money laundering and Terrorist financing.

- **Back office personnel:** These employees may also need special training, like TSD, LOD, CMO, Treasury back-office, NRB Operations & CRM.

- **Audit and compliance staff:** These are the employees charged with overseeing, monitoring and testing AML & CFT controls, and they should be trained about changes in regulation, money laundering methods and enforcement, and their impact on the institution.

- **AML Compliance staff:** These are the employees who are placed in AML & CFT Division or CCC member of the Bank. While they likely do not need the general AML course that would be provided to most employees, this group needs specialized advanced training to be able to stay on top of new trends or changes that impact the institution and the way it manages risk. Often, this will require attending conferences or AML specific presentations that go into greater detail.

- **Senior Management and Board of Directors:** Money laundering issues and dangers should be regularly and thoroughly communicated to the Senior Management & Board of Directors. Arrange conferences/seminar on AML & CFT to keep Senior Management & Board members aware of the reputational risk that money laundering & terrorist financing poses to the institution.

- **Awareness of Customer**

  The customers of the bank are the prime groups that should be made aware of AML & CFT activities occurring through the banking channels. The customers should be made aware of the bad effects of executing ML & TF like harming the economy of the country, tarnishing the image of the country and developing a tendency to neglect the related laws & rules. In this connection, the branch/concerned division/department will place the awareness festoon in the suitable place of Branch premises and arrange awareness building initiatives like the distribution of leaflets, handbills, brochures, etc.

- **Awareness of Mass People**

  The mass people should be made aware of the AML & CFT activities and their bad effects on the society, economy and all over the country. In this connection, the bank should take different steps like circulating/ broadcasting/ telecasting appropriate advertisements and documentaries on radios, televisions and/ or other mass media, whichever deems best. The bank should also participate in awareness building initiatives often arranged by BFIU, Bangladesh Bank, the government and other regulatory bodies. Additionally, the bank will take different steps like using billboards, posters, festoons, distributing leaflets, handbills and using other media as well.

Human Resources Training & Development Center (HRTDC) and AML & CFT Division jointly/ individually should design an effective training program to identify the target audience.

11.8 Annual Performance Evaluation:

- Adequate Knowledge on AML & CFT;
- Training Status on AML & CFT;
- Job performance on AML & CFT issues on Branch/Division;
- Non-compliance on AML & CFT issues on Branch/Division;

During the performance evaluation of the employees, his/her knowledge and skill of compliance of laws/ bye-laws, rules/ regulations, orders and any instructions of the Bank or regulatory authority are taken into consideration under the Performance Appraisal System which has been approved in the 240th Meeting of Bank's Board of Directors, held on 25.01.2006, vide Board Memo No. 2006/5645 dated 23.01.2006. Besides, AML audit rating (Audit conducted by AML & CFT Division or Internal Audit Department), disciplinary issues of the respective employees due to audit objections or non-compliance of AML & CFT issues are also taken into consideration during finalize their performance rating.

11.9 AML Compliance Effectiveness Reviews:

Bank will re-evaluate the Human Resource Policy on AML & CFT in reasonable time or time-to-time that will assess how well our compliance program is functioning.

The management should be aware of the fact that vested groups in connection with Money Laundering try to entice employees of banks and financial institutions for transacting their ill-gotten money in and out of the banking channel. For that reason, we have to utilize an elaborate and industry standard screening mechanism to attract and retain employees with the highest level of integrity and competence. The Human Resources Division must ensure that employee screening mechanism is an integral part of the recruitment process.

CHAPTER 12

REPORTING

Obligations under Law	Section 2(Z) of MLPA, 2012 and Section 2(16) of ATA, 2009
Obligations under Rules	MLP Rules, 2019

Every bank is obliged to send various reports (Suspicious Transaction / Activity Report, Cash Transaction Report, Half-Yearly Report & etc.) to Bangladesh Financial Intelligence Unit (BFIU) without any delay or in due time. Besides they have to produce any documents that is sought by BFIU.

12.1 Cash Transaction Reporting

Every branch will prepare the monthly Cash Transaction Report (CTR) of Tk. 10 Lac and above for cash transaction per day (Including Online, ATM related any cash Deposit or Withdrawal separately) and send it to CCC/AML & CFT Division in due time every month as per BFIU Circular no. 26 dated 16/06/2020 through existing software named "FIU Reporting System (goAML)". After receiving CTR from all branches, centrally CCC/AML & CFT Division will submit the report to BFIU through web based application named "goAML". If the branch has not any such transaction, it should be report to the CCC/AML & CFT Division as 'There is no reportable CTR'. Besides, every branch needs to preserve its CTR in their own branch.

Recognition of Suspicious Cash Transactions:

- Branches need to identify whether there is any suspicious transaction reviewing the Cash Transactions Report;
- If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' separately to the CCC/AML & CFT Division through PrimeDefence;
- In addition to that CCC/AML & CFT Division conduct data validation and transaction monitoring on random basis and risk based approach.
- If any suspicious transaction is found, the CCC/AML & CFT Division will submit it as 'Suspicious Transaction Report' separately to the BFIU.

Accurate Customer Information:

- The branches have to send CTR data with accurate and full customer information in the PRIME BANK CTR Reporting System.
- In case of information of CTR reported customer- Name, Father's Name, Mother's Name, Spouse Name, Present, Permanent & Official address, Gender, Identity document like NID, Passport, Birth Registration Certificate, Driving License, e-TIN (if any), Date of Birth, Place of Birth, Nationality, Occupation details, contact no. etc. should be full and accurate where sending to Head Office (PRIME BANK CTR Reporting System).

Online CTR Submission:

- The branches have to send the CTR through our internal web based software "FIU Reporting System (goAML)";

- The branches have to ensure the accuracy & timeliness while reporting to CCC/AML & CFT Division;
- The CCC/AML & CFT Division needs to prepare the accumulated CTR received from its all branches;
- The CCC/AML & CFT Division must ensure the accuracy and timeliness while reporting to BFIU.
- CCC/AML & CFT Division has to inform BFIU through the message board of 'goAML' web in case of no transaction is found to be reported as CTR.
- Moreover, CCC/AML & CFT Division as well as branch must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

12.2 Suspicious Activity (SA) /Suspicious Activity Reporting (SAR)/Suspicious Transaction Reporting(STR):

Suspicious activity can be identified both during the on-boarding or ongoing due diligence of a client as well as during the transaction monitoring process and may be raised by any employee of a reporting organization.

Under Section 25(1)(d) of MLPA, 2012, ROs shall have to report any doubtful transaction or attempt of such transaction as defined under Section 2(z) of the same act as suspicious transaction report to the BFIU immediately on its own accord.

Suspicious Activity (SA) arises from suspicion relating to general behavior of the person in question which creates the knowledge or belief that he or she may be involved in illegal activities out of which proceeds might be generated. Any suspicious attempted transaction also falls in this category.

Suspicious Activity Reporting **(SAR)** means reporting related to Customer suspicious activity (SA), where there might be no involvement of transaction.

Generally **STR** means a formatted report of suspicious transactions where there is reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seems to be usual manner. Suspicion basically involves a personal and subjective assessment. Branches have to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

As per Section 2(z) of Money Laundering Prevention Act, 2012 (including all amendments -2015)

'Suspicious Transaction' means such transactions —

a) which deviates from usual transactions;

b) 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;

c) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by BFIU from time to time.

As per Section 2(16) of Anti-Terrorism Act, 2009 (including all amendments -2012 & 2013)

'suspicious transaction' means such transactions —

a) which is different from usual transactions;

b) which invokes presumption that,

   1. it is the proceeds of an offence under this Act,

   2. it relates to financing of terrorist activities or a terrorist person or entity;

c) which is any other transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.

   ISAR — means bank's internal STR/SAR that has been closed in Branch or Division level after getting document/justification/explanation which is satisfactory to branch/division.

Evaluation of Internal Suspicious Activity Report (ISAR)

- All officials engaged in our branches/different divisions must be aware to identity the suspicious activity of Customer and he/she must report it to BAMLCO/DAMLCO/AML&CFT Division/CCC.
- All relevant officials must be aware about STR/SAR reporting process and if any suspicious activity/transaction is occurred by any desk then it should be reported by the respective desk official to BAMLCO/DAMLCO/AML&CFT Division/CCC through PrimeDefence.
- BAMLCO/DAMLCO should evaluate that report and if found any suspicious matter then he should obtain approval from Head of Branch or Head of Division and submit to the CAMLCO/ AML& CFT Division through the system.
- User guidelines for PrimeDefence (STR & SAR Reporting System) may be followed for detail process.

Identification/Recognition of Suspicious Transactions

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

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

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

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 branches 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 Trade Based Money Laundering (TBML). In this regard the study of foreign exchange remittances may help detect the offence.
- The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities or sensitive / non co-operative jurisdictions.
- The commodity is transshipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense.
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.

- Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.
- Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management.

Red Flags pointing to Financing of Terrorism

Behavioral Indicators:

- The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- Use of false corporations, including shell-companies.
- Inclusion of the individual or entity in the United Nations 1267 and others Sanction 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.

Red Flags pointing to Credit Backed Money Laundering

- Customer under Customs authority / NBR / ACC observation or investigation.
- Negative / adverse news regarding Customer.
- Fake Documents / Mortgaged deeds.
- Certificates of deposits used as collateral.
- Loan proceeds used to purchase property in the name of a third party.
- Loan payments by third parties.
- Collateral pledged by a third party.
- Formation of a new company in the name of employees.
- Borrower request to disburse the loan by issuing cheques in favor of another Bank/ FIs/Third Parties.
- Large Cash Transaction inconsistent with customer's Business/Profession.

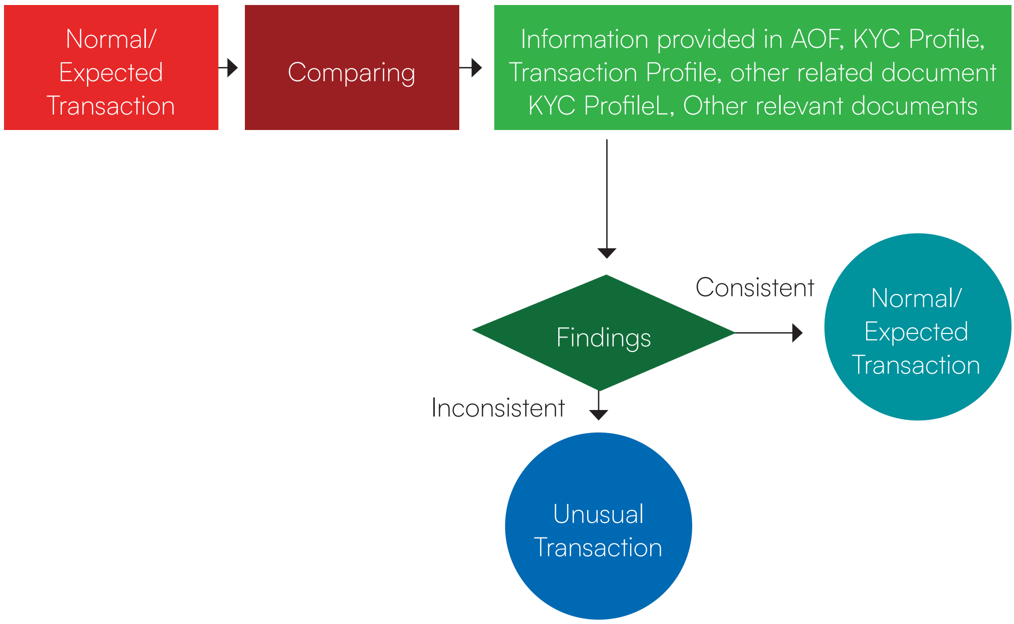
- Huge Credit Balance in the Loan Account.
- Transfer of funds between irrelevant Businesses.
- Multiple online Deposit/Withdrawal from irrelevant Locations.
- Over valuation of the Property to be Mortgaged.
- Sudden/unexpected payment on loans

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.

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

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



- **Suspicious Transaction Reporting Procedures:**

  The identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, branch/division should conduct the following 3 stages:

  Identification:

  This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of banks monitoring of unusual transactions may be automated, manually or both. Our Bank has been using software based Transaction Monitoring system where some specialized feature on that software which can help branch officials to detect unusual transactions or activities.

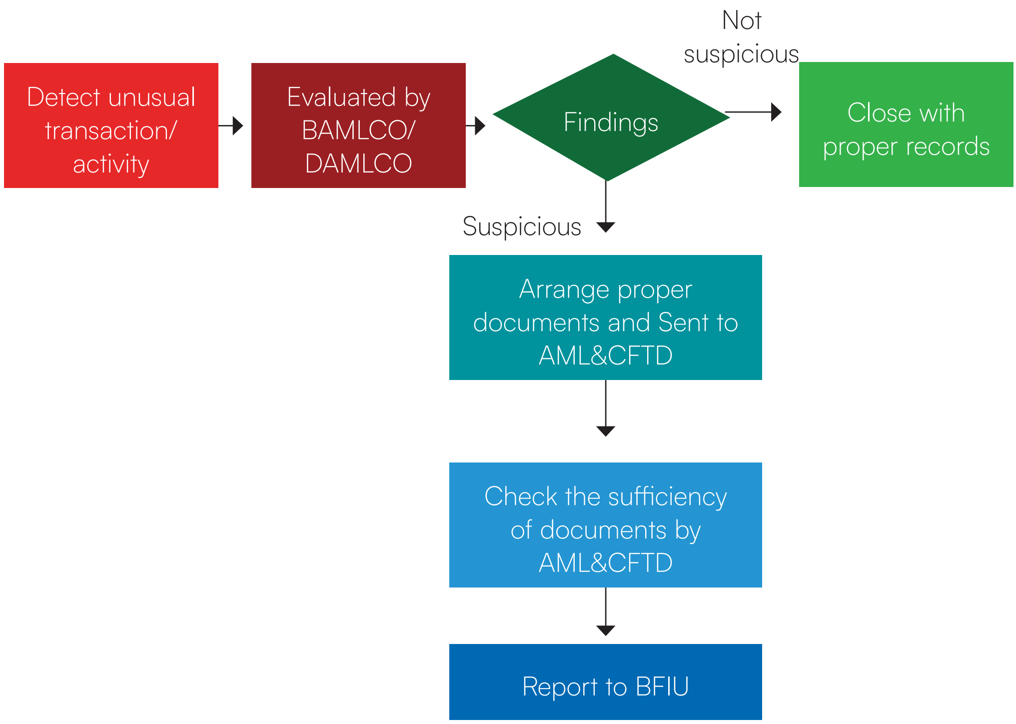
  Evaluation:

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

Disclosure:

This is the final stage and branch/division should submit STR/SAR to BFIU through AML & CFT Division if it still looks suspicious.

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



Filling an STR:

The final output of an AML & CFT compliance program is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the AML & CFT risk for banks. Therefore it is necessary for the safety and soundness of the PRIME BANK. The following matter should be taken regarding submission of an STR/SAR:-

1. After receiving any SAR/STR from any desk officer which is finally reportable to CCC, BAMLCO/DAMLCO should fill up all mandatory fields in PrimeDefence carefully;

2. The following documents should be attached with STR/SAR form in electronic format (scan copy):

    i) Account Opening Form along with submitted documents,

    ii) KYC Profile, Transaction Profile,

   iii) Account Statement for last one year,

   iv) Supporting Voucher/correspondence for reported transaction(s) (mandatory for STR),

   v) Copy of adverse news (mandatory of AMSAR & AMSTR)

   vi) Others (if any);

3. Finally STR should be submitted by 'HoB' to 'CAMLCO' of the CCC by separate Letter for every particular STR with 'Confidential' marked;
4. Office copy of all related documents should be preserved in separate file at branch level.

Review of SAR/STR documents:

The following matter should be taken while reviewing the documents related to SAR/STR:-

1. After receiving any SAR/STR from any desk officer, BAMLCO/DAMLCO should review and analyze all documents that are required;
2. Account Opening Form should be properly filled up along with all relevant information;
3. Reason should be briefly described;
4. Reported Transactions and reason should be relevant & accurate;

Tipping Off

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

12.1 Quarterly AML/CFT Meeting Minutes Report

As per BFIU Circular no. 26, section 1.3(5) BAMLCO will arrange AML & CFT meeting with other concerned important officials of the branch quarterly and will 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 UNSR including screening of Bank's approved designated sanctions list,
- Self-assessment,

- Record keeping,
- Training,

Branch will submit the quarterly meeting minutes (signed copy) along with copy of agenda and attendance to AML & CFT Division within 15th of following month after ending of each quarter.

12.2 Self-Assessment Reports & Independent Testing Procedures

For prevention of money laundering and combating the financing of terrorism and reviewing the Self-Assessment report from Branches as BFIU Circular No. 26 Annexure-'Ga' and proper judgment of Independent Testing Procedures, adequate manpower should be allocated to Internal Audit Department whose have to knowledge regarding AML/CFT related existing Laws, Rules, Instructions of BFIU Circular No. 26 Annexure-'Gha' and internal policy of the bank.

12.2.1 Responsibilities of the Branch regarding Self-Assessment Report

Banking system in Bangladesh is mainly based on branch banking. The branches of the banks are in every corner of the country and they have an active role in stimulating the economic growth of the country. It is very difficult for the CCC/AML & CFT Division or Internal Audit to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFIU has established a Self-Assessment Reporting system for the branches.

- According to the instructions of BFIU, branches of our bank need to conduct the Self-Assessment to evaluate them on a half yearly basis. Self-Assessment has to be done through a checklist that is circulated by BFIU Circular no. 26, dated 16/06/2020 (Annexure-Ga);
- Before finalizing the evaluation report, there shall have to be a meeting presided over by the Branch Relationship Manager with all concerned officials of the branch;
- All Questionnaire's answer of 'Self-Assessment' relating to 'Branch's Present Status' and 'Taken Initiative/Recommendation' should be accurate and relevant;
- In that meeting, there shall be a discussion on the branch evaluation report; if the identified problems according that report are possible to solve at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations shall have to be jotted down;
- In the subsequent quarterly AML/CFT Meetings at the branch, the progress of the related matters should be discussed;
- After end of every half year, the branch evaluation report along with the measures taken by the branch in this regard and adopted recommendations regarding the issue should be submitted to the Internal Audit Division and the AML & CFT Division of Head Office separately within the 15th of the next month.

12.2.2 Responsibilities of Internal Audit Division regarding Independent Testing Procedures

The audit must be independent (i.e. performed by people not involved with the bank's AML & CFT compliance). Audit is a kind of assessment of checking of a planned activity. Independent testing has to be done through a checklist that is circulated by BFIU Circular no. 26, dated 16/06/2020 (Annexure-Gha).

- The individuals conducting the audit should report directly to the board of directors/ senior management. Audit function shall be done by the Internal Audit Division of Head Office. At the same time external auditors could be appointed (if possible) to review the adequacy of the program.
- The Internal Audit Department of Head Office shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the CCC / AML & CFT Division.
- While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the Internal Audit Department should examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure.
- The Internal Audit Department should send a copy of the report with the rating of the branches inspected/audited by the Internal Control & Compliance Division to the CCC / AML & CFT Division of the bank.
- Internal Audit Department shall conduct inspection at least 10% Branches of PRIME BANK, specially on AML & CFT according to BFIU Circular No. 26 section 8.2[2] based on ITP.
- The Internal Audit Department will conduct inspections / audit activities on a minimum of 5% of the agent point on an annual basis to check the performance of agents related to money laundering and counter-terrorism financing activities and send a copy of the report to CCC / AML & CFT Division.

12.2.3 Responsibilities of Compliance Department regarding Independent Testing Procedures

Based on the received reports from the Internal Audit Division of Head Office, the Compliance Department shall collect the compliance report from branches.

12.2.4 Responsibilities of AML & CFT Division regarding Self-Assessment and Independent Testing Procedures

Based on the received self-assessment reports from the branches and submitted inspection/ audit reports (ITP) by the Internal Audit Division of Head Office, the Central Compliance Committee/AML & CFT Division shall prepare a check list based evaluation report on the inspected branches in a considered half year time. In that report, beside other topics, the following topics must be included:

(a) Total number of branch and number of self-assessment report received from the branches;

(b) The number of branches inspected/audited by the Internal Audit Department at the time of reporting and the status of the branches (branch wise achieved score);

(c) Same kinds of irregularities that have been seen in maximum number of branches according to the received self-assessment report and measures taken by the CCC/ AML & CFT Division to prevent those irregularities.

(d) The general and special irregularities mentioned in the report submitted by the Internal Audit Division and the measures taken by the CCC to prevent those irregularities; and

(e) Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as 'Unsatisfactory' and 'Marginal' in the received report.

Based on the validated branch evaluation report received from the branches, if there is any risky matter realized in any branch, CCC have to initiate to inspect that branch and it should be brought to the notice of the appropriate authorities.

Chapter 13

RECORD KEEPING

13.1 Legal Obligations

13.1.1 Obligations under MLPA, 2012 (Amendment in 2015)

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

13.1.2 Obligations under MLP Rules, 2019

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

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

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

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

13.1.3 Obligations under Circulars

According to section 12 of BFIU Circular-26 dated 16/06/2020:

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

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

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

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

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

13.1.4 Customer Information

Branch will keep a copy of or the references to, the evidence of the customer's identity obtained during the application of CDD measures in relation to the evidence of a customer's identity. Branch may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

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

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

13.1.5 Transactions

Branch records shall include:

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

13.1.6 Internal and External Suspicion Reports

Branch will make and retain:

- Records of actions taken under the internal and external reporting requirements; and
- When the nominated officer has considered information or other material concerning possible money laundering but has not made a report to BFIU, a record of the other material that was considered.
- Copies of reported STR/SAR/ should be preserved until further instructions received from BFIU.
- Copies of reported ISAR should be preserved.
- Records of all internal and external reports should be retained for five years from the date the report was made.

13.1.7 Training & Compliance Monitoring

Concern Divisions/Departments of Head Office shall keep the below records:

a. In relation to training:

- dates AML training was given;

- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

b. In relation to AML&CFT compliance monitoring:

- reports by the CAMLCO to senior management/Board; and
- records of consideration of those reports and of any action taken as a consequence.
- BFIU correspondent
- CCC meeting minutes
- Special inspection or regular visit of Divisions/Branches/Foreign Subsidiaries
- STR/SAR Files

13.2 Files with Records to be Kept by the Branch for AML/CFT Compliance [Digital or Printed copy]

A. Circular Files:

1. BFIU Circular File :
    a. All active BFIU Circular in chronological sequence;
2. Internal AML Circular File:
    a. All Instruction/Information Circulars issued by AML & CFT Division;
    b. Annual / Quarterly message of Managing Director & CEO on AML/CFT Compliance;
3. BAMLCO File
    a. BAMLCO Office Order
    b. Internal communication made by BAMLCO

B. Monitoring File:

4. Monitoring of High-Risk Account:
    a. Updated list of High-Risk A/Cs (At least quarterly basis);
    b. Sample of monitoring the transaction of High-Risk account on random basis with comments of BAMLCO;
5. Monitoring of PEPs/IPs Account:
    a. Updated list of PEPs/IPs Account (At least quarterly basis)

b. Sample of monitoring the transaction of PEPs/IPs Accounts on random basis with comments of BAMLCO;

6. Monitoring of Special Account/Transaction (Preferable):

a. Sample of monitoring the transaction of My First Account on random basis with comments of BAMLCO;

b. Sample of monitoring the transaction of NRT Account on random basis with comments of BAMLCO;

c. Sample of monitoring the transaction of House Wife Account on random basis with comments of BAMLCO;

d. Sample of monitoring of online transactions on random basis with comments of BAMLCO;

e. Monitoring of accounts receiving foreign remittances;

f. Monitoring of MONARCH and IPs/PEPs account;

7. Monitoring of Legacy Account (A/C Opened before 30th April, 2002) — If applicable:

a. Updated list of Legacy account with the date of KYC Review and present status (At least quarterly basis);

8. Monitoring of TP Violation:

a. TP Violation Report-Deposit (High Risk, Low Risk & New Accounts with comments of BAMLCO);

b. TP Violation Report-Withdrawal (High Risk, Low Risk & New Accounts with comments of BAMLCO);

9. Threshold Monitoring File :

a. Monitoring comments of BAMLCO in Channel Based Threshold Report;

b. List of top 20/50/100 Customer based on Branch size, volume and geographical location (monthly basis) — with comments of BAMLCO;

10. Monitoring of Structuring:

a. Monitoring evidence of cash deposits below CTR threshold;

b. Monitoring evidence of cash withdrawal below CTR threshold;

11. TP & KYC Review File:

a. Copy of Updated TP or List of accounts which TP & KYC have been revised;

C. Reporting File:

12. Cash Transaction Report:
    a. Month wise CTR Report with review comments of BAMLCO;
13. Half-Yearly Self-Assessment Report:
    a. Forwarding of Self-Assessment Report submitted to AML & CFT Division and Internal Audit Department;
    b. Copy of Half-yearly Self-Assessment Report;
    c. Copy of meeting minutes highlighting the discussion point and decision taken on draft of self-assessment report;
14. Internal SAR/STR File:
    a. Internal STR/SAR/ISAR reported to BAMLCO from different desks along with evidence of analyzing and comments of BAMLCO (if the activity or transaction reported through PrimeDefence, it is digitally stored in system);
    b. Quarterly/Annually summary report containing the data of Internal STR/SAR received by BAMLCO, number of internal STR/SAR closed at Branch end and number of STR/SAR submitted to Head Office;
15. STR/SAR Submission File:
    a. All STRs/SARs submitted to AML&CFT Division by Branch (currently it is electronically stored in PrimeDefence, previous record shall be preserved in hard copy);
16. A/C Query File:
    a. All Queries letter/email received from AML&CFT Division along with copy of reply through AML & CFT Portal (electronically stored in system);
17. Freeze Instruction File:
    a. All Freeze Instruction letters/emails received from AML&CFT Division along with copy of reply through AML & CFT Portal;
    b. List of Freeze account along with related instruction letters/emails should be preserve separately for future reference;

D. Other AML/CFT related Files:

18. Quarterly AML Meeting File:
    a. Notice of AML Meeting with agenda;
    b. Attendance of the meeting;

c. Minutes of the meeting;

d. Copy of Forwarding Letter/ Email submitted to AML & CFT Division;

19. AML/CFT Training File:

    a. AML/CFT Training Record File with copy of office order/certificate and updated cover note mentioning the name designation and date of AML training received;

20. AML/CFT related Inspection File:

    a. Copy of AML/CFT System Check conducted by BFIU or Bangladesh Bank along with submitted compliance report (if any);

    b. Copy of Independent Testing Procedure conducted by Internal Audit Division (if any);

    c. Copy of AML/CFT Inspection/Visit Report conducted by AML & CFT Division (if any);

21. Sanctions Screening File:

    a. User Creation Form of all users;

    b. Data of periodical screening containing the number of Alerts, number of False Match & number of True Match (Report can be generate from Prime Bank Automated Sanction Screening System);

    c. Records of TRUE MATCH reported to AML & CFT Division;

E. Other Documents/Guidance Notes:

- Money Laundering Prevention Act 2012
- Money Laundering Prevention (amendment) Act 2015
- Anti Terrorism Act 2009
- Anti Terrorism (amendment) Act 2012
- Anti Terrorism (amendment) Act 2013
- Money Laundering Prevension Rules-2019
- BFIU Circular No. 26
- PRIME BANK AML & CFT Risk Management Guidelines
- PRIME BANK TBML Risk Management Guidelines
- BFIU Guidance Notes on Politically Exposed Persons
- BFIU Guidelines for Beneficial Owner

- BFIU Guidelines on e-KYC
- Prudential Guidelines for Agent Banking Operation in Bangladesh

13.3 Records to be Kept by Subsidiary

Subsidiaries, if any, shall keep the records of their AML & CFT compliance requirements as specified in this guidelines and/or circulars of BFIU as per section 12 of BFIU Circular No. 26 which are relevant to them.

13.4 Records to be Kept by Head Office Division

Head Office Division shall keep records of their AML & CFT compliance requirements as specified in this guidelines and/or circulars of BFIU as per section 12 of BFIU Circular No. 26 which are relevant to them.

13.5 Records to be Kept by CCC / AML & CFT Division

CCC / AML & CFT Division shall keep records of their circulars, guidelines & instructions for implementation & supervision of AML & CFT compliance program of the bank as specified in this guidelines and/or circulars of BFIU as per section 12 of BFIU Circular No. 26 which are relevant to them.

13.6 Record keeping Formats and Retrieval of Records

To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of a financial institution, provided that they have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form, and that can be reproduced and recollected without undue delay. However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

ABBREVIATIONS

A

AML & CFT = Anti-Money Laundering & Combating the Financing of Terrorism
AOF = Account Opening Form
ATA = Anti Terrorism Act
ATM = Automated Teller Machine

B

BAMLCO = Branch Anti-Money Laundering Compliance Officer
BB = Bangladesh Bank
BDT = Bangladesh Taka
BFIU = Bangladesh Financial Intelligence Unit
BDN = Branches Development Network
BO = Beneficial Owner

C

CAMLCO = Chief Anti-Money Laundering Compliance Officer
CAP = Customer Acceptance Policy
CCC = Central Compliance Committee
CDD = Customer Due Diligence
CIP = Customer Identification Procedure
CMS = Card Management System
CTR = Cash Transaction Report

D

DAMLCO = Division Anti-Money Laundering Compliance Officer
DCAMLCO = Deputy Chief Anti-Money Laundering Compliance Officer
DD = Due Diligence
DNFBP = Designated Non-Financial Business and Professions

E

EDD = Enhanced Due Diligence
EFT = Electronic Funds Transfer
e-KYC = electronic KYC
EGMONT = Egmont Group of Financial Intelligence Units
EU = European Union

F

FATF = Financial Action Task Force, 40 Recommendations on Combating Money Laundering and Terrorist Financing
FAQ = Frequently Asked Question
FI = Financial Institution
FIU = Financial Intelligence Unit

G

GFET = Guidelines for Foreign Exchange Transactions

H

HKMA = Hong Kong Monetary Authority

I

IPs = Influential Persons
ITP = Independent Testing Procedure

K

KYC = Know Your Customer
KYE = Know Your Employee

M

MER = Mutual Evaluation Report
ML = Money Laundering
MLPA = Money Laundering Prevention Act
MLP Rules = Money Laundering Prevention Rules
MSB = Money Service Business
MVTS = Money or Value Transfer Service(s)
MAS- Monetary Authority of Singapore

N

NCC = National Coordination Committee
NCCT = Non-Cooperative Countries and Territories
NGO = Non Government Organization
NITA = Non Resident Investor Account
NPO = Non Profit Organization
NRTA = Non Resident Taka Account

O

OFAC = Office of Foreign Assets Control
Other institution = Any Financial Institution (i.e. Bank, NBFI, MSB & etc)?

P

PF = Proliferation Financing
Palermo Convention = The United Nations Convention against Transnational Organized Crime
PEPs = Politically Exposed Persons

R

RBA = Risk Based Approach
RTGS = Real Time Gross Settlement

S

SAR = Suspicious Activity Report
SDN List = Specially Designated Nationals List.
STR = Suspicious Transaction Report
SWIFT = Society for Worldwide Interbank Financial Telecommunication

T

TF = Terrorist Financing
TP = Transaction Profile

U

UCIC = Unique Customer Identification Code
UN = United Nations
UNODC = United Nations Office of Drugs and Crime
UNSCR = United Nations Security Council Resolution

V

Vienna Convention = The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

W

Wolfsberg Group = The Wolfsberg Group is a private association of thirteen (13) global Bank.

ANNEXURE

ANNEXURE-A

RISK REGISTER

1. Risk Register for Customer

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Retail Banking Customer				
A new customer.	Very Likely	Minor	Legal	• Ensure CDD before accepting customer/ transaction including Sanctions Screening. • Check the name of customer & beneficial owner through Automated Sanction Screening System. • Check Standard ID, verify sources of fund & address. • In case of high risk accounts ensure EDD. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • In case of PEPs/IPs/Head or High Official of Int'l Organization obtain prior approval from the Top Management / CAMLCO. • Monitoring the transaction. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Occasional transaction by a Walk-in customer up to BDT 50 thousand	Very Likely	Minor	=2(Medium)	• Simplified CDD should be ensured. • Collect complete Name, Address and Phone Number of walk-in customer. • Response: Acceptable Risk. Okay to go ahead.
Occasional transaction by a walk-in customer from BDT 50 thousand but less than BDT 5.00 lac	Very Likely	Minor	=2(Medium)	• Simplified CDD should be ensured. • Collect complete Name, Address and Phone Number of Applicant/ walk-in customer. • Collect Standard Photo ID and ensure verification/attestation. • Response: Acceptable Risk. Okay to go ahead.
Occasional transaction by a walk-in customer for BDT 5.00 lac and above	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Collect information through "KYC Profile Form for Walk-in Customer/ Bearer" Annexure-D of PBL ML & TF Risk Management Guideline • Response: Acceptable Risk. May go ahead but preferably reduce risk.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Non-resident customer (Bangladeshi).	Likely	Moderate	=2(Medium)	• CDD must be applied. • Check the name of customer & beneficial owner through Automated Sanctions Screening System. • Collect and check the NID/Passport, evidence of sources of fund & address. • Monitoring the transaction on regular basis. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold).	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID, verify sources of fund & address. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy the Bank official. • Monitor the transaction. • Report as STR if the transaction is not meaningful. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
A customer making series of transactions to the same individual or entity.	Likely	Moderate	=2(Medium)	• Identify the list of accounts involved with the transaction • Monitor the transaction. Obtain justification from the customer. • Report as STR if the transaction is not meaningful. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
A customer or a group of customer making lots of transactions to the same individual or group.	Likely	Moderate	=2(Medium)	• Identify the list of accounts involved with the transaction • Monitor the transaction. Obtain justification from the customer. • Report as STR if the transaction is not meaningful. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customer involved in outsourcing business.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID, verify sources of fund & address. • Screen the customer, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists. • Monitor the transaction. Obtain justification from the customer. • Report as STR if the transaction is not meaningful. • Response: Do not allow transaction until risk reduced.
Customer appears to do structuring to avoid reporting threshold.	Likely	Major	=3(High)	• EDD must be applied • Monitor the transaction on regular basis. • Review the transaction of the account with customer's business type and volume. • Report as STR if customer fails to justify the transactions. • Response: Do not allow transaction until risk reduced.
Customer appears to have accounts with several banks in the same area.	Likely	Moderate	=2(Medium)	• CDD must be applied. • Check Standard ID, verify sources of fund & address. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank. • Monitor the transaction on regular basis. • Report as STR if customer fails to justify the reason of maintaining multiple accounts. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID, verify sources of fund & address. • Monitor the transaction and activity of account. • Report as SAR/STR if any suspicious activity or transaction have been found. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customer is then subject of a Money Laundering or Financing of terrorism investigation by the order of the court.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Monitor the transaction and activity of the account. • Report as STR/SAR • Response: Do not allow transaction until risk reduced.
Negative news about the customers' activities/ business in media or from other reliable sources.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Monitor the transaction and activity of the account. • Report as STR/SAR • Response: Do not allow transaction until risk reduced.
Customer is secretive and reluctant to meet in person.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Review the CDD procedure to identify actual beneficial owner. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction on regular basis. • Conduct physical verification. • Response: Do not allow transaction until risk reduced.
Customer is a mandate who is operating account on behalf of another person/company.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Review the CDD procedure to identify actual beneficial owner. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction on regular basis. • Conduct physical verification. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Large deposits in the account of customer with low income.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Review the CDD procedure to identify actual beneficial owner. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction on regular basis. • Conduct physical verification. • Response: Do not allow transaction until risk reduced.
Customers about whom BFIU seeks information (individual).	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Review the CDD procedure to identify actual beneficial owner. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction on regular basis. • Conduct physical verification. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
A customer whose identification is difficult to check.	Likely	Major	=3(High)	• Follow the Customer Acceptance Policy of the Bank for opening new account. • Do not open the account or close the existing account. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Significant and unexplained geographic distance between the bank and the location of the customer.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Screen the customer, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Identify & justify the reasons behind the ground for selecting the respective branch. • Monitor the transaction closely. • Report STR/SAR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Customer is a foreigner.	Likely	Major	=3(High)	• Check Standard ID/Passport to confirm the identity. • Check the name of customer/beneficial owner against the designated sanction lists. • Check Additional Papers (Copy of VISA, Work Permit, Employer's Certificate in case of employee and any other document that satisfy identification and source of fund. • EDD must be applied. • In case of PEPs/Head or High Official of Int'l Organization obtain prior approval from the Top Management. • Monitor the transaction closely. • Ensure compliance of FATCA and FERA-1947. • Response: Do not allow transaction until risk reduced.
Customer is a minor.	Likely	Minor	=1(Low)	• CDD must be applied. • Beneficiary Owner information must be obtained. • Check Standard ID, verify sources of fund & address. • Monitor the transaction. • Response: Acceptable Risk. Okay to go ahead.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customer is Housewife.	Likely	Moderate	=2(Medium)	• CDD must be applied. • Beneficiary Owner information must be obtained. • Check Standard ID, verify sources of fund & address. • Monitor the transaction • Response: Acceptable Risk. May go ahead but preferably reduce risk.
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.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID, verify sources of fund & address. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Obtain prior approval from CAMLCO. • Monitoring the transaction closely. • Response: Do not allow transaction until risk reduced.
Customer opens account in the name of his/her family member who intends to credit large amount of deposits.	Likely	Major	=3(High)	• EDD must be applied. • Beneficiary Owner information must be obtained. • Screen the customer, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists. • Check Standard ID, verify sources of fund & address. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customers doing significant volume of transactions with higher-risk geographic locations.	Likely	Major	=3(High)	• EDD must be applied • Collect customer's business related information in detail and reason of transaction. • Collect the complete information counterparty (located in high risk jurisdiction) and check the name against designated sanction screening lists. • Monitor the transaction closely. • Report STR if any suspicious transaction/ activity found. • Response: Do not allow transaction until risk reduced.
A customer who brings in large amounts of used notes and/or small denominations.	Likely	Moderate	=2(Medium)	• CDD must be applied • Check Standard ID, verify sources of fund & address. • Monitor the transaction closely. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
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).	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, Trade License/ Business related papers, verify sources of fund & address. • Conduct physical verification on customer business place. • Monitor the transaction closely. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Customer is a money changer/ courier service agent / travel agent.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, Trade License/ Business related papers, verify sources of fund & address. • Conduct physical verification on customer business place. • Monitor the transaction closely. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, Trade License/ Business related papers, verify sources of fund & address. • Conduct physical verification on customer business place. • Monitor the transaction closely. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Customer is involved in Manpower Export Business.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, Trade License/ Business related papers, Export/Import License, verify sources of fund & address. • Conduct physical verification on customer business place. • Monitor the transaction closely. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Customer has been refused to provide banking facilities by another bank.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Check the name against designated sanction lists and negative news. • Conduct physical verification on customers' business and residential address. • Monitor the transaction closely. • Report as STR/SAR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Accounts opened before 30 April, 2002.	Likely	Moderate	=2(Medium)	• Marked as dormant if KYC is not updated. • Update KYC profile. • Check Standard ID, verify sources of fund & address. • CDD should be ensured. • Monitor the transaction. • Response: Do not allow any withdrawal until completion of KYC.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customers with complex accounting and huge transaction.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Collect the Tax Return Copy and other related documents. • Monitor the transaction closely. • Collect the reason of complex and huge transactions. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Received of donor fund, fund from foreign source by micro finance institute (MFI).	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, permission of competent authority for receiving foreign donation/aid, verify sources of fund & address. • Conduct physical verification. • Monitor the transaction closely. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Customer who are not maintaining any account with the Bank except Credit Card	Likely	Major	3(High)	• Complete Sanction Screening process and obtain report; • Legal agreement with customers for technology based product/services; • Complete the CDD process; • EDD must be applied; • Obtain approval from CAMLCO in case of PEPs/IPs; • Response: Do not allow transaction until risk reduced.
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source.	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, License issued by competent authority, verify sources of fund & address. • Complete KYC of all operators, beneficial owners. • Monitor the transaction closely. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Wholesale Banking Customer				

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
a new customer	Very Likely	Minor	=2(Medium)	• Ensure CDD before accepting customer/ transaction including Sanctions Screening. • Check the name of customer & beneficial owner through Automated Sanction Screening System. • Check Standard ID, verify sources of fund & address. • In case of high risk accounts ensure EDD. Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • In case of PEPs/IPs/Head or High Official of Int'l Organization obtain prior approval from the Top Management / CAMLCO. • Monitoring the transaction. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
a new customer who wants to carry out a large transaction	Likely	Moderate	=2(Medium)	• Ensure CDD before accepting customer/ transaction including Sanctions Screening. • Check Standard ID, verify sources of fund & address. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy the Bank official. • Monitor the transaction. • Report as STR if the transaction is not meaningful. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
a customer or a group of customers making lots of transactions to the same individual or group	Likely	Major	=3(High)	• Check Standard ID, verify sources of fund & address. • Check Additional papers as per satisfaction of Bank. • EDD must be applied. • Monitor the Transaction closely. • Collect the reason of transactions and list of counter parties. • Report as STR if the transaction is not meaningful. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Entity customer having operations in multiple locations.	Likely	Moderate	=2(Medium)	• Check Standard ID, Business related papers, verify sources of fund & address. • CDD must be applied. • Complete KYC of all operators, beneficial owners. • Monitor the transaction. • Conduct physical verification. • Encourage to opening the account to the nearest branch. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Customers about whom BFIU seeks information (large corporate).	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Screen the customer, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists and adverse media report. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction and activity of the account. • Report as STR/SAR if any unusual transaction/activity. • Response: Do not allow transaction until risk reduced.
Owner of the entity that are Influential Persons (IPs) and their family members and close associates.	Likely	Major	=3(High)	• Obtain senior management approval before establishing such business relationship. • Check Standard ID, verify sources of fund & address. • Screen the customer, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists and adverse media report. • Check Additional papers as per satisfaction of Bank. • Verify source of fund. • EDD must be applied. • Monitor the Transaction closely. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above).	Likely	Major	=3(High)	• Check Standard ID, verify sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Verify source of fund. • CDD must be applied. • Monitor the Transaction closely. • Response: Do not allow transaction until risk reduced.
a customer who has a business which involves large amounts of cash	Likely	Major	=3(High)	• Check Standard ID, verify sources of fund & address. • Check Additional papers as per satisfaction of Bank. • EDD must be applied. • Monitor the Transaction closely. • Collect the reason of transactions and list of counter parties. • Report as STR if the transaction is not meaningful. • Response: Do not allow transaction until risk reduced.
a customer whose identification is difficult to check	Likely	Major	=3(High)	• Do not open the account or in case of existing account close the account after giving proper notice to customer and obtaining approval from the line management. • Report as STR/SAR if any suspicious transaction/activity found. • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Likely	Major	=3(High)	• Check Standard ID, verify sources of fund & address. • Check Additional papers as per satisfaction of Bank. • EDD must be applied. • Monitor the Transaction closely. • Collect the reason of transactions and list of counter parties. • Report as STR if the transaction is not meaningful. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
A customer whose identification is difficult to check.	Very Likely	Major	=4(Extreme)	• Do not open the account or in case of existing account close the account after giving proper notice to customer and obtaining approval from the line management. • Report as STR/SAR if any suspicious transaction/activity found. • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
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	=3(High)	• Obtain senior management approval before establishing such business relationship. • Check Standard ID, verify sources of fund & address. • Screen the customer, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists and adverse media report. • Check Additional ID (valid driving license, Credit Card-if any, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • EDD must be applied. • Monitor the Transaction closely. • Comply with the instructions of FATCA and FERA-1947 if the customer is Foreign Individual. • Response: Do not allow transaction until risk reduced.
Charities or NPOs (especially operating in less privileged areas).	Likely	Major	=3(High)	• EDD must be applied • Check the permission, license issued by competent authority, verify sources of fund & address. • Complete KYC of all operators, beneficial owners. • Conduct physical verification to confirm the address and activity. • Monitor the transaction closely. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
a customer who brings in large amounts of used notes and/or small denominations.	Likely	Moderate	=2(Medium)	• CDD must be applied • Check Standard ID, verify sources of fund & address. • Monitor the transaction closely. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
customers conducting their business relationship or transactions in unusual circumstances, such as: - significant and unexplained geographic distance between the institution and the location of the customer - frequent and unexplained movement of accounts to different institutions - frequent and unexplained movement of funds between institutions in various geographic locations	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Collect the Tax Return Copy and other related documents. • Monitor the transaction closely. • Collect the reason of complex and huge transactions. • Report as STR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
a corporate customer whose ownership structure is unusual and excessively complex	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Review the CDD procedure to identify actual beneficial owner. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction on regular basis. • Conduct physical verification. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID, verify sources of fund & address. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Obtain prior approval from CAMLCO. • Monitoring the transaction closely. • Response: Do not allow transaction until risk reduced.
customers submits account documentation showing an unclear ownership structure	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Review the CDD procedure to identify actual beneficial owner. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction on regular basis. • Conduct physical verification. • Response: Do not allow transaction until risk reduced.
Customer/ Beneficial Owner/Partner is a foreigner.	Likely	Major	=3(High)	• Check Standard ID/Passport to confirm the identity. • Check the name of customer/beneficial owner against the designated sanction lists. • Check Additional Papers (Copy of VISA, Work Permit, Employer's Certificate in case of employee and any other document that satisfy identification and source of fund. • EDD must be applied. • In case of PEPs/Head or High Official of Int'l Organization obtain prior approval from the Top Management. • Monitor the transaction closely. • Ensure compliance of FATCA and FERA-1947. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customers about whom BFIU seeks information (large corporate).	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Screen the customer, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists and adverse media report. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction and activity of the account. • Report as STR/SAR if any unusual transaction/activity. • Response: Do not allow transaction until risk reduced.
Credit Card Customer				
Customer who changes static data frequently.	Likely	Major	=3(High)	• Review the CDD procedure. • Collect standard ID and other documents to verify customer's identity and sources of fund. • Conduct physical verification on customer's business/residential address. • Check Additional papers as per satisfaction of Bank. • Monitor the Transaction closely. • Report as STR/SAR if the transaction is not meaningful. • Response: Do not allow transaction until risk reduced.
Credit Card customer.	Very Likely	Minor	=2(Medium)	• Check Standard ID, verify sources of fund & address. • Check Additional papers as per satisfaction of Bank. • CDD should be ensured. • Monitor the Transaction closely. • Response: Acceptable Risk. May go ahead.
Structuring Payments/ Overpayments : Balance on cards may move into regular credit where card holders pay too much or where merchants give credits to an account	Likely	High	3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Check the name against designated sanction lists and negative news. • Conduct physical verification on customers' business and residential address. • Monitor the transaction closely • Report as STR/SAR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments.	Very Likely	Moderate	=3(High)	• Check Standard ID, verify sources of fund & address. • Check Additional papers as per satisfaction of Bank. • EDD must be applied. • Monitor the Transaction closely. • Report as STR if the transaction is not match with customer declared source of fund. • Response: Do not allow transaction until risk reduced.
Transaction from High Risk Jurisdiction or frequent transactions from Off-Shore Tax Haven	Likely	Major	=3(High)	• EDD Should be ensure, • If found unusual transaction the card must be blocked , • STR should be reported, • Response :Do not allow card transaction.
Prepaid Card customer	Very Likely	Minor	=2(Medium)	• Check Standard ID, verify sources of fund & address. • Check Additional papers as per satisfaction of Bank. • CDD should be ensured. • Monitor the Transaction closely. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
International Trade Customer				
A new customer (Outward & inward remittance-through SWIFT).	Likely	Major	=3(High)	• CDD must be applied. • EDD must be applied if amount is more than $10,000. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check the name of customer/operator/ beneficial owner against the designated sanctions lists. • Conduct physical verification to understand customer's business. • IRC & ERC should be obtained (if required). • Check Additional papers as per satisfaction of Bank. • Monitor the transaction. • Obtain the information regarding purpose of remittance. • Report STR if any satisfactory reason not found. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
A new customer (Import/Export).	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check the name of customer/operator/ beneficial owner against the designated sanctions lists. • Conduct physical verification to understand customer's business. • IRC & ERC should be obtained. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction. • Obtain the information regarding purpose of remittance. • Report STR if any satisfactory reason not found. • Response: Do not allow transaction until risk reduced.
A new customer who wants to carry out a large transaction (Inward remittance)	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check the name of customer/operator/ beneficial owner against the designated sanctions lists. • Conduct physical verification to understand customer's business. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction. • Obtain the information regarding purpose of remittance. • Report STR if any satisfactory reason not found. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
A customer wants to conduct business beyond its line of business (import/ export/ remittance)	Likely	Major	=3(High)	EDD must be applied. Check Standard ID and other documents to verify customer's identity, sources of fund & address. Check the name of customer/operator/ beneficial owner against the designated sanctions lists. Conduct physical verification to understand customer's business. IRC & ERC should be obtained. Check Additional papers as per satisfaction of Bank. Monitor the transaction. Obtain the information regarding purpose of remittance. Report STR if any satisfactory reason not found. Response: Do not allow transaction until risk reduced.
Owner/ director/ shareholder of the customer is influential person(s) or their family members orclose associates.	Likely	Major	=3(High)	• Obtain senior management approval before establishing such business relationship. • EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check the name of customer/operator/ beneficial owner against the designated sanctions lists and adverse media report. • Conduct physical verification to understand customer's business. • IRC & ERC should be obtained. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction. • Obtain the information regarding purpose of remittance. • Report STR if any satisfactory reason not found. • Response: Do not allow transaction until risk reduced.

ML & TF Risk Register for Customer Risk	Likelihood	Impact	Risk score	Treatment/Action
Correspondent Banks.	Likely	Major	=3(High)	• To be satisfied about the nature of the business of the correspondent through collection of information. • Screen the name of directors, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists and adverse media report. • Obtain senior management approval before establishing correspondent relationship. • No relation with Shell Bank. • EDD must be applied before establishing correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standard for the prevention of Money Laundering & Terrorist Financing. • Obtain the extensive information about their policies & procedures on prevention of Money Laundering & Terrorist Financing. • Response: Do not allow transaction until risk reduced.
Money services businesses (remittance houses, exchange houses)	Likely	Major	=3(High)	• To be satisfied about the nature of the business of the correspondent through collection of information. • Screen the name of directors, beneficiary owner(s), authorized person(s), if any, and his/her outsourcing counterpart(s) against the designated Sanctions Lists and adverse media report. • Obtain senior management approval before establishing correspondent relationship. • No relation with Shell Bank/company. • EDD must be applied before establishing correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standard for the prevention of Money Laundering & Terrorist Financing. • Obtain the extensive information about their policies & procedures on prevention of Money Laundering & Terrorist Financing. • Response: Do not allow transaction until risk reduced.

2. Risk Register for Products & Services

Risk	Likelihood	Impact	Risk score	Treatment/Action
Retail Banking Product				
Development of new product & service of bank.	Likely	Moderate	=2(Medium)	• AML/CFT risk should be assessed. • Policy should be taken to mitigate the AML/CFT risk. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
private banking i.e., prioritized or privileged banking	Likely	Major	=3(High)	• EDD must be applied • Check Standard ID, verify sources of fund & address. • Review the CDD procedure to identify actual beneficial owner. • Check Additional ID (valid driving license, Credit Card-if any, Employer's Certificate-in case of employee, Utility Bill, Trade license, TIN and any other document that satisfy identification for the Bank • Monitor the transaction on regular basis. • Conduct physical verification. • Response: Do not allow transaction until risk reduced.
anonymous transaction (which may include cash)	Very Likely	Major	=4(Extreme)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Collect the information of bearer. • If the identity can't be verified, do not accept business relationship. • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
non face to face business relationship or transaction (except Simplified e-KYC account)	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Collect the information of bearer. • If the identity can't be verified, do not accept business relationship. • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.

Risk	Likelihood	Impact	Risk score	Treatment/Action
payment received from unknown or unrelated third parties	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • Report as STR if the transactions do not match with customer's declared source of fund. • Response: Do not allow transaction until risk reduced.
Occasional transaction by a Walk-in customer up to BDT 50 thousand	Very Likely	Minor	=2(Medium)	• Simplified CDD should be ensured. • Collect complete Name, Address and Phone Number of walk-in customer. • Response: Acceptable Risk. Okay to go ahead.
Occasional transaction by a walk-in customer from BDT 50 thousand but less than BDT 5.00 lac	Very Likely	Minor	=2(Medium)	• Simplified CDD should be ensured. • Collect complete Name, Address and Phone Number of Applicant/ walk-in customer. • Collect Standard Photo ID and ensure verification/attestation. • Response: Acceptable Risk. Okay to go ahead.
Occasional transaction by a walk-in customer for BDT 5.00 lac and above	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Collect information through "KYC Profile Form for Walk-in Customer/ Bearer" Annexure-D of PBL ML & TF Risk Management Guideline • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Accounts for students where large amount of transactions are made (student file).	Likely	Major	=3(High)	• EDD must be applied. • Obtain information of Beneficiary Owner. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction. • Report as STR. • Response: Do not allow transaction until risk reduced.
Locker Service	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Foreign currency endorsement in Passport	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check the validity of Passport and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Large transaction in the account of under privileged people	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Report as STR if customer can't justify the transaction. • Response: Do not allow transaction until risk reduced.
FDR (less than 1 million)	Very Likely	Minor	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
FDR (l1 million to 2.5 million)	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
FDR (2.5 million and above)	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Collect TIN and copy of Tax Return. • Check Additional papers as per satisfaction of Bank. • Report as STR if the transactions do not match with customer's declared source of fund. • Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Special scheme deposit accounts opened with big installment and small tenure.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Collect TIN and copy of Tax Return. • Check Additional papers as per satisfaction of Bank. • Report as STR if the transactions do not match with customer's declared source of fund. • Response: Do not allow transaction until risk reduced.
Multiple deposit scheme accounts opened by same customer in a branch or by same customer from different location.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Collect TIN and copy of Tax Return. • Check Additional papers as per satisfaction of Bank. • Report as STR if the transactions do not match with customer's declared source of fund. • Response: Do not allow transaction until risk reduced.
Open DPS in the name of family member Or Installments paid from the account other than the customer's account.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Collect information of Beneficial Owner. • Check Additional papers as per satisfaction of Bank. • Report as STR if the transactions do not match with customer's declared source of fund. • Response: Do not allow transaction until risk reduced.
Early encashment of FDR, special scheme etc.	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Collect the reason for early encashment. • Report as STR/SAR if any suspicious activity found. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Non face to face business relationship/ transaction.	Very Likely	Major	=4(Extreme)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Collect the information of bearer. • If the identity can't be verified, do not accept business relationship. • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
Payment received from unrelated/ un-associated third parties.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • Report as STR if the transactions do not match with customer's declared source of fund. • Response: Do not allow transaction until risk reduced.
Agent Banking with in the set Limit of BB	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Agent Banking beyond the set Limit of BB	Likely	Major	=3(High)	• CDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check prior notice or approval from Senior Management papers as per satisfaction of Bank. • The account may be treated as High Risk in subjective judgement. • Report to FID of Bangladesh Bank or report as STR/SAR if source of fund / purpose of the transaction is not clear. • Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
e-KYC Account				
A new customer want to open an account through e-KYC platform with a declaration to conduct monthly transaction (Deposit/ withdrawal) within 1.00 lac.	Very Likely	Minor	2 Medium	• NID must be verified successfully from EC portal; • SDD should be applied; • Threshold limit need to be set in system to ensure transaction within the threshold limit; • If customer intend to conduct regular transaction (exceeding the eKYC limit set by BFIU), additional documents need to be collect to ensure CDD before allowing regular transaction (monthly deposit/withdrawal more than 1.00 lac);
A new customer want to open an account through e-KYC platform with a declaration to conduct monthly transaction (Deposit/ withdrawal) more than 1.00 lac.	Very Likely	Moderate	3 High	• CDD should be applied when customer intend to conduct regular transaction (exceeding the eKYC limit set by BFIU) or confirm the regular eKYC. • Other documents to verify customer's identity, sources of fund & address. • Risk grading should be done and periodic KYC review required; • Report as STR/SAR if source of fund / purpose of the transaction is not clear. • Response: Do not allow transaction until risk reduced.
Retail Privilege Facilities				
Opening of SB, CD or FDR by Monarch Customer	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • The account may be treated as High Risk in subjective judgement. • Report as STR/SAR if source of fund is not clear. • Response: Do not allow transaction until risk reduced.
Consumer & SME Banking Product				
Repayment of loan EMI from source that is not clear or Payment received from unrelated third parties	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Report as STR/SAR if source of fund is not clear. • Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Repayment of full loan amount before maturity.	Likely	Major	=3(High)	• EDD must be applied. • Collect necessary documents as per satisfaction of Bank to confirm the source of fund. • Check Additional papers as per satisfaction of Bank. • Report as STR if source of fund is not clear. • Response: Do not allow transaction until risk reduced.
Loan amount utilized in sector other than the sector specified during availing the loan.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Report as STR/SAR. • Response: Do not allow transaction until risk reduced.
In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Report as STR/SAR. • Response: Do not allow transaction until risk reduced.
Source of fund used as security not clear at the time of availing loan.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the account closely. • Report as STR/SAR if any suspicious transaction/activity found. • Response: Do not allow transaction until risk reduced.
Wholesale Banking Product [Corporate & Institutional Banking, Commercial Banking, International Banking, Transaction Banking, Structured Financing, Treasury]				
Development of new product & service of bank.	Likely	Moderate	=2(Medium)	• AML/CFT risk should be assessed. • Policy should be taken to mitigate the AML/CFT risk. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Payment received from unrelated third parties.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Collect information of beneficial owner. • Check Additional papers as per satisfaction of Bank. • Report as STR/SAR if source of fund is not clear. • Response: Do not allow transaction until risk reduced.
High Value FDR	Very Likely	Moderate	=3(High)	• EDD must be applied.
Term loan, SOD(FO), SOD (G-work order), SOD (Garment), SOD (PO), Loan General, Lease finance, Packing Credit, BTB L/C	Very Likely	Moderate	=3(High)	• Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Confirm the purpose of loan. • Monitor the transactions. • Report as STR/SAR if any suspicious activity found. • Response: Do not allow transaction until risk reduced.
BG(bid bond), BG(PG), BG(APG)	Very Likely	Moderate	=3(High)	
L/C subsequent term loan, DP L/C	Very Likely	Moderate	=3(High)	
C.C(H), SOD(G-Business), STL	Very Likely	Moderate	=3(High)	
Syndication Financing	Very Likely	Moderate	=3(High)	
OBU (funded or non-funded facilities)	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Confirm the purpose of loan. • Monitor the transactions. • Report as STR/SAR if any suspicious activity found. • Response: Do not allow transaction until risk reduced.
Digital Financial Services				
Development of new product & service of bank.	Likely	Moderate	=2(Medium)	• AML/CFT risk should be assessed. • Policy should be taken to mitigate the AML/CFT risk. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Credit Card				
Supplementary Credit Card Issue	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check the name of Card Holder against designated sanctions lists.. • Check Additional papers as per satisfaction of Bank. • KYC of principle card holder should be updated. • Monitor the transactions. • Report as STR if any suspicious activity found. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Frequent use of Card Cheque.	Likely	Moderate	=2(Medium)	• CDD should be ensured & EDD may be applied (if required). • Confirm the purpose of transactions. • Monitor the transactions. • Report as STR if any suspicious activity found. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant).	Likely	Moderate	=2(Medium)	• Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • Report as STR if any suspicious activity found. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Credit card issuance against ERQ and RFCD accounts.	Likely	Moderate	=2(Medium)	• Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • Report as STR if any suspicious activity found. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
International Trade				
Line of business mismatch (import/ export/remittance)	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • Report as STR/SAR if any suspicious transaction or activity found. • Response: Do not allow transaction until risk reduced.
Under/Over invoicing (import/export/ remittance)	Likely	Major	=3(High)	• EDD must be applied. • Check Additional papers as per satisfaction of Bank. • Verify the declared price with local or international standard price. • Report as STR/SAR if any discrepancy found. • Response: Do not allow transaction until risk reduced.
Retirement of import bills in cash (import/export/ remittance).	Likely	Major	=3(High)	• EDD must be applied. • Monitor the transaction. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Do not allow transaction until risk reduced.
Wire transfer	Likely	Moderate	=2(Medium)	• CDD must be applied. • In case of threshold cross-border wire transfer of 1000 or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected & preserved and has to be sent to intermediary/beneficiary bank. • In case of threshold domestic wire transfer of at least 25,000 BDT, full and accurate information of the originator has to be collected & preserved and has to be sent to intermediary/beneficiary bank. • For the domestic wire transfers below the threshold full and meaningful originator information has to be preserved. • If the purpose of the transaction is not meaningful stopped the transaction and report as STR. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance).	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Collect the purpose of the transaction. • If the purpose of the transaction is mismatched stopped the transaction and report as STR. • Response: Do not allow transaction until risk reduced.

3. Risk Register for Business practices/delivery methods or channels

Risk	Likelihood	Impact	Risk score	Treatment/Action
Retail Banking Product				
Direct to the customer	Very Likely	Minor	=2(Medium)	• CDD must be applied • Check Standard ID, verify sources of fund & address. • Monitor the transaction closely. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
online/internet	Very Likely	Minor	=2(Medium)	• CDD must be applied • Check Standard ID, verify sources of fund & address. • Monitor the transaction closely. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
third-party agent or broker	Likely	Major	=3(High)	• Complete Merchant KYC. • Visit Merchant point physically and conduct feasibility analysis. • EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Do not allow transaction until risk reduced.
BEFTN /RTGS/ BACH	Very Likely	Minor	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction closely and verify the reason transactions. • If the purpose of transaction is not clear, report as STR. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Online (multiple small transaction through different branch)	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Collect the reason of online transactions. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction closely and verify the reason of online transaction. • If the pattern of transaction mismatched with customer business/profession report as STR. • Response: Do not allow transaction until risk reduced.
IDBP	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transaction closely and verify the reason transactions. • If the purpose of transaction is not clear, report as STR. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Third party agent or broker (if any)	Likely	Major	=3(High)	• Complete Merchant KYC. • Visit Merchant point physically and conduct feasibility analysis. • EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Response: Do not allow transaction until risk reduced.
Credit Card				
New Merchant sign up	Likely	Major	=3(High)	• EDD should be ensured. • Check Trade License and other business related documents to verify customer's business & address. • Complete KYC procedure for all beneficial owners. • Check Additional papers as per satisfaction of Bank. • Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
High volume transaction through POS / Agent Point	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • If the transaction does not match with customer's declared income, report as STR. • Response: Do not allow transaction until risk reduced.
Alternate Delivery Channel				
Large amount withdrawn from ATMs	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Check the TP and monitor the transactions. • Report as STR if the transactions do not match with declared income. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Larger amount transaction from different location and different time (mid night) through ATM.	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • If the transaction does not match with customer's declared income, report as STR. • Response: Do not allow transaction until risk reduced or investigation should conduct against the transactions..
Large amount of cash deposit in CDM.	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Check the TP and monitor the transactions. • Report as STR if the transactions do not match with declared income. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Huge fund transfer through internet.	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Check the TP and monitor the transactions. • Report as STR if the transactions do not match with declared income. • Response: Acceptable Risk. May go ahead but preferably reduce risk.
Customer to business transaction- Online Payment Gateway -Internet Banking	Likely	Moderate	=2(Medium)	• CDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Check the TP and monitor the transactions. • Report as STR if any suspicious transaction found. • Response: Do not allow transaction until risk reduced.
Credit/Prepaid/ Debit Card transaction related with online gambling, betting, cryptocurrency, terrorist financing or donation	Likely	Major	=3(High)	• EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Monitor the transactions. • If the transaction does not match with customer's declared income, report as STR. • Response: Do not allow transaction until risk reduced.
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Likely	Moderate	=2(Medium)	• CDD should be ensured. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Review TP in accordance with declared source of fund. • Report as STR if the transactions do not match with declared income and customer's profession. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103) .	Likely	Moderate	=2(Medium)	• CDD should be ensured & EDD must be applied. • Check Standard ID and other documents to verify customer's identity, sources of fund & address. • Check Additional papers as per satisfaction of Bank. • Review TP in accordance with declared source of fund. • Report as STR if the transactions do not match with declared income and customer's profession. • Response: Acceptable Risk. May go ahead but preferably reduce risk.

4. Risk Register for Country/jurisdiction

Risk	Likelihood	Impact	Risk score	Treatment/Action
Retail Banking Product				
Import and export from/ to sanctioned country.	Very Likely	Major	=4(Extreme)	• All cross boarder transaction must be screened though Automated Sanctions Screening. • In case of findings of any Sanctions Country involved with Import/Export hold the transaction/procedure and conduct EDD. • Collect explanation from the Exporter/ Importer. • Check Additional papers as per satisfaction of Bank. • In case of finding True Match or involvement of Sanctions Country with the Export/Import procedure reject the Transaction and Report to BFIU through AML & CFT Division of Head Office. • Response: Unacceptable Risk. Do not allow transaction.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Import and export from/to High Risk Country	Very Likely	Major	=4(Extreme)	• All cross boarder transaction must be screened though Automated Sanctions Screening. • In case of findings of any High Risk Country involved with Import/Export hold the transaction/procedure and conduct EDD. • Collect explanation from the Exporter/ Importer. • Check Additional papers as per satisfaction of Bank. • In case of finding True Match or involvement of Sanction Country with the Export/Import procedure reject the Transaction and Report to BFIU through AML & CFT Division of Head Office. • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
Transshipments, container, flag vessel etc. under global sanctions.	Very Likely	Major	=4(Extreme)	• All cross boarder transaction must be screened though Automated Sanctions Screening. • In case of findings of any Sanction Country involved with Import/Export hold the transaction/procedure and conduct EDD. • Collect explanation from the Exporter/ Importer. • Check Additional papers as per satisfaction of Bank. • In case of finding True Match or involvement of Sanction Country with the Export/Import procedure reject the Transaction and Report to BFIU through AML & CFT Division of Head Office. • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
Establishing correspondent relationship with sanctioned bank and/or country.	Very Likely	Major	=4(Extreme)	• Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Establishing correspondent relationship with poor AML&CFT practice country.	Very Likely	Major	=4(Extreme)	• Particular attention should be paid & EDD must be applied while establishing a correspondent banking relationship • Detailed information on the beneficial ownership of such banks shall have to be obtained. • Extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained. • Approval from senior management should be obtained • Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
Customer belongs to higher-risk geographic locations such as identified by FATF or FSRBs	Likely	Major	=3(High)	• Particular attention should be paid & EDD must be applied while accepting a Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas • Check the name against designated Sanctions Lists. In case of match do not open the account or freeze the account and report to BFIU through AML & CFT Division of Head Office. • Response: Do not allow transaction until risk reduced.
Any bank that provide service to 'Shell Bank'	Very Likely	Major	=4(Extreme)	• Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
Any bank that allow payable through account.	Likely	Major	=3(High)	• Particular attention should be paid & EDD must be applied while establishing a correspondent banking relationship. • Detailed information on the beneficial ownership of such banks shall have to be obtained. • Extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained. • Approval from senior management should be obtained. • EDD must be applied. • Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Any country identified as destination of illicit financial flow.	Likely	Major	=3(High)	• Particular attention should be paid & EDD must be applied while accepting a customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas. • Check the name against designated Sanction Lists. In case of match do not open the account or freeze the account and report to BFIU through AML & CFT Division. • Response: Do not allow transaction until risk reduced.
Branches in a Border Area	Very Likely	Moderate	=3(High)	
Area identified as high risk in the NRA.	Likely	Major	=3(High)	
Countries subject to UN embargo/ sanctions.	Very Likely	Major	=4(Extreme)	• Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
Transaction from High Risk Jurisdiction or frequent transactions from Off-Shore Tax Haven	Likely	Major	=3(High)	• EDD Should be ensure, • If found unusual transaction the card must be blocked , • STR should be reported, • Response :Do not allow card transaction.
Unusual Purchase of goods or services in countries regarded by an institution as posing a heightened risk for money laundering	Likely	Major	=3(High)	• EDD Should be ensure, • If found unusual transaction the card must be blocked , • STR should be reported, • Response :Do not allow card transaction.

5. Register for Regulatory Risk

Risk	Likelihood	Impact	Risk score	Treatment/Action
Not having AML/ CFT guideline	Likely	Major	=3(High)	There must have AML/CFT Guidelines in the Bank.
Not forming a Central Compliance Committee (CCC)	Likely	Major	=3(High)	CCC must be formed in the Bank as per guidelines of BFIU.
Not having an AML&CFT Compliance Officer	Likely	Major	=3(High)	Bank must nominate a CAMLCO as per guidelines of BFIU to oversee the AML/CFT activities of the Bank. .
Not having Branch Anti Money Laundering Compliance Officer	Likely	Major	=3(High)	Every Branch have to nominate a BAMLCO for ensuring AML/CFT compliance.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Not having an AML&CFT program	Likely	Major	=3(High)	The concerned Division will ensure AML/CFT compliance program regularly.
No senior management commitment to comply with MLP and AT Act	Likely	Major	=3(High)	There must have senior management commitment to comply with MLP and AT Act. A message should be forwarded to all employee of the Bank from the desk of CEO with an instruction to be compliant on AML/CFT issues.
Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	Unlikely	Major	=2(Medium)	All AML/BFIU circular must be followed. In case of failure administrative action will be taken against the concerned officer(s).
Uniformed account opening form not followed while opening account	Unlikely	Major	=2(Medium)	All branches must followed uniform account opening form while opening accounts.
Non screening of new and existing customers against UNSCR Sanction and OFAC lists	Unlikely	Major	=2(Medium)	All branches must screen new (including account holder, signatory, beneficial owner, legal intermediary) and existing customers against the designated sanction lists of UNSCR, OFAC, GoB and other list approved by Bank management.
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Unlikely	Major	=2(Medium)	All branches must follow Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.
Complete and accurate information of customer not obtained	Likely	Major	=3(High)	All branches must obtain complete and accurate information of customer. Where obtaining complete information is not possible, Branch will not open the account or will close the existing account complying the instruction of BFIU Circular No. 26 dated 16.06.2020.
Failure to verify the identity proof document and address of the customer	Likely	Major	=3(High)	Do not open the account or close the existing account. Report as STR/SAR if needed. Response: Do not allow transaction to occur or reduce the risk to acceptable level.
Beneficial owner identification and verification not done properly	Likely	Major	=3(High)	Marked "Stop Payment" on the account till verification has been done properly. In case of non-cooperation from the customer close the account and report as STR/SAR. Response: Do not allow transaction until risk reduced.
Customer Due Diligence (CDD) not practiced properly	Likely	Major	=3(High)	Marked "Stop Payment" on the account till CDD has been done properly. In case of non-cooperation from the customer close the account and report as STR/SAR. Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
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.)	Likely	Major	=3(High)	Do not open the account or marked "Stop Payment" on the account till EDD has been performed. In case of non-cooperation from the customer close the account and report as STR/SAR. Response: Do not allow transaction until risk reduced.
Failure to complete KYC of customer including walk in customer	Likely	Major	=3(High)	Response: Do not allow transaction until risk reduced.
Failure to update KYC of customer	Likely	Major	=3(High)	Marked "Stop Payment" on the account till TP & KYC has been updated. In case of non-cooperation from the customer close the account and report as STR/SAR. Response: Do not allow transaction until risk reduced.
Keep the legacy accounts operative without completing KYC	Likely	Major	=3(High)	Marked "Stop Payment" on the account till TP & KYC has been updated. In case of non-cooperation from the customer report as STR/SAR. Response: Do not allow transaction until risk reduced.
Failure to assess the ML & TF risk of a product or service before launching	Likely	Major	=3(High)	AML/CFT risk should be assessed before launching. Policy should be taken to mitigate the AML/CFT risk associated with the new product/service. Response: Do not allow transaction until risk reduced.
Failure to complete the KYC of Correspondent Bank	Likely	Major	=3(High)	Do not establish business relationship or close the relationship. Response: Do not allow transaction until risk reduced.
Senior Management approval not obtained before entering into a Correspondent Banking relationship	Likely	Major	=3(High)	Do not establish business relationship or RMA. Response: Unacceptable Risk. Do not allow transaction to occur or reduce the risk to acceptable level.
Failure to comply with the instruction of BFIU by bank Foreign subsidiary	Likely	Major	=3(High)	Foreign subsidiary must be complied with the instruction of BFIU. In case of any failure it should be reported to BFIU through AML & CFT Division of Head Office. Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Failure to keep record properly	Likely	Major	=3(High)	Preserve all records relevant with the account for 5 years after closer the account. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee.
Failure to report complete and accurate CTR on time	Likely	Major	=3(High)	Branches should be more careful to report complete accurate CTR on time. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee.
Failure to review CTR	Likely	Major	=3(High)	CTR should be reviewed by Branches before submission to detect unusual or suspicious transaction. Administrative action can be taken to the concerned branch/employee.
Failure to identify and monitor structuring	Likely	Moderate	=2(Medium)	Branch should check the transactions below CTR threshold carefully to detect structuring. Branch should preserve the proof of monitoring. If found structuring in any account it should be reported as STR.
Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Likely	Major	=3(High)	All account should be review on regular basis. All complex or unusual transaction should be reviewed and analyzed by BAMLCO immediately after detection. Any transaction suspected with terrorist financing should be reported as STR within the same day. All employees should be well aware and careful regarding detection of unusual/ suspicious transactions. All activities should be recorded properly.
Failure to conduct quarterly meeting properly	Unlikely	Major	=2(Medium)	At least quarterly meeting should be arranged to review the AML/CFT activities of Branch. Notice should be served and minutes should be preserved. The implementation status of the decision taken in the last meeting need to be check on the following meeting.
Failure to report suspicious transactions (STR)	Likely	Major	=3(High)	Branches should be more careful to detect and report STR on time. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee(s).
Failure to conduct self assessment properly	Likely	Moderate	=2(Medium)	Branch should be more vigilant and realistic for preparing Self-Assessment Report.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Failure to submit statement/ report to BFIU on time	Likely	Major	=3(High)	Branches should be more careful to submit statement/report on time. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee(s).
Submit erroneous statement/ report to BFIU	Likely	Major	=3(High)	BAMLCO should review the statements/ reports carefully before submission for ensuring error free reporting. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee(s).
Not complying with any order for freezing or suspension of transaction issued by BFIU.	Likely	Major	=3(High)	Branches should be very prompt in responding freeze instructions received from BFIU. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee(s).
Not submitting accurate information or statement sought by BFIU or BB.	Likely	Major	=3(High)	BAMLCO should review the statements/ reports carefully before submission for ensuring error free reporting. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee(s).
Not submitting required report to senior management regularly	Likely	Moderate	=2(medium)	Required reports must be submitted to senior management regularly for avoiding penalty by BFIU.
Failure to rectify the objections raised by BFIU or bank inspection teams on time	Likely	Major	=3(High)	All objections raised by BFIU or bank inspection teams must be rectified on time. Response: Do not allow transaction until risk reduced.
Failure to obtain information during wire transfer	Likely	Major	=3(High)	Obtain information of applicant & Beneficiary as per instructions of BFIU Circular No. 26 dated 16.06.2020. In case of lack of information refuse or stop the transaction. Report as STR if needed. Response: Do not allow transaction until risk reduced.
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely	Major	=3(High)	Follow the instructions of BFIU Circular No. 26 dated 16.06.2020 meticulously. In case of failure penalty may be imposed by BFIU. Administrative action can be taken to the concerned branch/employee(s). Response: Do not allow transaction until risk reduced.

Risk	Likelihood	Impact	Risk score	Treatment/Action
Failure to scrutinize staff properly	Likely	Major	=3(High)	Concerned division will scrutinize staff properly before appointment. Response: Do not allow until risk reduced.
Failure to circulate BFIU guidelines and circulars to branches	Likely	Major	=3(High)	Concerned division must circulate BFIU guidelines and circulars to branches. Response: Acceptable Risk
Inadequate training/ workshop arranged on AML & CFT	Likely	Major	=3(High)	Concerned division should taken adequate measure to provide proper training (mandatory) to all Staff members and also arrange refreshers training on regular interval.
No independent audit function to test the AML program	Likely	Major	=3(High)	Internal Audit & Inspection Department should be conducted AML System Check as per Independent Testing Checklist to all branches on annual basis and submit a copy to AML & CFT Division.

ANNEXURE-B

KYC DOCUMENTATION

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Individuals / Joint Account	• NID or valid Passport or Birth Registration Certificate (Printed copy, with seal & signature from the Registrar). NB: From Passport, NID & Birth Registration Certificate, one is mandatory. In case of submitting the birth registration certificate, any other photo id (issued by a Government department or agency) of the person has to be supplied with it. If he does not have a photo id, then a certificate of identity by any renowned people has to be submitted according to the bank's requirement. That certificate must include a photo which is duly attested by the signing renowned person. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.	• Salary Certificate (for salaried person). • Employed ID (For ascertaining level of employment). • Self-declaration acceptable to the bank. (commensurate with declared occupation) • Documents in support of beneficial owner's income (incase of house wife, students & etc.). • Trade License (if the customer declared to be a business person). • TIN Certificate / Acknowledgement receipt of return of income (if any) . • e-TIN which issued after 2020. • 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 related documents. NRTA : • Photocopy of valid passport along with copy of VISA required. • Photocopy of work permit required.	• 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/spouse's name (i.e. Water/Electricity/ Telephone/Gas). • If account holder is house owner, Municipal Tax Receipt (not older than 2020). • If the customer address given in AOF and customer's permanent address mentioned in NID is same and Branch can verify the NID successfully, it can be treated as address verification proof along with Customer's declaration. • Residential address appearing on an official document prepared by a Government Agency. • Rental agreement. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Physical verification report by RM/Branch Officials. • Third party verification report. • Rental House utility bill/utility card on satisfaction of the BAMLCO/RM/ dealing officer.

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Sole Proprietorships or Individuals doing business	• NID or valid Passport or Birth Registration Certificate (Printed copy, with seal & signature from the Registrar). • 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 association, cloth Merchant association, hawker's association etc.) • Any other documents that satisfy to the bank.	• Updated Trade License. • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN issued recently . • BIN, IRC, ERC (if any). • Self declaration acceptable to the bank. (commensurate with nature and volume of business) • Documents of property sale. (if injected any fund by selling personal property) • Other Bank statement (if any) • Document of FDR encashment (if any fund injected by en-cashing personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan (if any) • Personal borrowing (if any)	• 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 (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Partnership	• Partnership deed/ partnership letter • Registered partnership deed (if registered) • Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. • NID or valid Passport or Birth Registration Certificate (Printed copy, with seal & signature from the Registrar) of all partners. • 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 association, cloth Merchant association, hawker's association etc.) • Any other documents that satisfy to the bank.	• Updated Trade License. • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN issued recently . • BIN, IRC, ERC (if any). • Documents of property sale. (if injected any fund by selling personal property of a partner) • Other Bank statement (if any) • Document of FDR encashment (if any partner injected capital by enchasing Personal FDR) • Document of foreign remittance (if any fund comes from outside the country) • Bank loan • Personal Borrowing (if any)	• Physical verification report by RM/Branch Officials. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Third party verification report. • 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 customer or his/her parent's/spouse's name (i.e. Water/Electricity/ Telephone/Gas). • Residential address appearing on an official document prepared by a Government Agency. • Rental agreement.

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Private Limited Companies	• NID or valid Passport of all the directors. • List of directors with updated Form XII & Schedule X. • Certificate of incorporation. • RJSC Amendment Certificate (if any • Memorandum and Articles of Association • 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 (only for assets client). • Updated Trade License • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN recently issued. • BIN, IRC, ERC (if any). • VAT registration. • Other Bank statement • Bank loan	• Physical verification report by RM/Branch Officials. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Third party verification report. • 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 customer or his/her parent's/spouse's name (i.e. Water/Electricity/ Telephone/Gas). • Residential address appearing on an official document prepared by a Government Agency. • Rental agreement.

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Public Limited Companies	• NID or valid Passport of all the directors. • List of directors with updated Form XII & Schedule X. • Certificate of incorporation. • RJSC Amendment Certificate (if any). • Memorandum and Articles of Association. • Certificate of commencement of business. • 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 (only for assets client). • Updated Trade License • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN recently issued. • BIN, IRC, ERC (if any). • VAT registration. • Other Bank statement(if any). • Bank loan. •	• Physical verification report by RM/Branch Officials. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Third party verification report. • 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 customer or his/her parent's/spouse's name (i.e. Water/Electricity/ Telephone/Gas). • Residential address appearing on an official document prepared by a Government Agency. • Rental agreement.

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
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. • Copy of NID or valid Passport of the operator (s).	N/A	N/A
NGO	• Copy of NID or valid 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	• Physical verification report by RM/Branch Officials. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Third party verification report.

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Charities or Religious Organizations	• Copy of NID or valid 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	• 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).
Clubs or Societies	• Copy of NID or valid 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 (if registered). • Other Bank statement • Certificate of Grant/ Aid • Subscription • If unregistered declaration of authorized person/ body.	• 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).

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Trusts, Foundations or similar entities	• Copy of NID or valid Passport of the trustee (s), author of the trust & beneficiaries. • 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. • Reasonable measures to verify trust document through independent means (e.g. Registry of Trust, Notary).	• A copy of last available financial statements duly certified by a professional (if registered). • Tax waiver certificate or NBR clearance. • Other Bank statement • Certificate of Donation or related doc.	• 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).

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Financial Institutions (NBFI)	• Copy of NID or valid Passport of the operator (s). • Certificate of incorporation • Memorandum and Articles of Association • Certificate of commencement of business • List of directors in form-XII & X. • 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 (only for assets client). • Trade License • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN recently issued. • BIN (if any) • VAT registration • Cash flow statement	• Physical verification report by RM/Branch Officials. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Third party verification report.

Customer type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/ RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)
Embassies	• Valid Passport with visa of the authorized official • Clearance of the foreign ministry • Other relevant documents in support of opening account	N/A	• Physical verification report by RM/Branch Officials. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Third party verification report.
Beneficial owner	• Beneficial owner of legal arrangements - Detail has been set out in Annexure-I		

Important -

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

ANNEXURE-C

KYC PROFILE FORM FOR WALK-IN CUSTOMER/BEARER

চলন্ত গ্রাহক/বাহক কর্তৃক লেনদেনের ক্ষেত্রে প্রযোজ্য কেওয়াইসি প্রোফাইল ফরম

Name (নাম) ঃ	
Mobile No. (মোবাইল নম্বর) ঃ	Occupation (পেশা) ঃ
Date of Birth (জন্ম তারিখ) ঃ	Nationality (জাতীয়তা) ঃ
Father's Name (পিতার নাম) ঃ	
Mother's Name (মাতার নাম) ঃ	
Present Address (বর্তমান ঠিকানা) ঃ	
Permanent Address (স্থায়ী ঠিকানা) ঃ	
Identity information পরিচিতিমূলক তথ্যাদি (NID/Passport/Birth Registration Certificate জাতীয় পরিচয়পত্র/পাসপোর্ট/জন্ম সনদপত্রের নম্বর) ঃ Type of ID (পরিচয় পত্রের ধরণ) ঃ .... ID No. (পরিচয় পত্র নম্বর) ঃ............................ Expiry Date (মেয়াদোত্তীর্ণের তারিখ) ঃ......................... (According to instruction of BFIU Circular No.26, attested copy of Photo ID must be collected for above Tk.50,000/= (fifty thousand) transaction by bearer / walk-in customer. (বিএফআইইউ সার্কুলার নং-২৬ এ বর্ণিত নির্দেশনা অনুসারে গ্রাহক ব্যতিত অন্য কোন ব্যক্তি / ওয়াক-ইন-কাস্টমার কর্তৃক ৫০,০০০/= (পঞ্চাশ হাজার) টাকার অধিক লেনদেনের ক্ষেত্রে প্রেরণকারী/আবেদনকারী/জমাকারী/উত্তোলনকারীর ছবিযুক্ত আইডি কার্ডের সত্যায়িত কপি আবশ্যিকভাবে গ্রহণ করতে হবে)	
A/C Title & Number (হিসাবের নাম ও নম্বর) ঃ	
Relation with Beneficiary/Account Holder (প্রাপক/গ্রাহকের সাথে সম্পর্ক) ঃ	
Value of Transaction (লেনদেনের মূল্য/পরিমান) ঃ	
Reason of Transaction / Source of Fund (লেনদেনের কারণ / অর্থের উৎস) ঃ	

I/We solemnly declare that the information mentioned above is/are correct. I/We shall/will also submit any type of additional information/documents, if required. আমি/আমরা এই মর্মে ঘোষণা করছি যে, উপরে প্রদত্ত তথ্যসমূহ সত্য। এর অতিরিক্ত কোন তথ্য প্রয়োজন হলে আমি/আমরা তা প্রদান করব।

Signature with date (তারিখসহ স্বাক্ষর) ঃ	

N.B.: In case of issuing Pay Order/DD/TT name and full address of beneficiary must be obtained in Application Form. বি.দ্র.ঃ পে-অর্ডার/ডিডি/টিটি ইস্যুর ক্ষেত্রে প্রাপক/বেনিফিশিয়ারীর নাম ও পূর্ণাঙ্গ ঠিকানা অবশ্যই আবেদন ফরমে গ্রহণ করতে হবে।

For Bank Use Only

Collected Documents Verified (পরিচিতিমূলক তথ্য বা উপাত্তের সঠিকতা যাচাই করা হয়েছে কি না) ? Yes (হ্যাঁ) No (না)

Signature with date

Signature with date

ANNEXURE- D

ANTI - MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM QUESTIONNAIRE

As per BFIU Circular No 26, Dated 16 June 2020

A. BASIC INFORMATION		
1.	Name of the Institution :	
2.	Registered Address :	
3.	Website Address :	
4.	Principal Business Activities :	
5.	Regulatory Authority :	
6.	Operational Status : • Does your Bank maintain a physical presence in the licensing country?	☐ Yes ☐ No

B. OWNERSHIP / MANAGEMENT		
7.	Is your institution listed in any stock exchange? If so, which stock exchange?	☐ Yes ☐ No

8.	If "No" to Q7, please provide a list of the major shareholders holding more than 10% shares in your institution.	☐ Yes ☐ No

C. ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CONTROLS		
If you answer "no" to any question, additional information can be supplied at the end of the questionnaire.		
	I. General AML & CFT Policies, Practices and Procedures:	
9.	Does your institution have policies and procedures approved by your institution's board or senior management to prevent money laundering and Combat Financing of Terrorism?	☐ Yes ☐ No
10.	Does your institution have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML/CFT framework?	☐ Yes ☐ No
11.	Has your institution developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions?	☐ Yes ☐ No
12.	Does your institution have a policy prohibiting accounts/relationships with shell banks? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)	☐ Yes ☐ No
13.	Does your institution permit the opening of anonymous or numbered accounts by customers?	☐ Yes ☐ No
14.	Does your institution have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	☐ Yes ☐ No
15.	Does your institution have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates?	☐ Yes ☐ No
16.	Does your institution have policies and procedures that require keeping all the records related to customer identification and their transactions? If "Yes", for how long?	☐ Yes ☐ No
	II. Risk Assessment	
17.	Does your institution have a risk-based assessment of its customer base and their transactions?	☐ Yes ☐ No

18.	Does your institution determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?	☐ Yes ☐ No
	III. Know Your Customer, Due Diligence and Enhanced Due Diligence	
19.	Has your institution implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?	☐ Yes ☐ No
20.	Does your institution have a requirement to collect information regarding its customers' business activities?	☐ Yes ☐ No
21.	Does your institution have a process to review and, where appropriate, update customer information relating to high risk client information?	☐ Yes ☐ No
22.	Does your institution have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?	☐ Yes ☐ No
23.	Does your institution complete a risk-based assessment to understand the normal and expected transactions of its customers?	☐ Yes ☐ No
	IV. Reportable Transactions for Prevention and Detection of ML/TF	
24.	Does your institution have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	☐ Yes ☐ No
25.	Where cash transaction reporting is mandatory, does your institution have procedures to identify transactions structured to avoid such obligations?	☐ Yes ☐ No
26.	Does your institution screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities or under the UN security Council Resolution?	☐ Yes ☐ No
27.	Does your institution have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?	☐ Yes ☐ No
	V. Transaction Monitoring	
28.	Does your institution have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as travelers checks, money orders, etc?	☐ Yes ☐ No
	VI. AML Training	
29.	Does your institution provide AML& CFT training to relevant employees of your organisation?	☐ Yes ☐ No
30.	Does your institution communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?	☐ Yes ☐ No
31.	Does your institution provide AML training to relevant third parties if they are employed to carry out some of the functions of your organization?	☐ Yes ☐ No

Space for additional information:
(Please indicate which question the information is referring to.)

....
....
....
....
....
....

D. GENERAL		
32.	Does the responses provided in this Declaration applies to the following entities:	
	• Head Office and all domestic branches	☐ Yes ☐ No
	• Overseas branches	☐ Yes ☐ No
	• Domestic subsidiaries	☐ Yes ☐ No
	• Overseas subsidiaries	☐ Yes ☐ No
	If the response to any of the above is "No", please provide a list of the branches and /or subsidiaries that are excluded, including the name of the institution, location and contact details.	

I, the undersigned, confirm to the best of my knowledge that the information provided in this questionnaire is current, accurate and representative of the anti-money laundering and anti-terrorist financing policies and procedures that are established in my institution.

I also confirm that I am authorized to complete this questionnaire on behalf of my institution.

Signature	:	
Name	:	
Designation	:	
Date	:	
Contact No	:	
Email	:	

ANNEXURE- E

POLITICALLY EXPOSED PERSONS (PEPS), INFLUENTIAL PERSONS (IPS) & BENEFICIAL OWNER (BO)

1. 1 Politically Exposed Persons (PEPs)

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

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 the 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-

1.2 Who are Politically Exposed Persons (PEPs)?

- 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, e.g. 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

1.3 Who are Domestic PEPs (Known as Influential Persons; IPs in Bangladesh

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

1.4 Chief or similar high-ranking positions in an international organization.

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 & IPs is not intending to cover middle ranking and more junior individuals as mentioned in 1.2, 1.3 and 1.4.

1.5 Who should be considered a family member of a PEP?

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. Respective Bank 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, Bank 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.

1.6 Close associates of a PEP

A 'known close associate' of a PEP 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.

2. Various scenario 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 customer due diligence 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 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. Bank 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.

3. PEPs versus Risk

3.1 Do all PEPs pose the same 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 Bank has considered in its risk assessment.

This guidance discusses on how Bank may differentiate between PEPs. In this guidance, the terms 'lower risk' and 'higher risk' are used to recognize that Bank 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.

3.2 What are some indicators that a PEP might pose a lower risk?

The following indicators suggest a PEP poses a lower risk:

- If he/she is seeking access to a product the 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)

3.3 What are indicators that a PEP might pose a higher risk?

The following indicators suggest a PEP poses a higher risk:

a) Higher risk indicator — product

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

b) Higher risk indicators — 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, Bank 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

c) Higher risk indicators — personal and professional

The following characteristics might suggest a 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 (e.g. 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.

4. What are reporting organizations' obligations under the Regulations?

4.1 The Regulations required that Bank should 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 the Bank's 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 Bank have 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.

4.2 The Regulations state that in determining whether these systems and procedures are appropriate, Bank 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.

4.3 Bank should 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), Bank 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 reporting organization to consider relevant factors when meeting these obligations. Bank's assessment and its decision to apply relevant enhanced due diligence measures need to be clearly documented.

4.4 BFIU expects that Bank have 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. Bank 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 is 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.

4.5 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.

4.6 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, Bank needs to comply with the requirement not to establish, or to terminate, a business relationship.

4.7 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 that the Bank has assessed in relation to the customer. Bank should apply more extensive measures for relationships assessed as high risk and less extensive measures for lower risk customers.

4.8 What measures may reporting organizations take in lower risk situations?

In lower risk situations a reporting organization may take the following measures:

- Conduct enquiries about a a PEP's 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, reporting organizations 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 PEP's family and close associates is subject to less frequent formal review than it was considered high risk

4.9. What measures should be taken by Bank in higher risk situations?

In higher risk situations Bank should 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 PEP's family and close associates) is subject to more frequent and thorough formal review as to whether the business relationship should be maintained

4.10 Beneficial owners of legal entities who are PEPs

Reporting organizations 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 reporting organization 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, reporting organization 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 reporting organization 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 the reporting organization.

GUIDELINES FOR BENEFICIAL OWNER

Identification of Beneficial Owner

Who is a beneficial owner?

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.

1. 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.

2. 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 on the customer;

   c. the person on whose behalf a transaction is conducted

3. 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.

I. Why is it important to identify the beneficial owner?

1. 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.

2. 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.

II. Ways in which beneficial ownership information can be hidden/obscured

a) 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,

b) Bearer shares and bearer share warrants,

c) Use of legal persons as directors,

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

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

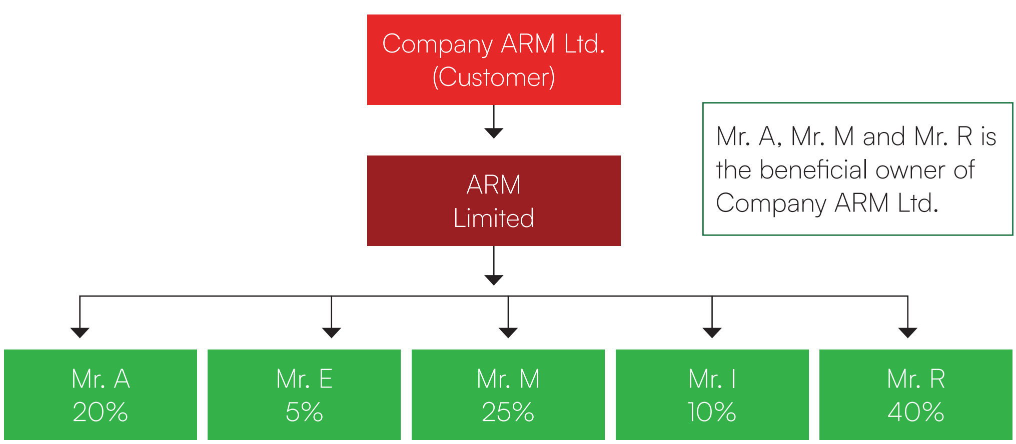
f) Trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,

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

III. 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. Few examples are as follows:

a) Simple ownership



IV. Effective Control

1. 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).

2. 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.

V. Beneficial owner of legal arrangements

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

2. 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.

3. 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).

4. 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.

VI. Applying a risk-based approach

1. 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.

2. One should apply enhanced customer due diligence and make a suspicious transaction report to the Bangladesh Financial Intelligence Unit (BFIU) where there are reasonable grounds for suspicion of money laundering or terrorist financing,

3. 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.

ANNEXURE- F

STANDARD KYC DOCUMENTATION FOR PERIODIC KYC REVIEW [CONSUMER OR PAYROLL OR RETAIL CUSTOMER]

Customer Type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)	Use of Form
Individuals or Join	• NID or valid Passport or Birth Registration Certificate (Printed copy, with seal & signature from the Registrar).	• 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 (incase of house wife, students & etc.). • Trade License (if the customer declared to be a business person). • TIN Certificate / Acknowledgement receipt of return of income (if any) . • e-TIN which issued after 2020. • 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 related documents. NRTA : • Photocopy of valid passport along with copy of VISA required. • Photocopy of work permit required.	• 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/ spouse's name (i.e. Water/ Electricity/Telephone/Gas). • If account holder is house owner, Municipal Tax Receipt (not older than 2020). • If the customer address given in AOF and customer's permanent address mentioned in NID is same and Branch can verify the NID successfully, it can be treated as address verification proof along with Customer's declaration. • Residential address appearing on an official document prepared by a Government Agency. • Rental agreement. • Acknowledgement receipt of thanks / KYC review letter through postal/couriers service. • Physical verification report by RM/Branch Officials. • Third party verification report. • Rental House utility bill/utility card on satisfaction of the BAMLCO/ RM/ dealing officer.	• Personal Information Form or Beneficial Owner Form (if required). • Personal KYC Profile Form (New Risk Grading Form)

REVIEW [CONSUMER OR PAYROLL OR RETAIL CUSTOMER]

Customer Type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)	Use of Form
Sole Proprietorships or Individuals doing business	• NID or valid Passport or Birth Registration Certificate (Printed copy, with seal & signature from the Registrar).	• Updated Trade License. • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN which issued after 2020. • BIN, IRC, ERC (if any).	• Physical verification report by RM/Branch Officials. • Acknowledgement receipt of thanks / KYC review letter through postal/ couriers service. • Third party verification report. • 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 customer or his/her parent's/ spouse's name (i.e. Water/Electricity/ Telephone/Gas). • Residential address appearing on an official document prepared by a Government Agency. • Rental agreement.	• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form or Beneficial Owner Form (if required). • Non-Personal KYC Profile Form (New Risk Grading Form).
Partnership	• Partnership deed/ partnership letter or Registered partnership deed (if registered). • Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. • NID or valid Passport of partners • Ownership documents of the Business (i.e. purchase documents of the shop or inheritance documents or rental deed). • Membership certificate of any association. (if applicable) (i.e. Chamber of commerce, market association, trade association i.e.; Hardware association, cloth Merchant association, hawker's association etc.). • Any other documents that satisfy to the bank. • N.B.: If not provided earlier	• Updated Trade License • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN which issued after 2020. • BIN, IRC, ERC (if any).		• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form or Beneficial Owner Form (if required). • Non-Personal KYC Profile Form (New Risk Grading Form). •

Customer Type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)	Use of Form
Private Limited Companies	• NID or valid Passport of all the directors. • List of directors with updated Form XII & Schedule X. • Certificate of incorporation. • RJSC Amendment Certificate (if any) • Memorandum and Articles of Association. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Nature of the company's business. • Expected annual 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. • N.B.: If not provided earlier	• A copy of last available financial statements duly authenticated by competent authority (only for assets client). • Updated Trade License • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN which issued after 2020. • BIN, IRC, ERC (if any). • VAT registration. •		• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form or Beneficial Owner Form (if required). • Non-Personal KYC Profile Form (New Risk Grading Form).
Public Limited Companies	• NID or valid Passport of all the directors. • List of directors with updated Form XII & Schedule X. • Certificate of incorporation. • RJSC Amendment Certificate (if any). • Memorandum and Articles of Association. • Certificate of commencement of business. • Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. • Nature of the company's business. • Expected annual 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. • N.B.: If not provided earlier	• A copy of last available financial statements duly certified by a professional accountant. (only for assets client). • Updated Trade License. • TIN • BIN, IRC, ERC (if any). • VAT registration.		• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form or Beneficial Owner Form (if required). • Non-Personal KYC Profile Form (New Risk Grading Form).

Customer Type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)	Use of Form
Govern-ment Owned Entities	• Statue of formation of the entity. • Copy of NID or valid Passport of the operator (s). • N.B.: If not provided earlier	N/A		• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form (only for signatories). • Non-Personal KYC Profile Form (Govt.) (New Risk Grading Form).
Charities or Religious Organiza-tions	• Copy of NID or valid Passport of the operator (s). • Documents of nature of the Organizations. • Certificate of registration issued by competent authority (if any). • Bye-laws (certified). • List of Management Committee/ Directors. • N.B.: If not provided earlier	• Certificate of Grant/Aid/ donation or NGO Affairs Bureau. • Any other legal source.		• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form or Beneficial Owner Form (if required). • Non-Personal KYC Profile Form (New Risk Grading Form).
Clubs or Societies	• Copy of NID or valid Passport of the operator (s). • Documents of nature of the Organizations. • Certificate of registration issued by competent authority (if any) • Bye-laws (certified). • List of Management Committee/ Directors. • N.B.: If not provided earlier	• Certificate of Grant/ Aid / donation. • Subscription fees. • If unregistered declaration of authorized person/ body.		• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form or Beneficial Owner Form (if required). • Non-Personal KYC Profile Form (New Risk Grading Form).
Financial Institutions (NBFI)	• Copy of NID or valid Passport of all the directors. • Certificate of incorporation. • Memorandum and Articles of Association. • Certificate of commencement of business. • List of directors in form-XII. • 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. • N.B.: If not provided earlier	• A copy of last available financial statements duly certified by a professional accountant (only for assets client). • Trade License • TIN Certificate / Acknowledgement receipt of return of income. • e-TIN which issued after 2020. • BIN (if any) • VAT registration		• Page 1&2 of Non-Personal AOF (if required). • Personal Information Form or Beneficial Owner Form (if required). • Non-Personal KYC Profile Form (New Risk Grading Form).

Customer Type	Standard Identification document	Document for verification of source of funds (one or more according to satisfaction of BAMLCO/RM)	Address verification procedure to justify the existence of Customer (one or more as per convenient)	Use of Form
NGO	Copy of NID or valid Passport of the operator (s). Documents of nature of the NGO. Certificate of registration issued by competent authority. Bye-laws (certified). List of Management Committee/ Directors. N.B.: If not provided earlier	A copy of last available financial statements duly certified by a professional accountant. (only for assets client) TIN Certificate / Acknowledgement receipt of return of income. e-TIN which issued after 2020. BIN (if any). Certificate of Grand/ Aid/ Donation.		Page 1&2 of Non-Personal AOF (if required). Personal Information Form or Beneficial Owner Form (if required). Non-Personal KYC Profile Form (New Risk Grading Form).
Trusts, Foundations or similar entities	Copy of NID or valid Passport of the trustee (s), author of the trust & beneficiaries. Certified true copy of the Trust Deed Bye-laws (certified). Power of attorney allowing transaction in the account. Reasonable measures to verify trust document through independent means (e.g. Registry of Trust, Notary). N.B.: If not provided earlier	Tax waiver certificate or NBR clearance. Certificate of Donation.		Page 1&2 of Non-Personal AOF (if required). Personal Information Form or Beneficial Owner Form (if required). Non-Personal KYC Profile Form.
Embassies	Valid Passport with visa of the authorized official. Clearance of the foreign ministry. Other relevant updated documents in support of opening account / operations.	N/A		Page 1&2 of Non-Personal AOF (if required). Personal Information Form or Beneficial Owner Form (if required). Non-Personal KYC Profile Form.

Transaction Profile (TP):

- KYC Profile Form (Monthly Transaction: Monthly Deposit & Monthly Withdrawal). Annual Turnover / Transaction = (Monthly Deposit + Monthly Withdrawal) * 12

Customer Signature requirement:

- In case of changes of personal information - customer signature is mandatory on Personal Information Form (PIF).
- In case of changes of entity's information - customer signature is mandatory on 2 page of Non-personal Account Opening Form.

- If there is no change found in customer's personal information, BAMLCO/RM will collect the updated documents of Customer and BAMLCO/RM fill-up only KYC Profile Form with declaration "No changes found".
- Customer signatures need to obtain on photocopy documents and NID of existing account must be verified by Branch officials.

Beneficial owner:

- who owns 20% or more percent of a company or legal arrangements?
- who has effective control of the customer?
- the person on whose behalf a transaction is conducted

Additional or further Documentation:

- FATCA Form (if not obtained earlier).
- Photo and NID/Passport/ Birth Certificate of the Nominee along with nominee declaration. Nominee Form old or new is acceptable. In case of Nominee is a Minor, procedure of obtaining Legal Guardian & his/her documents to be followed.
- Branch to check De-Dup against each signatory/director and also do sanctions screening if it is required new customer ID creation to tag with the account. If any signatory/director is found in existing Customer IDs, it must be mentioned on the form for subsequent tagging with account.
- During the KYC review, considering the existing AOF documentation - If any other documentation lapses are found with AOF that could be taken care of on a case-to-case basis.

Document upload:

Branch/RM should send these KYC review documents to LOD through Prime Intellect (PI) menu 'Periodic KYC Review' and preserve these hard copies KYC review documents with original AOF.

Other instructions:

Joint account:

- Personal document of each joint Account Holder is required for periodic KYC review.
- For personal information change/update, PIF with customer signature required.

NRTA Accounts (already marked in CBS):

** For existing savings account holders currently residing aboard, need to mark as NRTA in CBS and periodic KYC will be reviewed subsequently.

My First Account:

- Updated document of Guardian/Signatory/Beneficial owner.
- Applicant/Guardian/Beneficial Owner Personal Information Form required (if not obtained earlier).

Business Segment & RM Code change:

- Customer's business segment change is not under purview of periodic KYC review.
- RM Code change is not under purview of periodic KYC review.
- ** For changing of Business Segment & RM Code Branch/RM should request to LOD separately according to the existing procedure.

Mobile number & SS card change:

- Branch should take special caution & necessary actions to update/change SS Card when customer change/update of Mobile Number in PIF.

Prime Bank PLC.
Prime View: Plot- SE(F) 7, Bir Uttam Mir Shawkat Sharak,
Gulshan Avenue, Dhaka-1212
PABX: +880 (2)223387265
Fax: 880-2-5506868
email:info@primebank.com.bd

nymphea | www.nymphea-bd.com