IPDC Finance PLC

Manual on Prevention of Money Laundering and Terrorist Financing

Version 4.0

December 8, 2024

Approval Level: Board of Directors
Approval Date: December 2024

Owner: Chief Anti-Money Laundering Compliance Officer
Review Frequency: 36 months
Next Review Date: December 2027

Contents

PREFACE

Money Laundering and Terrorist financing have emerged as the alarming financial crime in the global economy. To combat these, Bangladesh has enacted the "Money Laundering Prevention (Amendment) Act 2015" and "Anti-Terrorism (amendment) Act 2013". Besides, BB vide DFIM circular # 7 dated 4 October 2012 has declared "Money laundering and Terrorist Financing Risk" as one of the core risks of the financial institutions. In this regard, Bangladesh Financial Intelligence Unit (BFIU) has also issued a "Guidance Note on prevention of money laundering and terrorist financing." To further strengthen AML & CFT, BFIU circular 28 dated 30 May 2023 has been published specifying duties of Financial Institutions. As per the circular, financial institutions should develop their policy after taking into consideration all these regulatory promulgations. In this context, IPDC Finance Limited (referred to as "IPDC") declares its policy named hereafter "Policy on PREVENTION OF MONEY LAUNDERING (AML) and TERRORIST FINANCING (CTF)"

IPDC has embraced its statutory obligations to assist in the detection of terrorist activity and the laundering of proceeds of crime by knowing its customers through identification, verification, and ongoing monitoring, reporting suspicious transactions/ suspicious Activities, and record-keeping obligations. IPDC will also ensure all its employees are aware of AML and CTF and what these terms mean, detail the roles and responsibilities of its employees concerning AML/CTF, and clearly document the requirements of the Money Laundering Prevention (Amendment) Act 2015, Money Laundering Prevention Rules, 2019, Anti-Terrorism (Amendment) Act 2012, Anti-Terrorism Rules, 2013, and other AML related circulars issued by the BB from time to time.

To ensure compliance with these enactments, IPDC established a Central Compliance Unit (CCU) (Sec: 3.1) under the leadership of CAMLCO who is at least the third rank in seniority in the organizational hierarchy. Besides, IPDC has designated one high-level officer as Deputy Chief Anti-Money Laundering Compliance Officer (Deputy CAMLCO) in the CCU and Branch Anti-Money Laundering Compliance Officer (BAMLCO) at the branch level. The CAMLCO is the Head of CCU and has more than seven years of working experience in a management role/administrative level, whereas the DCMLCO has a minimum experience of five years.

Compliance requirements of the above enactments, which IPDC or its employees should always bear in mind, are as follows:

1. Report to BB proactively and immediately facts on suspicious, unusual, or doubtful transactions (STR/SAR) likely to be related to money laundering. [Ref: 25(1)(d) of MLP (Amendment) Act 2015]
2. Maintain confidentiality while sharing customer's account-related information. [Ref: MLP (Amendment) Act 2015 and Anti-Terrorism (Amendment), 2013.
3. Not to disclose the fact that an STR or related information is being reported to BFIU. [Ref: Sec 6 of MLP (Amendment) Act 2015 and FATF Recommendation # 21]
4. Not to open or maintain a numbered or anonymous account.
5. Know Your Employee (KYE) and Know Your Customer (KYC)
6. Exercising Enhanced Due Diligence (annexure: 2) while opening accounts of PEPs & IP. [AML circular # 14 dated 25 September 2007]
7. Customer Due Diligence (Chapter 4) should be exercised when customers are identified, accepted, monitored, and reported for suspicious transactions.
8. Self-assessment of the effectiveness of the AML /CFT program should be carried out half yearly by the AML Compliance Officers, and the results of the same are to be communicated to the Head of CCU. [AML circular # 15]
9. The IA&C division and external auditors of the company have applied independent testing procedures to check the adequacy of AML controls/policies. [AML circular # 15]
10. IPDC record retention policy [Annexure-A]

The rest of the chapters have been developed in accordance with the compliance requirements of the above enactments and continuing business needs. Every IPDC employee has a duty to understand and comply with this policy, and hence, HR must obtain a declaration to that effect from every employee.

Chapter One: Introduction

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

Money laundering significantly impacts a country's economy, impeding the social, economic, political, and cultural development of societies worldwide. Both money laundering and terrorist financing can weaken individual financial institutions and threaten a country's overall financial sector reputation. Combating money laundering and terrorist financing is, therefore, a key element in promoting a strong, sound, and stable financial sector.

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

1.1 Defining Money Laundering

Money laundering can be defined in several ways. Most countries subscribe to the definition adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention)1 and the United Nations Convention Against Transnational Organized Crime (2000) (Palermo Convention):

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

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

- 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), which is recognized as the international standard setter for anti-money laundering (AML) efforts, defines the term ―money laundering succinctly as ―the processing of criminal proceeds to disguise their illegal origin to ―legitimize the ill-gotten gains of crime.

Money Laundering is defined in Section 2 (v) of the Money Laundering Prevention (Amendment) Act 2015 as follows:

1.2 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 to reporting requirement under this Act may be avoided.

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

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

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

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

1.3 Purpose of Money Laundering*:*

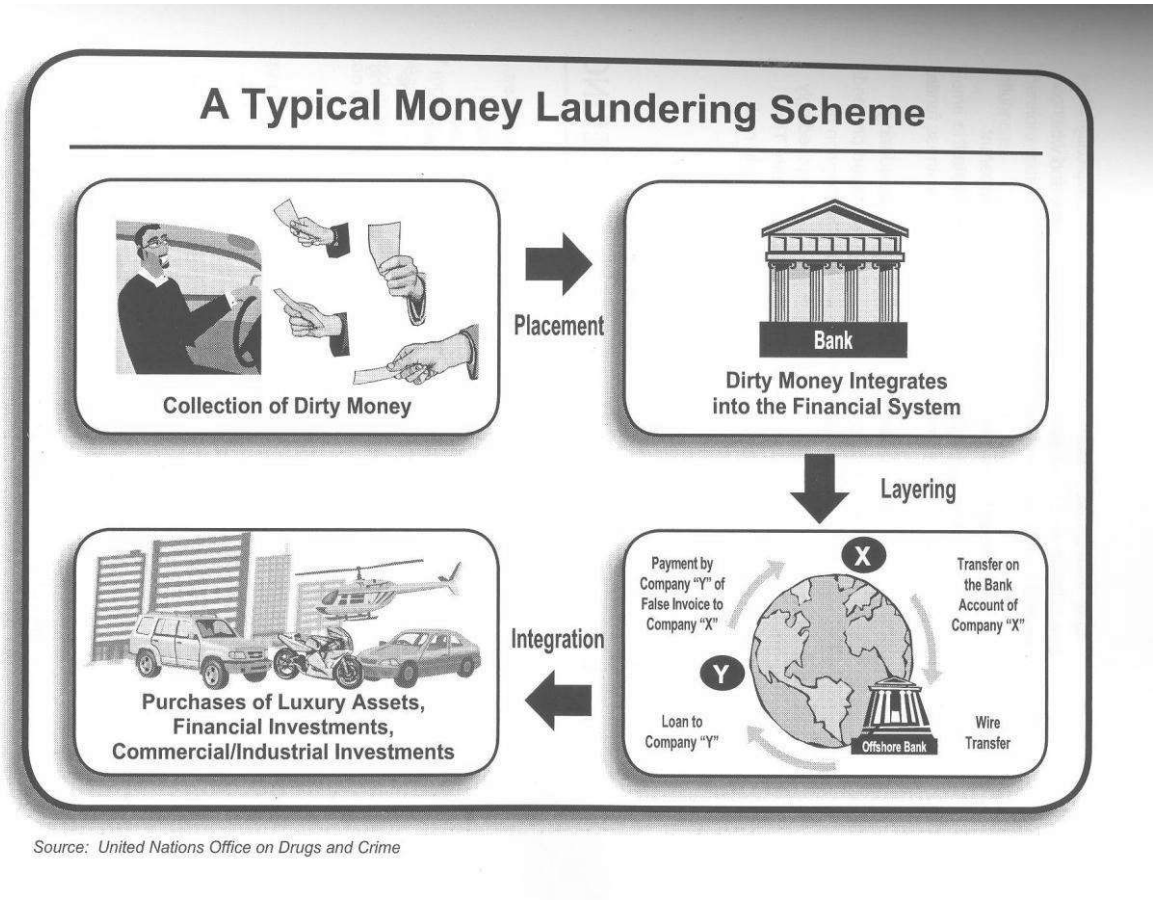
The purpose of money laundering is to break the connection between the money and the crime that generated the money. In other words, money laundering disguises or conceals the illicit origin of money generated by criminal activities.

Criminals engage in money laundering for three main reasons:

i. Money is required to organize and run criminal activity for financial gain. Because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and supplements finance for new crimes. It also pays the criminals for an expensive lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.
ii. A trail of money earned through illegal activities can become evidence of crime. Criminals must conceal or disguise the source of their wealth to avoid prosecution.
iii. The proceeds from crime often become the target of investigation and seizure. To cover ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or alternatively, give them a legitimate look.

1.4 Money laundering process involves 3 steps:

Money laundering is not a single act but a process accomplished in 3 basic stages: placement, layering, and integration, which may comprise numerous transactions by the launderers. A typical money laundering scheme is illustrated below:



Source: United Nations Office on Drugs and Crime

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

PLACEMENT: EXAMPLE

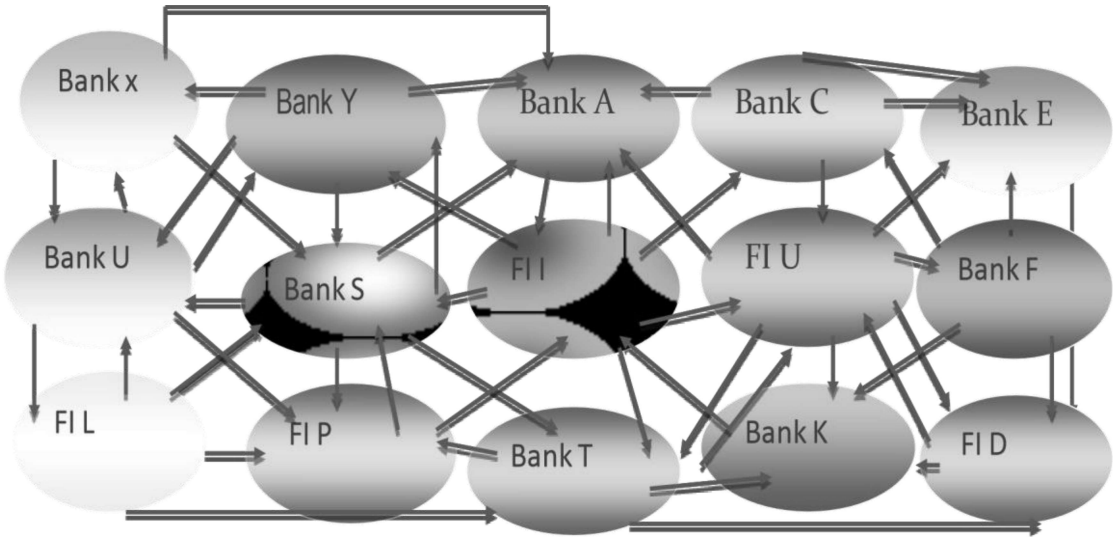
Mr. Baker, a human trafficker, earned Tk.10.00 crore by illegal means and placed the same as under

BANKS	**FINANCIAL INSTITUTIONS**	**INSURANCE COMPANIES**	**STOCK EXCHANGE**
6.00 crore	1.00 crore	2.00 crore	1.00 crore
By opening	By opening	By making 5	By purchasing Shares of Different
30 accounts in 30 banks	10 accounts in 10 institutions.	Life Policies for Family Members.	

Layering means a series of transactions or movement of funds to distance them from their source. That is a complex web of transactions that confuse the audit trail .

LAYERING: EXAMPLE

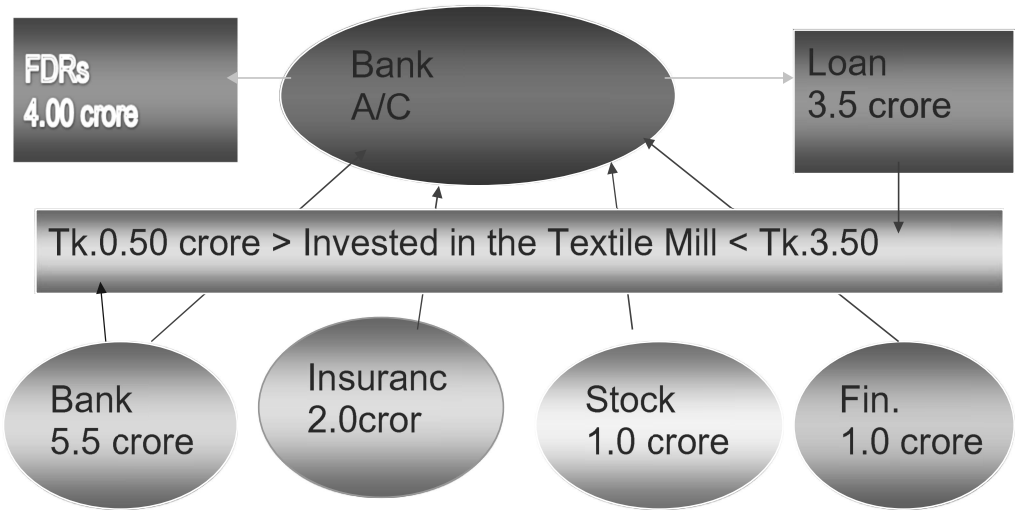
Mr. Baker moved money deposited in the banks through a series of economically meaningless transactions.



Integration means the re-entry of funds into the financial system appearing as a regular business, e.g., through investment in real estate, luxury assets, or business. In short, the layered funds are brought back into the legitimate economy or legitimate use.

INTEGRATION: EXAMPLE

Mr. Baker formed a company namely M/S Shah Ali Textile Ltd and opened an A/C in Bank X



The three basic steps may occur as separate and distinct phases simultaneously or, more commonly, overlap. The steps used depend on the available laundering mechanisms and the requirements of the criminal organizations.

Money laundering predicate offense is the underlying criminal activity that generated proceeds, which, when laundered, results in the offense of money laundering. This includes:

1. corruption and bribery
2. counterfeiting currency
3. counterfeiting deeds and 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 woman 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 obtaining money or trying to obtain money or valuable goods giving someone false assurances of employment abroad.
17. dowry
18. smuggling and offences related to customs and excise duties
19. tax related offenses
20. infringement of intellectual property rights
21. terrorism or financing in terrorist activities
22. adulteration or the manufacture of goods through infringement of tittle
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; and
28. Any other offence(s) declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official (Bangladesh) Gazette, for the purpose of this Act.

1.5 Combating Terrorist Financing (CTF)

Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. According to the Section 7 of the Anti-Terrorism (Amendment) Act, 2013 of Bangladesh, financing of terrorism means: Offences relating to financing terrorist activities

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

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

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

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

1.6 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. However, funds used to support terrorism may originate from legitimate

sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

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

1.7 Scope and Objective of the Policy

This policy is applicable for all sorts of products, operations, and activities IPDC is operating. In branches/ subsidiaries, the Company would ensure compliance with the internal regulations on AML/ CTF or that of the Bangladesh Financial Intelligence Unit (BFIU) wherever are more exhaustive.

The objective of this policy is to ensure that IPDC has designed and implemented processes and procedures that are consistent with regulatory guidelines and the objectives and purposes of the AML/CTF Act.

The overall framework for AML and CTF regime in IPDC is designed so that the business units will take responsibility for:

- verifying the true identity of customers prior to providing the designated services (customer due diligence and Know Your Customer);
- reporting all suspicious transactions to Bangladesh Financial Intelligence Unit (BFIU);
- keeping appropriate records for the stipulated time as determined by Bangladesh Financial Intelligence Unit (BFIU);
- provide, from time to time, information as required by Bangladesh Financial Intelligence Unit (BFIU); and
- developing implementing and complying with all AML/CTF related regulatory requirements.
- Commitment of IPDC against money laundering and terrorist financing.
- Arranging necessary training, monitoring and reporting periodic reports relevant to AML & CFT for all of IPDC branch and products.

Chapter Two: Vulnerabilities for IPDC and their mitigation

Money launderer may use different financial products like lease, loans, deposit scheme etc. to launder their money. Possible ways of laundering mechanism of ill money through use of IPDC‟s products or services are discussed below.

2.1 Vulnerabilities Of Products And Services

2.1.1 Lease/Term Loan Finance

Money launderers and terrorist financer can use this instrument for placement and layering of their ill gotten money.

Front company can take lease/term loan finance from IPDC and repay the loan from illegal source, and thus bring illegal money in the formal financial system in absence of proper measures. The company can also repay the loan amount even before maturity period if they are not asked about the sources of fund. In case of financial or capital lease, the asset purchased with IPDC„s financing facility can be sold immediately after repayment of the loan through illegal money and sold proceeds can be shown as legal.

2.1.2 Factoring

IPDC introduced its Factoring financing recently considering its different market segment. Using its complex business mechanism, the supplier and the buyer may ally together to legalize their proceeds of crime. Without conducting any bona fide transaction, the supplier may get finance from IPDC and IPDC may get repayment from buyer. IPDC may focused on getting repayment without considering the sources fund which can be taken as an opportunity by the money launderer to place their ill gotten money.

There are three kinds of Factoring products with IPDC as listed below:

i. Factoring: IPDC factoring provides advance cash against invoices or bills.
ii. Work Order: IPDC offers financing against work order (WO) to bridge the gap between time and processing the order receipt of payment.
iii. Distributor Finance: IPDC distributor finance provides advance cash against lift/instruction.

Those products are vulnerable for money laundering & Terrorist financing. Because customer may make payment by using illegal money.

2.1.3 Private Placement of Equity/Securitization of Assets

IPDC offer financing facilities to firms through private placement of equity and securitization of assets. IPDC sell those financial instruments to private investors who may take this as an opportunity to make their money legal. Later the money launderers can sell these instruments and bring their money into the formal financial system.

2.1.4 Personal Loan/Car Loan/Home Loan

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

2.1.5 SME/Women Entrepreneur Loan

Small, medium and women entrepreneurs can take loan facilities from IPDC and repay that (in some cases before maturity) with illegally earned money. They even do so only to validate their money by even not utilizing the loan. This way they can bring the illegal money in the financial system.

2.1.6 Deposit Scheme

IPDC sell deposit products with at least a three months maturity period. The depositor may encash their deposit money prior to the maturity date with prior approval from Bangladesh Financial Intelligence Unit (BFIU), foregoing interest income. This deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong measures.

2.1.7 Loan Backed Money Laundering

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

2.1.8 IPDC DANA

IPDC DANA is a Retailer Financing ecosystem in to facilitate access to finance for the retailers in an easy, low cost, collateral-free and structured manner. The ecosystem binds IPDC with corporates, its distributors, and retailers in the same digital platform. It enables retailers to lift products using their available credit under DANA at a low cost from their distributors and make repayments with single or multiple tranches within the defined credit period. Money laundering may occur in collaboration of multiple parties involved in the process. Customers may take frequent loans and repay early using illegally obtained money and hence placing illegal money in the economic system.

2.2 Mitigation Process

To mitigate the vulnerabilities an integrated risk based system should be followed to assess the relevant risk sectors and implement the appropriate risk based due diligence. A Risk Based control process should be as follows:

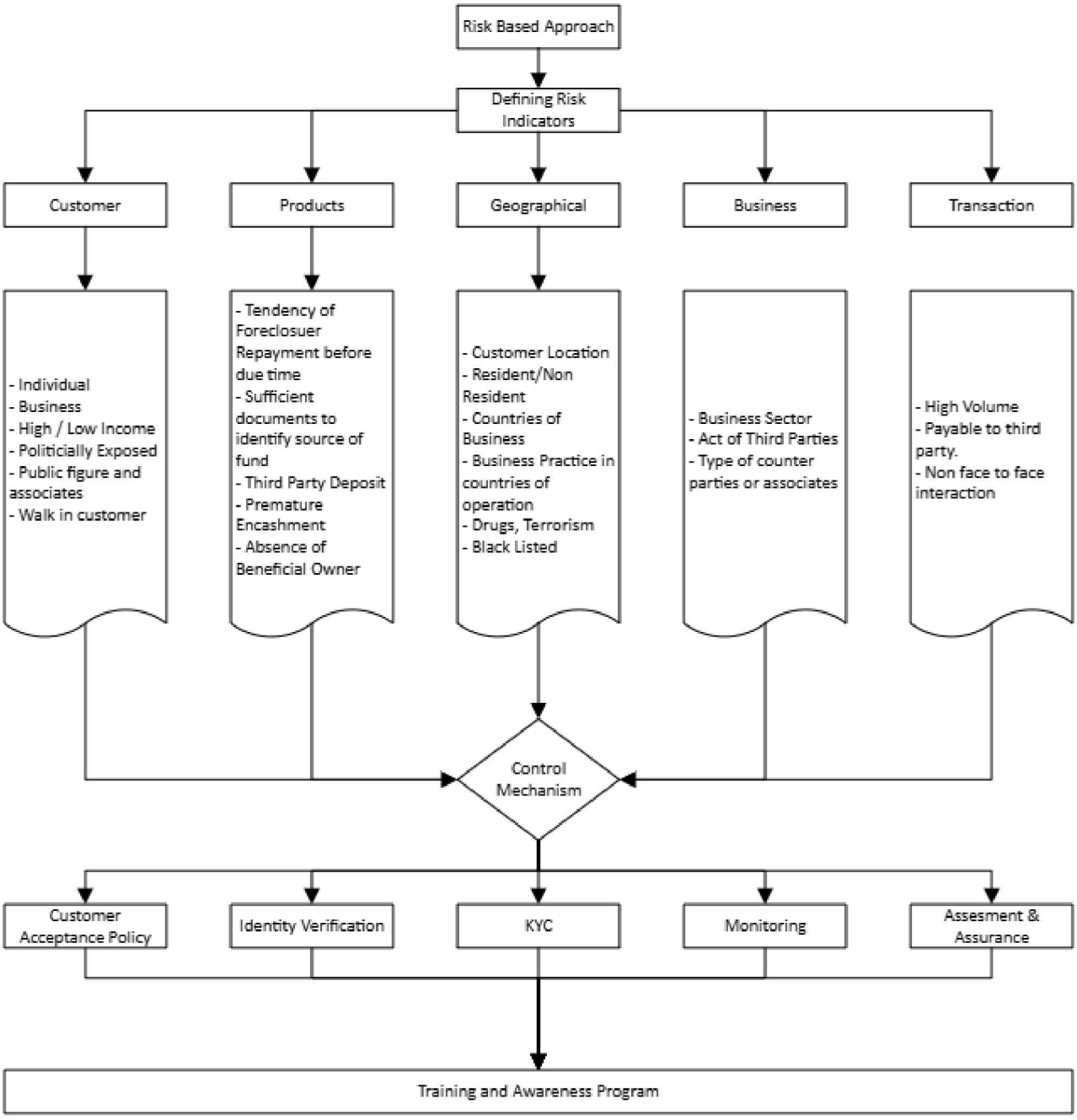


Fig: Risk Based Approach

2.2.1 Customer Identification:

It is mandatory to collect and verify the correct and complete identification of customers to prevent money laundering and terrorist financing and to keep IPDC free from any such risk.

To protect IPDC from risks of money laundering or/and terrorist financing by customers willful or unwilling activities, Customer Due Diligence should strictly be followed at different stages such as:

- while establishing relationship with the customer.

- while conducting financial transaction with the existing customer.

IPDC must ensure the following things to mitigate customer identity related risks:

- To be sure about the customer's identity and purpose of establishing relationship with us, IPDC will collect adequate information up to its satisfaction
- If a person operates an account on behalf of the customer, IPDC must satisfy itself that the person has due authorization to operate. Correct and complete information of the person, operating the account, is to be collected.

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

- While establishing and maintaining business relationship and conducting financial transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering (such as the countries and territories listed as high risk country in FATFs public statements) enhanced due diligence shall have to be ensured.

- Complete and correct information of identity of the persons besides the customer, shall have to be collected and preserved if a customer operates an account on behalf of another person in his/her own name.

- The controller or the owner of the customer shall have to be identified.

- While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised. Following instructions shall have to be followed to ensure Enhanced Due Diligence (EDD). Detailed procedure of EDD is annexed in **Appendix** 2.

2.2.2 Product vulnerabilities:

IPDC must identify and mitigate product-based vulnerabilities in the following ways:

- IPDC must be cautious regarding repayment before due time.

- We must collect the sufficient document to identify the source of fund.

- Have to be cautious in terms of third party deposit.

- Premature encashment of deposit products.

2.2.3 Geographical vulnerabilities:

IPDC must identify and mitigate geographical vulnerabilities in the following ways:

- IPDC must be cautious about customer location and the customer's residential status.
- Understand the business practice in countries of operation.
- Careful about those countries those are famous in drugs and terrorist activities.
- Careful about border area's business activities.

2.2.4 Business vulnerabilities:

IPDC must identify and mitigate business vulnerabilities in the following ways:

- Which sector the customer operates its business.
- Complete and correct information from reliable sources to identity the beneficial owners shall have to be collected and preserved. To this subsection, a person will be treated as a beneficial owner if:

a) he has controlling share of a company or/and

b) hold 20% or more shares of a company.

- Type of counter parties or associates.

2.2.5 Transaction vulnerabilities:

We must identify and mitigate transaction vulnerabilities in the following ways:

- We must be cautious on high volume transaction.
- No non face to face interaction is acceptable.
- Need extra cautious where customer request to pay to a third party.
- Careful about border area's business activities.

Chapter Three: Compliance Program

The compliance program should be documented, approved by the Board of Directors, and communicated to all levels of the organization. As part of its AML/CFT policy, CCU communicate clearly to all employees on annual basis through a statement from the Chief Executive Officer that clearly sets IPDC's policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities.

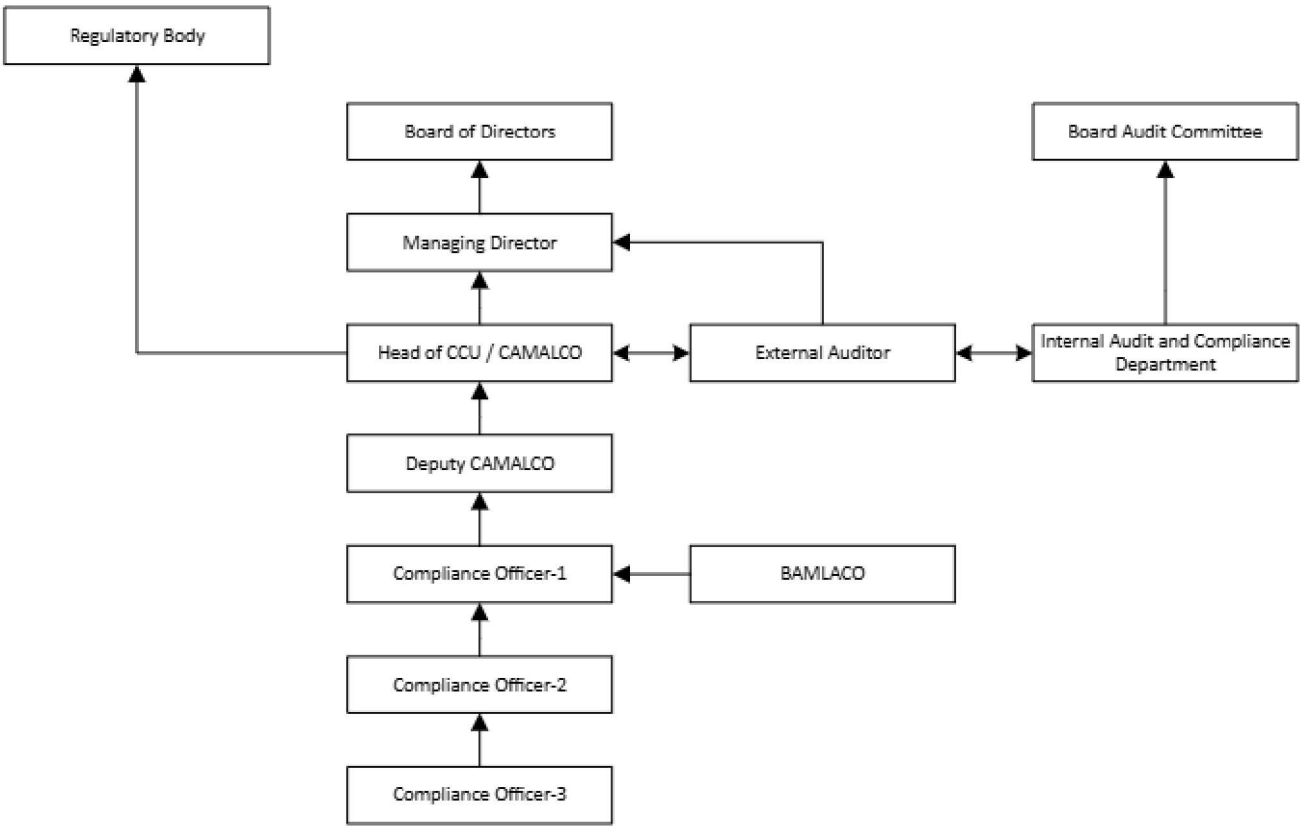
3.1 Central Compliance Unit

Central Compliance Unit (CCU) of IPDC will ensure the compliance of the MLP (Amendment) Act 2015 and Anti Terrorist (Amendment) Act, 2013 and Bangladesh Financial Intelligence Unit (BFIU) regulations. IPDC had already established Central Compliance Unit (CCU) in 2012.

3.1.1 Formation of CCU:

The CCU will be headed by a senior level employee whose position cannot be lower than the third rank in seniority in organizational hierarchy and a minimum of seven years of working experience, with a minimum of three years at a management level/ administrative level. The Head of CCU will also be considered as the CAMLCO of the Company. S/he will be assisted by Deputy CAMLCO with minimum five years of Banking experience & three other designated officers among which two will be from the general banking and information system department and none from the Internal Audit department. The organogram of CCU is shown below.

Fig: Formation of Central Compliance Unit



The designated CAMLCO/Head CCU should be a central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to financial institution's AML/CFT program.

CCU will issue the instructions to be followed by the branches; these instructions will be prepared based on combination of issues in monitoring of transactions, internal control, policies, and procedures from the point of view of preventing money laundering & terrorist financing.

3.1.2 Departmental Duties/Responsibilities

The chain of duties and responsibilities at branches are as under:

Personnel	Duties/Responsibilities
Officer in charge of Accounts or vested with the authority to open new accounts	- To interview the potential customer - To verify the introductory reference/customer profile. - To arrive at threshold limit for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions. - To ensure non opening of accounts in the name of terrorist/banned organizations. - To adhere with the provisions of *Money Laundering Prevention (Amendment) Act 2015 and Anti Terrorism (Amendment) Act 2013*.

	- To comply with the guidelines issued by Bangladesh Financial Intelligence Unit (BFIU) and by the company from time to time in respect of opening and conduct of account.
Head of Risk	- To assess the money laundering and terrorist financing risk involve in the operating activities of the company evaluate the adequacy and effectiveness of the control set for safeguarding the company against such risks.
Head of Operations	- To scrutinize and ensure that the information furnished in the account opening form/customer profile/ threshold limit are in strict compliance with KYC guidelines before authorizing opening of account. - To certify regarding compliance with KYC guidelines and report suspicious transactions to CAMLCO/Chief Executive.
Internal Auditor	- To verify and record his comments on the effectiveness of measures taken by the concerned officials and the level of implementation of KYC guidelines.
CAMLCO	- Implements and enforces Institution's anti-money laundering policies - Reports suspicious clients to Bangladesh Bank on Institution's behalf - Informs Controller of Branches of required actions (if any)
Top Management	- Prompt reporting of information regarding suspicious transactions to concerned law enforcing authority in consultation with Solicitors.

3.1.3 Responsibilities of CCU

a) Update CAMLCO and DCAMLCO information in 'BFIU Compliance Officer Portal' and written way as per attachment number X each year in the first half of January or whenever a change is made in the positions.

b) preparing an overall assessment report after evaluating the self-assessment reports received from the branches and submitting it with comments and recommendations to the chief executive of IPDC.

c) Preparing an assessment report based on the submitted checklist of inspected branches by the Internal Audit Department on that quarter.

d) Submitting a half-yearly report to BFIU within 60 days after end of a quarter. Prepare a report on steps taken on AML & CFT with progress and recommendation for MD & CEO. This will also include any steps taken by BFIU regarding AML & CFT. This report will be presented to the board/highest management level meeting and a copy of the same will be submitted to BFIU within two months form the end of Half year.

e) CCU will establish internal compliance and control by nominating BAMLCO at each branch. The nominated person's roles and responsibilities will be notified officially. His roles and responsibilities are:

- Manage the transaction monitoring process.
- Report any suspicious activity to Branch Manager, and if necessary to the CAMLCO.
- Provide training to Branch Employee.
- Communicate to all Employee in case of any changes in national or its own policy.
- Submit branch returns to CAMLCO timely.
- Monitor the KYC process.
- Arrange meeting on AML/CFT in monthly basis.
- Check the UN sanctioned list before opening any Account.

f) CCU will circulate instructions for branches to follow which will incorporate customer due diligence to prevent money laundering and terrorist financing, transaction monitoring, internal control and any policy and process relevant to it.

g) CCU will arrange a minimum of 4 meetings each year where it will review organizations' overall AML and CFT conditions, take necessary decisions and provide decisions to follow.

3.1.3.1 Responsibilities of CAMLCO:

The Chief AML/CFT Compliance Officer may choose to delegate duties or rely on suitably qualified Employee for their practical performance whilst remaining responsible and accountable for the operation of the designated functions. The major responsibilities of a CAMLCO are as follows:

1) To implement and enforce corporate-wide AML/CFT policies, procedures, and measures. The CAMLCO will directly report to the Managing Director for his responsibility. The CAMLCO shall also be responsible to coordinate and monitor day to day compliance with applicable AML/CFT related laws, rules, and regulations as well as with its internal policies, practices, procedures, and controls.

2) To monitor, review and coordinate application and enforcement of the IPDC compliance policies including AML/CFT Compliance Policy. This will include - an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity, and a written AML/CFT training plan.

3) To monitor changes of laws/regulations and directives of Bangladesh Financial Intelligence Unit (BFIU) and revise IPDCs internal policies accordingly.

4) To respond to compliance questions and concerns of the Employee and advise branches assist in providing solutions to potential issues involving compliance and risk.

5) To ensure that the IPDCs AML/CFT policy is complete and up to date, to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered.

6) To develop the compliance knowledge of all Employee, especially the compliance personnel and conduct training courses.

7) To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, branch/unit heads and compliance resources to assist in early identification of compliance issues.

8) To assist in review of control procedures to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses.

To monitor the business through self-testing for AML/CFT compliance and take any required corrective action.

9) To manage the STR/SAR process:
    - reviewing transactions referred by branch compliance officers as suspicious.
    - reviewing the transaction monitoring reports.
    - ensuring that internal Suspicious Activity Reports (SARs):
        a) are prepared when appropriate.
        b) To reflect the uniform standard for ―suspicious activity involving possible money laundering or terrorist financing‖ established in IPDCs policy.
        c) are accompanied by documentation of the branch's decision to retain or terminate the account as required under IPDCs policy.
        d) are advised to other branches who are known to have a relationship with the customer.
        e) are reported to the Chief Executive Officer when the suspicious activity is judged to represent significant risk to IPDCs including reputation risk.

- ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager.
- maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner.
- managing the process for reporting suspicious activity to BFIU after appropriate internal consultation.

3.1.3.2 Responsibilities of Deputy CAMLCO:

The major responsibilities of a Deputy CAMLCO are as follows:

- Assisting CAMLCO in implementing and enforcing Institution's anti-money laundering policies.
- Monitor reports regarding suspicious clients to Bangladesh Bank on Institution's behalf.
- Controlling flow of information to BAMLCO for required actions (if any)
  - To implement and enforce corporate-wide AML/CFT policies, procedures and measures. DCAMLCO will directly report to the CAMLCO for his responsibility. DCAMLCO shall also be responsible for coordinating and monitoring day to day compliance with applicable AML/CFT related laws, rules and regulations as well as with its internal policies, practices, procedures and controls.
  - To monitor, review and coordinate application and enforcement of the IPDC compliance policies including AML/CFT Compliance Policy. This will include - an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity, and a written AML/CFT training plan.
  - To monitor changes of laws/regulations and directives of Bangladesh Bank and revise IPDCs internal policies accordingly.
  - To respond to compliance questions and concerns of the Employee and advise branches assist in providing solutions to potential issues involving compliance and risk.
  - To ensure that the IPDCs AML/CFT policy is complete and up to date, to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered;
  - To develop the compliance knowledge of all Employee, especially the compliance personnel and conduct training courses.
  - To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, branch/unit heads and compliance resources to assist in early identification of compliance issues.
  - To assist in review of control procedures to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses.
  - To monitor the business through self-testing for AML/CFT compliance and take any required corrective action.
  - To manage the STR/SAR process:
    - reviewing transactions referred by branch compliance officers as suspicious.
    - reviewing the transaction monitoring reports.
    - ensuring that internal Suspicious Activity Reports (SARs):
      - are prepared when appropriate.
      - To reflect the uniform standard for ―suspicious activity involving possible money laundering or terrorist financing established in IPDCs policy.
      - are accompanied by documentation of the branch's decision to retain or terminate the account as required under IPDCs policy.

- are advised to other branches who are known to have a relationship with the customer.
- are reported to the Chief Executive Officer when the suspicious activity is judged to represent significant risk to IPDCs including reputation risk.

- ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager.
- maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner.
- managing the process for reporting suspicious activity to BFIU after appropriate internal consultation.

3.2 Responsibility Of Branch Anti-Money Laundering Compliance Officer

There has to be a Branch Anti Money Laundering Compliance Officer (BAMLCO) at each branch. Either Branch Manager or Branch Operations Manager or any person having three years' experience and sufficient knowledge on general banking and AML & CFT program, laws, rules, instructions from BFIU and policy of the organization shall be the BAMLCO. The responsibilities of a BAMLCO are as follows:

- Manage the transaction monitoring process
- Report any suspicious activity to CCU
- Provide training to Branch Employee
- Communicate to all Employee in case of any changes in national or its own policy
- Submit branch returns to CAMLCO timely.
- Arrange quarterly meetings with other members of the branch regarding AML and CFT and discuss existing laws, regulations and instructions from BFIU to review and take steps regarding
  - Customer knowledge
  - Transaction review
  - Suspicious transaction identification and reporting
  - Local and UN sanction resolution following
  - Salf assessment activity
  - Record storadge
  - Training
- Manage the transaction monitoring process.
- Report any suspicious activity to the Branch Manager, and if necessary to CAMLCO.
- Provide training to Branch Employee.
- Communicate to all Employee in case of any changes in national or its own policy.
- Submit branch returns to CAMLCO timely.
- Monitor the KYC process.
- Arrange meeting on AML/CFT in monthly basis.
- Check the UN sanctioned list before opening any Account.
-

3.3 Employee Training And Awareness Program

To ensure the proper compliance of anti-money laundering and combating terrorist financing activities a robust training program must be in place. Employees in different business functions need to understand policy, procedures, and controls affect them in their day-to-day activities. IPDC shall arrange yearly (for General Training) or half yearly (for Job Specific and New Joiner's) training program to ensure proper compliance of money laundering and terrorist financing prevention activities. Following training procedures to be followed by the Company for prevention of Money Laundering and Terrorist Financing activities:

3.3.1 Employee Awareness

Employee must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All employees must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities.

3.3.2 Education and Training Programs

All relevant Employees should be educated in the process of the ―Know Your Customer requirements for money laundering and terrorist financing prevention purposes. The training in this respect should cover not only the need to know the identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant Employee should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity. Generally, all trainings could be divided in to two types:

a. General training
b. Job Specific Training

(a) General Training

A general training program must be organized on a yearly basis, which include the following:

- General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies.
- Legal framework, how AML/CFT related laws apply to IPDC.
- Policies and systems regarding customer identification and verification, due diligence, monitoring.
- How to react when faced with a suspicious client or transaction.
- How to respond to customers who want to circumvent reporting requirements.
- Stressing the importance of not tipping off clients.
- Suspicious transaction reporting requirements and processes.
- Duties and accountabilities of employees.

(b) Job Specific Training

- **New Employee Training**

For a new employee the compliance policy statement must be sign-off at the beginning of the joining and he/she must have a on the job training from the departmental head regarding the importance of money laundering and terrorist financing activities. The respective new employee must go through the yearly training on AML/CTF.

- **Customer Service/Relationship Managers**

Retail and investment departments employee who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to the organization's strategy in the fight against money laundering and terrorist financing. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

- **Operation Department**

Operation department employees who received completed Account Opening, FDR, DPS related application forms and cheques for deposit into customer's account or other investments must receive training in the processing and verification procedures. In addition, the need to verify the identity of the customer must be understood, and training should be given in the organization's account opening and customer/client verification procedures. Employees should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML/CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted, or the transactions proceeded with and must know what procedures to follow in these circumstances.

- **Credit Officers**

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

- **Audit and compliance officer**

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

- **Senior Management Commitment and role of the Board of Directors**

The most important element of a successful AML/CTF program is the commitment of senior management, including the chief executive officer/managing director and the board of directors. Money laundering and terrorist financing issues must be communicated to the board. An anti-money laundering compliance report should be submitted in each board meeting. The message from top management and the board of directors will be "Zero Tolerance" in case of money laundering and terrorist financing

- **AML/CFT Compliance Officer**

The AML/CFT Compliance Officer should receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, Bangladesh Financial Intelligence Unit (BFIU) directives and internal policies. In addition, the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

3.3.3 Training and Awareness Procedures for Trainers

The trainers to be followed the below steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.

- Identify the audience by functional area as well as level of employee/management. New hires should receive training different from that given to veteran employees.

- Determine the needs that are being addressed, e.g., issues uncovered by audits or examinations, created by changes to systems, products or regulations.

- Determine who can best develop and present the training program.

- Create a course abstract or curriculum that addresses course goals, objectives, and desired results.

- Establish a training calendar that identifies the topics and frequency of each course.

- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.

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

3.4 Suspicious Transaction Reporting (STR)

According to the provision of section 25 (1) (d) of MLP (Amendment) Act, 2015, the IPDC should report to BB proactively and immediately, facts on suspicious, unusual, or doubtful transactions likely to be related to money laundering. Because BB has the power to call STR from FIs related to financing of terrorism according to section 15(a) of Anti-terrorism (Amendment) Act, 2013.

3.5 Self Assessment Procedure

Self-Assessment is a procedure performed by the AML compliance officer to assess how effectively AML/CFT program is going on around the company. Such procedure must be carried on a half yearly basis. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms.

The self-assessment should conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions, and recommendations. The self-

assessment should advise management whether the internal procedures and statutory obligations of IPDC have been properly discharged.

Self-assessment will be done on the following areas:

- The percentage of officers/employees that received official training on AML/CFT.
- The awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and Bangladesh Financial Intelligence Unit (BFIU)'s instructions and guidelines.
- The arrangement of AML/CFT related meeting on regular interval.
- The effectiveness of the customer identification during opening an individual, corporate, and other account.
- The risk categorization of customers by the branch.
- Regular update of customer profile upon reassessment.
- Identification of Suspicious Transaction Reports (STRs).
- The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees.
- The measures taken by the branch during opening of account of PEPs.
- Consideration of UN Sanction List while conducting any business.
- The compliance with AML/CFT weaknesses/irregularities, as the bank's Head Office and Bangladesh Financial Intelligence Unit (BFIU)'s inspection report mentioned.

A standard checklist for self-assessment as advised by Bangladesh Financial Intelligence Unit (BFIU) (Central Bank of Bangladesh) has been attached in Annexure 3. The self-assessment will be done by each branch on half early basis. The report will be finalized after meeting with branch manager where the draft will be discussed for the problems identified. If the identified problems cannot be resolved, then the necessary actions must be determined and added to the finalized report. Progress made on the items will be discussed in the quarterly meetings in the branch. The report must be sent to internal audit within 15th of the next month to Head office audit and compliance unit with all issue, description, recommendation and actions taken.

Internal audit unit will assess the reports sent from branches. It will visit and notify CCU if any branch has a report section that is deemed risky.

3.6 Independent Testing Procedure

Internal audit team shall perform their own and regular yearly inspection when they will perform the independent testing procedure as per annexure: Independent Testing. Based on the checklist, it will assess the branch's AML and CFT activity to prepare a report on the branch with a rating defined for the branch. In addition to regular yearly inspection, internal audit will visit 10% of the branches to perform independent testing procedure as per checklist in annexure to assess AML and CFT activity and submit a report with branch score.

Internal audit will submit all branch reports with ratings to central compliance unit.
The Internal Audit and Compliance team of IPDC shall perform at least annually an independent testing on the adequacy of AML controls across the organization. Results of independent testing procedure should be communicated to the Board Audit Committee. The Board may appoint external auditors to perform independent testing procedures each year to review the adequacy of controls if require or statutory auditors may review the internal control and reporting process of AML/CFT of the Company within the scope of their appointment. Both Internal Audit and External Audit should focus their audit program on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient.

Such independent testing will cover the following areas:

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

The tests include:

- Interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the IPDC‟s anti-money laundering procedures.
- sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms.
- test of the validity and reasonableness of any exemption granted by IPDC management; and
- test of the record keeping system according to the provisions of the laws. Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken.

A standard checklist for independent testing procedure as advised by Bangladesh Financial Intelligence Unit (BFIU) (Central Bank of Bangladesh) has been attached in Annexure 4.

3.7 Self-Assessment Report and Independent Testing report

11. The Central compliance unit will assess self-assessment report submitted from each branch and independent testing report submitted by internal audit team, based on this reports, CCU will prepare a checklist based report for the branches visited in the half year. Among others, this report will cover:
    a. Total number of branches and number of self-assessment report submitted by branches.
    b. Number of branches visited/assessed by internal audit in the assessment period and and their status (with branch wise score)
    c. In the submitted self-assessment report, if multiple branch as same type of non comliance, steps are taken to prevent the noncompliance with specific mention of the noncompliance.
    d. Special and general noncompliance in the independent testing report submitted by internal audit and actions taken to prevent these noncompliance by central compliance unit.
    e. Rating development and compliance assurance plan for branches rated as "unsatisfactory" and "marginal" in the reports.

    This repor will be included in CCU report mentioned in section 3.1 (half yearly report submitted by CCU).
12. In the banch self-assessment report, if any branch is deemed risky, then the branch must be visited by internal audit immediately with special attention brought by CCU to relevant authority.

3.8 Independent Audit Function

Independent audit function is very important to ensure the effectiveness of AML/CFT program. Auditors should act independently and report directly to the Board of Directors if there is any breach of policy and procedure. Auditors' responsibilities regarding compliances are as follows:

A standard checklist for Independent Testing as advised by Bangladesh Financial Intelligence Unit (BFIU) (Central Bank of Bangladesh) has been attached in Annexure 4.

3.8.1 Internal audit

The responsibilities of internal auditors are:

- Address the adequacy of AML/CFT risk assessment.
- Examine/attest the overall integrity and effectiveness of the management systems and the control environment.
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures, and processes, and whether they comply with internal requirements.

- Perform appropriate transaction testing with particular emphasis on high-risk operations (products, service, customers, and geographic locations).
- Assess the adequacy of the IPDC processes for identifying and reporting suspicious activity.
- Communicate the findings to the board and/or senior management in a timely manner.
- Track previously identified deficiencies and ensures that management corrects them.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Employee accountability for ensuring AML/CFT compliance.

- Comprehensiveness of training, in view of specific risks of individual business lines.

- Participation of personnel from all applicable areas of the Company.

- Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.

- Penalties for noncompliance and regulatory requirements.

3.8.2 External Auditor

IPDC may, if requires, facilitate the external auditors in reviewing whether the AML policies have been complied or not by the management.

Chapter Four: Customer Due Diligence (CDD)

The adoption of effective Know Your Customer (KYC) program is an essential part of risk management policies. Having sufficiently verified/corrected information about customers —Knowing Your Customer (KYC) - and making use of that information underpins all AML/CFT efforts and is the most effective defense against being used to launder the proceeds of crime.

Know Your Customer (KYC) is part of Customer Due Diligence (CDD) We need to perform CDD before on board of a customer. Additionally, we need to review customer profiles every five years for Low Risk customer and one year for High Risk customer.

4.1 Parts of CDD

1. CDD will be based on customer risk on different times:
    a. During relationship establishment with customer
    b. When there are more transactions then determined.
    c. When any transactions is deemed money laundering or terrorist financing
    d. When it is deemed that previously collected document is not enough for a certain customer
    e. If performing CDD might cause tipping of information, then STR will be submitted but to CDD will be done to not to arise suspicion.
2. IPDC can and shall perform CDD till it is satisfied of the customers actual intention of establishment of business relationship.
3. For each account, actual beneficial owner has to be detected. In this case, customer data should be collected in the following manner:
    a. If any customer operates an account on behalf of another person, then full information has to be collected and stored for both customer and persons.
    b. If any customer is influenced by any other person, then the person's information will also be collected.
    c. In the case of organizational customer, beneficiary information has to be collected. If anyone has controlling ownership, then he will be considered a beneficiary owner.
    d. If no controlling ownership is established for b and c, information of chief executive officer will be collected.
    e. To determine actual beneficiary and action steps, government guidelines on beneficial owner will be followed.

Other guideline Regarding CDD

1. IPDC will perform and store CDD information appropriately.
2. IPDC will perform customer KYC. KYC format might be different for different product, but all KYC form should contain KYC attached in Annexture no X. The KYC form must not be a part of customer account opening form and will not be filled up by the customer.
3. IPDC will maintain unique customer ID for each customer to avoid duplication of customer information and ease of customer and transaction monitoring.

Steps if CDD can not be performed

If due to customers non cooperation or information obtained regarding customer is not reliable or customer information is unavailable, IPDC shall take following actions:

1. IPDC shall not open customer account/establish business relationship/maintain no transaction and if necessary, will cancel existing business relationship.
2. In case of account closure, higher management approval must be taken, and customer will be notified of the same with reason explained.
3. The record regarding non cooperating of account or account closure will be shared with CCU. If necessary CCU will circulate the information to other branches for necessary actions.
4. In necessary cases STR will be submitted regarding such customer/probable customer/rejected customer or entity.

4.2 Know Your Customer (KYC) Procedure

4.1.1 Know Your Customer (KYC):

Where IPDC is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, and to identify the beneficial owner, and to take reasonable measures to verify the identity of the beneficial owner and unable to obtaining information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

The following points should be taken care of in this regard

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

- **Identifying Real Person**
  The prospective customer should be interviewed personally. This will safeguard against opening of fictitious account. Face to face communication is must.

- **Document is not enough**
  The best identification documents possible should be obtained from the prospective customer i.e., those that are the most difficult to obtain illicitly.

- **Reliance on Third party**
  For the use of third-party the following criteria should be meet:

  (a) IPDC relying upon a third party should immediately obtain the necessary information.

(b) (b) IPDC should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) We should satisfy ourselves that the third party is regulated, supervised, or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements.

4.1.2 Electronic Know Your Customer (e-KYC):

Bangladesh Financial Intelligence Unit (BFIU) has recently introduced a new concept of e KYC vide circular BFIU circular-25; dated: January 8, 2020. In this circular, Bangladesh Financial Intelligence Unit directs Financial Institutions to on-board simplified customer using digital platform. In this process, customer will be onboarded and verified digitally.

In line with BFIU, IPDC has started onboard customer with help of video call for non-face to face customer and further planned to adopt more features of e-kyc when required under the Guidelines on Electronic Know Your Customer (e-KYC)

4.3 Components Of Kyc Program

KYC should be the core feature of IPDC‟s risk management and control procedure and be complemented by regular compliance reviews and audit.

Essential elements should start from the risk management and control procedures and should include-

a. Customer acceptance policy
b. Customer identification
c. Ongoing monitoring of high-risk accounts, and
d. Identification of suspicious transactions

4.2.1 Customer acceptance policy

The following points should be taken care off while accepting the customers:

1) No account should be opened in anonymous or fictitious name.

2) Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grades.

3) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.

4) Not to open an account or close an account where the IPDC is unable to apply appropriate customer due diligence measures i.e., IPDC 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 us.

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

6) Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

7) The status of a customer may change as relation with a customer progress. The transaction pattern, volume of a customer's account may also change. in such case monitoring of customer's activities throughout the business relation must be done in a very professional way.

4.2.2 Monitoring of high-risk accounts, and identification of suspicious transactions.

High value single transaction conducted in a single Demand Draft, Pay Order, Transfer by any person or institution or any person/institution involved in a financial transaction that may pose reputational and other risks to IPDC. In this case if a transaction appears abnormal in relation to the usual transaction of the concerned person or institution that transaction will be treated as ―high value and suspicious.

4.2.3 Customer Identification

According to the AML Circular No. 24 dated 03/03/2010, for the purpose of KYC Procedure a "Customer" is means:

- any person or institution maintaining an account of any type with an IPDC.

- the person or institution as true beneficial owner in whose favor the account is operated.

- the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc.) under the existing legal infrastructure.

4.2.3.1 What Constitutes a Customer's Identity?

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

- The physical identity (e.g. Birth Certificate, TIN/VAT Registration, Passport/National ID, Driving License etc.); and

- The activity undertaken.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary. It needs to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector.

4.2.3.2 KYC for Individual Customers

IPDC shall obtain following information while opening accounts or establishing other relationships with individual customers:

- Correct name and/or names used.
- parent's names.
- date of birth.
- current and permanent address.
- details of occupation/employment and sources of wealth or income
- Contact information, such as – mobile/telephone number.

Relationship Officer of IPDC should always bear in mind the following points:

1) IPDC will not allow non-face to face contact to any business relationship.
2) Care should be taken in accepting documents which are easily forged, or which can be easily obtained using false identities.
3) In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders should be verified.
4) Any subsequent change to the customer's name, address, or employment details of which the IPDC becomes aware should be recorded as part of the Know Your Customer process.
5) All documents collected for establishing relationship must be filed in with supporting evidence. Where this is not possible, the relevant details should be recorded on the applicant's file.
6) Details of the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not require or request staff to breach account opening procedures as a favor to an applicant.
7) In the case of socially or financially disadvantaged people such as the elderly, the disabled, students and minors, the identity of these persons can be verified from an original or certified copy of alternative document, preferably one with a photograph. Certificate or confirmation from lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant is acceptable to IPDC in this regard. The Certifier must sign the copy document and clearly indicate his position or capacity on it with a contact address and phone number. However, IPDC shall not allow „high value" transactions to this kind of customers.
8) The normal identification procedures set out above should be followed. Moreover, in case of minor parent's/ legal guardians KYC procedure must be followed.

9) Identification documents which do not bear photographs or signatures are not acceptable. More importantly checking of authenticity of the identity documents is must.
10) To verify the customer permanent and present address Passport/ NID and recent utility bill's copy can be checked.
11) The original, certified copy of (i) Current valid passport; (ii) Valid driving license; (iii) National ID Card; (iv) Employer provided ID Card, bearing the photograph and signature of the applicant should be used to identify the customer:

4.4 Business segment wise KYC requirements

4.4.1 KYC for Corporate Bodies and Other Entities

The principal requirement for the corporate bodies is to verify its legal existence and to look who is behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a ―brass plate company where the controlling principals cannot be identified.

The following documents should be obtained from companies:

- Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business.

- Certified copy of the Memorandum and Articles of Association, or by-laws of the client.

- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts.

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

- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full-time employees, officers or directors of the company.

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

- Copies of the form X and form XII.

Where the business relationship is being opened in a different name from that of the applicant, the institution should also satisfy itself that the reason for using the second name makes sense.

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

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

A letter issued by a corporate customer (listed in any exchanges) is acceptable in lieu of passport or other photo identification documents of their shareholders, directors, and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again. When authorized signatories change, identities of all current signatories should be taken and must verify.

4.4.2 KYC for Companies Registered Abroad

Care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their destination. In such circumstances, institutions should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

4.4.3 KYC for Partnerships and Unlisted Businesses

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

4.4.4 Powers of Attorney/ Mandates to Operate Accounts

Establish the identities of holders of powers of attorney, the grantor of the power of attorney. Records of all transactions undertaken in accordance with a power of attorney should be kept.

4.4.5 Transaction Monitoring Process

The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for Financial Institutions to be vigilant for any significant changes or inconsistencies in the pattern of transactions.

Possible areas to monitor could be: - -
transaction type
- frequency
- unusually large amounts
- geographical origin/destination
- changes in account signatories

Loan/ Credit transactions:

- Customer uses cash collateral to obtain loan/facility.
- End use of loan proceeds not consistent with purpose.
- Borrower settling "problem" loans by large amounts of cash suddenly with no reasonable explanation of funds/source.
- Purpose of loan does not make economic sense, or provision of cash collateral.
- Using cash deposit for collateralizing a loan.
- Loan proceeds unexpectedly channeled offshore.

4.4.6 Duties if Customer Due Diligence (CDD) cannot be performed

If completion of CDD cannot be performed due to uncooperative nature of the client and/or if the information provided is found to be incredible after assessment, FI may take into the following actions:

1. Bank/FI may not open account of such client or may close the account if appropriate.
2. Before closure of such accounts, approval from top management is necessary and the account holder must be informed via notice detailing the reason behind such closure of account.

Suspicious Transaction (STR) may be reported on case-to-case basis in this regard.

A standard KYC Template Attached in **Appendix # 3 & 4.**

4.4 Steps for combating with terrorist financing by IPDC:

To prevent the possibility of borrowing customers to undertake such activities as money laundering and channelizing of loan funds for terrorist financing, it is important to undergo detailed profiling of the borrowing customer to identify the owners, understand their business and thereby form a fact-based opinion on them.

The following steps will form the core component for the selection of the borrower who in IPDC"s opinion may be considered as safe for conducting business:

1. Performing extensive Know Your Customer (KYC) exercise on the prospective client. The legal status of the legal person / entity will be verified through proper and relevant documents. This will include Trade License / Partnership Deeds / Memorandum and Articles of Association according to the constitution of the firm, along with copies of the list / register of directors. Satisfactory evidence of the identity of each of the principal beneficial owners being all directors of limited companies along with any owner holding 20% interest or more or with principal control over the company's assets will be obtained.

2. Appraisal of the credit proposal will involve extensive person to person contact between IPDC officials and customer's representatives, physical visits to the business premises, enquiries within the trade circles and with related trade parties in the peer group etc. A detailed understanding of the business activity proposed to be financed will be made from the above

exercise. If any negative opinion is formed through this exercise or resistance is faced in collecting adequate information or access to business premises, the relationship will not proceed any further.

At the disbursement stage, the control will be made by ensuring that all disbursements are made by account payee cheques to confirm that the intended beneficiary of the financing is indeed the recipient of the fund. All loans are disbursed for specific terms either as lease financing, short term facilities or term loans. In case of lease financing, the beneficiary of the disbursement cheque will be the vendor of the goods to be procured. In the other cases, payment will have to be made to the customer.

As a deterrent to diversification of funds, the following undertaking will be included in the Letter of Agreement which is executed between the IPDC and the borrower at the time of availing the credit facilities:

"The borrower shall apply the proceeds of the loan exclusively for the purpose of the Project as set out in (Section number of the Agreement). Furthermore, the borrower undertakes not to apply the proceeds of the loan, either directly or indirectly, for carrying out any activities, including terrorist activities, which are prejudicial to the well-being of the state, in any form whatsoever."

4.5 Know Your Employee (KYE)

Know Your Employee (KYE) program means the process to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job description, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, dual control, and other deterrents should be firmly in place.

HR department is to ensure the compliance of proper KYE procedure, background screening of prospective and current employees including criminal history. Only obtaining the related documents is not enough to ensure this compliance, authenticity of the documents must be ensured at the time of appointment of the employee(s).

A Standard KYE Template is Attached in A**ppendix - 07**

Chapter Five: Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR)

5.1 Definition of STR/SAR

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

Suspicious transaction means such transactions which deviates from usual transactions; of which there is ground to suspect that,

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

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

(3) which is, for the purposes of ALM/CFT Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit (BFIU) from time to time.

5.2 Identification and Evaluation of STR/SAR:

The identification and evaluation process of STR/SAR includes the following:

5.2.1. Identification STR/SAR

Generally, the detection of unusual transactions/activities may something is sourced as follows:

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

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

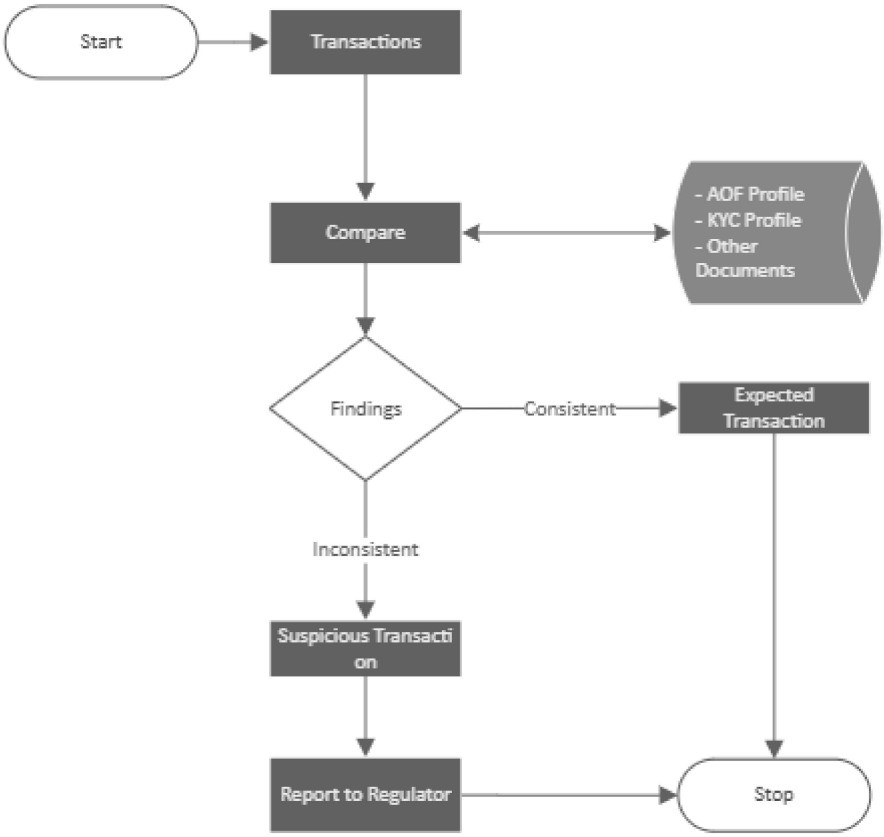


Fig: STR identification Process

5.2.2. Evaluation and Disclosure

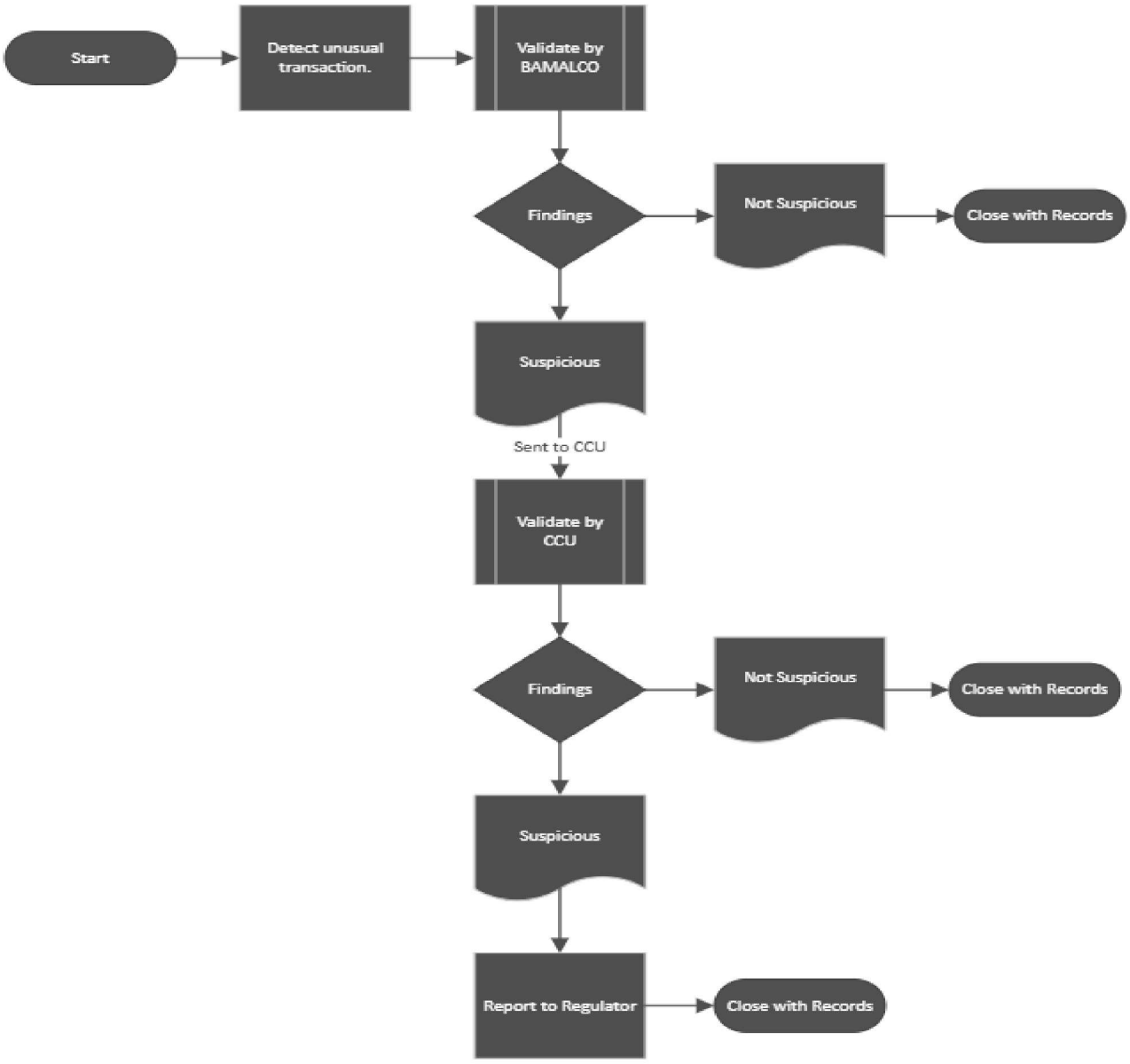
These problems must be in place at branch level and Central Compliance Unit (CCU). After identification of STR/SAR, at branch level BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage concerned BAMLCO must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

At the final stage we should submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU) if it is still suspicious.

5.3 REPORTING OF STR/SAR

As per the MLP (Amendment) Act, 2015 and Anti Terrorist (Amendment) Act, 2013 ; IPDC is obligated to submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU). Such report must come to the Bangladesh Financial Intelligence Unit (BFIU) from CCU. As per the STR format specified by Bangladesh Financial Intelligence Unit (BFIU).

STR reporting procedure is described below:



Figs: STR Reporting Process

1. If any suspicious transaction is identified, BAMLCO will be notified immediately by the identifier officer. The BAMLCO will immedialtrly analyse the transaction and arrange the observations in his report in detail. If the described transactions are deemed suspiclious, then the report with all supporting documents will be immediately sent to CCU
2. CCU will analyses the report appropriately with its supporting documents. After his review, he will submit STR report in BFIU goAML web portal following goAML Manual.
3. If any transaction is not deemed suspicious in branch level but considered suspicious by the CCU, then it will also be reported as STR in BFIU.
4. IPDC shall store STR information till no further instruction is received from BFIU.

5.4 TIPPING OFF

Tipping off‟ means to disclose to the concern person regarding the reporting/investigation process. The offence of „tipping off‟ occurs when information or any other matter which might prejudice the investigation is disclosed to the suspect of the investigation (or anyone else) by someone who knows or suspects (or, in the case of terrorism, has reasonable cause to suspect) that: an investigation into money laundering has begun or is about to begin, or the police/investigating authority have been informed of suspicious activities, or a disclosure has been made to another employee under internal reporting procedures.

As per section 6 of MLP (Amendment) Act, 2015 and FATF Recommendation 21 prohibits IPDC, their directors, officers, and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the IPDC is seeking to perform its CDD obligation in those circumstances.

5.4.1 Penalties of Tipping Off

Under section 6 of MLP (Amendment) Act, 2015, if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

5.5 INDICATORS OF STR

Moving Customers:

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

Out of market windfalls:

If you think a customer who just appeared at your institution sounds too good to be true, you might be right. Pay attention to one whose address is far from your institution, especially if there is no special

reason why you were given the business. Aren't there institutions closer to home that could provide the service?

Suspicious Customer Behavior:

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

Suspicious Customer Identification Circumstances:

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information when opening an account.
- Customer's permanent address is outside the IPDC service area.
- Customer asks many questions about how the financial institution disseminates information about the identification of a customer.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

Suspicious Cash Transactions:

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

Suspicious Non-Cash Deposits:

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

Suspicious Activity in Credit Transactions:

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

Suspicious Commercial Account Activity:

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

Suspicious Employee Activity:

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

Other Suspicious Activity

Suspicious transaction basically means a transaction which is unusual or a transaction which we know or reason to believe that the proceeds came from illegal activities, a transaction may be suspicious in various ways, some insights of suspicious transaction but not limited may be as follows:

- Request of early encashment.
- A DPS (or whatever) calling for the periodic payments in large amounts.
- Lack of concern for significant tax or other penalties assessed when cancelling a deposit.
- Gaps in critical information.
- Attempt to conceal information.
- Unnecessarily complex structure of transaction.
- Excessive request for secrecy of information.
- Unnecessary use of intermediaries.
- Doubtful beneficiary of the fund.
- A transaction which we know or reason to believe is unusual for the type of business the customer is in-has no business or apparent lawful purpose.
- Structuring of transaction to evade record keeping or reporting requirements.
- Loan transaction or credit facilities with inherently risky collateral or geographical characteristics.
- Unusual fund transfer from border areas.

Inherently risky industries or geographical areas.

5.6 Cash Transaction report CTR

1. If any account has transaction such that, in a single day, the total cash transaction in a single day (cash deposit) is equal or more then 1 million, then BAMLCO will notify this as CTR by CCU.
2. The CTR report has to be submitted by 21th of next month using goAML web as per instractions in goAML manual.
3. If no submitable cash transaction is found for a month, then “No submitable cash transaction found” message will be notified to CCU. CCU will submit a list of such branches using the “goAML Message Board” to BFIU.
4. All branches must store its CTR information. Dureation of the staorgade will be five years from the date of BFIU submission.

Chapter Six: Record Keeping

IPDC should maintain all necessary records on transactions for a period of at least five years as specified by the Guidance Notes issued by Bangladesh Financial Intelligence Unit (BFIU) or for such periods as specified by IPDC‟s documents retention policy (whichever is higher). This will enable the Company to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) to provide, if necessary, evidence for prosecution of criminal activity.

The records prepared and maintained by IPDC on its customer relationship and transactions should be such that:

- requirements of legislation and Bangladesh Financial Intelligence Unit (BFIU) directives are fully met.
- competent third parties will be able to assess IPDC„s observance of money laundering policies and procedures.
- any transactions effected via IPDC can be reconstructed.
- any customer can be properly identified and located.
- all suspicious reports received internally and those made to Bangladesh Financial Intelligence Unit (BFIU) can be identified; and
- IPDC can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.

Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. pertaining to:
    (1) the customer.
    (2) the beneficial owner of the account or product.
    (3) the non-account holder conducting any significant one-off transaction.
    (4) any counterparty.

- details of transaction including:
    (1) nature of such transactions.
    (2) volume of transactions customer’s instruction(s) and authority(ies).
    (3) source(s) of funds.
    (4) destination(s) of funds.
    (5) book entries.
    (6) custody of documentation.
    (7) date of the transaction.
    (8) form in which funds are offered and paid out.
    (9) parties to the transaction
    (10) identity of the person who conducted the transaction on behalf of the customer

These records of identity must be kept for at least five years or for such periods as specified in IPDC‟s Documentation Retention Policy (whichever is higher) from the date when the relationship with the customer has ended. This is the date of:

(1) Closing of an account
(2) Providing of any financial services
(3) Carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
(4) Ending of the business relationship; or
(5) Commencement of proceedings to recover debts payable on insolvency.

6.1 Retrieval Of Records

The relevant records of the clients must be maintained in a systematic manner as prescribed in the record retention policy of the Company thus may retrieve easily and provide the customer's information or customer's transaction record without any delay for the requirement of regulatory body, law enforcing authority or for the purpose of internal use.

6.2 STR And Investigation

We should not destroy any STR related records of customer or transaction without the consent of the BFIU even though the fifteen-year limit may have been elapsed. A register has to be maintained for all STR records, investigations and inspection made by the investigating authority or Bangladesh Financial Intelligence Unit (BFIU) and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

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

6.3 Training Records

IPDC shall maintain training records which include: -

(i) details of the content of the training programs provided.
(ii) the names of Employee who have received the training.
(iii) the date/duration of training.
(iv) the results of any testing carried out to measure Employees understanding of the requirements; and
(v) an on-going training plans.

6.4 Branch Level Record Keeping

Branch must ensure to keep the following records at the branch level in the form of shadow hard copy.

(1) Information regarding Identification of the customer,

(2) KYC information of a customer,
(3) Transaction report,
(4) Suspicious Transaction/Activity Report generated from the branch,
(5) Exception report,
(6) Training record, and
(7) Information provided to the Head Office or competent authority.

Chapter Seven: Statement of Compliance

IPDC should obtain a Statement of Compliance with the Policy on Prevention of Money Laundering and Terrorist Financing from its all employees. Such statement of compliance should be dully signed by the respective employee and should be preserved in the employees‟ personal files.

In the Statement of compliance, every employee should solemnly declare and confirm the following:

1. A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.

2. A statement that compliance with rules and regulations is the responsibility of everyone in the financial institution in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations cannot be an excuse for non-compliance.

3. A statement that should direct staff to a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.

4. A statement that employees will be held accountable for carrying out their compliance responsibilities.

The CAMLCO officer should ensure that all new employees of the Company shall read this policy, understand the implications there of and signs the „Statement of Compliance‟. After signing off, it should be sent to HR for maintain in his/her personal file.

Chapter Eight: Confidentiality of Information

All information generated, exchanged, or provided with any personnel of the Company in the context of Anti Money Laundering/ Combating Terrorist Financing must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with provisions on privacy and data protection, where applicable.

Under MLP (Amendment) Act, 2015 and Anti Terrorist (Amendment) Act 2013, IPDC or its employees‟ shall not share account related information to investigating authority i.e., Anti-Corruption Commission (ACC) or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh

Besides, section 6 of MLP (Amendment) Act, 2015 and FATF Recommendation 21 prohibits IPDC, their directors, officers, and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the IPDC is seeking to perform its CDD obligation in those circumstances. If any person, institution, or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

Chapter Nine: Offences and Punishments

9.1 Penalties for non-compliance of Money Laundering Prevention (Amendment) Act 2015

According to section 25 (2) of MLP (Amendment) Act, 2015 , if any reporting organization violates the directions mentioned in sub-section (1) of section 25 of MLP (Amendment) Act, 2015, Bangladesh Financial Intelligence Unit (BFIU) may-

(a) impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty five) lacs on the reporting organization; and
(b) in addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities of the said organization or any of its branches or as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

In addition to the above-mentioned provisions there are some new provisions of penalties in the section 23 of MLP (Amendment) Act, 2015. These are:

(a) If any reporting organization fails to provide with the requested information timely under this section, Bangladesh Financial Intelligence Unit (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, Bangladesh Financial Intelligence Unit (BFIU) may suspend the registration or license of the organization or any of its branches for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.
(b) If any reporting organization provides with false information or statement requested under this section, Bangladesh Financial Intelligence Unit (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, Bangladesh Financial Intelligence Unit (BFIU) may suspend the registration or license of the organization or any of its branches for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.
(c) If any reporting organization fails to comply with any instruction given by Bangladesh Financial Intelligence Unit (BFIU) under this Act, Bangladesh Financial Intelligence Unit (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 non-compliance and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Financial Intelligence Unit (BFIU) may suspend the registration or license of the organization or any of its branches for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.
(d) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Financial Intelligence Unit (BFIU) under clause (c) of sub-section 23(1) of MLP (Amendment) Act, 2015, Bangladesh Financial Intelligence Unit (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.

(e) If any person or entity or reporting organization fails to pay any fine imposed by Bangladesh Financial Intelligence Unit (BFIU) under sections 23 and 25 of this Act, Bangladesh Financial Intelligence Unit (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 Bangladesh Financial Intelligence Unit (BFIU), and in this regard if any amount of the fine remains unrealized, Bangladesh Financial Intelligence Unit (BFIU) may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.

(f) If any reporting organization is imposed fine under sub-sections 23 (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit (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 Employee or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

9.2 Penalties for non-compliance of Anti-Terrorism (Amendment) Act, 2013

(a) If any reporting agency fails to comply with the directions issued by Bangladesh Financial Intelligence Unit (BFIU) under section 15 or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Financial Intelligence Unit (BFIU) not exceeding Taka 25 (ten) lacs and Bangladesh Financial Intelligence Unit (BFIU) may suspend the registration or license with intent to stop operation of the said agency or any of its branches within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency. [U/S 16(3) of Anti Terrorist (Amendment) Act, 2013]

(b) If any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Financial Intelligence Unit (BFIU) according to sub-section 16 (3) of ATA, Bangladesh Financial Intelligence Unit (BFIU) may recover the amount from the reporting agency by debiting its accounts maintained in any bank or financial institution or Bangladesh Financial Intelligence Unit (BFIU) and in case of any unrealized or unpaid amount, Bangladesh Financial Intelligence Unit (BFIU) may, if necessary, apply before the concerned court for recovery. [U/S 16(4) of Anti Terrorist (Amendment) Act, 2013]

9.3 "Safe Harbor" Provision for Reporting

Safe harbor laws encourage financial institutions to report all suspicious transactions by protecting financial institutions and employees from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. In section (28) of MLP (Amendment) Act, 2015 provides the safe harbor for reporting.

Appendix 1: Database of OFAC or Bangladesh Financial Intelligence Unit (BFIU) to be checked

Relationship Manager must be checked the following database before making any relationship with client(s) and distribute the list time to time by CAMLCO:

i. Checking the Office of Foreign Assets Control (OFAC) Lists

Before engaging in any money service activity (including but not limited to check cashing, money orders and wire transfers) which potentially may involve money laundering, and on an ongoing basis, we will check to ensure that a customer does not appear on the OFAC "Specifically Designated Nationals and Blocked Persons" List, SDN List, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website Because the OFAC Website is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may, if necessary, access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated, and we will document our review.

ii. Comparison with Bangladesh Financial Intelligence Unit (BFIU) provided lists of terrorists and other criminals IPDC may receive, from time to time, list of known or suspected terrorists form Bangladesh Financial Intelligence Unit (BFIU). Within a reasonable period after an account is opened or transaction is completed (or earlier, if required by another laws and regulation or directive issued in connection with an applicable list), we will determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any government agency.

Appendix 2: Enhance Due Diligence (EDD) for PEPs, Influential Persons and High-Level Management in International Organizations

While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised. Following instructions shall have to be followed to ensure Enhanced Due Diligence (EDD):

- take reasonable measures to establish the source of wealth and source of funds.
- ongoing monitoring of the transactions must be conducted; and
- The Account Opening Officer should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents.

In keeping with the assessment of risk and the allowance for simplified CDD where risk is low, there is a requirement to have EDD where risk is high e.g., relationship with PEPs.

The instructions in relation to Politically Exposed Persons as contained in AML circular no. 14 dated 25 September 2007 stand substituted as follows:

While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised.

PEPs mean *"Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials"*.

All instructions as detailed for PEPs shall equally apply if business relationship is established with the family members and close associates of these persons who may pose reputational risk to the IPDC.

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

(a) a risk management system shall have to be introduced to identify risks associated with the opening and operating accounts of PEPs.
(b) obtain CAMLCO approval for establishing business relationships with such customers.
(c) take reasonable measures to establish the source of wealth and source of funds.
(d) ongoing monitoring of the transactions must be conducted; and

(e) IPDC should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents, if any.

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

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

Responsibilities in case of "Influential Persons":

Bank/FI must identify the true underlying beneficiaries against the account and/or client. If establishing and maintaining banking relationship with such personnel is deem risky, Bank/FI must follow the instructions as cited as above from point "b" to "d"

By "Influential Person" it is meant-"individuals who are or have been entrusted domestically with prominent public functions, for example Head of State or of Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials."

Instructions appropriate for Influential persons shall also be applicable for close associates.

No middle ranking or more junior individuals shall be deemed as "Influential Person" as quoted in this paragraph.

Responsibilities in case of Head of any International Organization or High-Level Officers:

Bank/FI has to identify whether the account and/or client is truly benefiting the head of any international organization or any high-level officers.

If establishing and maintaining banking relationship with such personnel is deem risky, Bank/FI must follow the instructions as cited as above from point "b" to "d" and instructions as suggested in "e" should also be followed in appropriate cases. Instructions appropriate for head of any international organization or any high-level officers shall also be applicable for his/her close associates.

By "Head of International Organization or High-Level Officers" it is meant- 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"

Instructions as appropriate for “Head of International Organization or High-Level Officers” are also applicable for their close associates.

No middle ranking or more junior individuals shall be deemed as “Head of International Organization or High-Level Officers” as quoted in this paragraph.

Ongoing monitoring of accounts and transactions

On-going monitoring is an essential aspect of effective CDD procedures. Effectively internal control system may reduce the risk if relationship managers understand normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account’s activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk sensitive. For all accounts, we must ensure proper systems in place to detect unusual or suspicious patterns of activity. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert management to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being “washed” through the account.

There should be intensified monitoring for higher risk accounts. IPDC should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors.

To ensure that records remain up-to-date and relevant, there is a need for IPDC to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated.

However, if IPDC becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

IPDC has developed clear standards on what records must be kept on for customer identification and individual transactions and their retention period. As the starting point and natural follow-up of the identification process, IPDC should obtain customer identification papers and retain copies of them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

Appendix 3: KYC: Individual Loan

KYC PROFILE FORM FOR INDIVIDUALS (LOAN PRODUCTS)

Customer/Account Name _____

Account/Reference No. _____ Client ID _____

Loan Type ☐ Home Loan ☐ Auto Loan ☐ Personal Loan ☐ Others (please specify) _____

Identification and Address Verification

Original Passport/National ID/Smart ID sighted and photocopy obtained ☐ Yes ☐ No

Passport / NID / Smart ID No. | | | | | | | | | | | | | | | | |

Comment _____

Have the documents (i.e NID, E-TIN, etc.) verified with the available database? ☐ Yes ☐ No ☐ Not Applicable

Comment (if applicable) _____

Verification of the actual owner of the account

Branch official/Relationship Manager met with the applicant ☐ Yes ☐ No ☐ Not Applicable

Comment (if applicable) _____

Has it been established that the customer is the ultimate beneficiary of the loan? ☐ Yes ☐ No ☐ Not Applicable

Comment (if applicable) _____

Verification of business/occupation and income

Is the primary occupation/business and its legal status verified? ☐ Yes ☐ No ☐ Not Applicable

Comment (if applicable) _____

Are sufficient legal evidences obtained? ☐ Yes ☐ No ☐ Not Applicable
(e.g. Employee ID Card, Employment Certificate, Trade License, etc.)

Comment (if applicable) _____

Is the source of income verified? ☐ Yes ☐ No ☐
Not Applicable

Comment (please specify) _____

Verifications of EMI, client's contribution, etc.

Comments (if applicable) Number of monthly installments commensurate with the client's monthly income? ☐ Yes ☐ No ☐ Not Applicable

Does the amount of client's contribution/Pre-payment conform with his/her Net-Worth? ☐ Yes ☐ No ☐ Not Applicable

Comment (if applicable) _____

AML-FT Risk Assessment

Risk Score (to be ascertained as per IPDC Finance Limited's "Money Laundering and Terrorist Financing Risk Based Assessment Guidelines" and existing regulatory guidelines.) ☐ Low ☐ Medium ☐ High

Comments on Risk Score, if any

Has the purpose of the loan been assessed properly taking into consideration the risk of utilization of the amount for terrorist financing/illicit business? ☐ Yes ☐ No

Comment _____

Is any of the names of the applicant(s)/ co-applicant(s)/ guarantor(s) found in the sanction list or any other blacklist? (If yes, the please give detailed description in the comment section below) ☐ Yes ☐ No

Prepared by

Name _____

Designation _____

Signature with date

Supervisor/Head of Credit Administration

Name _____

Designation _____

Signature with date

When was the client and account related information reviewed and updated? D D M M Y Y Y Y

Reviewed by

Name _____

Designation _____

Signature with date

Appendix 4: KYC Institutional

KYC PROFILE FORM, INSTITUTIONAL / অ-ব্যক্তিক গ্রাহক পরিচিতি সম্পর্কিত ফরম, ব্যাঙ্কি

1. Account Title / [হিসাবের শিরোনাম]

2. Branch ID & Account No / [শাখার কোড এবং হিসাব নম্বর]

3. CIF No. / [সি আই এফ নং]

4. Client's Name / [গ্রাহকের নাম]

5. Name of account opening officer / [হিসাব খোলার কর্মকর্তার নাম]

Documents / দলিলাদি

If photocopy is obtained, in applicable cases
ফটোকপি গৃহীত কিনা (প্রযোজ্য ক্ষেত্রে)

6. Trade License no. / [ট্রেড লাইসেন্স নং] ☐ Yes / হ্যাঁ ☐ No / না

7. Memorandum of Association/ Partnership Deed / [স্মারক সংঘ/অংশীদারী দলিল] ☐ Yes / হ্যাঁ ☐ No / না

8. Certificate of Incorporation / [সার্টিফিকেট অব ইনকর্পোরেশন] ☐ Yes / হ্যাঁ ☐ No / না

9. E-TIN no. / [ই-টিন নং] ☐ Yes / হ্যাঁ ☐ No / না

10. VAT Registration number / [ভ্যাট রেজিঃ নং] ☐ Yes / হ্যাঁ ☐ No / না

11. Board Resolution / [বোর্ড রেজল্যুশন] ☐ Yes / হ্যাঁ ☐ No / না

12. Information on Beneficial Owner / [হিসাবের প্রকৃত সুবিধা ভোগী সম্পর্কিত তথ্যাদি]

(KYC in details must be completed for all shareholders holding at least 20% shares. Besides, KYC in details must be completed for all controlling shareholders. [২০% বা এর অধিক একক শেয়ার হোল্ডার এর বিস্তারিত তথ্যাদি সংগ্রহ পূর্বক কেওয়াইসি সম্পাদন করতে হবে। এছাড়াও কোম্পানীর নিয়ন্ত্রণকারী শেয়ারহোল্ডার এর বিস্তারিত তথ্যাদি সংগ্রহ পূর্বক কেওয়াইসি সম্পাদন করতে হবে। প্রকৃত সুবিধা ভোগী চিহ্নিত করত কেওয়াইসি সম্পাদন করতে হবে।]

13. What is the source of fund? How source of fund has been verified (if applicable)? / [প্রদেয় অর্থের উৎস কি? তহবিলের উৎস কিভাবে নিশ্চিত করা হয়েছে? (প্রযোজ্য ক্ষেত্রে)]

14. Is the source of fund consistent with the profession of the client? / [গ্রাহকের পেশার সাথে প্রদেয় অর্থের উৎস সামঞ্জস্যপূর্ণ কিনা?]

Justify the consistency by giving details description of client's profession / [গ্রাহকের পেশার বিস্তারিত বর্ণনা পূর্বক সামঞ্জস্যতা নিশ্চিত করুন]

15. Risk Score / [রিস্ক স্কোর] ☐ Low / [নিম্ন] ☐ Medium / [মধ্যম] ☐ High / [উচ্চ] ☐ Extreme / [অতি উচ্চ]

Comment /[মন্তব্য]

Account opening form scanned by [আবেদন ফরমের স্ক্যান সম্পন্নকারী কর্মকর্তা]

Risk score to be ascertained as per IPDC Finance Limited's "Money Laundering and Terrorist Financing Risk Based Assessment Guidelines". Risk treatment action plan to be provided in details under the Comment field. [আইপিডিসি ফাইন্যান্স লিমিটেড-এর "Money Laundering and Terrorist Financing Risk Based Assessment Guidelines" এর নির্দেশনা মোতাবেক রিস্ক স্কোর নিরুপন করতে হবে। প্রাপ্ত রিস্ক স্কোরের বিপরীতে ঝুঁকি মোকাবেলায় গ্রহনীয় পদক্ষেপ সমূহ মন্তব্য কলামে বিস্তারিত ভাবে লিপিবদ্ধ করতে হবে]

Name of Relationship Manager, Signature (with seal) and date
[রিলেশনশীপ ম্যানেজারের নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

Approving Officer's Name, Signature (with seal) and Date
[অনুমোদনকারী কর্মকর্তার নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

Is any of the Names of the applicant/nominee/beneficiary is found in the sanction list or any other blacklist? If the answer is Yes, then give detailed description in the comment field [আবেদনকারী/ নমিনী/ বেনিফিসিয়ারির কারোর নাম স্যাংশন লিষ্ট বা অন্য কোন নিষিদ্ধ তালিকায় পাওয়া গেছে কি? উত্তর হ্যাঁ হলে মন্তব্য অংশে বিস্তারিত লিখুন]

☐ Yes [হ্যাঁ] ☐ No [না]

Comment [মন্তব্য]:

Verifying Officer's Name, Signature (with seal) and Date
[যাচাইকারী কর্মকর্তার নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

16. Last date of review/update of account and customer information / [হিসাব ও গ্রাহকসংক্রান্ত তথ্যাদি সর্বশেষ পর্যালোচনা/হালনাগাদ করার তারিখ]

Name, Signature (with seal) of review/updating officer and Date
[পর্যালোচনা এবং হালনাগাদকারী কর্মকর্তার নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

☐ Please open [হিসাবটি খুলুন] ☐ Do not open [হিসাবটি খুলবেন না]

Signature and Date with Seal of Approving Officer
[অনুমোদনকারী কর্মকর্তার সীলসহ স্বাক্ষর ও তারিখ]

Account Opening date [হিসাব খোলার তারিখ] d d m m

Maturity Date [মেয়াদ পূর্তির তারিখ] d d m m

Signature and Date with Seal of Account Opening Officer
[হিসাব খোলার কর্মকর্তার সীলসহ স্বাক্ষর ও তারিখ]

Account opening form scanned by [আবেদন ফরমের স্ক্যান সম্পন্নকারী কর্মকর্তা]

Signature and Date
[স্বাক্ষর ও তারিখ]

Name [নাম]

Appendix 5: KYC Deposit

KYC PROFILE FORM, INDIVIDUAL / গ্রাহক পরিচিতি সম্পর্কিত ফরম, ব্যাক্তি

1. Account Title / [হিসাবের শিরোনাম]

2. Branch ID & Account No / [শাখার কোড এবং হিসাব নম্বর]

3. CIF No. / [সি আই এফ নং] Group CIF No. / [গ্রুপ সি আই এফ নং]

4. Client's Name / [গ্রাহকের নাম]

5. Name of account opening officer / [হিসাব খোলার কর্মকর্তার নাম]

Documents / দলিলাদি

If photocopy is obtained, in applicable cases
ফটোকপি গৃহীত কিনা (প্রযোজ্য ক্ষেত্রে)

6. Birth Registration Certificate / [জন্ম নিবন্ধন সনদ নং]	☐ Yes / হ্যাঁ	☐ No / না
7. Passport number / [পাসপোর্ট নং]	☐ Yes / হ্যাঁ	☐ No / না
8. National ID number / [জাতীয় পরিচয় পত্র নং]	☐ Yes / হ্যাঁ	☐ No / না
9. Commissioner Certificate / [কমিশনার সনদ]	☐ Yes / হ্যাঁ	☐ No / না
10. E-TIN / [ই-টিন]	☐ Yes / হ্যাঁ	☐ No / না
11. Driving License number / [ড্রাইভিং লাইসেন্স]	☐ Yes / হ্যাঁ	☐ No / না

12. Information on Beneficial Owner / [হিসাবের প্রকৃত সুবিধা ভোগী সম্পর্কিত তথ্যাদি]
(Beneficial owner of the account must be identified and KYC of beneficial owner must be completed in details [হিসাবের প্রকৃত সুবিধা ভোগী চিহ্নিত করতঃ কেওয়াইসি সম্পাদন করতে হবে]

13. What is the source of fund? How source of fund has been verified (if applicable)? / [প্রদেয় অর্থের উৎস কি? তহবিলের উৎস কিভাবে নিশ্চিত করা হয়েছে? (প্রযোজ্য ক্ষেত্রে)]

14. Is the source of fund consistent with the profession of the client? / [গ্রাহকের পেশার সাথে প্রদেয় অর্থের উৎস সামঞ্জস্যপূর্ণ কিনা?]
Justify the consistency by giving details description of client's profession / [গ্রাহকের পেশার বিস্তারিত বর্ণনা পূর্বক সামঞ্জস্যতা নিশ্চিত করুন]

15. Risk Score / [রিস্ক স্কোর] ☐ Low / [নিম্ন] ☐ Medium / [মধ্যম] ☐ High / [উচ্চ] ☐ Extreme / [অতি উচ্চ]
Comment / [মন্তব্য]

Risk score to be ascertained as per IPDC Finance Limited's "Money Laundering and Terrorist Financing Risk Based Assessment Guidelines". Risk treatment action plan to be provided in details under the Comment field. [আইপিডিসি ফাইন্যান্স লিমিটেড-এর "Money Laundering and Terrorist Financing Risk Based Assessment Guidelines" এর নির্দেশনা মোতাবেক রিস্ক স্কোর নিরুপন করতে হবে। প্রাপ্ত রিস্ক স্কোরের বিপরীতে ঝুঁকি মোকাবেলায় গ্রহনীয় পদক্ষেপ সমূহ মন্তব্য কলামে বিস্তারিত ভাবে লিপিবদ্ধ করতে হবে]

Name of Relationship Manager, Signature (with seal) and date
[রিলেশনশীপ ম্যানেজারের নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

Approving Officer's Name, Signature (with seal) and Date
[অনুমোদনকারী কর্মকর্তার নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

Is any of the Names of the applicant/nominee/beneficiary is found in the sanction list or any other blacklist? If the answer is Yes, then give detailed description in the comment field [আবেদনকারী/ নমিনী/ বেনিফিসিয়ারির কারোর নাম স্যাংশন লিষ্ট বা অন্য কোন নিষিদ্ধ তালিকায় পাওয়া গেছে কি? উত্তর হ্যাঁ হলে মন্তব্য অংশে বিস্তারিত লিখুন]

☐ Yes [হ্যাঁ] ☐ No [না]

Comment [মন্তব্য]:

Verifying Officer's Name, Signature (with seal) and Date
[যাচাইকারী কর্মকর্তার নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

---

16. Last date of review/update of account and customer information / [হিসাব ও গ্রাহকসংক্রান্ত তথ্যাদি সর্বশেষ পর্যালোচনা/হালনাগাদ করার তারিখ]

Name, Signature (with Seal) of review/updating officer and Date
[পর্যালোচনা এবং হালনাগাদকারী কর্মকর্তার নাম, স্বাক্ষর (সীলসহ) ও তারিখ]

☐ Please open [হিসাবটি খুলুন] ☐

Signature and Date with Seal of Approving Officer
[অনুমোদনকারী কর্মকর্তার সীলসহ স্বাক্ষর ও তারিখ]

Account Opening date [হিসাব খোলার তারিখ] d d m m ☐☐☐☐ Maturity Date [মেয়াদ পূর্তির তারিখ] d d m m ☐☐☐☐

Signature and Date with Seal of Account Opening Officer
[হিসাব খোলার কর্মকর্তার সীলসহ স্বাক্ষর ও তারিখ]

Account opening form scanned by [আবেদন ফরমের স্ক্যান সম্পন্নকারী কর্মকর্তা]

Name [নাম]

Signature and Date
[স্বাক্ষর ও তারিখ]

Appendix 6: Internal Suspicious Activity Report Form

Strictly Private & confidential

To	Chief Anti Money Laundering Compliance Officer	Date:
From	Name (Mr./ Ms)	Branch/Department
	Job Title	SAR Ref No.

***Note**: This form may be completed in **English**. For any queries, please contact AMLCO. Please provide full details of the transaction(s) and any other relevant data. Attach copies of relevant documents/transaction notes.*

Customer/ Business Name	Transaction Date(s)
Account Number(s)	Copies of Transactions and Account Details Attached Yes/No
Description of Transaction(s). *(Nature of transaction, Origin & destination of Transaction etc.)*	
Source of Funds and Purpose of Transaction (*If you can, try to tactfully ask the customer*)	
Reasons why you think the transaction is suspicious (*Give as much details as possible*) Signatures of Bank Employee.	
TO BE COMPLETED BY CAMLCO.	
ACTION TAKEN TO VALIDATE Acknowledgement sent to the originator on _____. Reviewed account documentation Discuss with the relationship manager/ branch manager. Other.	
AGREED SUSPICIOUS. Yes/No	
COMMENTS / NOTES OF CAMLCO	
Signature CAMLCO Date.	

Appendix 7: Know Your Employee

FULL NAME (ENGLISH)	☐ MR. ☐ MS.
FULL NAME (BENGALI)	
EMPLOYEE ID	
DESIGNATION	
DEPARTMENT	
LOCATION	
DATE OF JOINING	
TYPE OF EMPLOYMENT	☐ PERMANENT ☐ CONTRACTUAL
PROBATION PERIOD	
CONFIRMATION DATE	
BANK ACCOUNT NUMBER	
INSURANCE ID	
DO YOU EVER HAVE ANY CRIMINAL RECORDS	☐ YES ☐ NO
PHOTOCOPY OF PASSPORT RECEIVED	☐ YES ☐ NO

DATE OF BIRTH (DD/MM/YYYY)				
PLACE OF BIRTH	COUNTRY		DISTRICT	
NATIONAL ID				
PASSPORT NUMBER				
TIN NUMBER (IF ANY)				
DUAL CITIZENSHIP (IF ANY)	COUNTRY		PASSPORT NO.	
GENDER				
BLOOD GROUP				
RELIGION				
MARITAL STATUS				

EDUCATIONAL QUALIFICATION			RESULT	ORIGINAL SEEN
	SCHOOL			
	COLLEGE			
	UNIVERSITY			
PHOTOCOPY OF EDUCATIONAL CERTIFICATES RECEIVED	☐ YES		☐ NO	
PREVIOUS EMPLOYMENT	EMPLOYER'S NAME		RELEASE ORDER RECEIVED FROM PREVIOUS EMPLOYER	
	ADDRESS			
	DESIGNATION			
	DEPARTMENT			
	CONTACT NUMBER			
	FAX NUMBER			

EMERGENCY CONTACT NAME	
RELATIONSHIP WITH EMPLOYEE	
PRESENT ADDRESS	
PERMANENT ADDRESS	
PHONE NUMBER (MOBILE)	
PHONE NUMBER (RESIDENT)	
PHONE NUMBER (OFFICE)	
EMAIL ADDRESS (PERSONAL)	
EMAIL ADDRESS (OFFICE)	

I hereby certify that the above-mentioned information is correct and accurate to the best of my knowledge.

SIGNATURE

DATE

DETAILS OF PROFESSIONAL REFEREES

Please provide the names and addresses of referees to verify your employment history over the past 3 (three) years. One of the referees should be your former employer (if any). Please note that we will approach your references on a confidential basis for verification.

EMPLOYEE NAME: ……..
DESIGNATION : ……..
DEPARTMENT : ……..

NAME OF REFEREE 1	☐ **MR.** ☐ **MS.**	
DESIGNATION		
PLACE OF EMPLOYMENT		
ADDRESS (OFFICE)		
CONTACT NUMBER (OFFICE)		
E-MAIL (OFFICE)		
ADDRESS (RESIDENCE)		
CONTACT NUMBER (RESIDENCE)		
CONTACT NUMBER (MOBILE)		
E-MAIL (PERSONAL)		

NAME OF REFEREE 2	☐ **MR.** ☐ **MS.**	
DESIGNATION		
PLACE OF EMPLOYMENT		
ADDRESS (OFFICE)		
CONTACT NUMBER (OFFICE)		
E-MAIL (OFFICE)		
ADDRESS (RESIDENCE)		
CONTACT NUMBER (RESIDENCE)		
CONTACT NUMBER (MOBILE)		

E-MAIL (PERSONAL)	

Signature : _____

Name : _____

Date: _____ Designation : Head of Human Resources

Appendix 8: List of Abbreviations

AML	Anti-Money Laundering
CAMLCO	Chief AML Compliance Officer
BAMLCO	Branch Anti-Money Laundering Compliance Officer
BFIU	Bangladesh Financial Intelligence Unit (BFIU)
CDD	Customer Due Diligence
CCU	Central Compliance Unit
CEO	Chief Executive Officer
CTR	Cash Transaction Report
CPV	Contact Point Verification
CTF	Combating Terrorist Financing
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Client
IPDC	IPDC Finance Limited
MLPA	Money Laundering Prevention Act
MD	Managing Director
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
SOP	Standard Operating Procedure
SDN	Specifically Designated Nationals and Blocked Persons
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
TP	Transaction Profile
BB	Bangladesh Financial Intelligence Unit (BFIU)
Body	Board of Directors
BAC	Board Audit Committee

Appendix 9: Self Assessment report

আর্থিক প্রতিষ্ঠানের নাম : IPDC OF BANGLADESH LTD

_ _ _ _ _ _ _ _ শাখা। Date:

শাখা কর্তৃক Self Assessment পদ্ধতির মাধ্যমে নিজস্ব অবস্থান নির্ণয়

প্রতিটি আর্থিক প্রতিষ্ঠানের শাখা মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও প্রতিষ্ঠানের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নবর্ণিত প্রশ্নমালার বিস্তারিত উত্তর প্রদানের মাধ্যমে Self Assessment পদ্ধতিতে নিজেদের অবস্থান নির্ণয় করবে ঃ

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
১. শাখায় মোট কর্মকর্তার সংখ্যা কত (পদানুযায়ী)? কতজন কর্মকর্তা মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন? (শতকরা হার)	প্রশিক্ষণ সংক্রান্ত রেকর্ড যাচাই করতে হবে।		
২.ক) শাখার মানিলন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা (BAMLCO) জেষ্ঠ্য ও অভিজ্ঞ কিনা? বিগত দুই বছরে তিনি মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণ পেয়েছেন কি না? খ) শাখায় মানি লন্ডারিং প্রতিরোধ কার্যক্রম যথানিয়মে পরিপালিত হচ্ছে এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় মনিটরিং ও পর্যালোচনা করে থাকেন কিনা?	BAMLCO কর্তৃক KYC কার্যক্রমের যথার্থতা মনিটরিং করা হয় কিনা? যথাযথভাবে Transaction মনিটরিং এবং সন্দেহজনক লেনদেন রিপোর্ট (ইন্টারনাল রিপোর্টসহ) করা হয় কিনা? যথাযথভাবে রেকর্ড সংরক্ষণ করা হয় কিনা? STR সনাক্তকরণে ব্যবস্থা নেয়া হয় কিনা?		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
৩. BAMLCO সহ শাখার কর্মকর্তাগণ মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?	বিষয়টি যাচাইয়ের পদ্ধতি কী?		
৪. শাখা পর্যায়ে ত্রৈমাসিক ভিত্তিতে মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক সভা অনুষ্ঠিত হয় কিনা?	সভার আলোচ্যসূচি সকলের অবগতির জন্য বণ্টন করা হয় কিনা? সভায় কী কী গুরুত্বপূর্ণ সিদ্ধান্ত গৃহীত হয়েছে? সভায় গৃহীত সিদ্ধান্ত কিভাবে বাস্তবায়িত হয়?		
৫. সকল প্রকার হিসাব খোলা ও লেনদেন পরিচালনার ক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং সময়ে সময়ে বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা ?	গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয় কিনা? হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) সনাক্ত করা হয় কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরীখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কিনা?		
৬. ক) ঝুঁকির ভিত্তিতে শাখা তাদের গ্রাহকদের শ্রেণীবিন্যাস/শ্রেণীকরণ করে কিনা?	করে থাকলে এ পর্যন্ত কতটি উচ্চ ঝুঁকি সম্পন্ন হিসাব শাখায় খোলা হয়েছে? এ ধরনের হিসাব খোলা ও পরিচালনার ক্ষেত্রে শাখা কী পদক্ষেপ গ্রহণ করেছে?		
৭. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানিলন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কি না?	এ বিষয়ক নিজস্ব নীতিমালা প্রণয়ন করা হয়েছে কিনা? হলে উক্ত নীতিমালা শাখায় কিভাবে বাস্তবায়িত হচ্ছে?		
৮. শাখা গ্রাহকের KYC Profile এর তথ্য বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা মোতাবেক নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে কিনা?	কী পদ্ধতিতে এরূপ মূল্যায়ন সম্পাদিত হয়ে থাকে?		
৯. সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধীন সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধের লক্ষ্যে শাখা কী ধরনের পদক্ষেপ গ্রহণ করেছে?	জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলুশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও লেনদেন কার্যক্রম যাচাই করা হয় কিনা?		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
	শাখা এ বিষয়ক নিজস্ব কোন Mechanism অনুসরণ করে কি না? এরূপ কোন ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা?		
১০. এ যাবৎ শাখা কর্তৃক কতগুলো সন্দেহজনক লেনদেন (STR) শনাক্ত করা হয়েছে?	শাখায় সন্দেহজনক লেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখায় সন্দেহজনক লেনদেন রিপোর্টিং এর জন্য Internal Reporting Mechanism চালু রয়েছে কিনা? শাখা পর্যায়ে নিস্পত্তিকৃত Internal Report সংরক্ষণ করা হয় কিনা?		
১১. মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন, সার্কুলার, প্রশিক্ষণ রেকর্ড, বিবরণী ও অন্যান্য এএমএল/সিএফটি সংক্রান্ত বিষয়াবলীর আলাদা নথি শাখা কর্তৃক সংরক্ষণ করা হয় কিনা? আইন, সার্কুলার ইত্যাদির কপি শাখার সকল কর্মকর্তা/কর্মচারীদের সরবরাহ করা হয় কিনা?	সংরক্ষিত হয়ে থাকলে হ্যাঁ অথবা না হয়ে থাকলে না, আংশিক হলে কী কী সংরক্ষিত আছে তা লিখুন।		
১২. বিএফআইইউ মাস্টার সার্কুলার অনুসারে শাখায় PEPs, প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা?	উত্তর হ্যাঁ হলে এই হিসাব খোলা ও পরিচালনার ক্ষেত্রে কী কী ধরণের সতর্কতা অবলম্বন করা হচ্ছে?		
১৩. আর্থিক প্রতিষ্ঠানের প্রধান কার্যালয়, বাংলাদেশ ব্যাংক ও বাংলাদেশ ফাইন্যন্সিয়াল ইন্টেলিজেন্স ইউনিট-এর পরিদর্শন প্রতিবেদনে উল্লেখিত মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ পরিপালন বিষয়ক দুর্বলতা/অনিয়মসমূহ নিয়মিত করা হয়েছে কিনা?	না হয়ে থাকলে প্রতিবন্ধকতাসমূহ কী কী?		

শাখা মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তার নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ	শাখা ব্যবস্থাপকের নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ

IPDC Finance Limited
Internal Audit & Compliance Department
_____ Branch
Period : _____ to _____

Appendix 9: Independent Testing Procedures

Branch Inspection Checklist

Sl.	Area		Questions	Evaluation parameter	Score	Obtained score	Comments
1	Branch Compliance Unit	1	Is there any experienced and senior executive as BAMLCO at the Branch?	BAMLCO should have at least three (3) years of experience in Bank/FIs See office order regarding nomination as BAMLCO. It is feasible to nominate branches second in command or any experienced Executive as BAMLCO.	1		
		2	Did s/he attend any training session related to Anti Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in last two years? Is s/he adequately aware regarding existing acts, rules of AML and CFT, time to time issued directives and guidance notes by BFIU and own policy of the company regarding AML and CFT?	Verify based on interview and evidence.	2		
		3	"Money Laundering Prevention Act, Anti-Terrorism Act and related issued policies and/or directives have complied appropriately." - In order to ensure this issue, whether the BAMLCO monitor and review the issue after a certain period and regular interval?	Evaluate BAMLCO's monitoring and reviewing process, as well as, verify its adequacy based on scrutiny.	3		

		4	Whether any attempt has been made to protect AML and CFT related risks as per directives issued by BFIU and own policy of the company?Is there any adequate process to monitor customer transactions including high risk accounts?	Evaluate attempt taken by the branch regarding risk of Money Laundering and Financing of Terrorism.Evaluate the BAMLCO's monitoring and reviewing process on the transactions of all accounts including high risk accounts, as well as, check its adequacy based on verification.	4		
		5	Is there any account maintained of PEPs, influential persons, chief or high level officials of international organization at the branch as per BFIU master circular?	Verify whether the safety measures have been taken in case of opening and operating of such accounts according to BFIU master circular. Although there is no account of PEPs, influential persons, chief or high level officials of international organization, if any process exist for implementation of instruction as per BFIU master circular than the branch will earn full marks.	3		
		6	Is Branch Self-Assessment procedure works appropriately and effectively as per BFIU instructions?	Review the Self-Assessment report of the branch. Provide score on the basis of practice and implementation of Self-Assessment report.	6		
2	Knowledge of Executives / Staffs on AML and CFT and increase of awareness and taking	1	How many Executives / Staffs had taken formal training on AML and CFT?	It will be considered as satisfactory level subject to completion of training of 100% Executives / Staffs. Provide number based on rate of training.	3		
		2	Are they (Executives / Staffs of the branch) aware about the existing acts, rules of AML and CFT, time to time issued directives and guidance notes by BFIU and own policy of the company regarding AML and CFT?	Evaluate based on consultations with branch's relevant Executives / Staffs.	4		
		3	Is there any meeting, presided over branch manager, called for evaluation of AML/CFT activities on quarterly basis?	Collect minutes of the meeting and examine its applicability.	5		
		4	Is there any attempt made to implement the directives issued by BFIU and the company's own policy regarding AML and CFT?		3		

	step to reduce risks						
3	Know Your Customer (KYC) Procedure	1	In case of opening all type of accounts and transacting in the same, whether the KYC procedure is being complied at satisfactory level in accordance with Money Laundering Prevention Act, Anti-Terrorism Act and BFIU's master circulars?	Examine 4/5 sample accounts of each type. Provide number in following subject matter on the basis of satisfaction – - How authenticity of the identification of the customer is confirmed? - How is this preserved at the branch? Is the source of income confirmed at the time of ensuring KYC? - Whether the process of identification of beneficial owner and verification of the same is at satisfactory level? - Whether the additional information (EDD) is collected for high risk customers?	6		
		2	Does the branch classify / categorize their customers based on risk category as per BFIU's master circular?	Verify whether the instruction provided through BFIU's master circular is complied.	6		
		3	Do they collect necessary additional information in case of high risk customers?	Examine what types of information is collected and whether those are sufficient enough.	5		
		4	Whether the branch update the customer's KYC Profile after re-evaluation on regular interval?	Evaluate the process of updating / reassessing of KYC Profile.	5		

4	Compliance of Anti-Terrorism Act, 2009	1	What step does the branch take to protect from financing in terrorism as per Anti-Terrorism Act, 2009?	Provide score on satisfaction of the following matters-- Does the branch kept the list of suspected people of terrors, terrorism and involved in expansion of weapon published by different UNSCR and the banned entities and individuals declared by Bangladesh Government and whether monitor the accounts and transactions as per the list?- Does the branch maintain any own mechanism regarding this matter?- Does the branch inform BFIU regarding the accounts of this type of the person or entity, if any?	5		
5	Suspicious Transaction Report (STR) and Cash Transaction Report (CTR)	1	Are all the employees of the branch aware about STR?	Does the branch have Internal Reporting Mechanism for reporting Suspicious Transaction? Whether all employees are aware about the matter?	5		
		2	Does the branch have any appropriate method for identifying Suspicious Transaction regarding Money Laundering and Financing of Terrorism? How many Suspicious Transaction (STR) have been reported to CCU from BAMLCO as of to date?	Though Suspicious Transaction happen in the branch and if it is not reported by BAMLCO to CCU than it considers as unsatisfactory. - Verify through file and system whether any process has been implemented to identify STR at the branch. Provide score on satisfaction of the following matters- - Is there any process to identify Suspicious Transactions at the Branch? - Whether the resolved Internal Reports at branch level have been kept appropriately at the branch?	4		
		3	Does the branch do Cash Transaction Report (CTR) accurately and properly?	Check the evidence in this regard. Verify the cash register/statement of minimum one month and based on this evaluate the accuracy of the submitted CTR report of the respective month by examining the same.	2		

6	Submission of statement to CCU	1	How many statements are submitted to CCU by the branch? Does the branch submit the same in due time?	Check the evidence in this regard. It will be considered as unsatisfactory in case of late submission or non-submission of the statements.	3		
		2	Does the branch do Self-Assessment regularly? Whether the prepared statements are appropriate?	Check the evidence in this regard. It will be considered as unsatisfactory in case of incorrect and incomplete information.	3		
7	Record Keeping	1	Is there any policy for preserving KYC and Transaction records properly?	Check five (5) closed accounts. Verify whether the rules have been followed properly according to Money Laundering Prevention Act?	4		
		2	Do they provide information as per demand of regulatory bodies or CCU?	Check the evidence in this regard. It will be considered as unsatisfactory if information is not provided accurately and in timely manner.	3		
8	Overall Branch Activities regarding AML/CFT	1	Does Branch Manager (if he is not BAMLCO) play proper role in case of implementation of AML and CFT program?	Evaluate it based on discussion with Branch Manager and minutes of meeting held at the branch and branch's compliance status.	5		
		2	At the time of reviewing previous internal and external audit report, observe that, is there any irregularity and weakness pointed out in connection with AML/CFT and whether the branch has taken any action for rectification?	Review the latest audit report and verify the nature of action has been taken for rectification.	4		
		3	Are the overall activities of the branch satisfactory?	Evaluate it based on overall AML and CFT and performance of the branch manager.	6		
					100		

Overall evaluation of the Branch:

Score	Rating
90.01 - 100.00	Strong
70.01 - 90.00	**Satisfactory**
55.01 – 70.00	Fair
40.01 – 55.00	Marginal
40 and below	Unsatisfactory