DBH FINANCE PLC

Policy & Guidelines on AML and CFT

Approval Level	: Board of Directors
Approval Date	: December 14, 2023
Next Review Date	: 36 Months

Preface

The act of taking the proceeds of criminal activities and passing them off as legitimate is known as money laundering. It is a severe threat to the financial system that affects every nation in the world. If left unchecked, it might destroy the nation's infrastructure, payment methods, financial market, and sovereignty altogether. These days in the global economy, money laundering (ML) and terrorist financing (TF) have become major financial crimes. It significantly affects a nation's social, political, cultural, economic, and other developments. Both ML and TF have the potential to undermine specific financial institutions and endanger the nation's overall financial development. Promoting a robust, stable, and sound financial sector thus requires preventing money laundering and fighting the funding of terrorism.

To prevent ML and combat TF issues in a strong hand, the Government of Bangladesh has enacted "Money Laundering Prevention Act, 2009" (amended in 2015) and "Anti-Terrorism (Amendment) Act, 2009" (amended in 2013). In addition to that Money Laundering Prevention Rules, 2019 and Anti-Terrorism Rules, 2013 was also enacted by the concerned ministry. Besides, Bangladesh Financial Intelligence Unit (BFIU) has declared Money Laundering and Terrorist Financing Risk as one of the core risks of the financial institutions. In this regard, BFIU has also issued a latest guidance (Circular – 28 dated 30 May 2023) "Instructions to be followed by the Financial Institutions for prevention of money laundering, terrorist financing and proliferation financing". In this context, DBH Finance PLC. (hereinafter referred as "DBH") has formulated its own policy "Policy & Guidelines on AML and CFT" (hereinafter referred as AML/CFT Guidelines) with the approval of its Board of Directors.

The basic understanding of compliance is the following of internal guidelines in addition to norms (laws, regulations, and industry standards). The corporation and its personnel may face penalties from both civil and criminal courts for noncompliance, which may also cause harm to their reputation. On the other hand, a strong compliance program can shield businesses against costly procedures, excessive liability lawsuits, and reputational harm. Additionally, it can raise an organization's efficiency, which benefits the business over time.

A good compliance-

1. reduces organizational and individual risk;
2. enables less hesitance and increases confidence;
3. helps better data management for better decisions;
4. increases level of efficiencies and economies of scale;
5. helps to providing level playing field;
6. helps realizing the company's mission;
7. enhances relationships with regulators and other stakeholders;
8. reminds us that transparency is good business;
9. helps attract and retain talents and ensure employee's engagement; etc.

To ensure proper compliance of the Guidelines, DBH has established a Central Compliance Unit (CCU) headed by a senior official, whose seniority, as per requirement of Bangladesh Financial Intelligence Unit (BFIU), is not lower than three tiers from the Managing Director. Besides, DBH has designated one senior level officer as

Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO) and Branch Anti-Money Laundering Compliance Officer (BAMLCO) in the branch level. The CAMLCO is the Head of CCU and has vast working experience.

The concerned employees, management and, where necessary, the Board of Directors of DBH will ensure the following compliance requirements of the above enactments:

1. report to BFIU proactively and immediately on the facts of suspicious, unusual or doubtful, cash transactions (STR/SAR/CTR) likely to be related to ML/TF;
2. maintain confidentiality while sharing customer's account related information;
3. not to disclose STR/SAR/CTR related facts or other related information to anybody which are being reported to BFIU;
4. not to open or maintain any numbered or anonymous account;
5. ensure know your customer (KYC) and know your employee (KYE) while opening customer's account and appointment of employee, as the case may be;
6. apply enhanced due diligence while opening accounts of PEPs/IPs etc.;
7. customer due diligence should be exercised to the customer at the time of identification, acceptance, transaction, monitoring and reporting of STR/SAR/CTR;
8. self-assessment of the effectiveness of the AML/CFT program should be carried on half yearly basis by the BAMLCO and the results of the same to be communicated to the ICC and CCU;
9. the ICC shall carry out independent testing procedure (ITP) to check the adequacy of AML/CFT policies and conduct audit in case of major non-compliance, if any, and report to CCU for taking necessary action;
10. preserve, at least for 5(five) years, all necessary records on transactions, to comply with information requests from the competent authorities like BFIU and other legal authorities and
11. shall be fully complied with BFIU Circular # 28, dated: May 30, 2023 issued and to be issued by BFIU and other prevailing and or future laws and regulations relating to AML/CFT.

Each employee of DBH shall have to understand and comply with the AML/CFT Guidelines and a declaration to that effect must be obtained from them that they understand and are fully aware of the Prevention of Money Laundering and Combating Terrorist Financing.

In case of any conflict between this AML/CFT policy and the Money Laundering Prevention Act, 2012 and Anti-Terrorism Act, 2009, the Original Act, Regulations; and Circulars, Directive etc. of BFIU shall prevail.

Contents

Part-A: Prevention of Money Laundering

Chapter 1: Introduction

Money laundering is the generic term used to describe the process by which criminals try to disguise the original ownership and control of the proceeds of criminal conduct by making them appear legal. The processes by which criminally derived property may be laundered are extensive. Though criminal money may be successfully laundered without the assistance of the financial sector, the reality is that hundreds of billions of dollars of criminally derived money is laundered through financial institutions, every year. The nature of the services and products offered by the financial services industry carries the inherent risk of being abused by money launderers.

The act of laundering is committed in circumstances where a person is engaged in an arrangement of providing a service or product and that arrangement involves the proceeds of crime. These arrangements include a wide variety of business relationships e.g. banking, fiduciary and investment management.

The requisite degree of knowledge or suspicion will depend upon the specific offence but will usually be present where the person providing the arrangement, service or product; knows, suspects or has reasonable grounds to suspect that the property involved in the arrangement represents the proceeds of crime. In some cases, the offence may also be committed where a person knows or suspects that the person with whom he or she is dealing is engaged in or has benefited from criminal conduct.

It happens in almost every country in the world, and a single scheme typically involves transferring money through several countries in order to obscure its origins and the rise of global financial markets makes money laundering easier than ever, making it possible to anonymously deposit "dirty" money in one country and then have it transferred to any other country for use.

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

The process of money laundering and terrorist financing (ML/TF) is very cumbersome. The money launderers always try to invent more and more complicated and sophisticated procedures by using newer technology for money laundering. To address these challenges, the global community has taken various initiatives against ML/TF.

1.1 Defining money laundering

International perspective

Money laundering can be defined in a number of 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) and the United Nations Convention Against Transnational Organized Crime (2000) (Palermo Convention) as follows:

I. The conversion or transfer of property, knowing that such property is derived from any 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;
II. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;
III. 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.

FATF definition

The Financial Action Task Force (FATF), the recognized international body for setting standard for anti-money laundering efforts, defines money laundering as the processing of criminal proceeds to disguise their illegal origin in order to legitimize the ill-gotten gains of crime.

National legal framework

Section 2 (v) of the Money Laundering Prevention Act, 2012 defined ML as follows:

i. knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes: -
    a. concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
    b. assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
ii. smuggling money or property earned through legal or illegal means to a foreign country;
iii. knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or
iv. concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
v. converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
vi. acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
vii. performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
viii. participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above.

1.2 Purpose of money laundering

The purpose of money laundering is to cease the connections between the money and the crime from which ill money has been generated. In other words, money laundering disguises or conceals the illicit origin of money generated through criminal activities.

Launderers engaged themselves in money laundering for 4(four) main reasons:

i. to organize and run criminal activity using financial channel to get financial benefit;
ii. to conceal or disguise the source of their wealth to avoid prosecution;
iii. to cover ill-gotten gains from suspicion and protect them from seizure; and
iv. to conceal their existence or alternatively, give them a legitimate look.

1.3 Stages of money laundering

The money laundering cycle includes three distinct stages as follows:

1.3.1 The placement stage

The placement stage represents the initial entry of the "dirty cash" or proceeds of crime into the financial system. Generally, this stage serves two purposes: (a) it relieves the criminal of holding and guarding large amounts of bulky of cash; and (b) it places the money into the legitimate financial system. It is during the placement stage that money launderers are the most vulnerable for being caught. This is due to the fact that placing large amounts of money (cash) into the legitimate financial system may raise suspicions amongst officials.

The placement of the proceeds of crime can be done in a number of ways. Some common methods include:

i. Loan repayment: Repayment of loans or credit cards with illegal proceeds;
ii. Currency smuggling: The physical movement of illegal currency or monetary instruments over the border;
iii. Currency exchanges: Purchasing foreign money with illegal funds through foreign currency exchanges;
iv. Blending funds: Using legitimate cash from legal business to mix dirty funds with the day's legitimate sales receipts;
v. Gambling: Purchase of gambling chips or placing bets on sporting events; etc.

1.3.2 The layering stage

After placement comes the layering stage (sometimes called as structuring). The layering stage is the most complex and often entails the international movement of the funds. The primary purpose of this stage is to separate the illicit money from its source. This is done by the sophisticated layering of financial transactions that obscure the audit trail and break the link with the original crime.

During this stage, for example, the money launderers may begin by moving funds electronically from one country to another, then divide them into investments placed in advanced financial options or overseas

markets; constantly moving them to elude detection; each time, exploiting loopholes or discrepancies in legislation and taking advantage of delays in judicial or police cooperation.

1.3.3 The integration stage

The final stage of the money laundering process is termed as the integration stage. In this stage the ill-gotten money has been reverted from the criminal sources to be legitimate sources. Having been placed initially as cash and layered through a number of financial transactions, the criminal proceeds are now fully integrated into the financial system and can be used for any purpose.

There are many different ways in which the laundered money can be integrated back with the criminal; however, the major objective at this stage is to reunite the money with the criminal in a manner that does not draw attention and appears to result from a legitimate source. For example, the purchases of property, art work, jewelry, or high-end automobiles are common ways for the launderer to enjoy their illegal profits without drawing attention to legal authorities.

1.4 Money laundering predicate offenses

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

a) corruption and bribery;
b) counterfeiting currency;
c) counterfeiting deeds and documents;
d) extortion;
e) fraud;
f) forgery;
g) illegal trade of firearms;
h) illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;
i) illegal trade in stolen and other goods;
j) kidnapping, illegal restraint and hostage taking;
k) murder, grievous physical injury;
l) trafficking of woman and children;
m) black marketing;
n) smuggling of domestic and foreign currency;
o) theft or robbery or dacoity or piracy or hijacking of aircraft;
p) মানব পাচার বা কোন ব্যাক্তি কে বৈদেশিক কর্মসংস্থানের মিথ্যা আশ্বাস প্রদান করিয়া কোন অর্থ বা মূল্যবান দ্রব্য গ্রহণ করা বা করিবার চেষ্টা
q) dowry;
r) smuggling and offences related to customs and excise duties;
s) tax related offences;
t) infringement of intellectual property rights;
u) terrorism or financing in terrorist activity;
v) adulteration or the manufacture of goods through infringement of title;
w) offences relating to the environment;

x) sexual exploitation;

y) 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;

z) organized crime, and participation in organized criminal groups;

aa) racketeering; and

bb) any other offence declared as predicate offence by Bangladesh Financial Intelligence Unit (BFIU) with the approval of the Government, by notification in the Official Gazette, for the purpose of this Act.

1.5 Reporting organizations:

i. Banks;

ii. financial Institutions;

iii. insurer;

iv. money changer;

v. any company or institution which remits or transfers money or money value;

vi. any other Institution carrying out its business with the approval of Bangladesh Financial Intelligence Unit (BFIU);

vii.
   a. stock dealer and stock broker;
   b. portfolio manager and merchant banker;
   c. securities custodian;
   d. asset Manager;

viii.
   a. non-profit organization;
   b. non-government organization;
   c. cooperative society;

ix. real estate developer;

x. dealer in precious metals or stones;

xi. trust and company service provider;

xii. lawyer, notary, other legal professional and accountant; and

xiii. any other institution which BFIU may, from time to time, notify with the approval of the Government.

1.6 Scope and objective of the guidelines

This policy is applicable for all sorts of transactions, products, operations and other relevant activities of DBH including branch/es. The Company would ensure compliance with this AML/CFT Guidelines or as prescribed by law and/or the Bangladesh Financial Intelligence Unit (BFIU) circulars, directives etc. issued from time to time whichever more exhaustive.

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

The overall framework for AML/CFT regime designed in DBH so that the business units and other concerned will take responsibility for:

i. verifying true identity of customers prior to provide any service;

ii. reporting all STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU);
iii. keeping appropriate records at least for 5(five) years as determined by BFIU;
iv. providing, from time to time, information as required by BFIU and other regulatory authorities; and
v. developing, implementing and complying with all AML/CFT related legal requirements.

1.7 How to combat money laundering

Money laundering potentially devastates the economy, social security and safety. ML is a process of making crime worthwhile. It provides fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal initiatives. ML diminishes government tax revenue and therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. In order to preventing ML, DBH should always pay particular attention to the fundamental principle of good business practice i.e. Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Know Your Customer (KYC) and Know Your Employee (KYE). Having a sound knowledge of a customer's business or occupation and pattern of financial transactions and commitments-are the best methods by which DBH and its officials will try to recognize and protect ML/TF.

Chapter 2: Vulnerabilities of DBH

Money launderer may use different financial products like lease, loans, and deposit schemes etc. to launder their ill-gotten money. Possible ways of laundering mechanism of ill money through use of DBH's products or services are discussed as under:

Vulnerabilities of products and services

a) Housing/term loan finance

Money launderers can use this instrument for placement and layering of their ill- gotten money. Borrower can take lease/term loan finance from DBH and repay the loan from money earned through illegal sources, and thus bring illegal money enter into the formal financial system in absence of proper measures. The borrower can also repay the loan amount even before maturity period. In case of home loan, the asset purchased using DBH's finance can be sold immediately after repayment of the loan using dirty money and sold proceeds can be shown as legal.

b) Personal loan/car loan

A person can take personal loan from DBH and repay it by illegally earned money; thus s/he can launder money and bring it in the formal channel. Similarly, after taking personal loan or car loan, money launderers can repay those with their illegally earned money, and later by selling that asset, they can show the proceeds as legal money.

c) Deposit schemes

DBH collects deposit from customers for different maturity period but for not less than 3(three) month's tenure. Customers may take premature encashment of their deposit money with due approval from the competent authority. Moreover, Loan against Deposit (LAD) can be taken by the money launderer to show the money as a legitimate one. Thus, deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong surveillance.

Chapter 3: Mitigation process - ML/TF risk assessment

3.1 Introducing risk base approach

The risk-based approach is an essential component of the effective implementation of the FATF Recommendations. Government, competent authorities, financial institutions, designated non-financial business and professions (DNFBPs) and other reporting entities are sole responsible to understand, identify, assess, and take effective action to mitigate ML/TF risks.

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

i. compares the customer's account/transaction history to the customer's specific profile information and a relevant peer group, and/or examine the customer's account/transaction history against established ML criteria/scenarios, in order to identify patterns of suspicious activity or anomalies;
ii. establish a process to compare customer or transaction-specific data against risk-scoring models;
iii. be capable of recognizing patterns and of "learning" which transactions are normal for a customer, rather than designating certain transactions as unusual (for example, not all large transaction is unusual and may easily be explained); issue alerts if unusual transactions are identified;
iv. track alerts in order to ensure they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required; and
v. maintains an audit trail for inspection by the institution's audit function and by financial institutions supervisors.

These will help in design and implementation of this approach for mitigating ML/TF risks.

3.2 Assessing risks

DBH should be required to take appropriate steps to identify and assess ML/TF risk arisen from or through customers, products or services and transactions or delivery channels and geographical presence. DBH should document assessment result in order to be able to demonstrate their basis, keep assessment result up-to-date and provide assessment result to the competent authority.

3.3 Risk management and mitigation

Risk management is a systematic process of recognizing risk and developing both minimize and manage the risk. To mitigate the vulnerabilities of ML/TF risks, DBH should require to establish policies, controls and procedures that enable to manage and mitigate the risks that have been identified in assessment process. DBH also requires to monitor the implementation of those controls and to enforce more stringent policy, if necessary. The mitigation policies, controls and procedures must be approved by senior management.

3.4 Risk Management framework

A risk management framework consists of establishing the internal and external context within which the designated service is to be provided, risk identification, risk assessment or evaluation and risk treatment-mitigating, managing, control, monitoring and periodic reviews. A risk management framework is briefly stated in a tabular form as follows:

Stage-1: Risk identification

Identification of main ML/TF risks	Customer
	Product
	Sector
	Delivery Method
	Country/Jurisdiction
Identification of regulatory risks	Failure to report STR/SAR/CTR
	Inappropriate customer verification
	Inappropriate record keeping
	Lack of AML/CFT program

Stage-2: Risk assessment

Measure the size and importance of the risk	Likelihood-Chance of the risk happening
	Impact-The amount of loss or damage on risk
	Likelihood X Impact-Level of risk (risk score)

Stage-3: Risk treatment

Manage business risk	Minimize and manage risks
	Apply strategies, policies and procedures
Manage regulatory risk	Put in place system and controls
	Carry out risk plan and AML/CFT program

Stage-4: Risk monitoring and review

Monitor and review risk plan	Develop and carry out monitoring process
	Keep necessary records
	Review risk plan and AML/CFT program
	Execution internal audit or assessment
	Preparation AML/CFT compliance report

Recently Bangladesh Financial Intelligence Unit (BFIU) issued a Circular Letter No. 04: dated July 30, 2015 on Money Laundering and Terrorist Financing Risk Assessment Guidelines for Financial Institutions.

DBH on the basis of the above Guidelines assessed its risks with due approval from the Managing Director. The assessed score as per risk scoring matrix is attached at “Annexure-A” in this guideline as per Circular Letter#04, dated July 30, 2015 of BFIU. The risk score shall be reviewed after regular intervals depending on the changed business scenario.

Chapter 4: Customer identification and verification

A meaningful anti-money laundering compliance program should include identification and verification of customers at the stage of opening account or establishing financial transaction or relationship. Accordingly, the Company should ensure to:

a. verify the identity of any person/individual concern/company (hereinafter called as "customer") while pursuing to open an account to the extent reasonable and practicable;
b. maintain records of the information used to verify a customer's identity, including name, address and other identifying information; and
c. verify the UNSCR list (1267/1999 and 1373/2001), banned list of Bangladesh Government of known or suspected terrorists or terrorist organizations or other national or international sanction lists using DBH's own software to determine whether a person pursuing to open an account appears on any such lists.
d. Comply with foreign exchange regulation act 1947, while opening any FDR account in the name of a foreigner or non-resident Bangladeshis.

The following options are recommended for concerned officers of Head Office as well as branch/es to consider in developing customer identification process:

4.1 Customer identification

DBH should not keep anonymous or accounts in fictitious name/s. Company should undertake customer due diligence measures, including identifying and verifying the identity of their customers when:

a. establishing business relations;
b. carrying out occasional transactions;
c. there is a suspicion of money laundering or terrorist financing; and
d. the financial institution has doubts about the reliability or adequacy of previously obtained customer identification data.

In order to fulfill identification requirements DBH should, where necessary, take measures to:

i. verify the legal existence and structure of the entity by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity, as the case may be;
ii. verify that any person purporting to act on behalf of the customer is so authorized and identify that person;
iii. no account should be opened without satisfactory identification, and proper introduction, where applicable. In fact, before opening an account concerned officer should interview the customer to assess his need for opening an account, his business, engagement etc.;
iv. customer's residence (permanent and present) or place of business to be carefully considered. If it is not in the area where DBH or branch serves, in that case opening an account at that location may need to be justified;

v. the source of funds used to open the account shall be known and commensurate with the account opener's details.

4.2 Customer profiling

i. obtaining and documenting the customer's basic background and information;
ii. use that information to evaluate the appropriateness and reasonableness of the customer's transaction activity;
iii. the customer's expected transaction trends;
iv. net income; and
v. determine the source of the customer's funds.

4.3 Review of KYC profile

KYC shall be reviewed on a regular interval i.e. in case of high-risk customer at least once in a year and in case of low risk customer once in every two years for:

a. monitoring transactions and activities; or
b. renewal of an account; or
c. customer visited DBH; or
d. any change in introductory information of customer;
e. periodic discussions with the customer relating to their business activities or future plan of the business; or
f. any other activities as deemed necessary.

4.4 Taking special care

Responsible officer of loans & advances department should monitor customer's borrowing profile in the course of business to ascertain repayments or settlement of loan or loan drawdown is in line with the customer business activities. They shall also take special care on the following cases:

i. on high risk customer;
ii. in case of deposit of significant amount which inconsistent with customer profile; and
iii. deposit of funds into company's accounts, usually in amounts below the threshold limit set by Bangladesh Financial Intelligence Unit (BFIU).

4.5 Monitor inconsistent transactions with customer's business/personal profile

Responsible officer shall closely monitor the customer's account in case:

i. where they make payments in cash rather than using banking channel;
ii. operate retail business but made substantial payments against loan which indicates that the customer may have another undisclosed source of income; and
iii. deposit of large volume of cash which does not match with the customer's business profile.

4.6 Preserving customers records

DBH should preserve all necessary records of transactions as per Bangladesh Financial Intelligence Unit (BFIU) circular in force and such records must be sufficient to evidence for prosecution for criminal behavior. They should also keep records on customer identification e.g. NID, passport copy, identity card, driving license or any other documents acceptable to the Company, account files and business correspondence for a minimum of 5(five) years even after the account is closed as advised BFIU. These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

Chapter 5: Know your customer (KYC), customer due diligence (CDD) and enhanced due diligence (EDD)

Generally, Know Your Customer (KYC) policy is implementing to confirm a customer's identification program. The term is also used to refer to the regulation which governs these activities. KYC is mostly used in financial institutions and other reporting authorities as defined by the regulators. They use KYC to identify customers and ascertain relevant information in doing business/relationship with them. In wider terms, KYC processes are also employed by companies of all sizes for the purpose of ensuring AML/CFT compliances. KYC policies are becoming much more important globally to protect financial fraud, money laundering, terrorist financing etc.

Generally, DBH should never establish a relationship with a customer until it knows the customer's true identity. If a potential customer is unwilling to provide necessary information and documents, the relationship should not be established.

5.1 Benefits of introducing KYC

KYC-

a. helps detect suspicious activity in a timely manner;
b. promotes compliance with all relevant laws;
c. promotes safe and sound financial transactions and best business practices;
d. minimizes the risk that the Company may encounter for illicit activities;
e. reduces the risk of government seizure and forfeiture of a customer's loan collateral when they are involved in criminal activities or ML/TF issues, and
f. protects Company's reputational risk.

5.2 KYC procedures

a. Before opening an account, due diligence is required to be performed on all prospective customers. This process should be completed by fulfilling the documentation requirements (duly filled in application form, references, source of funds, applicable identities etc.) with a Know Your Customer (KYC) profile which is used to record a customer's source of fund, expected transaction activity at its most basic level.
b. Once the identification procedures are completed and relationship with the customer is established, DBH should monitor behavior of customers to ensure that it is consistent with the nature of business as was stated while establishing relationship/opened account. Concerned officer will be responsible for reporting suspicious transactions undertaken by the customer, review & updating customer's KYC profile for any significant changes in their lifestyle (e.g., change of employment status, increase in net worth etc.) and by monitoring the transaction activity over the customer's account on a periodic basis.
c. KYC profile must contain the basic information about the customer like name, address, tel/cell/fax numbers, e-mail address, line of business, annual sales and other relevant information. If the customer is a PEPs/IPs, the account is to be taken special care and requisite EDD should be done.
d. The KYC profile information will also include the observations of the concerned officer of Head Office or branch/es regarding business premises (whether rented or owned), type of customer's business, method

of transaction preferred by the customer (whether in cheque or cash). The concerned officer will record those observations and put signature on the KYC form.

e. The KYC profile leads to risk classification of the accounts as high/low risk.

5.3 Risk categorization on the basis of KYC

While opening accounts, the concerned officer must assess the inherent risks that the accounts might carry relating to "Money Laundering", and must classify the accounts as either "High Risk" or "Low Risk". The risk assessment may be made using the Risk Grading Matrix given at "Annexure-B" by which risk shall be categorized using numeric scale to denote risks.

5.4 Components of KYC

KYC should be the core feature of DBH'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.
e) As instructed by BFIU, DBH Shall implement Electronic Know your Customer (e-KYC)

5.5 Customer acceptance policy

Selection of customer is an important factor for Banks and NBFIs. DBH takes into consideration of all the relevant factors in case of opening/operating customer's accounts such as customer's background, business/personal activities, business risks, credit worthiness, political influence, social status, other basic information and other risk factors.

On the other hand, to prevent of ML/TF risks KYC, CDD, EDD, KYE are the important tools. Lack of precaution in the above-mentioned factors might result in serious customer and counterparty risks, especially reputation, operational, legal and compliance risks. Collection of sufficient information about the customer is the most effective defense for combating ML/TF activities. As per Money Laundering Prevention (Amendment) Act, 2015 each FI is required to keep satisfactory record of the customers. On the other hand, each FI is also required to make necessary arrangement to prevent transactions related to crimes as described in Anti-Terrorism (Amendment) Act, 2013. It also requires identifying, under these laws, suspicious transactions/activity with due care and diligence.

5.6 Monitoring of high-risk accounts and identification of suspicious transactions

High value single transaction conducted in a single DD, PO, TT and Electronic Transfer by any person or institution involved in a financial transaction may pose reputational and other risks to DBH. 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 transaction.

5.7 What does customer mean

As per Section – 2(j) of Money Laundering Prevention Act, 2012:
"Customer" means any person or persons or entity or entities that may be defined by Bangladesh Financial Intelligence Unit from time to time.

For the purpose of KYC procedure, a "Customer" means as per Circular # 28, dated May 30, 2023:

i. any person or institution maintaining an account of any type with DBH;
ii. the person or institution as true beneficial owner in whose favor the account is operated; and
iii. 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.

5.8 What constitutes a customer's identity

Identity generally means a set of attributes which uniquely defines a natural or legal person. There are two main constituents of a person's identity out of a range of legal persons (an individual, corporate body, partnership, etc.). For the purposes of this guidance, the two constituents are:

i. the physical identity (e.g. birth certificate, TIN/VAT registration, passport/NID, driving license etc.); and
ii. the activity undertaken.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Information of both residential and nationality status of a customer are also necessary tools of identity. 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.

5.9 KYC for individual customers

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

a. correct name and/or names used;
b. parent's names;
c. date of birth;
d. current and permanent address;
e. details of occupation/employment and sources of wealth or income; and
f. contact information, such as – mobile/telephone number etc.
g. Unique customer identification code (UCIC) to be allocated for each account holder , regardless of th e number of accounts maintained in the name of the account holder.

5.10 The following points should always bear in mind by responsible officer

The following points should always be borne in mind by a responsible officer while opening an account or making financial transaction with any prospective customer:

a. DBH shall not allow any non-face to face contact;
b. DBH shall determine the actual Beneficial Owner of each account in line with the guidelines issued by BFIU and preserve the information of that actual beneficial owner;
c. If any person is authorized to operate account with DBH on behalf of actual beneficial owner, then detailed and accurate information of that authorized person is to collected;
d. In case of company account, information of the beneficial owners who have controlling interest in the company is to be preserved;
e. In applicable cases, detailed and accurate information of Managing Director/ Chief Executive Officer of the company is to be preserved;
f. particular care should be taken in accepting documents/identities which are easily be made false or duplicate;
g. in respect of joint accounts where the surname and/or address of the account holders differ,
h. the name and address of all account holders should be verified;
i. any subsequent change of the customer's name, address, or employment details of which the DBH becomes aware should be recorded as part of the KYC process for review customer's profile;
j. all documents collected for establishing relationship must be filled in with supporting evidences;
k. details of the introducer 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;
l. 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 regulatory or regulated institution, a notary public, a member of the judiciary or a senior civil servant may be acceptable to DBH in this behalf. The Certifier must sign on the copied document and clearly indicate his position or capacity on it with a contact address and phone number;
m. the normal identification procedures set out above should be followed. Moreover, in case of minor parents/legal guardians KYC procedure must be followed;
n. documents of identity which do not bear photographs or signatures are not acceptable. More importantly, checking of authenticity of the documents is a must;
o. to verify the customer's permanent and present address passport/NID and recent utility bill's copy can be checked; and last but not least;
p. the original copy of (i) current valid passport; (ii) valid driving license; (iii) NID; (iv) employer provided ID card, bearing the photograph and signature of the applicant should be used to verify identify the customer and certified copies of the same should be procured and preserved for record.

5.11 KYC for corporate and other entities

The principal requirement for the corporate bodies is to verify its legal existence and find out person behind the entity to identify who are controlling business and the Company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the day to day affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose.

The following documents should be obtained from companies;

a. certificate of incorporation or duly certified by RJSC, address of the registered office, and place of business;
b. certified copy of Memorandum and Articles of Association, or by-laws of the customer;
c. copy of the board resolution to open account/maintain relationship with delegation of authority/ies to operate accounts;
d. explanation of the nature of the applicant's business, the source of funds, and a copy of the last available financial statements, where applicable;
e. satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 20.00% interest or more or with principal control over the Company's assets and any person/s 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;
f. 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;
g. copies of the Schedule X and Form XII; and
h. any other relevant documents require establishing relationship/financial transaction.

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 for the above case:

a. all of the directors who will be responsible for operation of the account;
b. all the authorized signatories for the account/transaction;
c. all the holders of powers of attorney to operate the account/transaction;
d. the beneficial owner(s) of the company, where applicable; etc.

Where the institution already knows their identities and identification records comply 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 for verification.

5.12 KYC for corporate registered abroad

Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such 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.

5.13 KYC for partnerships and other entities

In the case of partnerships and businesses of other entities whose partners/directors are not known to DBH, 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.

5.14 Powers of attorney/mandates to operate accounts

Confirm the identities of holder of power of attorney/mandate or the guarantor of any customer's account and must be supported with the resolution or valid deed, as the case may be. The records of all transactions undertaken in accordance with a power of attorney/mandate should be done with due care and record should be kept safely.

5.15 Transaction monitoring process

The nature of this monitoring will depend on the nature of customer's business. The purpose of monitoring of customer's business is to identify any significant changes or inconsistencies in the pattern of transactions. Possible areas to monitor could be:

i. transaction type;
ii. frequency of transaction;
iii. unusual large transaction;
iv. geographical origin/destination of transaction;
v. changes in authorized signatories;
vi. borrower settling "problem" loans by large amounts of cash suddenly with no reasonable explanation of funds/source; etc.

5.16 What to do if customer due diligence (CDD) will not possible

In case where CDD cannot be done due to non-cooperation by the customer and/or if the information provided is found uncertain/suspicious after assessment, DBH may take the following actions:

i. DBH shall not open account of such customer or may close existing account, if appropriate; and
ii. before closure of such accounts, approval from top management is necessary and the account holder shall be informed via notice detailing the reason behind such closure of account.
iii. iii. BAMLCO shall forward the necessary information of such accounts to Central Compliance Unit (CCU).
iv. Central Compliance Unit (CCU) may report STR to BFIU, if there is reasonable ground to do so.

STR/SAR may be proceeded to Bangladesh Financial Intelligence Unit (BFIU) when there is a reasonable ground to do so.

A standard KYC format has been attached at "Annexure-C" with the guidelines which have been prepared on the basis of template provided by BFIU towards introduction of Uniform Account Opening Form for FIs.

5.17 Politically exposed persons (PEPs) and influential persons (IPs)

5.17.1 Who are PEPs

As per BFIU Circular # 28, dated May 30, 2023 issued by Bangladesh Financial Intelligence Unit (BFIU) PEPs means: Individuals who are or have been entrusted with prominent public functions by a foreign country- i.e.

(i) heads of state or of government (ii) senior politicians (iii) senior government (iv) judicial or military officials (v) senior executives of state-owned corporations and (vi) important political party officials.

5.17.2 Who are IPs

As per Circular # 28, dated May 30, 2023 issued by Bangladesh Financial Intelligence Unit (BFIU) IPs means: Individuals who are or have been entrusted domestically with prominent public functions - i.e. (i) heads of state or of government (ii) senior politicians (iii) senior government officials (iv) judicial or military officials (v) senior executives of state-owned corporations and (vi) important political party officials.

5.18 Enhance due diligence (EDD) in case of PEPs, IPs and other relevant customers

5.18.1 Responsibilities in case of "politically exposed persons (PEPs)":

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):

i. takes reasonable measures to establish the source of wealth and source of funds;
ii. ongoing monitoring of the transactions has to be conducted; and
iii. the Account Opening Officer should observe all formalities as detailed in Foreign Exchange Regulation Act-1947 (as amended in 2015) while opening accounts of non-residents.
iv. Additional information is to be obtained from independent and reliable source;
v. Further steps to be taken to identify the purpose of opening account;
vi. In applicable cases, the approval of Chief Anti- Money Laundering Compliance Officer (CAMLCO) has to be obtained before opening such account;

In case where assessed risk is low simple CDD will be sufficient; but in case of high risk EDD shall have to apply in relationship to the PEPs. Bangladesh Financial Intelligence Unit (BFIU) through BFIU Circular # 28, dated May 30, 2023 clearly instructed to do EDD in case of PEPs.

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 DBH.

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

i. a risk management system shall have to be introduced to identify risks associated with the opening and operating accounts of PEPs;
ii. obtain senior management approval for establishing business relationships with such customers;
iii. take reasonable measures to establish the source of wealth and source of funds;
iv. ongoing monitoring of the transactions have to be conducted; and
v. DBH should observe all formalities as detailed in Foreign Exchange Regulation Act-1947 while opening accounts of non-residents, if any.
vi. a risk management system shall have to be introduced to identify the true beneficiary of such account and identify the risks associated with the opening and operating accounts of PEPs;

vii. obtain approval of Chief Anti-Money Laundering Compliance Officer (CAMLCO) for establishing business relationships with such customers;

viii. Same procedure are to be conducted in case of opening and operating accounts of close associates of PEPs;

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.

5.18.2 Responsibilities in case of "influential persons (IPs)":

DBH should identify the true underlying beneficiaries against the account and/or customer. While opening and/or operating or maintaining financial relationship with such persons, concerned employee should follow the instructions as cited from point 'ii' to 'iv' at para 5.18.1
Instructions appropriate for Influential persons shall also be applicable for close associates.
No middle ranking or junior individuals shall be deemed as "Influential Person" as quoted in this paragraph.

5.18.3 Responsibilities in case of head of any international organization or high-level officers:

DBH must identify whether the account and/or customer 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, DBH have to follow the instructions as cited from point 'ii' to 'iv' at para 5.18.1 and instructions as at 'v' 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.
"Head of International Organization or High-Level Officers" shall mean persons who are or have been entrusted with a prominent function by an international organization and shall include 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 junior individuals shall be deemed as "Head of International Organization or High-Level Officers" as quoted in this paragraph.

5.19 Ongoing monitoring of accounts and transactions

Effective internal control system may reduce the risk if relationship managers have an understanding of 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 have to 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 of higher risk accounts. DBH 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 DBH 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 DBH 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.

DBH has developed clear standards on what records must be kept for customer identification and individual transactions and their retention period. As the starting point and natural follow-up of the identification process, DBH should obtain customer identification papers and retain copies of them for at least 5(five) years after an account is closed.

Chapter 6: 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. For appropriate management of KYE 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. 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 format has been attached herewith at "Annexure-D".

Chapter 7: Compliance requirement of DBH against ML/TF

The compliance requirements of FIs have been specified in BFIU Circular # 28, dated: May 30, 2023 by Bangladesh Financial Intelligence Unit (BFIU). In this regard, Money Laundering Prevention Act, 2012 and Anti-Terrorism Act, 2009 and to be amended from time to time should also to be followed meticulously. The compliance requirement shall be documented and communicated to all levels of the employees of DBH to develop awareness against ML/TF and to prevent ML and combat TF. As part of its AML/CFT policy, CCU with assistance of the top management shall communicate clearly to all employees on annual basis through a statement from the Managing Director stating DBH's position against ML/TF and criminal activities.

A. Domestic requirement

7.1 Compliance requirement under domestic law

According to section 25(1) of Money Laundering Prevention Act, 2012 the responsibilities and other obligations prescribed by law of DBH in prevention of money laundering are: -

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

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

c) to provide with the information maintained under clauses (a) and (b) to Bangladesh Financial Intelligence Unit (BFIU) from time to time, on its demand;

d) if there be any doubtful transaction or attempt of such transaction as defined under clause (z) of section 2 of Money Laundering Prevention (Amendment) Act, 2015 the matter shall be reported as "suspicious transaction report" to the BFIU immediately on its own accord.

7.2 Board approved guidelines for preventing ML and combating TF

In pursuance of section 16(2) of Anti-Terrorism Act, 2009, and Bangladesh Financial Intelligence Unit (BFIU)'s circular # 28, dated: May 30, 2023, all FIs must have their own policy manual duly approved by their Board of Directors/topmost committee to prevent ML and combat TF. This policy manual must be in conformity with international standard and laws and regulations in force in Bangladesh and circulars issued by BFIU from time to time. The guidelines shall be circulated among all the concerned employees for information and necessary action to prevent ML and combat TF. FIs shall from time-to-time review and confirm meticulous compliance of the circulars issued by BFIU or Government through official gazette.

7.3 Appointment of CAMLCO, DCAMLCO and BAMLCO

To implement the policy manual and compliance of instructions of Bangladesh Financial Intelligence Unit (BFIU), DBH should:

i. designates one high level officer as Chief Anti-Money Laundering Compliance Officer (CAMLCO) and a senior level officer as DCAMLCO in the Central Compliance Unit (CCU); and

ii. designate one officer as Branch Anti-Money Laundering Compliance Officer (BAMLCO) at branch level.
iii. Detailed information of CAMLCO and DCAMLCO is to be forwarded to BFIU at the month of January of each year attaching enclosure (Annexure-KA) of the BFIU circular 28 of 30 May 2023.

7.4 Customer identification

DBH should mandatorily collect complete information and identification of customers and verify their correctness to keep themselves free from ML/TF risks. As per BFIU circular#28/2023, a customer is defined as:

i. any person or institution maintaining an account of any type with a FIs or having business relationship with FIs;
ii. the person or institution as true beneficial owner in whose favor the account is operated;
iii. 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;

7.5 Other measures

The following measures also to be taken under compliance requirement against ML/TF:

a) how to conduct CDD/EDD at different stages like- while establishing relationship with the customer or conducting financial transaction with the existing customer;
b) to be sure about the customer's identity through collection of adequate information towards satisfaction of the concerned employee i.e. doing CDD;
c) to be satisfied while operating any account by a person on behalf of the customer that the person has due authorization to operate the account and, in this case, correct and complete information of the person must be collected before opening/operating such account or transaction;
d) legal status and accuracy of information of the account's operator/s are shall be ascertained while any account is to operate by trustee and professional intermediaries i.e. lawyers/law firm, chartered accountants, etc.;
e) enhanced due diligence (EDD) shall have to be ensured with a person of the countries and territories that do not meet international standard in preventing ML/TF i.e. countries and territories listed as high-risk country in FATF's public statements while establishing and maintaining business relationship and conducting financial transaction;
f) in case of beneficial owner (i.e. the customer has controlling share of a company or/and holds 20.00% or more shares of a company) of an account, DBH shall have to collect and ensure:
    i. complete and correct information of identity of the persons besides the customer;
    ii. controller or the owner of the customer; and
    iii. complete and correct information of identity of the beneficial owners shall have to be collected and preserved.

7.6 What to do in case of PEPs and IPs while opening and/or operating account

While opening and/or operating account or at the time of financial transaction of PEPs/IPs, EDD shall have to be exercised. Following instructions shall have to be followed to ensure EDD:

i. DBH shall identify risks associated for opening and operating such accounts of PEPs/IPs;
ii. take reasonable measures to ensure source of wealth and source of funds;
iii. ongoing transactions monitoring process shall have to be done by the concerned officer; and
iv. all formalities shall have to be complied as per Foreign Exchange Regulation Act-1947 (as amended in 2015) while opening and operating accounts of non-resident PEPs/IPs;
v. KYC shall be reviewed on a regular interval basis or at least once in a year etc.

All instructions as detailed for PEPs/IPs shall be equally applicable if business relationship is established with family members and close associates of these persons who may pose reputational risk to DBH. The above instructions shall also be applicable to customers or beneficial owners who become PEPs/IPs after business relationship have been established.

7.7 Appointment and training

7.7.1 Employee screening

To prevent ML and combat TF, DBH shall have to undertake proper screening mechanism in appointment procedures so that ML/TF risks could be avoided.

7.7.2 Employee training

To ensure proper compliance of ML/TF activities of DBH shall arrange suitable in-house or outdoor training of officials on preventing of ML and combating TF. To ensure compliance with ML/TF related issues, DBH shall arrange suitable in-house or outdoor training program for all officials including CAMLCO and DCAMLCO. In this connection, all supporting documents including training materials are to be preserved.

7.8 Awareness of customers regarding ML/TF

At the time of opening or operating an account and/or doing KYC, concerned officer shall explain to the customers the reasons and/or grounds for asking documents or identities. The concerned officer shall also respond to the customer's query, if any. The Management of DBH may distribute leaflets among customers to make them aware of ML/TF and also arrange to stick posters in visible place at Head Office or every branch. DBH also requires to display trailer, documentary etc. in public or other media to make awareness under Corporate Social Responsibility with due approval of the competent authority.

7.9 Suspicious transaction report (STR)/suspicious activity report (SAR)

According to the provision of section 25(1)(d) of Money Laundering Prevention Act, 2012 (as amended in 2015) and section 2(16) of Anti-Terrorism Act, 2009 (as amended in 2013), DBH requires to submit report proactively and immediately to Bangladesh Financial Intelligence Unit (BFIU) on suspicious, unusual or doubtful transactions/activity report relating to ML/TF. (More details are in Chapter-10).

7.10 Cash transaction report (CTR)

According to the provision of BFIU Circular # 12, dated May 30, 2023, DBH requires to submit CTR to Bangladesh Financial Intelligence Unit (BFIU) on monthly basis on or before 21st of the next month using goAML software on doubtful cash transactions, if any, relating to ML/TF. (More details are in Chapter-11).

7.11 Procedure of self-assessment report

This policy requires that appropriate and timely self-assessments, tests, audits and evaluations shall be conducted to ensure that the DBH is in compliance with the regulations. Each and every branch shall assess their performance through self-assessment report on half yearly basis according to Circular # 28 dated: May 30, 2023 of the Bangladesh Financial Intelligence Unit (BFIU). This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The SAR should conclude with a report documenting the work performed, how it has been controlled/supervised and the resulting findings, conclusions and recommendations. The SAR should advise management whether the internal procedures and statutory obligations of DBH have been properly discharged. Each branch will assess its AML/CFT activities covering the following areas on half yearly basis and submit the report to CCU and ICC within next 15 (fifteen) days of each half year end:

i. the percentage of officers/employees that received official training on AML/CFT;
ii. the awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and BFIU's instructions, circulars and guidelines;
iii. the arrangement of AML/CFT related meeting on regular interval;
iv. the effectiveness of the customer identification during opening an individual, corporate and other account;
v. the risk categorization of customers by the branch;
vi. regular update of customer profile upon reassessment;
vii. the monitoring of customers' transactions;
viii. identification of Suspicious Transaction Reports/Suspicious Activity Report (STRs/SARs);
ix. the maintenance of a separate file containing MLPA, circulars, training records, reports and other ML related documents and distribution of those among all employees;
x. the measures taken by the branch during opening of account of PEPs/IPs;
xi. consideration of UNSCR 1267 and 1373 while conducting any business; and
xii. the compliance with AML/CFT weaknesses/irregularities, as the CCU/ICC of Head Office and BFIU"s inspection report mentioned.

Each branch will assess its AML/CFT activities on half yearly basis as per prescribed format (Annexure GA) issued by BFIU (Annexure – E of this policy). Branch Manager will hold meeting with all employees regarding the assessment and identify the problems (if any) prevailing in the branch. Branch Manager shall exert best effort to solve the identified problems. Each branch shall submit the Self-Assessment Report with recommendations to Central Compliance Unit (CCU) and Internal Control & Compliance (ICC) within 15 (fifteen) days of each half year end.

7.12 Independent testing procedures (ITP)

As per BFIU Circular # 28 dated: May 30, 2023 of the Bangladesh Financial Intelligence Unit (BFIU) testing on Prevention of Money Laundering is to be conducted on the branches by the internal audit personnel of ICC department and by an outside party such as the institution's external auditors. While conducting the same,

they should also look into whether the directives of BFIU issued from time to time in this respect are followed meticulously by the branches.

Mentionable that compliance of AML is the responsibility of each employee of DBH. Therefore, all guidelines related to AML be updated as and when required and circulated to ensure that all employees are aware of the Money Laundering Prevention Act, 2012 (as amended in 2015) and Anti-Terrorism Act, 2009 (as amended in 2013), BFIU's instructions, internal guidelines and other policies and procedures.

The test will cover the following areas:

i. activities of branch compliance unit/BAMLCO;
ii. knowledge of officers/employees on AML/CFT issues;
iii. customer Identification (KYC) process;
iv. process and action to identify STRs/SARs/CTRs;
v. regular submission of reports to CCU;
vi. proper record keeping; and
vii. overall AML/CFT 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 Company's AML/CFT procedures like:

i. sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
ii. test of the validity and reasonableness of any exemption granted by the financial institution; and
iii. 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 or to be taken and a deadline.

If any deficiency/problem is found after scrutinizing the Self- assessment Report, ICC department visits the branch immediately and inform the Central Compliance Unit (CCU) accordingly. ICC department examine the compliance status of AML/CFT issues and assign score for specific criteria as per prescribed checklist (Annexure GHA) of Independent Testing Procedure (ITP). Subsequently, the said inspection report including the score sheet shall be forwarded to Central Compliance Unit (CCU).

A standard ITP format has been attached at "Annexure-F" of this guideline as prescribed in Circular # 28/2023 of the BFIU.

7.13 Overall assessment report

In compliance with the BFIU Circular # 28, dated: May 30, 2023, the Central Compliance Unit of DBH requires to prepare an Overall Assessment Report on half yearly basis towards submission to the BFIU stating direction/recommendation, if any, of the Board or Top Management Committee.

Chapter 8: Compliance program of DBH against ML/TF

DBH considering the prevailing laws and regulations; and Bangladesh Financial Intelligence Unit (BFIU)'s Circulars should establish and maintain an effective AML/CFT program which should include the followings:

i. development of internal policies, procedures and controls mechanism;
ii. appointment of an AML/CFT compliance officer;
iii. ongoing employee training programs; and
iv. independent audit functions including internal and external audit functions to test AML/CFT programs.

The compliance policies should be documented, approved by the Board of Directors and communicated to all levels of the organization.

8.1 Formation of central compliance unit (CCU)

As per Bangladesh Financial Intelligence Unit (BFIU) instructions, the CCU will be headed by a senior level employee whose position cannot be lower than the third rank in seniority of organizational hierarchy and a minimum of 7(seven) years of working experience, with a minimum of 3(three) years at the managerial level/administrative level. The CAMLCO of the Company will be the Head of the CCU. S/he will be assisted by DCAMLCO & three other designated officers among which two will be from business department and another from any suitable department but none from the ICC department. The organogram of CCU is shown below:

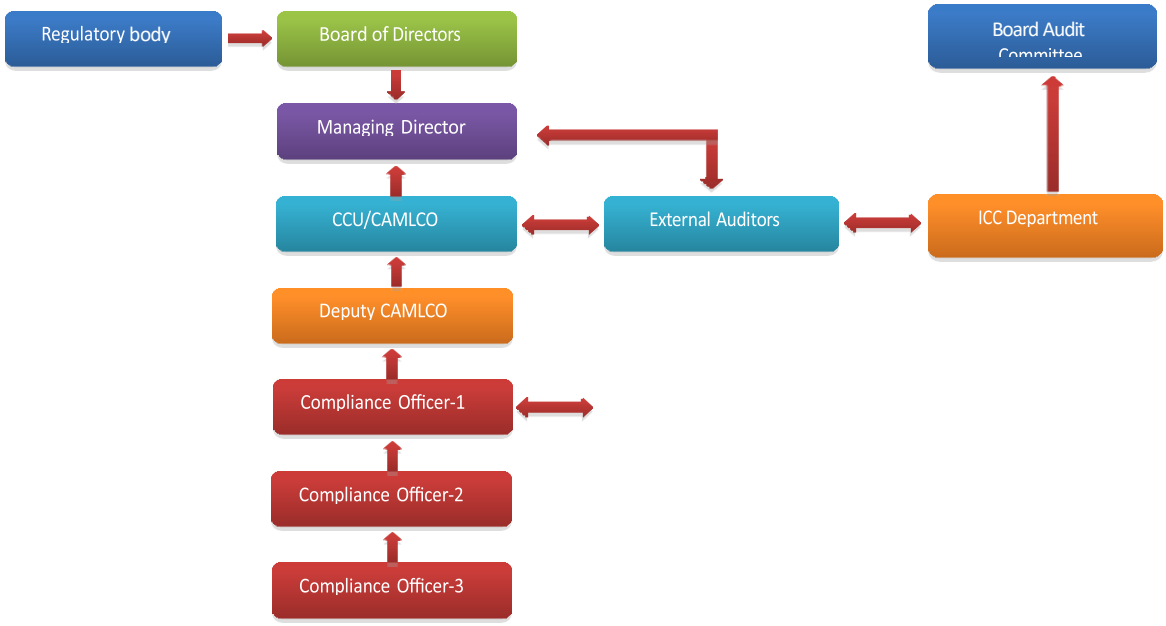

Figure: Formation of Central Compliance Unit

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

Compliance Unit (CCU) and Internal Control & Compliance (ICC) shall work as separate Unit/Department to ensure compliance with applicable laws and directives issued by BFIU.

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

8.2 Responsibilities of the officials of DBH

The responsibilities of the official's various departments are presented below on tabular form for easy understanding of and smooth implementation by the concerned employee/s:

Responsible Depts. or Officials	Responsibilities
Officer in charge who is responsible for opening new accounts/making transaction	a. To interview the potential customer; b. verify customer profile; c. to arrive at threshold limit for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions/activities; d. to restrict opening of accounts in the name of terrorist/banned organizations; e. to adhere with the provisions of Money Laundering Prevention (Amendment) Act, 2015; and f. 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 conducting
Chief Risk Officer	To assess the ML risk involves in operating activities of the Company and to evaluate adequacy and effectiveness of the control mechanism set for safeguarding the company's risks.
Head of Operations	a. To scrutinize and ensure that the information furnished in the account opening form/customer profile/threshold limit are in strict compliance with AML/CFT Guidelines before authorizing opening of account; and b. to certify regarding compliance with AML/CFT Guidelines and report suspicious transactions to CAMLCO/Managing Director.
Internal Auditor	To verify and record his comments on the effectiveness of measures taken by the concerned officials and the level of implementation AML/CFT Guidelines.
CAMLCO	a. To implement and enforce Company's AML policies; b. to ensure sending STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU); c. to inform DCAMLCO/BAMLCO required actions, if any, to be taken.
DCAMLCO	a. To assist CAMLCO to implement and enforce Company's AML policies; b. send STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU) through CCU; c. ensuring flow of information to BAMLCO towards reporting to CAMLCO and CCU; and

BAMLCO	a. ongoing monitoring of customer's KYC profile/CDD/EDD and transaction activities; b. report STR/SAR/CTR through branch manager to CAMLCO and CCU; c. provide AML training to branch employees; d. communicate and update to all employees in case of any changes in national or Company's own policies; e. organize a meeting with all executives/officers at least once after each quarter end as per Circular # 28/2023 of Bangladesh Financial Intelligence Unit (BFIU); and f. submit Self-Assessment Report and applicable returns to CAMLCO/CCU/ICC, as
Branch Manager	a. ensure that the AML program is effective within the Branch; b. overall responsibility to ensure that the Branch has an effective AML program in place and that it is working effectively.
Top Management	Prompt reporting of information regarding suspicious transactions to concerned law enforcing authority in consultation with the competent authority/ies.
Managing Director	Overall responsibility to ensure that DBH has AML program in place and that it is working effectively.

8.3 The responsibilities of CCU members

To ensure compliance of the Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013, DBH requires to establish a Central Compliance Unit (CCU) to arrange internal monitoring and control under the leadership of a high official at the Head Office whose seniority shall not be less than third from the official hierarchy. CCU will issue the instructions to be followed by each concerned officer of Head Office as well as branch/es; these instructions will be prepared on the basis of combination of issues in monitoring of transactions, internal control, policies and procedures from the point of view of preventing ML and combating TF. CCU shall be dedicated solely to perform the compliance functions. In every year, Central Compliance Unit (CCU) will organize at least 4 (four) meetings to discuss about the compliance status in relation to AML/CFT issue.

The responsibilities of a CCU shall include:

i. preparing an overall assessment report after evaluating the self-assessment reports received from the branches and submitting it with comments and/or recommendations to the Managing Director;
ii. preparing an assessment report on the basis of the submitted checklist of inspected branches by ICC department; and
iii. submitting a half-yearly overall assessment report to BFIU within 60 (sixty) days after end of each half year as per Bangladesh Financial Intelligence Unit (BFIU) Circular # 28/2023.
iv. preparing an 'Overall Assessment Report' after evaluating the self-assessment reports received from the branches and submitting it with comments and/or recommendations to the Managing Director;
v. Subsequently, submitting 'Overall Assessment Report' along with Managing Director's instructions and recommendation before the Board of Directors for getting approval;
vi. submitting a half-yearly overall assessment report to BFIU within 2 (two) months after end of each half year.

8.4 Appointment of chief AML/CFT compliance officer (CAMLCO)

DBH requires to designate a Chief AML/CFT Compliance Officer (CAMLCO) at its Head Office who has sufficient authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures. The CAMLCO will directly report to the Managing Director for his/her responsibility. The CAMLCO will 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.

The CAMLCO will be the head of CCU and s/he will be the central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to Company's AML/CFT program. The position of the CAMLCO cannot be lower than the third rank in seniority of organizational hierarchy. The CAMLCO should have a minimum of 7(seven) years of working experience, with a minimum of 3(three) years at a managerial/administrative level.

8.5 Responsibilities of CAMLCO

The major responsibilities of CAMLCO are as follows:

i. to monitor, review and coordinate application and enforcement of AML/CFT 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 or activities, and a written AML/CFT training plan;

ii. to monitor changes of laws/regulations and directives of Bangladesh Financial Intelligence Unit (BFIU) and revise its internal policies accordingly;

iii. to respond to compliance questions and concerns of the staff and advise branches/units and assist in providing solutions to potential issues involving compliance and risk;

iv. to ensure that Company's AML/CFT policy is complete and up-to-date, to maintain ongoing awareness of new and changing business activities and products;

v. to develop compliance knowledge of all staff, especially the compliance personnel and conduct training courses in this regard;

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

vii. to assist in review of control procedures in DBH to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses, if any;

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

ix. to manage the STR/SAR/CTR process by:

   a. reviewing transactions referred by branch or unit compliance officers as suspicious through CCU meeting;

   b. reviewing the transaction monitoring reports (directly or together with account management personnel);

   c. ensuring STR/SAR/CTR as the case may be:

- are prepared when appropriate;
- are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy;
- are advised branch/es of DBH who are known to have a relationship with the customer; and
- are reported to the Managing Director, and the Board of Directors when the suspicious activity is judged to represent significant risk to the institution, including reputation risk.

d. ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;

e. 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; and

f. managing the process for reporting suspicious activity to BFIU after appropriate internal consultation.

8.6 Responsibilities of deputy CAMLCO

The major responsibilities of deputy CAMLCO are as follows:

i. assisting CAMLCO in implementing and enforcing institution's AML/CFT policies;

ii. send STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU) through CCU;

iii. ensuring flow of information to BAMLCO towards reporting to CAMLCO and CCU; and

iv. to assist CAMLCO to take other required actions, if any, to be taken.

8.7 Responsibilities of BAMLCO

DBH requires designating Branch Anti-money Laundering Compliance Officer (BAMLCO) at every branch. BAMLCO will be the second man of a branch and have a minimum 3(three) year experience in related field. The responsibilities of a BAMLCO are as follows:

i. ongoing monitoring of customer's KYC profile/CDD/EDD and transaction activities;

ii. report any STR/SAR/CTR through branch manager to CAMLCO and CCU;

iii. provide AML training to branch employees;

iv. communicate and update to all employee in case of any changes in national or Company's own policy;

v. organizes a meeting with all executives/officers at least once after each quarter end as per Circular # 28/2023 of Bangladesh Financial Intelligence Unit (BFIU); and

vi. submit Self-Assessment Report and applicable returns to CAMLCO/CCU/ICC, as the case may be, on timely manner.

8.8 Employee training and awareness program

As per FATF recommendation no.18, a formal AML/CFT compliance program should include an ongoing employee training schedule. The importance of a successful training and awareness program cannot be overstated. Employees in different business functions need to understand how the financial institution's policy, procedures, and controls affect them in their day to day activities. As per the Circular # 28/2023, DBH shall have to arrange suitable training for officials to ensure

proper compliance of AML/CFT activities. Following training procedures to be followed by the Company for prevention of ML and combating TF:

8.8.1 Employee awareness

Employee must be aware of their own personal statutory obligations and that they will 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 STR/SAR/CTR.

8.8.2 Education and training programs

All relevant employees should be educated in the process of the KYC requirements to prevent ML and & combating TF. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Concerned employees 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 two types:

i. general training; and
ii. job specific training

General training

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

i. general information on the risks of ML and TF schemes, methodologies, and typologies;
ii. legal framework, how AML/CFT related laws apply to DBH;
iii. policies and systems with regard to customer identification and verification, due diligence, monitoring;
iv. how to react when faced with a suspicious customer or transaction;
v. how to respond to customers who want to avoid reporting requirements;
vi. stressing the importance of not tipping off customer information;
vii. STR/SAR/CTR requirements and processes; and
viii. duties and accountabilities of employees.

Job Specific Training

a. New employee training

For a new employee the compliance policy statement must be signed-off at the beginning of the joining and he/she must have an on the job training from the departmental head regarding the importance of AML/CFT activities. The new employee must also go through the yearly training on AML/CFT.

b. Customer service/relationship managers

Employees of the investment departments who are to deal 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

to fight against ML and TF. They must be made aware of their legal responsibilities and 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.

c. Operation department

Operation department employee who receives loan application forms and cheques for deposit into Company's account should receive training on the processing and verification procedures of customer profile/CDD/EDD. In addition, they need to be trained on the organization's account opening and customer verification procedures. Employee should be aware that the offer to deploy suspicious funds or the request to undertake a suspicious transaction may need to be reported to the CAMLCO (or alternatively a line supervisor).

d. 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.

e. Audit and compliance officer

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

f. Senior management commitment and role of the Board of Directors

The most important element of a successful AML/CFT program is the commitment of senior management, including the Managing Director and the Board of Directors. AML/CFT issues may be communicated to the Board from time to time, if necessary. The message from top management and the Board of Directors will be "Zero Tolerance" in case of AML and CFT.

g. AML/CFT compliance officer

The AML/CFT compliance officer should receive in depth training in all aspects of the AML/CFT legislation, Bangladesh Financial Intelligence Unit (BFIU) directives, circulars, guidelines and internal policies. In addition, the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of STR/SAR/CTR and on the feedback arrangements, and on new trends and patterns of criminal activities.

8.8.3 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 procedures. Auditor's responsibilities regarding compliances are as follows:

8.8.3.1 Internal audit

The responsibilities of internal auditors are:

- address on 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, regulatory and geographic locations);
- assess the adequacy of the DBH processes for identifying and reporting STR/SAR/CTR;
- communicate the findings to the CCU/Managing Director and/or Board 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;
- effectiveness of training, in view of specific risks of individual business lines; etc.

8.8.3.2 External Auditors'

External auditor shall play an essential part in reviewing the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External auditors should focus their audit programs on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient. DBH may, if requires, facilitate the external auditors in reviewing whether the ML policies have been complied or not by the management.

Chapter 9: Offence of money laundering and punishment

9.1 Offence

For the purpose of this Act money laundering shall be deemed to be an offence.

9.2 Punishment

According to section 25(2) of Money Laundering Prevention Act, 2012, if any reporting organization violates the directions mentioned in sub-section (1) of section 25 of Money Laundering Prevention Act, 2012, Bangladesh Financial Intelligence Unit (BFIU) or Regulating authority of reporting organization may-

a. imposes 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, service centers, booths or agents, or as the case may be, shall inform the registration or licensing authority about the fact so that the relevant authority may take appropriate measures against the organization.

In addition to the above-mentioned provisions there are some provisions of penalties in section 23 of Money Laundering Prevention Act, 2012. These are:

Under section 23(3): 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, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so that the relevant authority may take appropriate measures against the organization.

Under section 23(4): 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, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so that relevant authority may take appropriate measures against the said organization.

Under section 23(5): If any reporting organization fails to comply with any instruction given by Bangladesh Financial Intelligence Unit (BFIU) under this Act, BFIU may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day for each of such non-compliance and if any organization is fined more than 3(three) times in 1(one) financial year, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the

purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so that the relevant authority may take appropriate measures against the said organization.

Under section 23(6): 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 Money Laundering Prevention (Amendment) Act, 2015, 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.

Under section 23(7): 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, BFIU may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or BFIU, and in this regard if any amount of the fine remains unrealized, BFIU may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.

Under section 23(7): ক) এই আইনে বর্নিত অপরাধের অনুসন্ধান ও তদন্তে কোন তদন্তকারী সংস্থা কোন ব্যাংক বা আর্থিক প্রতিষ্ঠানের কোন গ্রাহকের হিসাব সংক্রান্ত দলিল ও তথ্যাদি উপযুক্ত আদালতের আদেশক্রমে অথবা বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটের মাধ্যমে সংগ্রহ করিতে পারিবে।

Under section 23(8): 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 staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative action.

Under section 4: Offence of money laundering and punishment

(1) For the purposes of this Act, money laundering shall be deemed to be an offence.

(2) কোন ব্যাক্তি মানিলন্ডারিং অপরাধ করিলে বা মানিলন্ডারিং অপরাধ সংগঠনের চেষ্টা, সহায়তা বা ষড়যন্ত্র করিলে তিনি অনূন্য ৪ (চার) বৎসর এবং অনধিক ১২ (বার) বৎসর পর্যন্ত কারাদন্ডে দন্ডিত হইবেন এবং ইহার অতিরিক্ত অপরাধের সাথে সংশ্লিষ্ট সম্পত্তির দ্বিগুণ মূল্যের সমপরিমান বা ১০ (দশ) লক্ষ টাকা পর্যন্ত, যাহা অধিক, অর্থদন্ডে দন্ডিত হইবেন।
তবে শর্ত থাকে যে, আদালত কর্তৃক ধার্যকৃত সময়সীমার মধ্যে অর্থদন্ড পরিশোধে বইলে, আদালত অপরিশোধিত অর্থদন্ড বিবেচনায় অতিরিক্ত কারাদন্ডে দন্ডিত করিবার আদেশ প্রদান করিতে পারিবেন।

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

(4) কোন সত্তা এই আইনের অধীন কোন অপরাধ সংগঠন করিলে, বা অপরাধ সংগঠনের চেষ্টা, সহায়তা বা ষড়যন্ত্র করিলে, ধারা ২৭ এর বিধান সাপেক্ষে, উপধারা (২) এর বিধান অনুসারে ব্যবস্থা গ্রহন করা যাইবে এবং অপরাধের সহিত সংশ্লিষ্ট সম্পত্তির মূল্যের অনূন্য দ্বিগুণ অথবা ২০ (বিশ) লক্ষ টাকা যাহা অধিক হয়, অর্থদন্ড প্রদান করা যাইবে এবং উক্ত প্রতিষ্ঠানের নিবন্ধন বাতিল যোগ্য হইবে।
তবে শর্ত থাকে যে, উক্ত সত্তা আদালত কর্তৃক ধার্যকৃত সময়সীমার মধ্যে অর্থদন্ড পরিশোধে বইলে, আদালত অপরিশোধিত অর্থদন্ড বিবেচনায় সত্তার মালিক, চেয়ারম্যান বা পরিচালক যে নামেই অভিহিত করা হোক না কেন, তাহার বিরুদ্ধে কারাদন্ডে দন্ডিত করিবার আদেশ প্রদান করিতে পারিবে।

(5) It shall not be a prerequisite to charge or punish for money laundering to be convicted or sentenced for any predicate offence.

Under section 5: Punishment for violation of an order for freezing or attachment

Any person who violates a freezing or attachment order issued under this Act shall be punished with imprisonment for a term not exceeding 3(three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or with both.

Under section 6: Punishment for divulging information

(1) No person shall, with an ill motive, divulge any information relating to the investigation or any other related information to any person, organization or news media.

(2) Any person, institution or agent empowered under this Act shall refrain from using or divulging 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.

(3) Any person who contravenes the provisions of sub-sections (1) and (2) 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.

Under section 7: Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information

(1) Any person who, under this Act-

(a) obstructs or declines to cooperate with any investigation officer for carrying out the investigation; or

(b) declines to supply information or submit a report being requested without any reasonable ground; shall be deemed to have committed an offence under this Act.

(2) Any person who is convicted under sub-section (1) shall be punished with imprisonment for a term not exceeding 1(one) year or with a fine not exceeding Taka 25 (twenty-five) thousand or with both.

Under section 8: Punishment for providing false information

(1) No person shall knowingly provide false information in any manner regarding the source of fund or self-identity or the identity of an account holder or the beneficiary or nominee of an account.

(2) Any person who violates the provision of sub-section (1) shall be punished with imprisonment for a term not exceeding 3(three) years or a fine not exceeding Taka 50(fifty) thousand or with both.

Under section 9: Investigation and trial of an offence

(1) আপাতত বলবৎ অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, এই আইনের অধীন অপরাধ সমূহ ধারা ২ (ঠ) তে উল্লিখিত তদন্তকারী সংস্থার কর্মকর্তা বা এতদুদ্দেশ্যে সরকারের সহিত পরামর্শক্রমে, বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক একাধিক তদন্তকারী সংস্থার কর্মকর্তাদের সমন্বয়ে গঠিত যৌথ তদন্তকারী দল তদন্ত করিবে।

(2) আপাতত বলবৎ অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, এই আইনের অধীন অপরাধ সমূহ Criminal Law (Amendment) Act 1958 (Act XL of 1958) এর Secction 3 এর অধীন নিযুক্ত স্পেশাল জজ কর্তৃক বিচার্য হইবে।

(3) অভিযুক্ত ব্যক্তি বা সত্তার সম্পত্তি অনুসন্ধান ও সনাক্তকরনের লক্ষ্যে তদন্ত কর্মকর্তা কর্তৃক এই আইনের পাশাপাশি অন্যান্য আইনে এতদুদ্দেশ্যে প্রদত্ত ক্ষমতাও প্রয়োগ করিতে পারিবে।

(4) তদন্তকারী সংস্থা এই আইনের অধীন সংঘটিত অপরাধ অনুসন্ধান বা তদন্ত কার্যক্রম পরিচালনার বিষয়টি বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কে অবহিত করিবে।

Under section 27: Offences committed by an entity

If any offence under this Act is committed by an entity, every proprietor, director, manager, secretary or any other officer, staff or representative of the said entity who is directly involved in the offence shall be deemed to be guilty of the offence, unless he is able to prove that the offence has been committed without his knowledge or he tried his best to prevent it.

Explanation: In this section “director” includes any member of the partnership entity or any of the Board of Directors of the entity, by whatever name called.

Under section 28: Protection of actions taken in good faith

No suit or prosecution or administrative measures or any other legal proceedings shall lie against the Government or any officer or staff of the Government or Bangladesh Financial Intelligence Unit (BFIU) or any officer or staff of BFIU or the Investigating Agency or any officer or staff of the Agency or any reporting organization or its Board of Directors or any of its officers or staff for anything which is done in good faith under this Act or Rules made thereunder for which any person is or likely to be affected.

Chapter 10: Suspicious transaction/activity report (STR/SAR)

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

According to the provision of section 25(1)(d) of Money Laundering Prevention Act, 2012 and section 14 of Anti-Terrorism (Amendment) Act, 2013 DBH should report to Bangladesh Financial Intelligence Unit (BFIU) proactively and immediately, facts on suspicious, unusual or doubtful transactions likely to be related to ML/TF; because BFIU has the power to call STR/SAR from FIs related to ML/TF.

10.1 General definition

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 one. Such report is to be submitted by financial institutions to Bangladesh Financial Intelligence Unit (BFIU).

10.2 Legal definition

Under section (2)(z) of Money Laundering Prevention Act, 2012 "suspicious transaction" means such transactions-

(a) which deviates from usual transactions;

(b) of which there is ground to suspect that,

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

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

(c) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit (BFIU) from time to time;

In Anti-Terrorism (Amendment) Act, 2013, STR/SAR refers to the transaction that relates to financing for terrorism or terrorist individual or entities.

One important thing may be noted that DBH do not require to establish any proof of occurrence of a predicate offence; it is a must to submit STR/SAR only on the basis of suspicion.

10.3 Obligations of such report

As per the Money Laundering Prevention (Amendment) Act, 2015, DBH is obligated to submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU). Such obligation also prevails under Anti-Terrorism (Amendment) Act, 2013. Other than the legislation, BFIU has also instructed the FIs to submit STR/SAR through BFIU Circular # 28, dated May 30, 2023.

10.4 Reasons for reporting of STR/SAR

STR/SAR is very crucial for the safety and soundness of our institutions and accordingly DBH should submit STR/SAR considering the followings:

i. it is a legal requirement in Bangladesh;
ii. it helps protect the reputation of DBH;
iii. it helps to protect DBH from unfounded allegations of assisting criminals, including terrorists;
iv. it helps the competent authorities to investigate money laundering, terrorist financing, and other financial crimes; etc.

10.5 Identification and evaluation of STR/SAR

Identification of STR/SAR is very crucial for DBH to mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place. Such identification may not only take place at the time of transaction but also at the time of doing KYC/CDD/EDD and attempt to transaction or financial relation.

10.5.1 Identification of STR/SAR

Identification of STR/SAR shall be started by identifying unusual transactions and activities. Transactions may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Concerned employee can take following steps to detect STR/SAR:

i. reviewing KYC profile;
ii. monitoring customer transactions; and
iii. using red flag indicator.

Simply, if any transaction/activity is consistent with the information provided by the customer; that can be treated as normal and expected. When such transaction/activity is not normal & expected, it may be treated as unusual transaction/activity.

In case of reporting of STR/SAR, DBH should conduct the following 3(three) stages:

a) Identification:

This stage is very vital for STR/SAR reporting. DBH need to monitor constantly the activities of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution having alert management mechanism and appropriate staff (e.g. the AML/CFT compliance officer) dealing with of unusual/suspicious transactions or activities. Training of staff on the identification of unusual/suspicious activity should always be an ongoing process. DBH must be vigilant in complying KYC meticulously and sources of funds of the customer to identify STR/SAR.

b) Evaluation:

After identification of STR/SAR, compliance officer or BAMLCO should evaluate the transaction/activity by interviewing the customer or through any other means. In the evaluation stage concerned officer/BAMLCO must be tactful considering the tipping off provision of the acts. If they are not satisfied, they should forward the report to CCU. After receiving report from Head Office/branch CCU should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stage of evaluation DBH should keep records complying the requirement of Money Laundering Prevention (Amendment) Act, 2015.

c) Disclosure:

This is the final stage to submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU), when there is valid reason/s to treat any transaction as suspicious, on the ground of ML/TF. For simplification a flow chart is given below to show STR/SAR identification and reporting procedures:

10.6 Reporting of STR/SAR

DBH as per Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013 are obligated to submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU). Such report must be sent to the BFIU from CCU by using specified format/instruction given by them.

10.7 Tipping off

"Tipping off" means to disclose to the concerned 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.

Section 6 of Money Laundering Prevention (Amendment) Act, 2015 and FATF Recommendation no. 21 prohibits reporting agencies, their directors, officers and employees from disclosing the fact that an STR/SAR or related information is being reported to Bangladesh Financial Intelligence Unit (BFIU). A risk exists that customers could be unintentionally tipped off when DBH is seeking to perform its CDD obligation.

10.8 Penalties of tipping off

As per section 6(2) & (3) of Money Laundering Prevention Act, 2012, the following penalties and/or punishment shall impose against any of the directors, officers and employees:

Section 6(2) of this Act: Any person, institution or agent empowered under this Act shall refrain from using or divulging 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.

Section 6(3) of this Act: Any person who contravenes the provisions of sub-sections (1) and (2) 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.

10.9 "Safe Harbor" provision for reporting

Safe harbor laws encourage reporting agencies 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. Section 28 of Money Laundering Prevention Act, 2012 provides the safe harbor for reporting.

10.10 Indicators of STR/SAR

10.10.1 Frequent change of customer address

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

10.10.2 Out of market windfalls

Concerned officer shall pay attention to those customers/clients whose address is far from the Company, especially if there is no special reason for the same, it should be investigated whether there are institutions closer to home that could provide service to the customer. If the customer is a business man, the distance to its operations may be an attempt to prevent DBH from verifying their business condition.

10.10.3 Suspicious customer behavior

Some typical behavior having intention to do suspicious transaction of a customer is:

i. unusual or excessively nervous demeanor;
ii. discusses on record-keeping or reporting duties with the apparent intention of avoiding them;
iii. threatens an employee in an effort to discourage required record keeping or reporting;
iv. reluctant to proceed with a transaction after being told it must be recorded;
v. 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;
vi. 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;
vii. a student uncharacteristically transacts large sums of money; and
viii. an agent, attorney or financial advisor act for another person without proper documentation such as a power of attorney etc.

10.10.4 Suspicious customer identification

Some typical examples having intention to hide identification towards suspicious transactions of a customer:

i. furnishes unusual or suspicious identification documents and is unwilling to provide personal data;
ii. is unwilling to provide personal background information when opening an account;
iii. permanent address is outside the FI‟s service area;
iv. asks many questions about how the financial institution disseminates information about the identification of a customer; and
v. reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

10.10.5 Suspicious non-cash deposits

Some typical examples of non-cash deposits having intention to do suspicious transactions of a customer:

i. deposits large numbers of consecutively numbered money orders or round figure amounts;
ii. deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business;

iii. funds out of the accounts are not consistent with normal business or personal items of the account holder; and
iv. funds deposited are moved quickly out of the account via payment methods inconsistent with the purpose of the account.

10.10.6 Suspicious activity in credit transactions

Some typical examples of credit transactions having intention to do suspicious transactions of a customer:

i. financial statements do not conform with the accounting principles;
ii. suddenly pays off a large problem loan with no reasonable explanation of source of funds; and
iii. produce/lien certificate of deposit and use as collateral of a loan/lease.

10.10.7 Suspicious commercial account activity

Some typical examples of commercial account activity having intention to do suspicious transactions of a customer:

i. business customer presents financial statements noticeably different from those of similar businesses; and
ii. large business presents financial statements that are not prepared by professional accountant.

10.10.8 Suspicious employee activity

Some typical examples of activities having intention to help customer to do suspicious transactions towards ML/TF of an employee:

i. exaggerates the credentials, background or financial ability and resources of a customer in written reports as per Company requirements;
ii. frequently is involved in unresolved exceptions or recurring exceptions on exception reports;
iii. lives a lavish lifestyle that could not be supported by his/her salary and background; and
iv. frequently overrides internal controls or established approval authority or avoid policy.

10.10.9 Suspicious activity in an FI setting

Some typical examples of activity of a customer in relation to suspicious transactions towards ML/TF using setting of financial institution:

i. request of early encashment;
ii. a DPS (or whatever) calling for the periodic payments in large amounts; and

Chapter 11: Reporting cash transaction report (CTR)

The Deputy Chief Anti-Money Laundering Compliance Officer (DCAMLCO) and Branch Anti-Money Laundering Compliance Officer (BAMLCO) will monitor and analyze the daily cash transactions and prepare Cash Transaction Report (CTR) as prescribed in the Circular # 28, dated: May 30, 2023 of Bangladesh Financial Intelligence Unit (BFIU) under Clause # 6. As per the circular:

1. in case of cash deposit or cash withdrawal and online cash deposit or any other online deposit or withdrawal in a particular account in a particular day, the transaction amount is Tk.10.00 lac and more through one or more transactions in a single/individual account, concerned officer will send a report to Central Compliance Unit (CCU) in Head Office by the end of the 1st week of subsequent month for onward submission of the same to BFIU within 21st day of the corresponding next month using goAML web of BFIU;
2. the DCAMLCO/BAMLCO will analyze the CTR(s) meticulously before reporting the same to CCU to identify any suspicious transaction or activity. If something is found suspicious or unusual, they will send them to CCU members for scrutiny and upward reporting as STR. If the CCU, after review, discovers any transection/s as suspicious/unusual they shall direct to the responsible officer to report the account/s as STR using the goAML web;
3. in case, if they don't find anything suspicious/unusual the CAMLCO will make a certification with the CTR report stating that "we have checked and didn't find anything suspicious in the CTR and will send the same to BFIU through the Message Board of the goAML web;
4. the Head Office as well branch/es will preserve the CTR report, if any, on monthly basis;
5. the Head Office as well branch/es will keep record of the CTR at least for 5(five) years from the date of the reporting;
6. in case of cash deposits of Government (including ministry and division) account, Government owned Organization, Semi-Government or Autonomous Organization CTR report is not applicable but in case of withdrawal the same shall be applicable; and
7. the CTR report is effective from July 2015.

Chapter 12: Record keeping

12.1 Statutory requirement

DBH should preserve all necessary records on transactions for a specific period as mentioned in the Companies Act, 1994.

However, in terms of section 25(1)(b) of Money Laundering Prevention Act, 2012, and FATF Recommendation no.11, DBH requires to preserve previous records of transactions of closed account (s) for at least 5(five) years from the date of closure. This will enable DBH to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Records relating to verification of identity generally comprise the followings:

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

Records relating to transactions generally comprise the followings:

a. details of personal identity, including the names and addresses, etc. pertaining to:
    - the customer;
    - the beneficial owner of the account or product;
    - the non-account holder conducting any significant one-off transaction; and
    - any counter-party.
b. details of transaction including:
    - nature of transactions;
    - volume of transactions, customer's instruction(s) and authority;
    - source/s of funds;
    - destination/s of funds;
    - book entries;
    - date of the transaction;
    - form in which funds are offered and paid out;
    - parties to the transaction; and
    - identity of the person who conducted the transaction on behalf of the customer.

As per the Money Laundering Prevention Act, 2012, the records of identities of customers shall have to be kept for at least 5(five) years from the date when the relationship with the customer has ceased. This is the date of:

a. closing of an account; or
b. providing of any financial services; or
c. carrying out of the one-off transaction; or
d. ending of the business relationship; or

e. commencement of proceedings to recover debts payable on insolvency.

12.2 Retrieval of records

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

12.3 STR /SAR/CTR and investigation records

DBH should not destroy any STR/SAR/CTR related records of customer or transaction without the consent of the Bangladesh Financial Intelligence Unit (BFIU) where: (1) Company has submitted a report of suspicious transaction; or (2) it is known that a customer or any transaction is under investigation, even after expiration of the maximum preservation period of 12 (twelve) years as per law or conclusion of the case, as the case may be. To ensure the preservation of such records DBH should maintain a register or tabular records of all investigations and inspection made by the investigating authority or BFIU and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

a. the date of submission and reference of the STR/SAR/CTR;
b. the date and nature of the enquiry;
c. the authority who made the enquiry, investigation with reference; and
d. details of the account(s) involved.

12.4 Training records

DBH shall maintain training records which include:

a. details of the content of the training programs provided;
b. the names of staff who have received the training;
c. the date/duration of training;
d. the results of any testing carried out to measure staffs understanding of the requirements; and
e. an on-going training plans.

12.5 Branch level record keeping

To ensure the effective monitoring and demonstrate compliance with the concerned regulations, DBH shall have to ensure the keeping or availability of the following records at the Head Office and/or branch level either in hard form or electronic form:

a. information regarding Identification of the customer;
b. KYC information of a customer;
c. transaction report;
d. STR/SAR/CTR generated from the Head Office/branch;
e. exception report;
f. training record; and
g. return submitted or information provided to the Head Office or competent authority.

12.6 Sharing of record/information

Financial Institutions shall share account related information only to the investigating agency as mentioned in the para 2 (ঠ) of the Money Laundering Prevention (Amendment) Act, 2015.

Chapter 13: Non face to face customer

13.1 Definition

Non-face-to-face account opening refers to a situation where the customer is not interviewed and the signing of account opening forms and identification of documents of the customer are not conducted in the presence of concerned officer of a financial institution.

13.2 What to do in case of non-face-to-face customer

Sometimes, DBH is required to open accounts on behalf of customers who do not present themselves for personal interview i.e. no face-to-face contact with the customer. In such situation collection of photographic and other related documents will not be an appropriate procedure. The following steps need to be taken under such circumstances:

a. apply Enhanced Due Diligence (EDD) or Enhanced Customer Due Diligence (Enhanced CDD);
b. apply extensive customer identification procedures for non-face-to-face customers;
c. shall not allow non-face-to-face contact to a resident in establishing relationship;
d. original current passport or ID card shall be verified and certified true copy thereon shall be obtained and preserved;
e. ensure that there are sufficient evidences to conform address and personal identity. The concerned employee shall take at least one additional check to safeguard against impersonation;
f. ask additional documents to complement those which are required for face-to-face customers;
g. independent contact with such customer;
h. third party introduction, where necessary;
i. update customer's information more frequently than face-to-face customers; and
j. in extreme cases, refusal of business relationship for high risk customers with the approval of the Managing Director.

The above should apply to all new as well as existing customers on the basis of materiality and risk, and accordingly due diligence should be conducted on the existing customers based on appropriate judgment.

Chapter 14: Statement of compliance

DBH should obtain a "Statement of Compliance" on prevention of money laundering and combating terrorist financing from its all employees. Such statement should be duly signed by respective employee and preserved in the employees' personal files.

In the statement of compliance, every employee should solemnly declare and confirm that as an employee of DBH I:

i. have read the Company's Guidelines on "Prevention of Money Laundering and Combating Terrorist Financing"; as well as circulars/directives of Bangladesh Financial Intelligence Unit (BFIU) and Government's Acts on Anti-Money Laundering and Anti-Terrorism and understood the implications thereof;

ii. shall comply the applicable laws and regulations and corporate ethical standards;

iii. shall comply all the rules and regulations in the normal course of my assignments. It is my responsibility to become familiar with the rules and regulations that relate to my assignment; and

iv. shall be held responsible for carrying out compliance responsibilities on prevention of Money Laundering and combating Terrorist Financing meticulously.

The CAMLCO should also ensure that all new employees of the Company shall read this policy, understand the implications there of and sign the "Statement of Compliance". After signing off, it should be sent to HR for preserving in the newly appointed employee's personal file.

A typical format on "Statement of Compliance" has been given at "Annexure-G" of this Guidelines.

Chapter 15: Confidentiality of information

All information generated, exchanged or provided with any personnel of the Company in the context of ML/TF must be on strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with provisions of regulation of the Government and Bangladesh Financial Intelligence Unit (BFIU).

15.1 Restriction on sharing of record/information as per Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013

i. Any person, institution or agent empowered under these Acts shall refrain from using or divulging 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 these Acts.

ii. Financial Institutions shall share account related information only to the investigating agency as mentioned in the para 2 (ঠ) of the Money Laundering Prevention (Amendment) Act, 2015. As per para 2 (ঠ) of the Money Laundering Prevention (Amendment) Act, 2015 "Investigating Agency" means –
তদন্তকারী সংস্থা অর্থ এই আনের অন্য কোন বিধানে ভিন্নরূপ কোন কিছু না থাকিলেঃ-
(অ) দফা (শ) এ বর্নিত "সম্পৃক্ত অপরাধ" তদন্তের জন্য সংশ্লিষ্ট আইনে ক্ষমতাপ্রাপ্ত তদন্তকারী সংস্থা ; তবে শর্ত থাকে যে, যে সকল সম্পৃক্ত অপরাধ বাংলাদেশ পুলিশ কর্তৃক তদন্তযোগ্য তাহা বাংলাদেশ পুলিশের অপরাধ তদন্ত বিভাগ (criminal investigation department) কর্তৃক তদন্ত করিতে হইবে;
(আ) সরকারের সহিত পরামর্শক্রমে বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক ক্ষমতা প্রাপ্ত উপ-দফা (অ) এ উল্লেখিত এক বা একাধিক তদন্তকারী সংস্থা।

15.2 Penalties for divulging information

Section 6 of Money Laundering Prevention (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 purpose 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.

Part-B

Combating the Financing of Terrorism

1. Introduction

Terrorist Financing has become a massive threat in recent years. As such, terrorist financing has become a great concern for all countries in the world. It is widely acknowledged to be an essential component of terrorist activity as terrorists are able to facilitate their activities only, if they have the financial resources to do so. The consequences of terrorist activities are tremendous and devastating. So, combating financing of terrorism is indispensable for the economy and also for the security of our country. The Government of Bangladesh has given top most priority to this issue. As such, Anti-Terrorism Act, 2009 was enacted by the Parliament of the People's Republic of Bangladesh, which has already been amended in 2012 and 2013. The Act has been effective from the June 11, 2008. In the Anti-Terrorism Act, 2009 terrorist financing has been termed as criminal activity and the role of Financial Institutions (FIs) to fight against financing of terrorism has been specified. It is considered that the fight against financing of terrorism is a combined effort and policy has been drawn accordingly.

2. What is terrorist financing

As per Section 7 of Anti-Terrorism Act, 2009:

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

a. to carry out terrorist activity;

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

2. Conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property mentioned in sub-section (1) was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act.

3. If any person is convicted of any of the offences mentioned in sub-section (1), the person shall be punished with rigorous imprisonment for a term not exceeding 20(twenty) years but not less than 4(four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or Taka 10(ten) lac, whichever is greater, may be imposed.

4. If any entity is convicted of any of the offences mentioned in the sub-section (1)-

a. steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of Taka 50(fifty) lac, whichever is greater, may be imposed; and

b. the head of that entity, whether he is designated a Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term no exceeding 20(twenty) years but not less than 4(four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of Taka 20(twenty) lac, whichever is greater, may be imposed unless he is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

3. International requirement on combating TF and proliferation of weapons of mass destruction

United Nations Security Council Resolution (UNSCR) 1267 and 1373 have been adopted under Article VII of UNSCR charter, which means these resolutions are obligatory for every jurisdiction. Accordingly, BFIU instructed FIs to take necessary action on UNSCR 1267 and 1373; banned list of Bangladesh Government by their BFIU circular # 28/2023 to:

i. introduce a Board approved policy regarding prevention of financing of terrorism and proliferation of weapons of mass destruction;
ii. instruct all concerned employees about their responsibilities and review the instruction, when necessary;
iii. introduce a software to keep records of updated lists of terrorists of UNSCR 1267 and 1373 or of Bangladesh government;
iv. monitor regularly the terrorists list of UNSCR or of Bangladesh Government to monitor whether any account, directly or indirectly, maintaining with DBH. If so, shall require to be reported directly to Bangladesh Financial Intelligence Unit (BFIU) without delay; and
v. stop transaction of account of any person or entity whose names are listed with UNSCER 1373 and banned list of Bangladesh Government and inform BFIU immediately.

In a nut shell, to comply with this direction DBH should require to monitor the UN sanction list and Bangladesh Government's banned list against ML/TF regularly and if any account or transaction is found to have any connection with the lists, shall have to inform BFIU immediately.

4. The link between ML and TF

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

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

5. Why DBH must combat financing of terrorism

1. Financing of Terrorism was termed as criminal activity under United Nations International Convention for the Suppression of the Financing of Terrorism in 1999. To reinforce the 1999 Convention, United Nations adopted UNSC Resolutions 1373 and 1390 directing member states to criminalize Financing of Terrorism and adopt regulatory measures to detect, deter and freeze terrorists' assets. The resolutions oblige all countries to deny financing, support and safe harbor for terrorists.
2. Bangladesh has been actively involved in multinational and international institutions. Its international relationship and business, banking business in particular are regulated by some domestic and international regulations. So, it is mandatory to abide by those regulations. Financial Action Task Force (FATF), the international standard setter, adopted 40 recommendations for AML/CFT in the year, 2012. So, DBH must be involved in international effort to CFT.
3. It is increasingly evident that terrorists and their organizations need to raise significant amounts of cash for a wide variety of purposes for recruitment, training, travel and materials as well as often payment for safe heaven protection. So, to root out terrorism, DBH must stop the flow of funds.
4. The consequences of allowing the financial system to facilitate the movement of terrorist money are so terrible that every effort must be made to prevent this from happening. So CFT is not only the regulatory requirement but also an act of self-interest.

6. Purpose of the policy

Both ML and TF have been identified as major threats to the financial services community. The management of DBH has recognized prevention of ML and combating TF as a team effort. This section outlines policies, procedures and measures to be taken for combating financing of terrorism.

7. Policy statement

Pursuant to the Money Laundering Prevention Act, 2012 (as amended in 2015) and Anti-Terrorism Act, 2009 (as amended in 2013), the Bangladesh Financial Intelligence Unit (BFIU) has issued a circular # 28, dated May 30, 2023 elaborating the responsibilities of FIs to prevent ML/ combat TF.

As such, DBH is committed to implement the provisions of the Anti-Terrorism (Amendment) Act, 2013, and also the guidelines and instructions issued by BFIU from time to time in respect of transaction monitoring systems and operational processes.

DBH is committed to assist and co-operate with the relevant law enforcement authorities, the BFIU whenever possible and to the fullest extent possible as per sub section 3 of section 15 of Anti-Terrorism Act, 2009.

It is the policy of DBH to adhere to all of the provisions of Anti-Terrorism Act, 2009 and other regulations by implementing this policy and subsequent procedures.

8. Enforcement

Management of DBH is responsible for ensuring that the directives are implemented and administered in compliance with the approved policy. Changes to the policy will require approval by the Board of Directors.

The Management of DBH is empowered to effect changes in operating procedures, standards, guidelines and technologies etc.

9. Exceptions to the policy

Requests for exceptions to this policy must be specific and may only be granted on specific items, rather than to entire sections. Concerned executives shall communicate their requests with exceptions to the Managing Director.

10. Procedure

All financial institutions must be committed to combat TF. Guidelines on Prevention of Money Laundering are written in Part-I of the guidelines.

DBH believes that strict adherence to the existing AML Policy Guidelines provides basic AML controls which also serves as primary controls for detection and combating of TF. Therefore, in addition to the existing AML Policy Guidelines, the following extra due diligence and vigilance will be exercised to detect and combat TF.

Under direct control of the Managing Director of DBH, AMD/DMD/SEVP/EVP and all Head of Divisions on their part, Central Compliance Unit for Prevention of Money Laundering and Combating Terrorist Financing headed by CAMLCO, DCAMLCO, all Branch Manager/s, Branch Anti-Money Laundering Compliance Officers (BAMLCO), compliance officers and all other employees including contracted and outsourced staffs will be responsible for ensuring compliance with the Money Laundering Prevention Act, 2012 and the Anti-Terrorism Act, 2009 and relevant directives/circulars of Bangladesh Financial Intelligence Unit (BFIU) in this regard.

11. General procedures for customer due diligence (CDD)/know your customer (KYC)

1. The new uniform account opening form and KYC profile have now become the integral part of establishing account relationship. They are mandatory and a vital reference point to all account relationship.
2. With regard to KYC/CDD, customer's risk assessment, record keeping and suspicious transaction reporting, concerned employees will follow the procedure as stated in the AML/CFT Guidelines.
3. As KYC/CDD is an important component of the AML/CFT process, the ongoing monitoring of individual transactions on customer accounts is crucial to improve the ability of the institution to detect criminal activities.
4. IT Division may develop automated systems and processes for classifying customers on the basis of the risk matrix provided by BFIU under new KYC Profile, monitoring transactions with the transaction profile provided by the customers & incorporating watch list as per UN Resolutions in software. These new systems will improve ability of the employees to detect unusual transactions, help the authorities to identify and respond to new money laundering and terrorist financing techniques.
5. DCAMLCO/Branch Manager/BAMLCO/Compliance Officer, as the case may be, will monitor customer's transaction regularly in order to identify suspicious transactions/activities related to both money laundering and terrorist financing. They will also oversee the day to day activities of the Branch and confirm compliance of the instructions of concerned authority.

6. If any news regarding involvement in terrorist financing is published in any reliable online/offline newspaper, then upon suspending/stopping the financial transaction of the suspected person, DBH shall immediatelysubmit the account related information & supporting documents of that account holder to BFIU. In addition to that, financial transaction of associated person (if any) are to be monitored meticulously;
7. Electronic database containing the name ofterrorists/groups declared by UN Resolution 1373(2001), Bangladesh Government and foreign FIU shall be preserved centrally.

12. Non-profit & NGO sector

Accounts of charities, NPOs, NGOs to be treated as high risk accounts and EDD will be performed at the time of opening and operating such accounts for combating TF.

13. Training and awareness of the employees

DBH will continue to devote considerable resource to establish and maintain employees' awareness of the risks of TF, and their competence to identify and report relevant suspicions in this area. The company is dedicated to a continuous program of increasing awareness and training of employees' at all appropriate levels in relation to their knowledge and understanding of CFT issues, their respective responsibilities and the various controls and procedures introduced by DBH to combat TF.

14. Self-assessment

This policy requires that appropriate and timely self-assessments, tests, audits and evaluations be conducted to ensure that DBH is in compliance with the CFT regulations. Each and every Branch shall assess their performance half yearly according to Circular no. 28, dated: May 30, 2023 of Bangladesh Financial Intelligence Unit (BFIU). The shortcomings identified be overcome and complied within next quarter.

15. Independent testing procedures

As per Circular No. 28, dated: May 30, 2023, of Bangladesh Financial Intelligence Unit (BFIU) testing on CFT is to be conducted by the ICC department. While conducting the same, they should also look into, whether the directives of Anti-Terrorism (Amendment) Act, 2013; and BFIU's directives issued from time to time in this respect are followed meticulously by the Branches.

Mentionable that Compliance of CFT is the responsibility of each employee of DBH. Therefore, all guidelines related to AML/CFT be updated as and when required and circulated and ensured that all employees are aware of the Anti-Terrorism Act, 2009, internal guidelines and other policies and procedures.

16. Monitoring

DBH shall effectively reciprocate monitoring of procedures and controls that meet the requirements of DBH's policy, standards and Rules and Regulations under Anti-Terrorism (Amendment) Act, 2013.

16.1 Monitoring process

Appropriate monitoring program for the activities and transactions routed through the customer's account should be instituted. Depending on the type and nature of the account, DBH may fix/set specific threshold to identify the customer activities that do not appear to commensurate with the customer's business activities.

16.2 Suspicious transaction/activity report (STR/SAR):

When there is a suspicion that funds are linked to terrorist financing, concerned officer will submit identified suspicious transaction/activity to their respective DCAMLCO, BAMLCO and Compliance Officer. They shall send a copy of the same with comments through the Branch Manager to CAMLCO without any dely. The STRs/SARs must be reported to Bangladesh Financial Intelligence Unit (BFIU) within shortest possible time after due verification through CCU. The utmost secrecy must be maintained while submitting STRs/SARs as per directives of BFIU.

17. Responsibilities

The management of DBH shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under the Anti-Terrorism Act, 2009 and shall report identified suspicious transaction/activity, if any, to Bangladesh Financial Intelligence Unit (BFIU) immediately.

The Board of Directors, or in the absence of the Board of Directors, the Managing Director shall approve and issue directions regarding the duties of its officers and shall ascertain whether the directives issued by BFIU under section 15 of Anti-Terrorism Act, 2009 (as amended in 2013), which are applicable to DBH as reporting agency, have been complied or not.

The responsibilities of the officials of DBH are presented below in tabular form for easy understanding and smooth implementation by the concerned employee/s:

Responsible Departments or Officials	Responsibilities
Officer in charge who is responsible for opening new accounts / making transaction	a. To interview the potential customer; b. verify customer profile; c. to arrive at threshold limit for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions/activities; d. to restrict non opening of accounts in the name of terrorist/banned organizations; e. to adhere with the provisions of Anti-Terrorism (Amendment) Act, 2013; and f. 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 conducting of

Chief Risk Officer	To assess the TF risk involves in operating activities of the Company and to evaluate adequacy and effectiveness of the control mechanism set for safeguarding the Company's risks.
Head of Operations	a. To scrutinize and ensure that the information furnished in the account opening form/customer profile/threshold limit are in strict compliance with AML/CFT Guidelines before authorizing opening of account; and b. to certify regarding compliance with AML/CFT Guidelines and report suspicious transactions to CAMLCO/Managing Director.
Internal Auditor	To verify and record his comments on the effectiveness of measures taken by the concerned officials and the level of implementation of AML/CFT Guidelines.
CAMLCO	a. To implement and enforce Company's CFT policies; b. send to STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU); c. to inform DCAMLCO/BAMLCO required actions, if any, to be taken.
DCAMLCO	a. To assist CAMLCO to implement and enforce Company's CFT policies; b. send STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU) through CCU; c. ensuring flow of information to BAMLCO towards reporting to CAMLCO and CCU; and d. to assist CAMLCO to take other required actions, if any, to be taken.
BAMLCO	a. Ongoing monitoring of customer's KYC profile/CDD/EDD and transaction activities; b. report STR/SAR/CTR through branch manager to CAMLCO/CCU; c. provide CFT training to branch employees while giving training on AML; d. communicate and update to all employees in case of any changes in national or Company's own policies; e. organize a meeting with all executives/officers at least once after each quarter end as per Circular # 28/2023 of Bangladesh Financial Intelligence Unit (BFIU); and f. submit Self-Assessment Report to CAMLCO/CCU and ICC, as the case may be, on
Branch Manager	a. Ensure that the CFT program is effective within the Branch; b. overall responsibility to ensure that the Branch has an effective CFT program in place and that it is working effectively.
Top Management	Prompt reporting of information regarding STR/SAR/CTR to concerned law enforcing authority in consultation with the competent authority/ies.
Managing Director	Overall responsibility to ensure that DBH has CFT program in place and that it is working effectively.

However appropriate disciplinary action will be initiated against the delinquent official for violation of this policy.

18. Penalties for non-compliance of Anti-Terrorism Act, 2009

(a) According to section 16(3), subsequently amended by section 15 of Anti-Terrorism (Amendment) Act 2013, if any reporting agency fails to comply with the directions laid down in section 16(1), the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Financial Intelligence Unit (BFIU) not exceeding Taka 25(twenty five) lac and BFIU may suspend the registration

or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh, or shall inform the registration or licensing authority about the fact so that the relevant authority may take appropriate measures against the said organization.

(b) According to section 16(4), subsequently amended by section 15 of Anti-Terrorism (Amendment) Act 2013, if the Board of Directors, or in the absence of the Board of Directors (BoD), Chief Executive Officer (CEO), by whatever name called, of any reporting agency fails to comply with the directions laid down in section 16(2), the Chairman of the BoD, or the CEO in relevant cases shall be liable to pay a fine not exceeding Taka 25 (twenty five) lakh and BFIU can terminate the person from the position or in relevant cases shall inform the relevant authority about the issue to take proper steps against him/her.

(c) According to section 16(5), subsequently amended by section 15 of Anti-Terrorism (Amendment) Act 2013, if any reporting agency fails to pay or does not pay any fine imposed by BFIU under section 16(3), or if the Chairman of the Board of Directors, or the Chief Executive Officer, fails to pay or does not pay any fine imposed by BFIU under section 16(4), BB may recover the amount from the reporting agency or by debiting its account maintained in any bank or FI or BB and if any amount of fine remains unrealized or unpaid, BFIU may, if necessary, make an application to the concerned court for recovery.

19. Schedule of Anti-Terrorism (Amendment) Act, 2013

Three schedules have been annexed at the end of this ATA Policy as “Schedule-1”, “Schedule-2” and “Schedule-3” as prescribed in the Anti-Terrorism (Amendment) Act, 2013 and accordingly DBH shall pursue those for combating TF.

"Schedule-1"

[See clause (3A) of section 2 of Anti-Terrorism (Amendment) Act, 2013]

a. Convention for the suppression of unlawful seizure of Aircraft done at the Hague on 16th December, 1970;

b. Convention for the suppression of unlawful acts against the safety of Civil aviation, done at Montreal on 23rd September, 1971;

c. Convention on the prevention and punishment of Crimes against internationally protected person, including diplomatic agents, adopted by the General Assembly of the United Nations on 14th December, 1973;

d. International convention against the taking of hostages adopted by the General Assembly of the United Nations on 17th December, 1979;

e. Convention on the physical protection of nuclear material, adopted at Vienna on 3rd March, 1980;

f. Protocol for the suppression of unlawful acts of violence at airports serving International Civil Aviation, supplementary to the convention for the suppression of unlawful acts against the safety of Civil Aviation, done at Montreal on 24th February, 1988;

g. Convention for the suppression of unlawful acts against the safety of maritime navigation, done at Rome on 10th March, 1988;

h. Protocol for the suppression of unlawful acts against the safety of fixed platforms located on the continental shelf, done at Rome on 10th March, 1988;

i. International convention for the suppression of terrorist bombings, adopted by the General Assembly of the United Nations on 15th December, 1997.

"Schedule-2"

[See section 18 of Anti-Terrorism (Amendment) Act, 2013]

1	2	3	4	5
Serial No.	Name of the entities	Address of the entities	Date of proscription	Remarks
01	Shahadat-e-Al Hikma party Bangladesh	House of Mizanur Rahman, Horogram, Natunpara bypass road, P.S. Rajpara, RMP, Rajshahi.	09-02-2003	
02	Jagrata Muslim Janata Bangladesh (JMJB)	No specific address available	23-02-2005	
03	Jamatul Mujahedin	No specific address available	23-02-2005	
04	Harkatul Jehad Al Islami	No specific address available	17-10-2005	
05	Hizbut Tahrir Bangladesh	H.M. Siddique Manson, 55/A, Purana Palton, Dhaka and 201/C, Palton Tower (3rd Floor), 27 Purana Palton Lane	22-10-2009	
06	Ansarullah Bangla Team	No specific address available	25-05-2015	
07	Ansar-Al-Islam	No specific address available	12-02-2017	
08	Allahr Dol	No specific address available	05-11-2019	
09	Jamatul Ansar Fil Hindal Sharqiya	No specific address available	09-08-2023	

"Schedule-3"

(See section 18 of Anti-Terrorism (Amendment) Act, 2013)

1	2	3	4	5
Serial No.	Name of the entities	Address of the entities	Date of proscription	Remarks

Annexure - A

Customer-wise Risk group	Likelihood	Impact	Risk score	Treatment/Action
New customer	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Customer who brings in large amounts of used notes and/or small denominations	Likely	Major	High	Do not allow transaction until risk is reduced- Follow EDD*
Customer whose business address and registered office are in the different geographic location	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
A customer whose identification is difficult to check	Very likely	Major	Extreme	Do not allow transaction to occur without reducing the risk to acceptable level- Follow EDD*
Customers conducting their business relationship or transactions in frequent and unexplained movement of accounts to different institutions	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
A non- resident customer	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
A corporate customer whose ownership structure is unusual and excessively complex	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Customers submits account documentation showing an unclear ownership structure	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income	Very likely	Major	Extreme	Do not allow transaction to occur without reducing the risk to acceptable level- Follow EDD*

Annexure - A (Cont.)

Customer-wise Risk group	Likelihood	Impact	Risk score	Treatment/Action
A customer comes with premature encashment of fixed deposit	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
A customer generally tries to convince for cash deposit but insists for financial instrument while withdrawing the deposit	Likely	Major	High	Do not allow transaction until risk is reduced- Follow EDD*
A customer who wants to settle his loan early (except swapping and default clients)	Very likely	Moderate	High	Do not allow transaction until risk is reduced- Follow EDD*
government employee having several large amounts of fixed deposit accounts	Likely	Major	High	Do not allow transaction until risk is reduced- Follow EDD*
Personal	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Individual Concern	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Businessmen	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Doctor	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Engineer	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Journalist	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Landlord	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Lawyer	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Pharmacist	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*

Annexure - A (Cont.)

Customer-wise Risk group	Likelihood	Impact	Risk score	Treatment/Action
Teacher	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Director	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
DBH Employee	Unlikely	Minor	Low	Response: Okay to go ahead.
Private Service Holder	Unlikely	Minor	Low	Response: Okay to go ahead.
Bank	Unlikely	Moderate	Low	Response: Okay to go ahead.
Insurance	Unlikely	Moderate	Low	Response: Okay to go ahead.
Manufacturing	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
NBFI	Unlikely	Minor	Low	Response: Okay to go ahead.
Partnership	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Private Limited Company	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Public Limited Company	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Co-operative	Very likely	Moderate	High	Do not allow transaction until risk is reduced- Follow EDD*
Public Sector	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Multinational	Unlikely	Minor	Low	Response: Okay to go ahead.
MLM	Very likely	Moderate	High	Do not allow transaction until risk is reduced- Follow EDD*
Corporate Finance	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Customer who brings in large amounts of used notes and/or small denominations	Likely	Minor	Low	Response: Okay to go ahead.
Agriculture Finance	Likely	Minor	Low	Response: Okay to go ahead.

Annexure - A (Cont.)

Customer-wise Risk group	Likelihood	Impact	Risk score	Treatment/Action
SME Finance	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Housing/Real estate Finance	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Equity Finance	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Syndication Finance	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Capital Market Investment	Unlikely	Minor	Low	Response: Okay to go ahead.
Investment in Bonds	Unlikely	Minor	Low	Response: Okay to go ahead.
Short-Term Deposit	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Long-Term Deposit	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Double Money	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Tripple Money	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
DPS	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Trade and Commerce	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Customer who brings in large amounts of used notes and/or small denominations	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Textile	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Jute and Jute-Products	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*

Annexure - A (Cont.)

Customer-wise Risk group	Likelihood	Impact	Risk score	Treatment/Action
Food Production and Processing Ind.	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Plastic Industry	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Leather and Leather-Goods	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Iron, Steel and Engineering	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Pharmaceuticals and Chemicals	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Cement and Allied Industry	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Telecommunication and IT	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Paper, Printing and Packaging	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Glass, Glassware and Ceramic Ind.	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Ship Manufacturing Industry	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Electronics and Electrical Products	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Power, Gas, Water & Sanitary Service	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Transport and Aviation	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Agriculture	Likely	Minor	Low	Response: Okay to go ahead.
Housing	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*

Annexure - A (Cont.)

Customer-wise Risk group	Likelihood	Impact	Risk score	Treatment/Action
Brokerage & Securities	Likely	Minor	Low	Response: Okay to go ahead.
Direct to the customer	Unlikely	Moderate	Low	Response: Okay to go ahead.
Customer who brings in large amounts of used notes and/or small denominations	Very likely	Moderate	High	Do not allow transaction until risk is reduced- Follow EDD*
Phone, Fax, E-mail	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Third-party, agent or broker	Very likely	Moderate	High	Do not allow transaction until risk is reduced- Follow EDD*
Non-face to face	Very likely	Moderate	High	Do not allow transaction until risk is reduced- Follow EDD*
Any country which is identified by credible sources as having significant level of corruption and criminal activity	Very likely	Major	Extreme	Do not allow transaction to occur without reducing the risk to acceptable level- Follow EDD*
Customer who brings in large amounts of used notes and/or small denominations	Likely	Major	High	Do not allow transaction until risk is reduced- Follow EDD*
Any country known to be a tax haven and identified by credible sources as providing funding or support for terrorist activities or that Have designated terrorist organizations operating within their country	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Any country identified by FATF or FSRBs as not having adequate AML&CFT system	Very likely	Major	Extreme	Do not allow transaction to occur without reducing the risk to acceptable level- Follow EDD*
Any country identified as destination of illicit financial flow	Very likely	Major	Extreme	Do not allow transaction to occur without reducing the risk to acceptable level- Follow EDD*
Branch in any land port, sea port city or any border area	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD*

Annexure - A (Cont.)

Customer-wise Risk group	Likelihood	Impact	Risk score	Treatment/Action
Customer/beneficial owner identification and verification not done properly	Likely	Major	High	Do not allow transaction until risk is reduced- Follow EDD*
Failure to keep record properly	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Failure to scrutinize staffs properly	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Failure to train staff adequately	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Not having an AML&CFT program	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Failure to report suspicious transactions or activities	Likely	Major	High	Do not allow transaction until risk is reduced- Follow EDD*
Not submitting required report to BFIU regularly	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Not having an AML&CFT Compliance Officer	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Failure of doing Enhanced Due Diligence (EDD) for high-risk customers (i.e., PEPs, IPs)	Likely	Major	High	Do not allow transaction until risk is reduced- Follow EDD*
Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*
Not submitting accurate information or statement requested by BFIU or BB	Unlikely	Major	Medium	May go ahead but preferably reduce risk- Follow standard CDD*

Annexure - B

RISK ASSESMENT FORM

Name of the Customer :

Customer ID:

Deposit Number :

1. Type of On-boarding	Score
Branch/Relationship Manager	2
Direct Sales Agent	2
Walk-in	3
Internet/Self check-in/Other/non Face to Face	5

2. Geographic Risks: (Client is-)	Score
Resident Bangladeshi	1
Non-resident Bangladeshi	2
Foreign Citizen	3
For Foreigners:	
Risk classification of country of origin	
Does client's country of citizenship feature in FATF/EU/OFAC/UN Black List/Grey List?	
No	0
Yes	5

3. Type of Customer:	Score
Is client a PEP/Chief or High Official of an International Organization, as per BFIU Circular?	
No	0
Yes	5
Is the client's family/close associates related to PEP/Chief or High Official of International Organization?	
No	0
Yes	5
Is client a IP? or his family/close associates related to IP?	
No	1
Yes (based on assessed risk)	5

4. Product and Channel Risk: (Type of Product)	Score
Savings account	1
Current account	4
FDR	3
Deposit Scheme upto 12 lac	1
Deposit Scheme above 12 lac	3
Forex account	5
S.N.D.	3
R.F.C.D.	5

5. Business and Activity Risk	Score
(a) Business	
Please pick Applicable from Annexure and put the relevant score in the next column	.....
(b) Profession	
Please pick Applicable from Annexure and put the relevant score in the next column	.....

6. Transactional Risks:	Score
What is the client's Average Yearly Transactions Worth?	
<BDT 1 million	1
From BDT 1 million to 5 million	2
From BDT 5 million to 50 million (5 crores)	3
More than BDT 50 million (5 crores)	5

7. Transparency Risk	Score
Does client has Provided credible source of funds	
No	5
Yes	1

Risk Grading:

Risk Type	Overall Score
Regular (< 15)	
High (≥ 15)	

Name of Official/ Relationship Manager Signature with Date	Name of Official/ Relationship Manager Signature with Date

Annexure - B (Cont.)

RISK ASSESMENT FORM

Name of the Customer :

Customer ID:

Deposit Number :

1. Type of On-boarding	Score
Branch/Relationship Manager	2
Direct Sales Agent	2
Walk-in	3
Internet/Self check-in/Other/non Face to Face	5

2. Geographic Risks: (Client is-)	Score
Resident Bangladeshi	1
Non-resident Bangladeshi	2
Foreign Citizen	3
For Foreigners:	
Risk classification of country of origin	
Does client's country of citizenship feature in FATF/EU/OFAC/UN Black List/Grey List?	
No	0
Yes	5

3. Type of Customer:	Score
Is client a PEP/Chief or High Official of an International Organization, as per BFIU Circular?	
No	0
Yes	5
Is the client's family/close associates related to PEP/Chief or High Official of International Organization?	
No	0
Yes	5
Is client a IP? or his family/close associates related to IP?	
No	1
Yes (based on assessed risk)	5

4. Product and Channel Risk: (Type of Product)	Score
Savings account	1
Current account	4
FDR	3
Deposit Scheme upto 12 lac	1
Deposit Scheme above 12 lac	3
Forex account	5
S.N.D.	3
R.F.C.D.	5

5. Business and Activity Risk	Score
(a) Business	
Please pick Applicable from Annexure and put the relevant score in the next column	.....
(b) Profession	
Please pick Applicable from Annexure and put the relevant score in the next column	.....

6. Transactional Risks:	Score
What is the client's Average Yearly Transactions Worth?	
<BDT 1 million	1
From BDT 1 million to 5 million	2
From BDT 5 million to 50 million (5 crores)	3
More than BDT 50 million (5 crores)	5

7. Transparency Risk	Score
Does client has Provided credible source of funds	
No	5
Yes	1

Risk Grading:

Risk Type	Overall Score
Regular (< 15)	
High (≥ 15)	

Name of Official/ Relationship Manager Signature with Date

Name of Official/ Relationship Manager Signature with Date

Annexure – C

Regular e-KYC

Customer ID : | Deposit Number:

Applicant's Name :

Father's Name :

Mother's Name :

Spouse's Name:

PHOTO CUSTOMER | PHOTO OTHERS

Date of Birth: D D M M Y Y Y Y Gender: Male Female Other

NID No: Nationality :

Current Address:

Permanent Address:

Mobile phone : Profession:

Monthly income: Sources of Fund:

Nominee 1:		Relation:		Photograph	
Nominee 2:		Relation:		Photograph	
Nominee 3:		Relation:		Photograph	
Nominee 4:		Relation:		Photograph	

Specimen signature/digital signature (where necessary) Yes No TIN / Other Document (if Any) :

1. Has risk grading done? If assessed risk high then conduct EDD as per BFIU circular.

Risk Type	Overall Score
Regular (< 15)	
High (≥ 15)	

Front Side of the NID : Yes No

Back Side of the NID : Yes No

2. Has UNSCRs check done? Yes No
3. Is the customer is IPs/PEPs? Yes No If Client is PEPs or IPs with higher risk, then conduct EDD as per BFIU circular
4. Is there any adverse media news against the customer? If any then conduct EDD? Yes No
5. Has the source of fund verified/justified? Yes No
6. Are any other documents obtained? Yes No If Any: .....
7. Has review of customer profile done (existing customer)? Yes No If so, date of review.....
8. Has the beneficial ownership checked? Yes No If there any beneficial owner found, then conduct CDD on beneficial owner. If beneficial owner is PEPS, then conduct EDD.
9. What is the average range and usual pattern of customer transactions (over 6/12 months)? .....
10. Is the amount matched with customer's income level: Yes No

11. Nominee details:

12. Source of fund and how it was verified:

13. Details of customer's occupation with nature:

Name of Official/ Relationship Manager Code & Signature with Date

Name of Official/ Relationship Manager Code & Signature with Date

Annexure – C (Cont.)

Simplified e-KYC

Customer ID :

Deposit Number:

Applicant's Name :

Father's Name :

Mother's Name :

Spouse's Name:

PHOTO CUSTOMER

PHOTO OTHERS

Date of Birth: D D M M Y Y Y Y

Gender: Male Female Other

NID No:

Current Address:

Permanent Address:

Mobile Phone :

Email :

Profession:

Nominee 1: Relation: Photograph

Nominee 2: Relation: Photograph

Nominee 3: Relation: Photograph

Nominee 4: Relation: Photograph

Specimen signature/digital signature (where necessary): Yes No

Front Side of the NID : Yes No

Back Side of the NID : Yes No

1. Has UNSCRs check done? Yes No
2. Has review of customer profile done (existing customer)? if so, date of review: D D M M Y Y Y Y
3. What is the average range of customer transaction (over 6/12 months)?
4. Source of fund and how it was verified:
5. Details of customer's occupation with nature:
6. Is the amount matched with customer's income level: Yes No

Name of Official/ Relationship Manager Code & Signature with Date

Name of Official/ Relationship Manager Code & Signature with Date

Annexure - D

DBH Finance PLC.

Know Your Employee Form

(Please go through this form first, then complete it in your own hand writing)

1)PERSONAL DETAILS:

Name :		
Designation :		Employee ID :
Department :		Date of Joining :
Age:	Date of Birth:	Place of Birth:
Nationality:	Religion:	Email:
Height:	Weight:	Blood Group:
NID No:	E-TIN:	Passport No:
Present Address: Phone:	Permanent Address: Phone:	Mailing/Contact Address: Phone:

2. FAMILY DETAILS:

Father's Name:			Occupation:		
Mother's Name:			Occupation:		
Marital Status:			Date of Marriage:		
Spouse's Name:			Occupation:		
Particulars of Children:			Particulars of other Dependants:		
Name	Date of Birth	Gender	Name	Date of Birth	Relationship

Particulars of Relatives (brothers, sisters & brother in laws & close relatives only)			
Name	Date of Birth	Relationship	Occupation

3. EDUCATION:

Name of the Institution	Years Attended		Degree	Year of Passing	Obtained CGPA Div/Class	Major Subjects (Graduation)
	From	To				

Training/Courses Attended (Professional/Occupational/Technical):

Title of Training/Courses	Dates		Institution	Location
	From	To		

Knowledge of Language (Please state good, fair & poor):

Language	Read	Write	Speak

Are you at present attending any studies/ evening courses?

Yes ☐ No ☐

If yes, please give details

Are you applying or you have any plan to go aboard for further studies?

Yes ☐ No ☐

If yes, please give details

4. EMPLOYMENT HISTORY:

(Please start with your present or most recent job first)

Name of the Employer & Nature of Business	Dates		Position held	Last Gross Salary	Reason for leaving
	From	To			

5. PERSONAL DISCLOSURE:

Do you suffer or have suffered from any serious illness or disability? Yes ☐ No ☐ If yes, please give particulars
Have you ever been dismissed/terminated or asked to leave your job? Yes ☐ No ☐ If yes, please mention by whom and when.
Have you ever been convicted of a crime? Yes ☐ No ☐ If yes, please mention nature of conviction & when:

6. OUTSIDE ACTIVITIES & INTEREST:

Membership: Are you now or have been a member of any social or professional clubs/association/societies?

Yes ☐ No ☐

If so, please give particulars

Name of Club/Society/Association	Dates		Nature of club/Society/Association	Office held, if any
	From	To		

Hobby & Interest: Please mention your hobbies & leisure time activities

Country visited: Please name the countries those you have visited

Visited Countries	Year of Visit	Purpose of Visit

7. ADDITIONAL INFORMATION:

Is there anything else you would like to add?

8. REFERENCES:

Two References: Relative		Non - Relative
Name:		Name:
Occupation:	Relation:	Occupation:
Address: Contact No:		Address: Contact No:

CERTIFICATE OF CORRECTNESS

I hereby certify that the particulars/answers furnished by me in this form are accurate to the best of my Knowledge & belief and that I have withheld nothing, which, if disclosed, would affect my employment in this company.

_____

Date _____ Signature of the Employee

Annexure - E

ডিবিএইচ ফাইন্যান্স পিএলসি.

—— শাখা।

শাখা কতৃর্ক Self-Assessment পদ্ধতির মাধ্যমে নিজস্ব অবস্থান নির্ণয়

প্রতিটি আর্থিক প্রতিষ্ঠানের শাখা মানিলন্ডারিং ও সন্ত্র সী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও প্রতিষ্ঠানের নিজস্ব মানিলন্ডারিং প্রতিরোধ ও সন্ত্রসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নবর্ণিত প্রশ্নমালা বিস্তারিত উত্তর প্রদানের মাধ্যমে Self-Assessment পদ্ধতিতে নিজেদের অবস্থান নির্ণয় করবে ঃ

প্রশ্নমালা	যাচাইয়ের মানদন্ড	*শাখার বর্তমান অবস্থা*	*গৃহীত কার্যক্রম বা সুপারিশ*
১. শাখায় মোট কর্মকর্তার সংখ্যা কত (পদানুযায়ী)? কতজন কর্মকর্তা মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন ? (শতকরা হার)	প্রশিক্ষণ সংক্রান্ত রেকর্ড যাচাই করতে হবে।		
২. ক) শাখার মানিলন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা (BAMLCO) জ্যেষ্ঠ ও অভিজ্ঞ কিনা? বিগত দুই বছরে তিনি মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণ পেয়েছেন কি না? খ) শাখায় মানিলন্ডারিং প্রতিরোধ কার্যক্রম যথানিয়মে পরিপালিত হচ্ছে এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় তদারকি ও পর্যালোচনা করে থাকেন কিনা?	BAMLCO কর্তৃক KYC কার্যক্রমের যথার্থতা তদারকি করা হয় কিনা? যথাযথভাবে লেনদেন পরিবীক্ষণ এবং সন্দেহজনক লেনদেন প্রতিবেদন দাখিল (ইন্টারনাল রিপোর্টসহ) করা হয় কিনা? যথাযথভাবে রেকর্ড সংরক্ষণ করা হয় কিনা? STR সনাক্তকরণে ব্যবস্থা নেয়া হয় কিনা?		
৩. BAMLCO সহ শাখার কর্মকর্তাগণ মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কাযে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?	বিষয়টি যাচাইয়ের পদ্ধতি কী?		
৪. শাখা পর্যায়ে ত্রৈমাসিক ভিত্তিতে মানিলন্ডারিং ও সন্ত্রাসী কার্যে 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 মানিলন্ডারিং 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		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীত কার্যক্রম বা সুপারিশ
	(Beneficial Owner) সনাক্ত করা হয় কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরিখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কিনা?		
৬. ঝুঁকির ভিত্তিতে শাখা তাদের গ্রাহকদের শ্রেণিবিন্যাস/শ্রেণিকরণ 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 সন্ত্রাসী কার্যে 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 রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোনো ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোনো ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদনুসারে হিসাব ও লেনদেন কার্যক্রম যাচাই করা হয় কিনা? শাখা এ বিষয়ক নিজস্ব কোনো Mechanism অনুসরণ করে কিনা? এরূপ কোনো 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 কোনো পদ্ধতি অনুসরণ করা হয় কিনা? শাখায় সন্দেহজনক লেনদেন দাখিলের জন্য Internal Reporting		

প্রশ্নমালা	যাচাইয়ের মানদন্ড	শাখার বর্তমান অবস্থা	গৃহীত কার্যক্রম বা সুপারিশ
	Mechanism চালু রয়েছে কিনা? শাখা পর্যায়ে নিষ্পত্তিকৃত Internal Report সংরক্ষণ করা হয় কিনা?		
১১. মানিলন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন, সার্কুলার, প্রশিক্ষণ রেকর্ড, বিবরণী ও অন্যান্য এএমএল/সিএফটি সংক্রান্ত বিষয়াবলির 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 এর 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 ধরনের সতর্কতা অবলম্বন করা হচ্ছে?		
১৩. আর্থিক প্রতিষ্ঠানের প্রধান কার্যালয়, বাংলাদেশ ব্যাংক ও বিএফআইইউ-এর পরিদর্শন প্রতিবেদনে উল্লেখিত মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ পরিপালন বিষয়ক দুর্বলতা/অনিয়মসমূহ নিয়মিত করা হয়েছে কিনা?	না হয়ে থাকলে প্রতিবন্ধকতাসমূহ কী কী?		

শাখা মানিলন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তার নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ	শাখা ব্যবস্থাপকের নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ

Annexure - F

অভ্যন্তরীণ নিরীক্ষা বিভাগ
আর্থিক প্রতিষ্ঠানের নাম; ডিবিএইচ ফাইন্যান্স পিএলসি.
প্রধান কার্যালয়

Independent Testing Procedure
শাখা পরিদর্শনের চেকলিস্ট

আর্থিক প্রতিষ্ঠানের অভ্যন্তরীণ নিরীক্ষা বিভাগ মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও প্রতিষ্ঠানের নিজস্ব মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নলিখিত প্রশ্নমালার যথাযথ উত্তর (ডকুমেন্ট ভিত্তিক) অনুসারে স্কোর প্রদানপূর্বক শাখার মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রমকে মূল্যায়ন করবে। অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক শাখার উপর প্রণীত বার্ষিক নিরীক্ষা প্রতিবেদনে (প্রযোজ্য ক্ষেত্রে পৃথক পরিদর্শন কর্মসূচির আওতায় শুধুমাত্র Independent Testing Procedure ভিত্তিক প্রতিবেদন প্রণীত হবে) মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রম মূল্যায়ন সংক্রান্ত আলাদা অধ্যায়ে সমুদয় বিষয়াদি সুপারিশসহ সন্নিবেশ করবে ।
(যাচাইয়ের মানদন্ড অনুসারে সম্পূর্ণরূপে পরিপালিত হলে সম্পূর্ণ স্কোর, আংশিক পরিপালনে আংশিক স্কোর এবং উত্তর নেতিবাচক হলে শূন্য স্কোর প্রদান করতে হবে।)

ক্রমিক নং	পরিদর্শন ক্ষেত্র	**প্রশ্নমালা**		যাচাইয়ের মানদন্ড	স্কোর	*প্রাপ্ত স্কোর*	মন্তব্য
১.	***শাখা পরিপালন ইউনিট***	১.	শাখায় একজন অভিজ্ঞ ও জ্যেষ্ঠ পরিপালন কর্মকর্তা (BAMLCO) রয়েছেন কি?	অফিস অর্ডার দেখুন। শাখার দ্বিতীয় কর্মকর্তা বা অভিজ্ঞ কোন উর্ধ্বতন কর্মকর্তাকে BAMLCO মনোনীত করা সমীচীন হবে।	১		
		২.	বিগত দুই বছরে তিনি মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণে অংশগ্রহণ করেছেন কি? মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে তিনি যথেষ্ট অবহিত কি?	সাক্ষাৎকার ও নথিপত্রের ভিত্তিতে যাচাই করুন।	২		
		৩.	মানিলন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং এর আওতায় জারীকৃত পলিসি এবং/অথবা নির্দেশনা যথানিয়মে পরিপালিত হচ্ছে- এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় তদারকি ও পর্যালোচনা করে থাকেন কি?	BAMLCO কর্তৃক তদারকি ও পর্যালোচনার প্রক্রিয়া যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করুন।	৩		
		৪.	বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা? BAMLCO কর্তৃক শাখায় পরিচালিত উচ্চ ঝুঁকিযুক্ত হিসাবসহ সকল হিসাবের লেনদেন পরিবীক্ষণ পর্যাপ্ত কি?	মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে শাখার গৃহীত পদক্ষেপ মূল্যায়ন করুন। BAMLCO কর্তৃক উচ্চ ঝুঁকিযুক্ত হিসাবসহ সকল হিসাবের লেনদেন পরিবীক্ষণ পদ্ধতি যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করুন।	৪		
		৫.	*বিএফআইইউ এর* সার্কুলার অনুসারে শাখায়	এ ধরনের হিসাব খোলা ও পরিচালনার	৩		

			PEPs, প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কমর্ক র্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা?	*ক্ষেত্রে বিএফআইইউ এর সার্কুলার* অনুসারে সতর্কতা অবলম্বন করা হচ্ছে কিনা তা যাচাই করুন। তবে PEPs, প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কমর্ক র্তার কোন হিসাব না থাকলেও যদি বিএফআইইউ এর সার্কুলার এ প্রদত্ত নির্দেশনা বাস্তবায়নের প্রক্রিয়া বিদ্যমান থাকে তাহলে শাখা *পূর্ণ* নম্বর প্রাপ্ত হবে।			
		৬.	বিএফআইইউ প্রদত্ত সেলফ্ অ্যাসেসমেন্ট শাখা কর্তৃক কতটুকু সঠিক ও কার্যকরভাবে সম্পাদিত হচ্ছে?	শাখার সেলফ্ অ্যাসেসমেন্ট রিপোর্ট পর্যালোচনা করুন। সঠিক ও কার্যকরভাবে সেলফ্ অ্যাসেসমেন্ট রিপোর্ট প্রণয়ন ও বাস্তবায়নের ভিত্তিতে *নম্বর প্রদান করুন।*	৬		
২.	***মানিলন্ডারিং* প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে কর্মকর্তাদের *জ্ঞান* ও সচেতনতা বৃদ্ধি *এবং ঝুঁকি* প্রতিরোধে গৃহীত ব্যবস্থা**	১.	শাখায় কতজন কর্মকর্তা মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন?	১০০% কমর্ক র্তার প্রশিক্ষণ সম্পন্ন *হলে তা* সন্তোষজনক বলে বিবেচিত হবে। প্রশিক্ষণের হার অনুসারে নম্বর প্রাপ্ত হবে।	৩		
		২.	*শাখার কর্মকর্তাগণ মানিলন্ডারিং* ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?	শাখার সংশিষ্ট কর্মকর্তাদের সাক্ষাৎকারের ভিত্তিতে মূল্যায়ন করুন।	৪		
		৩.	মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রম মূল্যায়নের জন্য একটি ত্রৈমাসিক ভিত্তিতে শাখা ব্যবস্থাপকের নেতৃত্বে কর্মকর্তাগণের সভা আয়োজন করা হয় কিনা?	সভার আলোচ্যসূচি সংগ্রহ ও এর কার্যকারিতা পরীক্ষা করুন।	৫		
		৪.	বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং ব্যাংকের নিজস্ব নীতিমালা অনুযায়ী মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা?	কী ধরনের ব্যবস্থা গ্রহণ করা হয়েছে যাচাই করুন।	৩		
৩.	***গ্রাহক পরিচিতি (KYC) নিরূপণ পদ্ধতি***	১.	সকল প্রকার হিসাব খোলা ও লেনদেন পরিচালনার ক্ষেত্রে মানিলন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং বিএফআইইউ কর্তৃক জারীকৃত সার্কুলারের নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা ?	প্রত্যেক ধরনের ৪/৫ টি হিসাবের নমুনা পরীক্ষা করুন। নিম্নোক্ত বিষয়ে সন্তুষ্টিসাপেক্ষে নম্বর প্রদান করুনঃ গ্রাহক পরিচিতির যথার্থতা কিভাবে *যাচাই করা হয়?* কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয়েছে কিনা? হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) *সনাক্ত করা* হয়েছে কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরিখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কিনা?	৬		

		২.	বিএফআইইউ কর্তৃক জারীকৃত সার্কুলারের নির্দেশনা অনুসারে শাখা যথাযথভাবে ঝুঁকির ভিত্তিতে তাদের গ্রাহকদের শ্রেণিবিন্যাস/ শ্রেণিকরণ করে কি?	বিএফআইইউ কর্তৃক জারীকৃত সার্কুলারের নির্দেশনা পরিপালিত হয় কিনা যাচাই *করুন।*	৬		
		৩.	উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে প্রয়োজনীয় *অতিরিক্ত তথ্য সংগ্রহ করা হয় কি?*	*কী* ধরনের তথ্য সংগ্রহ করা হয় এবং তা যথেষ্ট কিনা পরীক্ষা করুন।	৫		
		৪.	শাখা কি গ্রাহকের KYC Profile *নির্দিষ্ট সময় পর* পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে থাকে?	KYC Profile *পুনঃমূল্যায়ন ও হালনাগাদ পদ্ধতি মূল্যায়ন করুন।*	৫		
৪.	**সন্ত্রাস বিরোধী *আইন, ২০০৯ এর পরিপালন***		সন্ত্রাস বিরোধী আইন, ২০০৯ এর *অধীন* সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধের লক্ষ্যে শাখা কী ধরনের *কার্যকর* পদক্ষেপ গ্রহণ করেছে?	নিম্নোক্ত বিষয়ে সন্তুষ্টিসাপেক্ষে নম্বর *প্রদান করুনঃ* জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোনো *ব্যক্তি* বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক *তালিকাভুক্ত* কোনো *ব্যক্তি বা নিষিদ্ধ* ঘোষিত সত্তার নামের *তালিকা শাখায় সংরক্ষণ* ও তদনুসারে হিসাব ও লেনদেন *কার্যক্রম যাচাই করা হয় কিনা?* শাখা এ বিষয়ক নিজস্ব কোনো Mechanism অনুসরণ করে কিনা? এরূপ ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত *করা হয় কিনা ?*	৫		
৫.	**সন্দেহজনক লেনদেন প্রতিবেদন *(STR)* ও নগদ লেনদেন প্রতিবেদন *(CTR)***	১.	শাখার কর্মকর্তাগণ সন্দেহজনক লেনদেন প্রতিবেদন (STR) সম্পর্কে অবহিত আছেন কি?	শাখায় সন্দেহজনক লেনদেন দাখিলের *জন্য* Internal Reporting Mechanism চালু আছে কিনা? তা সকল কর্মকর্তা জানেন *কিনা?*	৫		
		২.	শাখায় মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত সন্দেহজনক লেনদেন চিহ্নিতকরণের কার্যকর পদ্ধতি চালু আছে কি? এ যাবৎ কতগুলো সন্দেহজনক লেনদেন প্রতিবেদন (STR) BAMLCO কর্তৃক CCU এর নিকট রিপোর্ট করা হয়েছে?	শাখায় সন্দেহজনক লেনদেন সংঘটিত হওয়া সত্ত্বেও যদি BAMLCO কর্তৃক CCU এর নিকট কোনো STR *না করা* হয়ে থাকে তাহলে তা অসন্তোষজনক বিবেচিত হবে। নথি ও সিস্টেম পরীক্ষা করে শাখায় STR সনাক্তকরণের জন্য কোনো পদ্ধতির প্রবর্তন করা হয়েছে কিনা তা যাচাই করুন। নিম্নোক্ত বিষয়ে সন্তুষ্টি সাপেক্ষে নম্বর *প্রদান করুনঃ* শাখায় সন্দেহজনক লেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখা পর্যায়ে নিষ্পত্তিকৃত Internal Report যথাযথভাবে সংরক্ষণ করা হয় *কিনা?*	৪		
		৩.	শাখা কর্তৃক যথাযথ ও সঠিকরূপে নগদ লেনদেন প্রতিবেদন (CTR) করা হয় কিনা?	এতদ্‌সংক্রান্ত নথি পরীক্ষা করুন। (কমপক্ষে এক মাসের নগদ লেনদেন) ক্যাশ রেজিস্টার/বিবরণী হতে পরীক্ষা করুন এবং এর ভিত্তিতে ঐ মাসে	২		

				দাখিলকৃত নগদ লেনদেন প্রতিবেদন পরীক্ষাপূর্বক নগদ লেনদেন প্রতিবেদন দাখিলের সঠিকতার বিষয়ে মূল্যায়ন করুন।			
৬.	**CCU বরাবর বিবরণী দাখিল**	১.	শাখা কর্তৃক কতটি বিবরণী CCU বরাবর দাখিল করা হয়েছে? শাখা কি যথাসময়ে বিবরণী দাখিল করে?	এতদ্‌সংক্রান্ত নথি পরীক্ষা করুন। বিলম্বে অথবা বিবরণী দাখিল না করলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
		২.	শাখা কর্তৃক নিয়মিতভাবে সেল্‌ফ অ্যাসেসমেন্ট করা হয় কিনা? প্রস্তুতকৃত বিবরণী যথাযথ কিনা?	এতদ্‌সংক্রান্ত বিবরণী পরীক্ষা করুন। তথ্যাদি সঠিক ও পরিপূর্ণ না হলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
৭.	**রেকর্ড সংরক্ষণ**	১.	গ্রাহক পরিচিতি (KYC) এবং লেনদেন সম্পর্কিত রেকর্ড যথাযথভাবে সংরক্ষণের বিধান আছে কি?	৫টি বন্ধ হিসাব পরীক্ষা করুন। এক্ষেত্রে মানিলন্ডারিং প্রতিরোধ আইন এর বিধান যথাযথভাবে অনুসরণ করা হয়েছে কিনা যাচাই করুন।	৪		
		২.	নিয়ন্ত্রণকারী কর্তৃপক্ষ বা CCU এর চাহিদা মোতাবেক রেকর্ডসমূহ সরবরাহ করা হয় কি?	এতদ্‌সংক্রান্ত নথি পরীক্ষা করুন। যথাসময়ে ও যথাযথ তথ্য সরবরাহ না করলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
৮.	**AML/CFT সম্পর্কিত শাখার সার্বিক কার্যক্রম**	১.	শাখা ব্যবস্থাপক (BAMLCO না হলে) মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কর্মসূচি বাস্তবায়নে যথাযথ ভূমিকা পালন করে কি?	শাখায় আয়োজিত সভার আলোচ্যসূচি ও শাখা ব্যবস্থাপকের সাথে সাক্ষাৎকার এবং এ বিষয়ে শাখার পরিপালন অবস্থার ভিত্তিতে মূল্যায়ন করুন।	৫		
		২.	পূর্ববর্তী অভ্যন্তরীণ ও বহিঃ নিরীক্ষা প্রতিবেদন পরীক্ষাকালে AML/CFT বিষয়ক কোনো অনিয়ম ও দুর্বলতার উল্লেখ আছে কিনা এবং শাখা কোনো সংশোধনমূলক ব্যবস্থা গ্রহণ করেছে কিনা?	সর্বশেষ নিরীক্ষা সংক্রান্ত রিপোর্ট পরীক্ষা করুন এবং কী ধরনের সংশোধনমূলক ব্যবস্থা নেওয়া হয়েছে যাচাই করুন।	৪		
		৩.	শাখার সার্বিক কার্যক্রম সন্তোষজনক কি?	শাখার মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ সংক্রান্ত সার্বিক কার্যক্রম এবং শাখা ব্যবস্থাপকের পারফরম্যান্সের ভিত্তিতে মূল্যায়ন করুন।	৬		

স্কোর	রেটিং
৯০$^{+}$-১০০	শক্তিশালী (Strong)
৭০$^{+}$-৯০	সন্তোষজনক (Satisfactory)
৫৫$^{+}$-৭০	মোটামুটি ভাল (Fair)
৪০$^{+}$-৫৫	প্রান্তিক (Marginal)
৪০ ও এর নিচে	অসন্তোষজনক (Unsatisfactory)

Annexure - G

To whom it may concern

Re: Statement of Compliance

I do hereby declare & confirm that as an employee of DBH, I:

1. have read the Company's Guidelines on "Prevention of Money Laundering and Combating Terrorist Financing"; as well as circulars/directives of Bangladesh Financial Intelligence Unit (BFIU), and Government's Acts on Anti-Money Laundering and Anti-Terrorism and understood the implications thereof;

2. shall comply the applicable laws and regulations and corporate ethical standards;

3. shall comply all rules and regulations in the normal course of my assignments. It is my responsibility to become familiar with the rules and regulations that relate to my assignment; and

4. shall be held responsible for carrying out compliance responsibilities on prevention of Money Laundering and combating Terrorist Financing meticulously.

Signature: ……
Name:
Designation:
Department:
Job location: