

PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING MANUAL



LANKAN ALLIANCE FINANCE LTD
Laila Tower (Level 10), 8 South Gulshan Avenue, Gulshan 1,
Dhaka-1212, Bangladesh.

Prevention of Money Laundering and Terrorist Financing Manual

Lankan Alliance Finance Limited



<u>Section-3: Compliance requirement</u>	14-24
3.1.1 Money Laundering Prevention Act,2012	14-18
3.1.2 Anti Terrorism (Amendment) Act 2012	18-21
3.2 Customer identification	21
3.3 Establishment of purpose of business relationship	22
3.4 Identification of ultimate beneficial owner	22
3.5 Client account monitoring	23
3.6 Reporting of suspicious circumstances/transactions (STR)	23
3.7 Correspondent business	23
3.8 Staff reliability	23
3.9 Communicating the policy	23-24
3.10 Anti Money Laundering controls	24
3.11 Employee appointment and training	24
3.12 Anti Money Laundering risk analysis	24
3.13 UN Sanctions	24
<u>Section-4: Central Compliance Unit and its reporting</u>	25-29
4.1 Establishment of Central Compliance Unit (CCU)	25
4.2 Responsibilities of CCU	25
4.3 Self assessment	25-26
4.4 Independent testing procedure	26-27
<u>Section 5: Appointment as CAMLCO</u>	27-29
5.1 Position of CAMLCO	27
5.2 Qualification and experience	27-28
5.3 Responsibilities	28-29
Section 6: Branch Anti Money Laundering Officer (BAMLCO)	29-30
Section 7: Responsibilities of other employees	30-31
Section 8: Money Laundering-training and awareness	31-38
8.1 Overview	31-32
8.2 Specific job training	32
8.2.1 New employees	32
8.2.2 Customer Service/Relationship Managers	32
8.2.3 Processing (Back Office) employees	33
8.2.4 Credit Officers	33
8.2.5 Audit and compliance employees	34
8.2.6 Senior Management/Operations Supervisors and Managers	34
8.2.7 Senior Management and Board of Directors	34
8.2.8 AML/CFT Compliance Officer	34

9.2.16	Minor	46
9.2.17	Corporate bodies and other entities	46-47
9.2.18	Companies registered abroad	47
9.2.19	Partnerships and unincorporated businesses	48
9.2.20	Powers of Attorney/ Mandates to operate accounts	48
9.2.21	Timing and duration of verification	48
9.3	Know Your Employee (KYE)	48
Section 10: Record Keeping		48-51
10.1	Statutory requirement	48-50
10.2	Retrieval of records	50
10.3	STR and investigations	50-51
10.4	Branch level record keeping	52-53
10.5	Training records	53
10.6	Sharing of record/information of/to a customer	53
Section 11: Risk Assessment Guidelines		51-101
11.1.1	Introduction	51
11.1.2	Obligation for ML & TF Risk Assessment & Ma	52-53
11.1.3	Assessing Risk	53
11.1.4	Risk Management and Mitigation	53
11.1.5	What is Risk	53
11.1.6	What is Risk Management	54
11.1.7	Which risks do LAFL need to consider	54
11.2	Risk Management Framework	54
11.2.1	Introduction	54-56
11.2.2	Risk Management Framework	56-58
11.2.3	The Risk Management process	59-63
11.2.3.1	Risk Identification	63
11.2.3.2	Risk Assessment	63
11.2.3.3	Calculation Risk Score	63-91
11.2.3.4	Risk Treatment	91-93
11.2.3.5	Monitor & Review	93
11.2.3.6.	Additional tools to help risk Assessment	93

Lankan Alliance Finance Limited

Prevention of Money Laundering and Terrorist Financing Manual

Section-1: Introduction

1.1 Short title

This manual may be called the Prevention of Money Laundering and Terrorist Financing Manual of Lankan Alliance Finance Limited

1.2 Background

Money Laundering is being employed by launderers worldwide to conceal the proceeds earned from criminal activities. It happens in almost every country in the world, and a single scheme typically involves transferring money through several countries in order to obscure its origins. And the rise of global financial markets makes money laundering easier than ever, making it possible to anonymously deposit “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. Combating money laundering and terrorist financing is, therefore, a key element in promoting a strong, sound and stable financial sector.

The United Nations (UN) was the first international organization to undertake significant actions to fight against money laundering through adopting several conventions and resolutions. Following UN action, the Financial Action Task Force on Money Laundering (FATF) was formed by G-7 countries in 1989 as the First intergovernmental body which has recommended 40 recommendations to combat money laundering in 1990. In October 2001, the FATF expanded its mandate to deal

If business relations already exist in that country, it has to be ensured that the business relationship is terminated regardless of LAFL's other contractual or legal obligations

1.4 Definition of Money Laundering

Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities, e.g., fraud, corruption, organized crime, or terrorism etc. According to Section 2(v) of the Money Laundering Prevention Act 2012 "money laundering" means:

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

participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

1.5 Reasons of Money Laundering

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

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

According to the article 7 of the Anti Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means: Offences relating to financing terrorist activities if:

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

1.8 Link between Money Laundering and Terrorist Financing the techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected. As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

1.9 Interpretation

In this manual, unless there is anything repugnant in the law, subject or context:

1.9.1 “Company” means Lankan Alliance finance limited (LAFL)

1.9.2 “The Board” means the Board of Directors of the company.

1.9.3 “The Management” means the persons who are in the policy implementation and operational aspect of the company.

1.9.4 “Managing Director” means the Chief Executive of the company.

1.9.5 “Executive” means an Executive of the company whether temporary or permanent classified as such and includes an Executive on probation.

1.9.6 “AML/CFT AMLD” means Anti-Money Laundering/Combating the Financing of Terrorism Anti-Money Laundering Department.

1.9.7 “APG” means Asia Pacific Group on Money Laundering.

1.9.8 “ATA” means Anti Terrorism Act.

can be shown as legal. So the money launderers and terrorist financier can use this financial instrument for placement and layering of their ill-gotten money.

2.2 Factoring

In international factoring there is a provision that the two firms must be member of Factor Chain International or some association that can ensure the credit worthiness of the firms. In absence of this kind of private sector watchdog in the local factoring, the supplier and the buyer may ally together to legalize their proceeds of crime. Without conducting any bona fide transaction the supplier may get finance from LAFL and LAFL may get repayment from buyer. LAFL may focus on getting repayment without considering the sources fund which can be taken as an opportunity by the money launderer to place their ill-gotten money.

2.3 Private placement of equity/securitization of assets

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

2.4 Personal loan/car loan/home loan

Any person can take personal loan from LAFL and repay it by illegally earned money; thus he/she can launder money and bring it in the formal channel. After taking home loan or car loan, money launderers can repay those with their illegally earned money, and later by selling that home/car, they can show the proce2.5 SME/Women entrepreneur loan

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

2.6 Deposit scheme

LAFL can sell deposit products with at least a six months maturity period. However, the depositor can encash their deposit money prior to the maturity date with prior approval from Bangladesh Bank, foregoing interest income. This deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong measures.

2.7 Loan backed money laundering:In the loan backed money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a loan or mortgage

2. Punishment for violation of a freezing or attachment order – (as per section 5 of MLPA 2012)

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

3. Punishment for divulging information – (as per section 6 of MLPA 2012)

(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 empowered under this Act shall refrain from using, publishing or divulging any Information collected, received, retrieved or known by him/herself during the course of employment or appointment by an institution or agent, or after the expiry of any contract of employment or appointment for any purpose other than the purpose of this Act.

(3) Whoever contravenes the provisions contained in sub-sections (1) and (2) shall be punishable by imprisonment of maximum period of 2 (two) years or a fine, not exceeding Tk. 50 (fifty) thousand or both.

4. Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information – (as per section 7 of MLPA 2012)

(1) Whoever, under this Act – Obstructs or declines to cooperate with any investigation officer carrying out the investigation; or Declines to supply information or submit a report when requested without any reasonable ground; He shall be held to have committed an offence under this Act.

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

5. Punishment for providing false information – (as per section 8 of MLPA 2012)

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

(2) Any person who violates the provisions contained in sub-section (1) will be punishable by imprisonment of maximum period of 3 (three) years or a fine not exceeding Tk. 50 (fifty) thousand or both.

6. Powers and Responsibilities of Bangladesh Bank in Preventing and Restraining the Offence of Money Laundering – (as per section 23 of MLPA 2012)

(1) For the purposes of this Act Bangladesh Bank shall have the following powers and responsibilities:

(2) Provide with the information, if not obliged otherwise by the existing laws or any other cause, to the investigating organization if requested by them for information related to money laundering or suspicious transaction investigation.

(3) If any reporting organization fails to provide requested information timely pursuant to this Section, Bangladesh Bank may impose fine such organization Tk. 10 (ten) thousand per day and up to a maximum of Tk. 5 (five) lacs. If an organization is fined more than 3 times in a financial year, Bangladesh Bank may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization.

(4) If any reporting organization provides false information or statement requested pursuant to this Section, Bangladesh Bank may impose fine to such organization not less than Tk. 20 (twenty) thousand but not more than Tk. 5 (five) lacs. If an organization is fined more than 3 times in a financial year, Bangladesh Bank may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization. (5) If any reporting organization fails to comply with any instruction given by Bangladesh Bank pursuant to this Act, Bangladesh Bank may fine such organization Tk. 10 (ten) thousand per day and up to maximum Tk. 5 (five) lacs for each such non compliance. If an organization is fined more than 3 times in a financial year, Bangladesh Bank may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization.

(6) If any reporting organization fails to comply with the freeze order or suspension order of transaction given by Bangladesh Bank under sub section 1(c) Bangladesh Bank may fine such organization not less than the balance held on that account but not more than twice of the balance at the time of issuance the order. (7) If any person or Reporting Organization fails to pay any fine imposed by Bangladesh Bank under sections 23 and 25 of this Act, Bangladesh Bank may recover the amount from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank. In this regard if any amount of the fine remains unrealized Bangladesh Bank may make an application before the court for recovery and the court may pass any order which it deems fit. (8) If any reporting organization is fined under sub-sections 3, 4, 5 and 6, Bangladesh Bank may impose a fine upon the responsible owner, director, employees and officials or persons employed on a contractual basis of that reporting organization, not less than

1. Offences relating to financing for terrorist activities– (as per section 7 of ATA 2012)

(1) If any person or entity knowingly supplies or expresses the intention to supply money, service, material support or any other property to

another person or entity and where there are reasonable grounds to believe that the full or partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity shall be treated committing the offence of financing for terrorist activities. (2) If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that full or partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization, then he or she or the said entity shall be treated committing the offence of financing for terrorist activities.

(3) If any person or entity knowingly makes arrangements for collecting money, services, material support or any other property for another person or entity and where there are reasonable grounds to believe that the full or the partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity will be treated committing the offence of financing for terrorist activities.

(4) If any person or entity knowingly instigate in such a manner, another person or entity to supply, receive, or arrange money, services, material support or any other property and where there are reasonable grounds to believe that the full or the partial amount of the same has been Used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or Terrorist organization then he or she or the said entity will be treated committing the offence of Financing for terrorist activities.

(5) If any person is found guilty of any of the offences set out in sub- sections (1) to (4), that Person will be sentenced to imprisonment for a term between a maximum of twenty and a Minimum of four years and in addition to this a fine may be imposed not less than the greater of twice the value of the property involved with the offence or taka 10(ten) lac.

(6) (1) If any entity is found guilty of any of the offences set out in subsections (1) to (4), steps May be taken under section 18 and in addition to this a fine may be imposed not less than the Greater of thrice the value of the property involved with the offence or taka 50(fifty) lac ; and

regional or bilateral contract, UN conventions or respective resolutions of UN Security Council ratified by the government. (4) The fund seized under subsection (3) shall be subject to disposal by the respective court pursuant to the respective contracts, conventions or respective resolutions of UN Security Council. (5) In order to perform the responsibilities set out in subsections (1) to (3), governmental, semi-governmental, autonomous bodies shall provide requested information or in certain cases spontaneously provide information to the Bangladesh Financial Intelligence Unit. Page 17 of 83

(6) The Bangladesh Financial Intelligence Unit on demand or in certain cases spontaneously provide information relating to terrorist activities or the financing for terrorist activities to the Financial Intelligence Units of other countries. (7) For the purpose of investigation relating to financing for terrorism law enforcement agencies shall have the right to access any document or file of any bank as per the following conditions: (a) with an order from an appropriate court or tribunal; (b) with the approval of Bangladesh Bank.

3. Duties of Reporting Organizations – (as per section 16 of ATA 2012)

(1) Each reporting organization shall take necessary measures, exercising appropriate caution and responsibility, to prevent and identify financial transactions through them connected to any offence committed under this act and if any suspicious transaction is identified, shall spontaneously report it to the Bangladesh Bank without any delay. (2) The Board of Directors, or in the absence of the Board of Directors the Chief Executive Officer or whatever may be called by, of each reporting organization shall approve and issue directions regarding the duties of its officers, and will ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting organizations, have been complied with. (3) If any reporting organization fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provide any wrong information or false information or statement, the said reporting organization shall be liable to pay a fine determined and directed by Bangladesh Bank, not exceeding Taka 10 (ten) lacs and Bangladesh Bank may suspend the registration or license with a purpose to close the operation of the said agency/organization or any branch, service centre, booth or agent of that organization within Bangladesh or where applicable, shall inform the registration/licensing authority about the subject matter to take appropriate action against the organization.

(4) If any Reporting Organization fails to pay any fine imposed by Bangladesh Bank under sub sections 3 of this Act, Bangladesh Bank may recover the amount from the reporting organizations by debiting their accounts maintained in any bank or financial institution or Bangladesh Bank. In this regard if any amount of the fine remains unrealized Bangladesh Bank may make an application before the relevant court for recovery.

3.2 Customer identification

➤ If a customer operate an account on behalf of another person in his/her own name, LAFL shall collect and preserve the complete and correct information of identity of the person(s) besides the customer.

➤ LAFL shall identify the controller or the owner of the customer.

➤ LAFL shall collect and preserve the complete and correct information of identity of the beneficial owner(s) of the customer. For this purpose, a person will be treated as a beneficial owner if:

(a) he has controlling share of a company and/or (b) hold 20% or more shares of a company. 3.5 Client account monitoring

LAFL shall monitor its customers' account(s) including their business pattern/behavior through inspection/record verification on annual basis to detect unusual/suspicious transactions. In case any unusual/suspicious transactions are found.

3.5 Client account monitoring

LAFL shall monitor its customers' account(s) including their business pattern/behavior through inspection/record verification on annual basis to detect unusual/suspicious transactions. In case any unusual/suspicious transactions are found, LAFL

3.6 Reporting of suspicious circumstances transactions (STR) :

3.6.1 According to Section 2(z) of MLPA 2012 suspicious transaction shall mean such transaction

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

3.6.2 In the above circumstances/transactions LAFL shall report to BB through STR. CAMLCO and BCAMLCO shall always be informed about all suspicious circumstances/transactions. 3.7 Correspondent business

LAFL shall pay special attention to business done only through correspondent.

3.7 Correspondent business:

LAFL shall pay special attention to business done only through correspondent

3.8 Staff reliability

3.12 Anti Money Laundering risk analysis

At the time of analyzing the credit risk, LAFL Executives shall analyze the Anti Money Laundering risk exposure considering product and client risk and mitigate the same.

3.13 UN sanctions

LAFL shall take all necessary actions on UNSCR 1267 and 1373 (targeted financial sanctions). To comply with this direction, LAFL shall prepare a software regarding the UN sanction list for regular searching and if find any account with it, shall inform BFIU immediately.

Section-4: Central Compliance Unit and its reporting

4.1

Sl. # Name of the members Status in CCU XXXX

Dy. CAMLCO 3 M YYYY Secretary

CCU is authorized to adopt new member(s) if they think proper. The quorum for CCU meeting will be four members present in person for that meeting. The Member Secretary shall keep the meeting records in proper manner.

4.2 Responsibilities of CCU

CCU will prepare and issue instructions to be followed by the branches; 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 and terrorist financing. CCU shall be dedicated solely to the organization's related responsibilities and perform the compliance functions. The responsibilities of CCU include:

- (i) Preparing an overall assessment report after evaluating the self assessment reports received from the branches and submitting it with comments and recommendations to the Managing Director on half yearly basis;
- (ii) Preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Compliance Department on that particular quarter;
- (iii) Submitting reports to BFIU according to the guidelines issued by BB.

4.3 Self assessment

4.4.1 LAFL internal compliance department shall perform the independent testing procedure covering the following areas and submit a report to the Board Audit Committee on annual basis:

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

4.4.2 The tests may include interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the financial institution's anti-money laundering procedures along with the following:

- sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- test of the validity and reasonableness of any exemption granted by the financial institution; and
- test of the record keeping system according to the provisions of the laws. Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline.

Section-5: Appointment as CAMLCO

The LAFL management shall designate one employee as CAMLCO allowing authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures in the company. CAMLCO will directly report to the Managing Director for his/her responsibility. 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.

5.1 Position of CAMLCO

The Chief AML/CFT Compliance Officer will be the head of CCU. The designated CAMLCO, directly or through CCU, should be a central point of contact for communicating with the regulatory

- Assists in review of control procedures in LAFL to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
- Monitors the business through self-testing for AML/CFT compliance and take any required corrective action;
- Determines the structure and resource levels of AML;
- Ensures resources are deployed effectively to support the Business in mitigating AML risks;
- Drives communication to the Board / CEO/ Audit Committee and other stakeholders with respect to issues concerning AML;
- Represents AML at Board, Management Committees and at senior corporate level as appropriate;
- Maintains relationships to external auditors, regulatory and other regulatory bodies;
- Controls, manages and administers AML's budget and resources planning processes;
- Is responsible for AML systems, technology, AML Risk Analysis, MIS and operations;
- Manages the Suspicious Transaction Report /Suspicious Activity Report process:
 - ❖ reviewing transactions referred by divisional, regional, branch or unit compliance officers as suspicious;
 - ❖ reviewing the transaction monitoring reports (directly or together with account management personnel);
 - ❖ ensuring that internal Suspicious Activity Reports (SARs): are prepared when appropriate;
 - reflect the uniform standard for “suspicious activity involving possible money laundering or terrorist financing” established in its policy;
 - are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy;
 - are advised to other branches of the institution who are known to have a relationship with the customer;
 - are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk .
 - ❖ ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;
 - ❖ maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner;

	<ul style="list-style-type: none"> • Be diligent regarding the identification (s) of account holder and the transactions relating to the account • Ensure all required documentation is completed satisfactorily • Complete the KYC Profile for the new customer • Ongoing monitoring of customers KYC profile and transaction activity <ul style="list-style-type: none"> • Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO
Customer Service Officer	<ul style="list-style-type: none"> • Support the Account Officer in any of the above roles • Perform the Account Officer roles in their absence
Operations Staff	<ul style="list-style-type: none"> • Ensure that all control points are completed prior to transaction monitoring Be diligent on transaction trends for clients • Update customer transaction profiles in the ledger/system
Branch Manager (Unit Head)	<ul style="list-style-type: none"> • Ensure that the program is effective within the branch/unit • First point of contact for any issues

Risk Management /Credit	<ul style="list-style-type: none"> • Perform Risk Assessment for the Business Officer/ Internal Control • Perform periodic Quality Assurance on the program in the unit Officer • Communicate updates in laws and internal policies
Operations & Technology Manager	Ensures that the required reports and systems are in place to maintain an effective program

- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

8.2 Specific job training

The nature of responsibilities/activities performed by the LAFL Executives is different from one another. So their training on AML/CFT issues should also be different for each category. Job specific AML/CFT trainings are discussed below:

8.2.1 New employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

8.2.2 Customer service/Relationship Managers

Executives who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to the organization's strategy in the fight against money laundering and terrorist financing. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with non-regular (walk-in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

8.2.3 Processing (Back Office) employees

The employees, who receive completed Account Opening, FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training in the processing and verification

the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

8.3 The Combating Terrorism (Amendment) Act, 2012

It should be noted that any training given on anti money laundering must include the subject of the Combating Terrorism (Amendment) Act, 2012, and how this now covers all financial crime, however small. A successful defense, under the Combating Terrorism (Amendment) Act, 2012, on the part of a member of staff of not having been trained to recognize and report suspicions, will leave the firm liable to prosecution for breach of the Regulations.

Not knowing the policies or procedures is not a defense. The regulations have implemented an 'ought' to know stance, and therefore all staff, referred to above must be trained.

8.4 Training procedures

The trainers can take the following steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick "why are they here" assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.
- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file.

8.5 Refresher training

It is of paramount importance that the message given to staff during training is: “There are no degrees of suspicion; you are either suspicious or you are not “when in any doubt, submit a suspicion report”.

8.7 Independent audit function

8.7.1 Why the audit function is necessary

To ensure the effectiveness of the AML/CFT program, LAFL should assess the program regularly and look for new risk factors. Financial institution like LAFL covered by laws should establish and maintain policies, procedures and controls which should include an appropriate compliance function and an audit function.

8.7.2 Why the audit function must be independent

The audit must be independent (i.e. performed by people not involved with the LAFL AML/CFT compliance staff). Audit is a kind of assessment of checking of a planned activity. Only those will check or examine the institution who does not have any stake in it. To ensure objective assessment it is important to engage an independent body to do audit.

8.7.3 Whom they report

The individuals conducting the audit should report directly to the board of directors/senior management.

8.7.4 The ways of performing audit function

Audit function shall be done by the internal audit. At the same time external auditors appointed by LAFL to conduct annual audit shall also review the adequacy of AML/CFT program during their audit.

8.7.5 Internal compliance department

LAFL internal compliance department should be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable. The responsibilities of internal compliance department are:

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

conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits, to the financial sector supervisors.

Section-9: Customer Due Diligence

9.1 Know Your Customer program The adoption of effective Know Your Customer (KYC) program is an essential part of financial institutions' risk management policies. Having sufficiently verified/corrected information about customers "Knowing Your Customer" (KYC) -and making use of that information underpins all AML/CFT efforts, and is the most effective defense against being used to launder the proceeds of crime. Keeping that in view, LAFL adopted adequate KYC program to minimize significant risks, especially legal and reputation risk. Sound KYC policies and procedures not only contribute to the LAFL overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences.

9.2 Know Your Customer procedure

Money Laundering Prevention Act, 2012 requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. According to FATF recommendation where LAFL is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, and to identify the beneficial owner, and to take reasonable measures to verify the identity of the beneficial owner and unable to obtaining information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

9.2.1 Nature of customer's business

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity LAFL shall update this information as appropriate, and as opportunities arise. In line with that information LAFL shall judge whether a transaction carried out by its customers is or is not suspicious.

9.2.2 Identifying real person

9.2.5 Customer acceptance policy: LAFL should be considered the factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to financial services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as public figures or politically exposed persons should be taken exclusively at senior management level. LAFL should also be considered the following aspects of customer relationship:

(i) No account should be opened in anonymous or fictitious name. (ii) Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grades. (iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk. (iv) Not to open an account or close an account where LAFL is unable to apply appropriate customer due diligence measures i.e. LAFL is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the financial institution. Decision by LAFL to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision. (v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity. (vi) Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. (vii) The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.

9.2.6 Customer identification

Customer identification is an essential element of KYC standards. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant,

- details of occupation/employment and sources of wealth or income

- Contact information, such as – mobile/telephone no.

The original, certified copy of the following Photo ID also play vital role to identify the customer:

- Current valid passport;

- Valid driving license;

- National ID Card;

- Employer provided ID Card, bearing the photograph and signature of the

applicant;

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, certificate from any local government organs, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which an institution is unfamiliar, either because of origin, format or language, the institution must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. Financial Institutions should also be aware of the authenticity of passports.

- One or more of the following steps is recommended to verify addresses:

9.2.12 Change in address or other details Any subsequent change to the customer's name, address, or employment details of which LAFL becomes aware should be recorded as part of the Know Your Customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

9.2.13 Record keeping All documents collected or gathered for establishing relationship must be filed in with supporting evidence. Where this is not possible, the relevant details should be recorded on the applicant's file. Institutions which regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issuance should be recorded. The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the institution's own understanding of the applicant's business. Once account relationship has been established, reasonable steps should be taken by the institution to ensure that descriptive information is kept up-to-date as opportunities arise. It is important to emphasize that the customer identification process does not end at the point of application. The need 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. It will also depend on the nature of the product or service being offered, and whether personal contact is maintained enabling file notes of discussion to be made or whether all contact with the customer is remote.

9.2.14 Introducer To identify the customer and to verify his/her identity, an introducer may play important role. An introduction from a respected customer, personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not require or request staff to breach account opening procedures as a favor to an applicant.

9.2.15 Persons without standard identification documentation

that the applicant company has not been, or is not in the process of being, dissolved, and struck off, wound-up or terminated. In addition, if LAFL becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made. No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

The following documents should normally be obtained from companies:

- Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.
- Where the business relationship is being opened in a different name from that of the applicant, the institution should also satisfy itself that the Reason for using the second name makes sense. The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:
 - All of the directors who will be responsible for the operation of the account / transaction.
 - All the authorized signatories for the account/transaction.
 - All holders of powers of attorney to operate the account/transaction.
 - The beneficial owner(s) of the company
 - The majority shareholders of a private limited company.

only be done in exceptional circumstances. Any such decision should be recorded in writing. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is itself suspicious.

9.3 Know Your Employee (KYE)

Institutions and businesses learn at great expense that an insider can pose the same ML/TF threat as a customer. It has become clear in the field that having co-equal programs to know your customer and to know your employee is essential. In an effort to identify and anticipate trouble before it costs time, money and reputation damage, LAFL shall look closely at the people inside their own organizations. Keeping that in mind, LAFL shall introduce a KYE program that will allow it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. The program will perform the background screening of prospective and current employees, especially for criminal history, to keep out unwanted employees and identifying those to be removed.

Section-10: Record keeping

10.1 Statutory Requirement

According to Section 25(1) of Money Laundering Prevention Act, 2012, LAFL shall retain correct and full records of customers' identification and transactions while operating an account of a customer. Again, according to FATF recommendation no. 11 LAFL shall maintain, for **at least five years**, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity. The records prepared and maintained by LAFL on its customer relationship and transactions should be such that:

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

Records relating to verification of identity will generally comprise:

- a description of the nature of all the evidence received relating to the identity of the verification subject;
- 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 will generally comprise:

- 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;
 - ❖ any counter-party;
- details of transaction including:
 - ❖ nature of such transactions;
 - ❖ volume of transactions customer's instruction(s) and authority(ies);

Where LAFL has submitted a report of suspicious transaction to BFIU or where it is known that a customer or any transaction is under investigation, it shall not destroy any records related to the customer or transaction without the consent of the BFIU or conclusion of the case even though the five-year limit may have been elapsed. To ensure the preservation of such records, LAFL CAMLCO shall maintain a register or tabular records of all investigations and inspection made by the investigating authority or Bangladesh Bank and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

- the date of submission and reference of the STR;
- the date and nature of the enquiry;
- the authority who made the enquiry, investigation and reference; and
- details of the account(s) involved.

10.4 Branch level record keeping

To ensure the effective monitoring and demonstrate their compliance with the concerned regulations, LAFL shall ensure the keeping or availability of the following records at the branch level either in hard form or electronic form:

- Information regarding Identification of the customer,
- KYC information of a customer,
- Transaction report,
- Suspicious Transaction/Activity Report generated from the branch,
- Exception report,
- Training record,
- Return submitted or information provided to the Head Office or competent authority.

10.5 Training records

LAFL will comply with the regulations concerning staff training, they shall maintain training records which include:

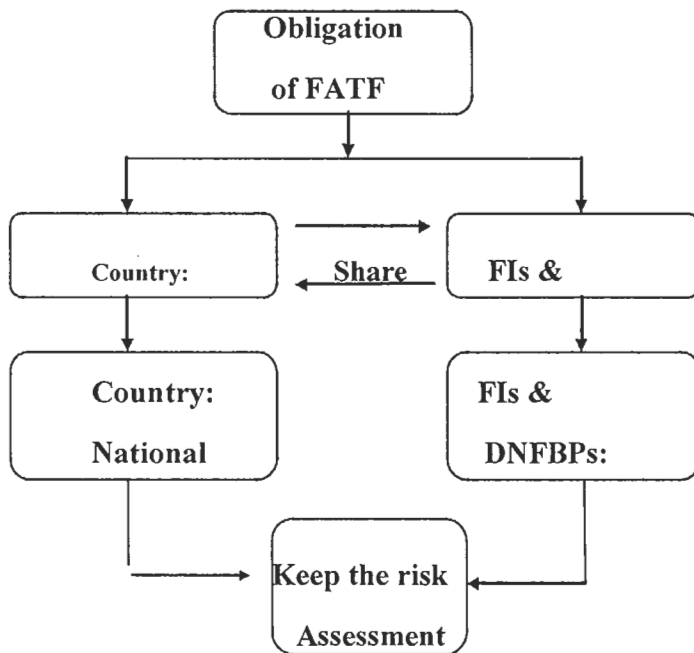
- details of the content of the training programs provided;
- the names of staff who have received the training;
- the date/duration of training;
- the results of any testing carried out to measure staffs understanding of the requirements; and
- an on-going training plan.

10.6 Sharing of record/information of/to a customer

Under MLPA 2012, and ATA, 2009 (as amended in 2012), LAFL shall not share account related information to investigating authority i.e., Anti Corruption Commission or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh Bank.

shall conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. Rule 21 also contains that RO-FI shall utilize this risk assessment report after having vetted by BFIU.

The obligation of FATF Recommendation-1 may be shown as follows:



Money Laundering Prevention Act, 2012 empowers BFIU sufficiently to establish a sound and efficient AML & CFT regime in Bangladesh. Every reporting organization has to comply with the instructions issued by BFIU under the power of Money

Laundering Prevention Act (MLPA), 2012 and Anti Terrorism Act (ATA), 2009 (including all amendments). This Guideline has been issued through BFIU circular letter aiming to strengthen AML&CFT regime in Bangladesh. Therefore, it is obligatory for LAFL to comply with this Guideline.

Money Laundering Prevention Act, 2012 empowers BFIU sufficiently to establish a sound and efficient AML & CFT regime in Bangladesh. Every reporting organization has to comply with the instructions issued by BFIU under the power of Money Laundering Prevention Act (MLPA), 2012 and Anti Terrorism Act (ATA), 2009 (including all amendments). This Guideline has been issued through BFIU circular letter aiming to strengthen AML&CFT regime in Bangladesh. Therefore, it is obligatory for LAFL to comply with this Guideline.

11.1.3 Assessing risk

LAFL should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks arisen from or through customers, products or services and transactions

Regulatory risk is associated with not meeting all obligations of all LAFL under the Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two Acts and instructions issued by BFIU. Examples of regulatory obligations are failure to report STR/SAR, unable or inappropriately verification of customers and lacking of AML&CFT program (how a business identifies and manages the ML&TF risk it may face) etc.

It is unrealistic that a FI would operate in a completely ML&TF risk-free environment. Therefore, it is suggested that a FI shall identifies the ML&TF risk it faces, and then works out the best ways to reduce and manage that risk.

11.2. Risk Management Framework

11.2.1 Introduction

The LAFL will have flexibility to construct and tailor their risk management framework for the purpose of developing risk-based systems and controls and mitigation strategies in a manner that is most appropriate to their business structure (including financial resources and staff), their products and/or the services they provide. Such risk-based systems and controls should be proportionate to the ML&TF risk(s) a FI reasonably faces.

The risk management framework discussed in this guideline aims to assist LAFL to develop and implement their AML&CFT programs in compliance with the existing legal and regulatory requirements and international standards and best practices.

For effective risk management, the LAFL should at all levels follow the principles below:

- Risk management contributes to the demonstrable achievement of objectives and improvement of performance, governance and reputation.
- Risk management is not a stand-alone activity that is separate from the main activities and processes of the FI. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning.
- Risk management helps decision makers making informed choices, prioritize actions and distinguish among alternative courses of action.
- Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

(a) establishing the internal and external context within which the designated service is, or is to be, provided. These may include:

-the types of customers;

-the nature, scale, diversity and complexity of their business; -their target markets;

-the number of customers already identified as high risk;

-the jurisdictions the FI is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML & CFT controls and listed by FATF;

-the distribution channels, including the extent to which LAFL deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;

-the internal audit and regulatory findings;

-the volume and size of its transactions, considering the usual activity of the LAFL and the profile of its customers.

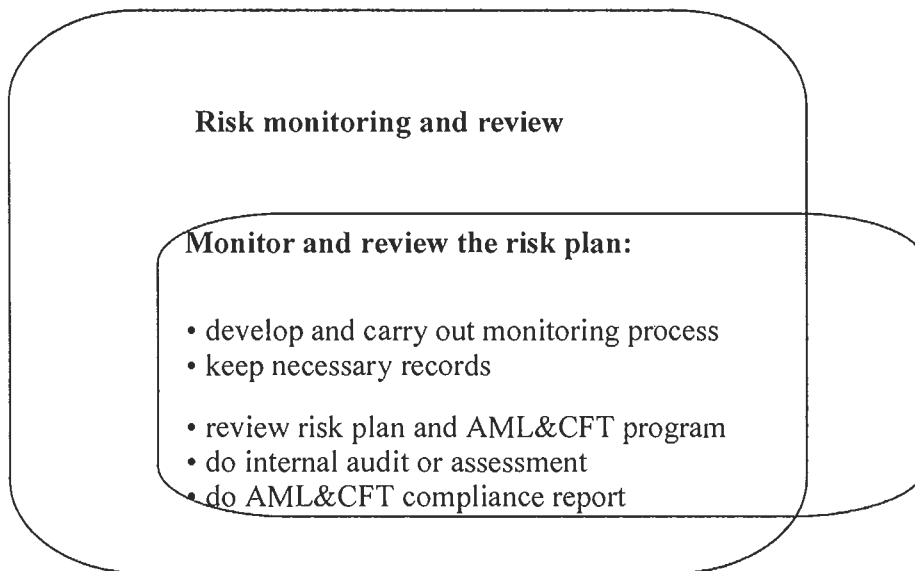
(b) risk identification;

(c) risk assessment or evaluation; and

(d) risk treatment (mitigating, managing, control, monitoring and periodic reviews).

In identifying and assessing the ML & TF risk to which they are exposed, LAFL should consider a range of factors which may include:

Figure 1: The risk management framework at a glance



12.2.3 The risk management process

12.2.3.1 Risk identification

Identify the main ML&TF risks:

- customers
- products & services
- business practices/delivery methods or channels
- country/jurisdiction

Identify the main regulatory risks:

- failure to report STRs/SARs
- inappropriate customer verification
- inappropriate record keeping
- lack of AML&CFT program

LAFI should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an

- a customer or a group of customers making lot of transactions to the same individual or group
- a customer who has a business which involves large amounts of cash
- a customer whose identification is difficult to check
- a customer who brings in large amounts of used notes and/or small denominations.
- customers conducting their business relationship or transactions in unusual circumstances, such as:
 - significant and unexplained geographic distance between the institution and the location of the customer
 - frequent and unexplained movement of accounts to different institutions
 - frequent and unexplained movement of funds between institutions in various geographic locations
- a non- resident customer
- a corporate customer whose ownership structure is unusual and excessively complex
- customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates
- customers submits account documentation showing an unclear ownership structure
- customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income
- a customer comes with premature encashment of fixed deposit
- a customer generally tries to convince for cash deposit but insists for financial instrument while withdrawing the deposit

- branch in any land port, sea port city or any border area

■ **Regulatory risk**

This risk is associated with not meeting the requirements of the Money laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (including all amendments) and instructions issued by BFIU.

Examples of some of these risks are:

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

11.2.3.2. Risk assessment:

For assessing risk, in this chapter we have used, the Table -1, which is a simple & generic table with Risk Score and Treatment. Risk Score can be found by blending likelihood and impact; the details will be explained later on. Table -1 is used, only the examples of customer risk assessment and developed phase by phase so that user can have a good idea of risk assessment.

- **Table 1: Risk Management Worksheet – risk**
- **Risk group:**

Customers				
Risk	Likelihood	Impact	Risk Score	Treatment/Action
A new customer	Unlikely	Moderate	Low	Okay to go ahead

transactions in significant and				Ensure that funds transfers which are
unexplained geographic distance between the institution and the location of the customer				out of character/inconsistent with the history, pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.
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: Ensure that funds transfers which are out of character/inconsistent with the history, pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.
Customers conducting their business relationship or transactions in frequent and unexplained movement of funds between institutions in various geographic locations	Unlikely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD: Ensure that funds transfers which are out of character/inconsistent with the history, pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.

Customers				
Risk	Likelihood	Impact	Risk Score	Treatment/Action
A non- resident customer	Likely	Moderate	Medium	May go ahead but preferably reduce risk - CDD: Apply KYC procedure, Obtaining and verifying Beneficial Owners, Source of Funds, Customer Acceptance Policy,
A corporate customer whose ownership structure is unusual and excessively complex	Unlikely	Major	High	Do not allow transaction until risk is reduced - Follow EDD: i) obtain a declaration from Governing Body/Board of Trustees//Director /Executive Committee/sponsors on ultimate control, purpose and source of funds etc; ii) obtain an undertaking from Governing Body/Board of Trustees/Executive Committee /sponsors to inform the bank/DFI about any change of control or ownership during operation of the Account and iii) obtain a fresh Resolution of the Governing Body/Executive Committee of the entity in case of change in person(s) authorized to operate the account. iv) obtain approval of senior management to commence or continue the business relationship.

sources of legitimate family				
income				<p>ii) Update details of funds providers, if any along with customer's profile; and</p> <p>iii) Identify and verify funds providers if monthly credit turnover exceeds an appropriate threshold to be decided by LAFL</p>
A customer comes with premature encashment of fixed deposit	Likely	Moderate	Medium	<p>May go ahead but preferably reduce risk- Follow standard CDD:</p> <p>Ensure that funds transfers which are out of character/ inconsistent with the history, pattern, purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.</p>
A customer generally tries to convince for cash deposit but insists for financial instrument while withdrawing the deposit	Unlikely	Major	High	<p>Do not allow transaction until risk is reduced - Follow EDD: Obtaining and verifying addition information e.g. occupation, volume of assets, nature of the business, source of funds or source of wealth, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner and obtaining</p>

				relationship.
A customer who wants to settle his loan early	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD: Ensure that payment made which are out of character/ inconsistent with the history/business/source of fund, pattern, purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.
Government employee having several large amounts of fixed deposit accounts	Likely	Moderate	Medium	May go ahead but preferably reduce risk - CDD: Apply KYC procedure, Obtaining and verifying Beneficial Owners, Source of Funds, Customer Acceptance Policy,

PRODUCTS AND SERVICES

Risk group:	Products and Services			
Risk	Likelihood	Impact	Risk Score	Treatment/Action
Payment received from unknown or unrelated third parties	Unlikely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD: Ensure that payment made which are

BUSINESS-PRACTICE/DELIVERY METHODS OR CHANNELS

Risk group:	Business Practice/Delivery Methods or Channels			
Risk	Likelihood	Impact	Risk Score	Treatment/Action
Direct to the customer	Likely	Moderate	Medium	May go ahead but preferably reduce risk- Follow standard CDD: Ensure that payment made which are out of character/ inconsistent with the history/business/source of fund, pattern, purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.

COUNTRY/JURISDICTION

Risk group:	Country/Jurisdiction			
Risk	Likelihood	Impact	Risk Score	Treatment/Action
Any country which is identified by credible sources as having significant level of corruption and criminal activity	Unlikely	Major	High	Do not allow transaction until risk is reduced - Follow EDD: Obtaining verifying and additional information e.g. screening customer with UN Sanction list, occupation, volume of assets, nature of the business, source of funds or source of wealth, available information through public databases, internet, etc.), follow customer acceptance policy of LAFL and obtaining approval of

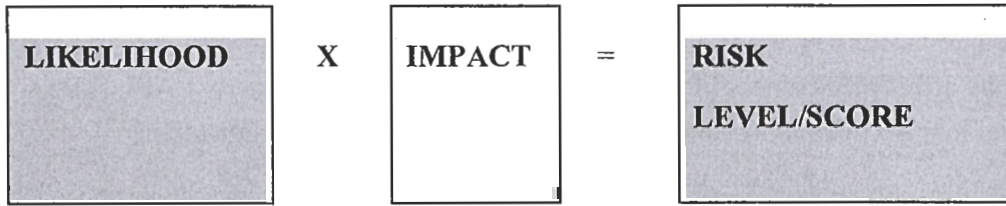
				and verifying source of Fund document, nature of customer's business and also following customer acceptance policy. Perform on- going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
--	--	--	--	---

REGULATORY RISK

Risk group:	Regulatory Risk			Treatment/Action
	Likelihood	Impact	Risk Score	
Customer/beneficial owner identification and verification not done properly	Unlikely	Major	Medium	Follow standard CDD: GAP Analysis, Self Assessment, Independent testing procedure, frequent training, KYE and setting specific action point against shortfall or any non compliance. As per policies of LAFL it is the responsibility of each employee to become familiar with rules and regulations that relate to his or her assignment. Moreover, disciplinary

				framework for a consecutive period of six months.
Failure to scrutinize staffs properly	Unlikely	Major	Medium	<p>Follow standard CDD:</p> <p>Before appointing any employee LAFL shall perform the screening mechanism through KYE in details with proper records/documents.</p> <p>LAFL shall introduce a KYE program that will allow it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. The program will perform the background screening of prospective and current employees, especially for criminal history, to keep out unwanted employees and identifying those to be removed.</p>
Failure to train staff adequately	Unlikely	Major	Medium	<p>Follow standard CDD:</p> <p>Within two months of appointment all employees (including trainees and temporary personnel) responsible for</p>

Not having an AML&CFT Compliance Officer	Unlikely	Major	Medium	Follow standard CDD: GAP Analysis, Self Assessment, Independent testing procedure, frequent training, KYE and setting specific action point against shortfall or any non compliance.
Failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, IPs)	Unlikely	Major	Medium	Follow standard CDD: GAP Analysis, Self Assessment, Independent testing procedure, frequent training, KYE and setting specific action point against shortfall or any non compliance.
Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Unlikely	Major	Medium	Follow standard CDD: GAP Analysis, Self Assessment, Independent testing procedure, frequent training, KYE and setting specific action point against shortfall or any non compliance.
Not submitting accurate Information or statement requested	Unlikely	Major	Medium	Follow standard CDD: GAP Analysis, Self Assessment, Independent testing procedure, frequent training, KYE and setting



- **Likelihood scale**

A likelihood scale refers to the potential of an ML&TF risk occurring in the business for the particular risk being assessed. Three levels of risk are shown in Table 2, but LAFL can have as many as they believe are necessary. This likelihood can be ascertained based on the available information, group consultation or by applying subjective judgment. LAFL shall engage all concerned and competent personnel in ML & TF risk management process including ascertaining the likelihood scale.

Table 2: Likelihood scale

Frequency	Likelihood of an ML&TF risk
Very likely	Almost certain: it will probably occur several times a year
Likely	High probability it will happen once a year
Unlikely	Unlikely, but not impossible

- **Impact scale**

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen.

In assessing the possible impact or consequences, the assessment can be made from several viewpoints. It does not cover everything and it is not prescriptive. Impact of an ML&TF risk could, depending on individual FI and its business circumstances, be rated or looked at from the point of view of:

(Figure 2) and risk score table (Table 4) shown below. Four levels of risk score are shown in Figure 2 and Table 4, but the FI can have as many as they believe are necessary

	May go ahead but preferably reduce risk- Follow standard CDD
Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

- **Risk Assessment and Management Exercise:**

- From the above discussion, LAFL will have an idea to calculate risk score by blending likelihood and impact, the risk matrix and risk score and can assess the risks of individual customer, product/service, delivery channel and risks related to geographic region by using the simplified risk management worksheet (Table-01). It can also fix up its necessary actions against the particular outcomes of risks. All the exercises done by LAFL would be called together "**Risk Registrar**".

Once threat levels and risk scores have been allocated LAFL can be entered in the risk management worksheet (*Table 5*) next to the risk.

Table 5: Risk management worksheet – threat level and risk score

Risk group	Customers			
Risk	Likelihood	Impact	Risk score	Treatment/Action
New customer <i>(example only)</i>	Likely <i>(example only)</i>	Moderate <i>(example only)</i>	Medium <i>(example only)</i>	
Customer who brings in large amounts of used notes and/or small denominations <i>(example only)</i>	Likely <i>(example only)</i>	Major <i>(example only)</i>	High <i>(example only)</i>	
Customer whose business address and	Very likely <i>(example only)</i>	Major <i>(example only)</i>	Extreme <i>(example only)</i>	

Table 6: Risk management worksheet – risk treatment or action

Risk group	Customers			
Risk	Likelihood	Impact	Risk score	Treatment/Action
New customer <i>(example only)</i>	Likely <i>(example only)</i>	Moderate <i>(example only)</i>	Medium <i>(example only)</i>	Standard ID check
Customer who brings in large amounts of used notes and/or small denominations <i>(example only)</i>	Likely <i>(example only)</i>	Major <i>(example only)</i>	High <i>(example only)</i>	Standard + additional ID check
Customer whose business address and registered office are in the different geographic location <i>(example only)</i>	Very likely <i>(example only)</i>	Major <i>(example only)</i>	extreme <i>(example only)</i>	Do not accept as customer

Another way to reduce the risk is to use a combination of risk groups to modify the overall risk of a transaction. LAFL may choose to use a combination of customer, product/service and country risk to modify an overall risk.

It is important to remember that identifying, for example, a customer, transaction or country



risks. It is usually expressed as an acceptable/unacceptable level of risk. Some questions to ask are:

- What risks will the LAFL accept?
- What risks will the LAFL not accept?
- What risks will the LAFL treat on a case by case basis?
- What risks will the LAFL send to a higher level for a

decision? The risk matrix can be used to show the risk appetite of the LAFL

In a risk-based approach to AML & CFT the assessment of risk appetite is a judgment that must be made by the FI. It will be based on its business goals and strategies, and an assessment of the ML & TF risks it faces in providing the designated services to its chosen markets.

Figure 3: Sample risk matrix showing risk appetite

 What is the chance it will happen?	Very Likely	Acceptable Risk Medium	Unacceptable Risk High	Unacceptable Risk Extreme
	Likely	Acceptable Risk Low	Acceptable Risk Medium	Unacceptable Risk High
	Unlikely	Acceptable Risk Low	Acceptable Risk Low	Acceptable Risk Medium
		Minor	Moderate	Major
		 HOW Serious is the risk? IMPAC		

- ii) incorporate market information relevant to the global AML & CFT environment which may assist the banks to make decisions regarding its risk management strategy
- iii) enable relevant, accurate and timely information to be available to a relevant officer (for example, the AML & CFT Compliance Officer) within the LAFL
- iv) allow LAFL to identify, quantify, assess and monitor business activities relevant to ML & TF risk(s)
- v) allow LAFL to monitor the effectiveness of and compliance with its internal AML & CFT systems and procedures
- vi) allow LAFL to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.

It should be noted that LAFL can adopt other strategies in addition to taking into account of any of the above factors (where relevant), if it considers this approach is appropriate in accordance with its risk management framework.

11.3.2 Ongoing Risk Monitoring

A FI's ongoing monitoring of its risk management procedures and controls may also alert

LAFL to any potential failures including (but not limited to):

- a) failure to include all mandatory legislative components
- b) failure to gain board and/or executive approval of the AML & CFT program
- c) insufficient or inappropriate employee due diligence
- d) frequency and level of risk awareness training not aligned with potential exposure to ML & TF risk(s)
- e) changes in business functions which are not reflected in the AML & CFT program (for example, the introduction of a new product or distribution channel)
- f) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML & CFT program

11.3.3 Higher risk scenario

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

a) Customer risk factors

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

a) Country or geographic risk factors

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML & CFT systems
- Countries subject to sanctions, embargos or similar measures
- Countries identified by credible sources as having significant levels of corruption or other criminal activity
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country

c) Product, service, transaction or delivery channel risk factors

- Priority financial service
- Anonymous transactions (which may include cash)
- Non-face-to-face business relationships or transactions
- Payment received from unknown or un-associated third parties.

11.3.5 Risk variables

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

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

11.3.6 Counter Measures for Risk

11.3.6.1 Enhanced due diligence measures

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

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

Section-12: Suspicious transaction report

12.1 Definition of STR

Generally Suspicious Transaction Report (STR) means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be usual manner.

According to Section (2)(z) of MLPA, 2012 “suspicious transaction” means such transactions which deviates from usual transactions; of which there is ground to suspect that,

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

In Anti Terrorism Act, 2009 (as amended in 2012), STR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. One important thing is that according to the guidance notes issued by BB, LAFL need not to establish any proof of occurrence of a predicate offence; it is a must to submit STR only on the basis of suspicion.

12.2 Obligation and reasons for submission of STR

As per the Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (as amended in 2012) and Bangladesh Bank circulars issued from time to time, LAFL is obligated to submit STR to BB. STR is very crucial for the safety and soundness of LAFL and hence CCU of LAFL should consider the following while submitting STR to BB through using specified format (Appendix-B):

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

12.3 Identification and evaluation of STR

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

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

Identification

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

12.4 Risk-based approach

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

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

12.5 Tipping off

□

Section 6 of MLPA 2012 and FATF Recommendation 21 prohibits financial institution, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the LAFL is seeking to perform its CDD obligation in those circumstances. The customer's awareness of a possible STR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation

12.6 Penalties of tipping off

Under section 6 of MLPA, 2012, if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

12.7 "Safe Harbor" provision for reporting

Safe harbor laws encourage financial institutions to report all suspicious transactions by protecting financial institutions and employees from criminal and

- Customer asks many questions about how LAFL disseminates information about the identification of a customer.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

12.8.5 Suspicious activity in credit transactions

- A customer's financial statement makes representations that do not conform to accounting principles.
- Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.

Customer purchases certificates of deposit and uses them as collateral for a loan.

12.8.6 Suspicious commercial account activity

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

12.8.7 Suspicious employee activity

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

Section-13: Conclusion

13.1 Governing Law

This Prevention of Money Laundering and Terrorist Financing Manual shall be governed by the existing circulars and guidelines issued by Bangladesh Bank and laws and regulations of the Government of the Peoples Republic of Bangladesh.

19. Previous experience:

Sl. #	Name of organization	Position	Duration

20. Professional qualification:

Sl. #	Name of degree	Institution	Year

21. Academic qualification:

Exam Title	Concentration/ Major	Institute	Result	Passing Year

22. Reference(s):

		Reference - 1	Reference - 2
Name	:		
Organization	:		
Designation	:		

Department	:	
Duration	:	

Description	Information compiled by	Verified by	Authorized by
Signature	:		
Name	:		
Designation	:		
Remarks	:		

Appendix-B

Suspicious Transaction Report (STR)

A	Reporting institution		
1	Name of the FI:		
2	Name of the Branch:		
B	Details of report		
1	Date of sending report		
2	Is this the addition of an earlier report?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
3	If yes, mention the date of previous report		
C	Suspect account details		

	4	Address	
	5	Date of opening	
	6	Whether introducer is maintaining good relation	

□

—

Reasons for considering the transaction(s) as unusual/suspicious

- a.
- a. Identity of clients
- b. Activity in account
- c. Background of client
- d. Multiple accounts
- e. Nature of transaction
- f. Value of transaction
- g. Other reason (please specify)

(Mention summary of suspicious and consequence of events)
[To be filled by the CAMLCO]

K Has LAFL taken any action in this context? If yes, give details.

L Documents to be enclosed

1. Account opening form along with submitted documents;
 2. KYC profile, Transaction profile;
 3. Account statement for last one year;
 4. Supporting voucher/correspondence mention in sl. # H

Signature:

(CAMLCO or Authorized officer of CCU)

Name:

Designation:

Phone #:

Date:

