2023

Reading Material
on
Financial Crime and Compliance

KAMAL HOSSAIN
Additional Director
Bangladesh Financial Intelligence Unit

INSTITUTE OF BANKERS BANGLADESH | Dhaka

Short Profile of Mr. Kamal Hossain

Mr. Kamal Hossain, Additional Director of Bangladesh Financial Intelligence Unit (BFIU) is engaged with policy formulation and coordination on anti money laundering (AML) and combating financing of terrorism (CFT). He was actively engaged in drafting legal instruments on AML & CFT and implementation mechanism of Targeted Financial Sanction of UN Security Council Resolutions in Bangladesh. Maintaining national and international cooperation, coordinating the AML&CFT initiatives is also his major task as a 'Primary Contact Person' of BFIU. Besides, he worked as a team member in several projects of Policy and Development Group (PDG) and Risk Trend and Methods Group (RTMG) of Financial Action Task Force (FATF)-the international standard setter on AML &CFT, Asia Pacific Group on Money Laundering (APG) and Egmont Group. He has assessed AML &CFT regime of Thailand and Solomon Islands as an APG Financial Expert. He is also a member of country expert team of UNODC to review USA and Switzerland on UNCAC implementation.

Mr. Kamal Hossain completed M. Com (Management) from Dhaka University and Master in Bank Management (MBM) from Bangladesh Institute of Bank Management (BIBM). He is also a Certified Anti Money Laundering Specialist (CAMS). He has participated as resource person or national delegate in several training program, workshop, seminar, plenary meetings and working group meeting of Counter Terrorism Implementation Task Force (CTITF) and Counter Terrorism Executive Director (CTED) of UN, State Party Meeting and Working Group Meeting of UNCAC, FATF, Egmont Group and APG in more than 30 (thirty) countries. He showed his potential as a resource person in home and abroad including Expert Group Meeting on Anti Corruption of World Bank, UNODC and FATF, Expert Group Meeting of AML&CFT Typology in Qatar, Russia, South Korea, and CTITF Global Expert Meeting on Targeted Financial Sanction in UN Head Quarter, New York etc. He worked as Short Term Consultant of World Bank on Illicit out Flow of Funds (IFF) from Developing Countries, as expert member on Lausanne Process for Developing Step by Step Process to recover stolen asset from foreign jurisdictions adopted in State Party Conference of UNCAC and Stolen Asset Recovery Initiatives (StAR) of World Bank and UNODC.

Content

Module A: Conceptual Issues and Terminology

A.1 Financial Crime

The term financial crime has no internationally accepted definition. Generally, financial crimes are defined as such criminal activities carried out by individuals or criminal organizations to provide economic benefits through illegal methods. The UK's Financial Services and Markets Act 2000 (FSMA 2000), Section 6(3) broadly defines the term which include: 'any offence involving fraud or dishonesty; misconduct in or misuse of information relating to, a financial market; or handling the proceeds of crime'. In a broad term it refers to any illegal activity that involves the use of financial systems, institutions, or instruments for illicit purposes, typically with the goal of generating profits for the perpetrators. Financial crimes can take many different forms, from money laundering to fraud, embezzlement, insider trading, and cybercrime.

These crimes are often committed by individuals or groups seeking to profit from illegal activities, such as drug trafficking, human trafficking, or terrorism. Financial crimes can have serious consequences for individuals and society as a whole, including economic instability, loss of public trust in financial institutions, and erosion of the rule of law.

A.1.1 Common Forms of Financial Crime

- Fraud Forgery
- Corruption and Bribery
- Tax Evasion
- Insider Trading and Market Manipulation
- Loan Scam
- Money Laundering
    - Trade Based Money Laundering (TBML)
    - Credit Backed Money Laundering (CBML)
- Terrorist Financing
- Proliferation of Financing of WMD
- Online gaming and Bating
- Online illegal FX Trading
- Crypto Currency/Virtual Currency Trading
- Illegal Multi Level Marketing (MLM)
- Hundi/ Hawala

A.1.2 Key Stakeholders of Countering Financial Crime

- Reporting Organizations (ROs)
- Bangladesh Financial Intelligence Unit (BFIU)

- Investigating Agencies
    - Anti-Corruption Commission (ACC)
    - Criminal Investigation Department (CID), Bangladesh Police
    - Bangladesh Securities and Exchange Commission (BSEC)
    - Customs Intelligence and Investigation Directorate (CIID)
    - Central Intelligence Cell (CIC) of National Board of Revenue
    - Department of Narcotics Control (DNC)
    - Directorate of Environment
- Intelligence Agencies
- Regulatory Authority, like-
    - Bangladesh Bank (BB)
    - Bangladesh Securities and Exchange Commission (BSEC)
    - Insurance Development and Regulatory Authority (IDRA)
    - NGO Affairs Bureau
    - Microcredit Regulatory Authority (MRA)
    - Department of Social Service
    - Self-Regulatory Bodies
- Different Ministries, like-
    - Ministry of Commerce
    - Ministry of Finance
    - Ministry of Information Technology and Communication
    - Ministry of Telecommunication

A.1.3 Financial Crime and Financial Institutions

Financial institutions can be involved in financial crime in three ways: as victim, as perpetrator, or as an instrumentality. Under the first category, financial institutions can be subject to the different types of fraud including, e.g., misrepresentation of financial information, embezzlement, check and credit card fraud, securities fraud, insurance fraud, and pension fraud. Under the second (less common) category, financial institutions can commit different types of fraud on others, including, e.g., the sale of fraudulent financial products, self dealing, and misappropriation of client funds. In the third category are instances where financial institutions are used to keep or transfer funds, either wittingly or unwittingly, that are themselves the profits or proceeds of a crime, regardless of whether the crime is itself financial in nature. One of the most important examples of this third category is money laundering.

A.2 Money Laundering (ML):

Money laundering (ML) is a financial crime that involves disguising the proceeds of illegal

activities such as drug trafficking, bribery, or fraud as legitimate funds. The goal is to make the funds appear legitimate so they can be used without detection. It can be defined in a number of ways. But the fundamental concept of money laundering is the process by which proceeds from a criminal activity is disguised to conceal their illicit origins. Most countries adopted to the following definition as recommended by Financial Action Task Force (FATF) which was delineated in the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;
- The concealing or disguising the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

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

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

i. knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes: -
    (1) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
    (2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
ii. smuggling money or property earned through legal or illegal means to a foreign country;
iii. knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or

disguising its illegal source; or

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

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

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

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

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

A.2.1 Stages of Money Laundering

Process of money laundering can be done through three stages i.e. Placement, Layering and Integration. However, it is important to remember that it is not essential that money launderer will follow all the tree stages in all ML cases.

These stages of Money Laundering are briefly elaborated below:

i. The Placement Stage:

The placement stage represents the initial entry of the proceeds of crime as cash/cash equivalents into the financial system. These illicit proceeds may be placed in financial system in number of ways; for example:

- Cash Deposits in Bank Accounts/ Fixed Deposits
- Multiple Small Deposits to Bank in the same account or in multiple accounts or Multiple deposits under reporting thresholds
- Purchases of Foreign Currency Notes, Bonds and/ or Financial Instruments etc.
- Using third parties to make deposits or Using Services of Traders who may also deposit illegal money with their funds or using legitimate cash intensive businesses to co-mingle illicit funds with the day`s legitimate sales receipts, etc.

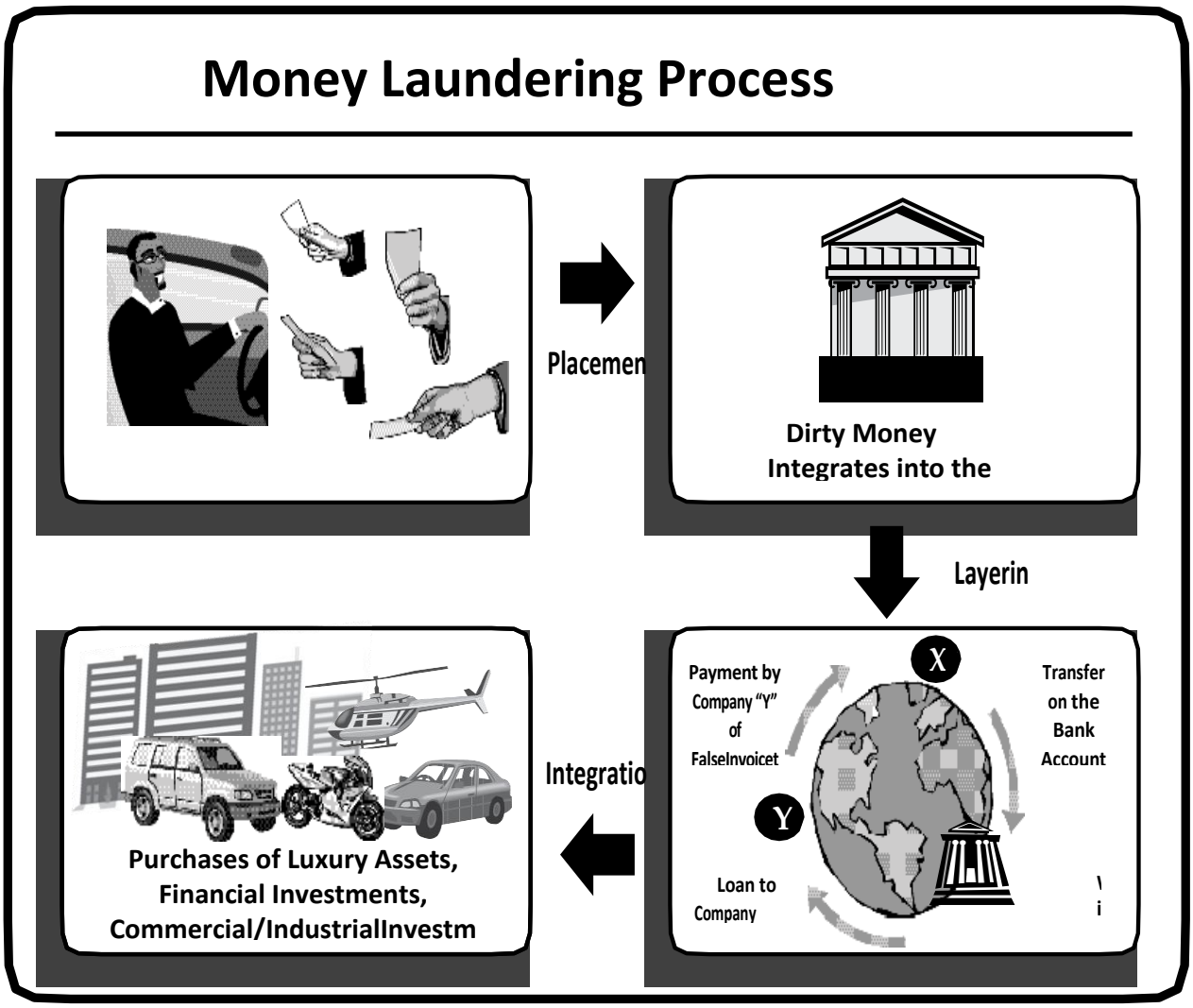
ii. The Layering Stage:

This stage of Money Laundering embodies the process of separating the proceeds of criminal activity from their origin through multiple unrelated transactions without having economic value. This is usually done by sophisticated layering of financial transactions that obscure the audit trail and affect the link with original crime. Layering of financial transaction may comprise the following examples:

- Transfer/ movement of funds from one account to others, from one institution to others, from one territory to others and/ or from one country to others.
- Investing illicit funds with various business firms as an investor etc.
- Temporary loan adjustments for self and associates.
- Investing illegal funds in multiple investments i.e. in real estate, luxury items, valuables, prize bonds, stock markets, etc.

iii. The Integration Stage

- This stage expresses the process of re-uniting the laundered money back into the legitimate economy. This is accomplished by conducting apparently legitimate transactions to disguise the illegal origins of funds, allowing the laundering of funds to be disbursed back to the criminals. There are many different ways, in which the laundered money can be integrated back with the criminal; For Example:
- Lending the funds back to the launderers
- Repaying the proceeds to the launderer as apparently the payment against goods supplied and services rendered.
- Depositing the funds abroad or as collateral for financing facility.
- Investing in real sector or purchasing luxurious goods, car, apartment, etc.



A.2.2 Additional Elements of ML Offences in Bangladesh

Section 2(v) of MLPA, 2012 meets all the required elements in criminalizing ML offences in Bangladesh, whoever it contains some additional elements considering the local context like-

- sub section 2(v) ii i.e smuggling money or property earned through legal or illegal means to a foreign country,
- sub section 2(v)iv i.e concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act (MLPA 2012) may be avoided and
- sub section 2(v) vi i.e acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence.

A.2.3 Punishment for ML Offence in Bangladesh

Money laundering is a criminal offence under section 4(1) of Money Laundering Prevention Act, 2012; punishments for money laundering are-

Punishments for Individual

1. Any person who commits or abets or conspires to commit the offence of money laundering, shall be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lakhs, whichever is greater: but if fail to pay the said fine then court may also add additional imprisonment for a term equivalent of the fine.
2. In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved in or related with money laundering or any predicate offence.

Punishment for Entity

3. Any entity which commits an offence under this section shall be punished as per section 27, sub-section (2) and with a fine of not less than twice of the value of the property or taka 20(twenty) lakhs, whichever is greater and in addition to this the registration of the said entity shall be liable to be cancelled. But, if fail to pay the said fine then court may imprisonment for a term equivalent of the fine to the Proprietor, Chairman or director or any other name mentioned of the entity.

A.2.4 Predicate Offence of ML in Bangladesh

Predicate offences are the offences that generate proceeds of crime and those proceeds of crime laundered in different ways. Sub section 2(cc) of MLPA, 2012 define predicate offences as the

offences committed within or outside the country, the money or property derived from is laundered or attempt to be laundered.

Inclusion of Predicate Offences

As per FATF standard inclusion of predicate offences is done generally by two ways.

- One is Listing Approach-Bangladesh is following this approach and
- Second is Threshold Approach i.e based on the magnitude of criminal liability, severity and penal provisions.
- Some countries are also following mixed approach i.e mix of Listing and Threshold Approach.

There are 29 offences included as Predicate Offences for money laundering in Section 2(CC) of MLPA. Those are as follows:

1. corruption and bribery;
2. counterfeiting currency;
3. counterfeiting deeds and documents;
4. extortion;
5. fraud;
6. forgery;
7. illegal trade of firearms;
8. illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;
9. illegal trade in stolen and other goods;
10. kidnapping, illegal restrain and hostage taking;
11. murder, grievous physical injury;
12. trafficking of women and children;
13. black marketing;
14. smuggling of domestic and foreign currency;
15. theft or robbery or dacoity or piracy or hijacking of aircraft;
16. human trafficking or obtaining money or attempt to obtain money or valuable goods giving someone false assurances of employment abroad;
17. dowry;
18. smuggling and offences related to customs and excise duties;
19. tax related offences;

20. infringement of intellectual property rights;

21. terrorism or financing in terrorist activities;

22. adulteration or the manufacture of goods through infringement of title;

23. offences relating to the environment;

24. sexual exploitation;

25. insider trading and market manipulation using price sensitive information relating to the capital market in share transactions before it is published for general information to take advantage of the market and attempting to manipulate the market for personal or institutional gain;

26. organized crime, and participation in organized criminal groups; and

27. Racketeering
28. Offences that are subject to be trialed in the Cyber Tribunal established under Section 68 of Information and Communication Technology (ICT) Act, 2006[1]
29. Pornography[2]

A.2.5 Reporting Organizations (ROs)

There are 17 (seventeen) types of Reporting Organizations (ROs). Sub-section 2(w) of MLPA, 2012 includes following organizations as reporting organizations of BFIU:

(i) bank;

(ii) financial institution;

(iii) insurer;

(iv) money changer;

(v) any company or institution which remits or transfers money or money value;

(vi) any other institution carrying out its business with the approval of Bangladesh Bank;

(vii) (1) stock dealer and stock broker,
(2) portfolio manager and merchant banker,
(3) securities custodian,
(4) asset manager;

(viii) (1) non-profit organization (NPO),
(2) non-government organization (NGO),

[1] Section 2(cc) (28) of the said Act has empowered Bangladesh Financial Intelligence Unit (BFIU), with the approval of the Government, by notification in the official Gazette, to include any other offence as predicate offence for the purpose of this Act. With the empowerment of the said provision, BFIU has included the 02 (two) offences as predicate offences of ML through a gazette notification (SRO No 85-Ain/2023, dated-23 May 2023).

[2] ibid

(3) cooperative society;

(ix) real estate developer;

(x) dealer in precious metals or stones;

(xi) trust and company service provider;

(xii) lawyer, notary, other legal professional and accountant;

As per the provision of 2(w)(xiii) of MLPA, 2012 BFIU may include any other institution as reporting organization with the approval of the Government from time to time by notification.

A.2.6 Duties and Responsibilities of Reporting Organizations

Section 25(1) of MLPA state that "In preventing money laundering the reporting organizations shall, along with the duties and responsibilities specified by rules, comply with the following other responsibilities, namely: -

1. to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
2. if any account of a customer is closed, to preserve previous records of such account and its transactions for at least 5(five) years from the date of such closure;
3. to provide with the information maintained under clauses (a) and (b) to Bangladesh Financial Intelligence Unit from time to time, on its demand;
4. if any doubtful transaction or attempt of such transaction as defined under clause (n) of section 2 is observed, to report the matter as 'suspicious transaction report' to the Bangladesh Financial Intelligence Unit immediately on its own accord.

A.2.7 Investigating Agencies of ML Case

Money laundering case can be investigated by one or more than one investigating authority (joint investigation) based on related predicate offences. Money Laundering Prevention Rules (MLPR), 2019 specified the following authorities as investigative agencies:

- Anti-Corruption Commission (ACC)
- Department of Narcotics Control (DNC)
- Criminal Investigation Department (CID), Bangladesh Police
- Bangladesh Securities and Exchange Commission (BSEC)
- Bangladesh Customs
- National Board of Revenue (NBR)
- Directorate of Environment

Agencies responsible for enquiry and investigation of the offences described in Money Laundering Prevention Act, 2012 are listed as follows in the schedule of Money Laundering Prevention Rules (MLPR), 2019:

Sl No	Predicate Offences	Agencies responsible for enquiry and investigation Money Laundering Cases
1	Corruption and bribery	Anti-Corruption Commission
2	Counterfeiting of currency	Criminal Investigation Department (CID), Bangladesh Police.
3	Counterfeiting of documents	CID, Bangladesh Police
4	Extortion	CID, Bangladesh Police
5	Cheating	CID, Bangladesh Police
6	Racketeering	CID, Bangladesh Police
7	Trading of illegal weapons	CID, Bangladesh Police
8	Trading of Illegal drugs and narcotics	Directorate of Narcotics Control, CID of Bangladesh Police.
9	Illegal trade of stolen goods and others.	Bangladesh Customs, CID, Bangladesh Police.
10	Abduction, illegal detention and seizing	CID, Bangladesh Police
11	Murder, severe physical injury	CID, Bangladesh Police
12	Women and children trafficking	CID, Bangladesh Police
13	Smuggling	National Board of Revenue, CID, Bangladesh Police
14	Local and foreign currency trafficking	National Board of Revenue, CID, Bangladesh Police
15	Theft or robbery or piracy or aircraft robbery	CID, Bangladesh Police
16	Human trafficking	CID, Bangladesh Police
17	Dowry	CID, Bangladesh Police
18	Smuggling and custom related offences	National Board of Revenue, CID, Bangladesh Police
19	Tax related offences	National Board of Revenue

20	Infringement of Copyright	CID, Bangladesh Police
21	Terrorist financing	CID, Bangladesh Police
22	Adulteration or production of goods by breaching right	CID, Bangladesh Police
23	Environmental crime	Directorate of Environment, CID, Bangladesh Police
24	Sexual exploitation	CID, Bangladesh Police
25	Insider trading and market manipulation	Bangladesh Securities and Exchange Commission
26	Organized crime	CID, Bangladesh Police
27	Taking money by threatening	CID, Bangladesh Police
28*	Offences that are subject to be trialed in the Cyber Tribunal established under Section 68 of Information and Communication Technology (ICT) Act, 2006	CID, Bangladesh Police
29*	Pornography	CID, Bangladesh Police

* With the empowerment of Section 2(cc) (28) of MLPA 2012, these 02 offences have been as predicate offences of ML through a gazette notification (SRO No 85-Ain/2023, dated-23 May 2023.

For terrorism and terrorist financing case Bangladesh Police is the investigating agencies as per the provision of Anti-Terrorism Act, 2009.

A.3 Bangladesh Financial Intelligence Unit (BFIU)

Bangladesh Financial Intelligence Unit (BFIU) is the central agency to fight against money laundering (ML), terrorist financing (TF) and financing of proliferation (PF) of weapons of mass destruction (WMD). Established under the provision of MLPA, 2002 as Anti Money Laundering Department in June, 2002 and renamed as BFIU in 2012. It is responsible for analyzing Suspicious Transaction/Activity Reports (STRs/SARs), Cash Transaction Reports (CTRs) and information related to ML, TF and PF received from reporting organizations (ROs) and other sources. Thereafter, BFIU produces intelligence and disseminate the same to the relevant competent authorities. The unit is also empowered to supervise ML, TF and PF related activities of the ROs. BFIU has also been entrusted with the responsibility of exchanging information related to ML, TF and PF with its foreign counterparts.

A.3.1 Establishment and Nature of BFIU

BFIU was established as per the provision of section 24 of MLPA, 2012. As mentioned above for shouldering the responsibilities mentioned in the MLPA, 2002 Bangladesh Bank established Anti Money Laundering Department (AMLD) in June, 2002 and this AMLD was renamed as BFIU in 2012. Section 24 of MLPA, 2012 ensures the operational autonomy of BFIU. It states that-

"(1)To exercise the powers and responsibilities conferred by this Act there shall be a central agency called Bangladesh Financial Intelligence Unit, which shall

(a) have a separate seal and letter head pad;

(b) have its own office within Bangladesh Bank premise;

(c) Bangladesh Bank shall provide necessary office space, manpower, fund, administrative benefits and other ancillary requirements;

(d) There shall be a whole time Chief Officer of BFIU to be appointed contractually by the Government through a scrutiny committee headed by the Governor, Bangladesh Bank on certain terms and conditions and with status equivalent to that of Deputy Governor of Bangladesh Bank;

(e) for all administrative affairs Chief Officer of BFIU shall take prior approval from Governor, Bangladesh Bank;

(f) for formulation and implementation of required policies and guidelines on AML &CFT Chief Officer shall take prior approval of the Government;

(g) on request of Chief Officer of BFIU, Bangladesh Bank may depute required officials/staff and, as per requirement, request the Government for officials/staff on deputation from the Government or law enforcement agencies; and

(h) contractual consultant may be appointed in it on Chief Officer's requirement.

(2) For the purposes of this Act, the governmental, semi-governmental, autonomous organizations or any other relevant institutions or organizations shall, upon any request or spontaneously, provide the Bangladesh Financial Intelligence Unit with the information preserved or gathered by them.

(3) For the purpose of this Act, Bangladesh Financial Intelligence Unit may, upon request or if necessary spontaneously provide money laundering and terrorist financing related information to other government agencies.

(4) The Bangladesh Financial Intelligence Unit shall provide with information relating to money laundering or terrorist financing or any suspicious transactions to the Financial Intelligence Unit of another country on the basis of any contract or agreement entered into with that country under the provisions of this Act and may ask for any such information from any other country.

(5) The Bangladesh Financial Intelligence Unit may also provide with such information to the Financial Intelligence Units of other countries spontaneously where there is no such contract or agreement under sub-section (4).”

A.3.2 Main Functions of BFIU

As per the provisions of MLPA, 2012 and Anti Terrorism Act (ATA) 2009, the main functions of BFIU are as follows:

- Receive Suspicious Transaction/Activity Reports (STRs/SARs) from the reporting organizations and Cash Transaction Reports (CTRs) from banks and financial institutions; and receive the complaints from different sources.
- Analyze the STRs/SARs from Reporting Organizations (ROs) and CTRs from banks and financial institutions; and the complaints received from different sources.
- Produce financial intelligence reports and disseminate those to investigating agencies for further action(s).
- Maintain a database of all STRs/SARs, CTRs and related information.
- Issue necessary directions and guidance notes from time to time for reporting organizations to prevent money laundering (ML), terrorist financing (TF) and proliferation financing (PF) activities.
- Ensure compliance of the respective Acts and Rules/Regulations/Directives through onsite and off-site supervision of the reporting organizations.
- Monitor the implementation of UNSC Resolutions including UNSCR 1267 and its successors, UNSCR 1373 and UN Security Council Resolutions related to proliferation financing of weapons of mass destruction.
- Impart training to the officials of the reporting organizations, investigating authorities, prosecutors, regulatory agencies and other related organizations or institutions.
- Sign Memorandum of Understanding (MoU) with foreign FIUs to exchange financial intelligence on ML, TF & PF.
- Provide and collect information to/from other FIUs under bilateral arrangements.
- Cooperate and work together with various international organizations including FATF, APG, EGMONT Group, World Bank, IMF, ADB, and UNODC regarding AML & CFT issues.
- Perform secretarial job for UN bodies, National Coordination Committee (NCC) and Working Committee on AML & CFT (WC) and take necessary steps to implement the decisions taken in the committees.
- Work as the secretariat of inter-agency Task Force for Stolen Asset Recovery (StAR).

- Perform activities related to the Central Task Force for preventing illegal Hundi activities, illicit flow of fund and money laundering and monitor implementation of the decisions of the meetings.
- Arrange regular meeting with Anti-Corruption Commission (ACC), Bangladesh Police and other relevant agencies and monitor the implementation of the decisions of the meeting.
- Arrange regular meeting with various regulators like BSEC, IDRA, MRA, NGOAB and different Self-Regulatory Bodies (SRBs).
- Carry out other related functions to prevent and combat money laundering, terrorist financing and proliferation financing activities respectively.
- Create public awareness against ML, TF & PF

A.3.3 Authorities and Responsibilities of BFIU

BFIU's authorities and responsibilities are mentioned in the MLPA, 2012, ATA, 2009 and Rules there under. **Section 23 of MLPA** mentioned that authorities and responsibilities of Bangladesh Financial Intelligence Unit in restraining and preventing the offence of money laundering.

(1) For the purposes of this Act, Bangladesh Financial Intelligence Unit shall have the following authorities and responsibilities, namely: -

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

b) notwithstanding anything contained in any other law, obtain necessary information or report from reporting organizations;

c) an order may be issued to any reporting organization to suspend or freeze transactions of any account for maximum of 7 (seven) times by 30 (thirty) days eachif there are reasonable grounds to suspect that any money or property has been deposited into the account by committing any offence or money of an account has been or might be used to commit a crime or an offence:

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

e) conduct on-site inspections on the reporting organizations, if necessary.

f) arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by Bangladesh Financial Intelligence Unit;

g) Carry out any other functions including monitoring activities of the reporting organizations necessary for the purposes of this Act.

(2) If any investigating agency makes a request to provide it with any information in any investigation relating to money laundering or suspicious transaction, then Bangladesh Financial Intelligence Unit shall provide with such information where there is no obligation for it under any existing law or for any other reason.

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

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

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

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

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

(7A)While conducting enquiry and investigation of the offences under this Act an investigation agency may obtain documents and information related to the customer of a bank or financial institution through an order by the competent court or Bangladesh Financial Intelligence Unit.

(8) If any reporting organization is imposed fine under sub-sections (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit may also impose a fine not less than taka 10 (ten) thousand but not exceeding taka 5 (five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions."

As per Section 25 (2) of MLPA

If any reporting organization violates the provisions of sub-section (1), Bangladesh Financial Intelligence Unit may-

(a) impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty-five) lacs on the reporting organization; and

(b) in addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities of the said organization or any of its branches, service centers, booths or agents, or as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

According to the provision of section 15 and 20A of ATA, 2009, authorities and responsibilities of BFIU are:

(1) Bangladesh Bank may take necessary steps to prevent and identify any transaction carried out by any reporting agency with intent to commit an offence under this Act and for this purpose it shall have the following powers and authority, namely:-

(a) to call for a report relating to any suspicious transaction from any reporting agency, analyze or review the same and to collect additional information relating thereto for the purpose of analyzing or reviewing the same and maintain record or database of them and, as the case may be, provide with the said information or report to the police or other concerned law enforcement agencies for taking necessary actions;

(b) if there is reasonable ground to suspect that a transaction is connected to terrorist activities, to issue a written order to the respective reporting agency to suspend or freeze transactions of that

relevant account for a period not exceeding 30 (thirty) days and, if it appears necessary to reveal correct information relating to transactions of the said account, such suspension or freezing order may be extended for an additional term not exceeding 6 (six) months by 30 (thirty) days at a time;
(c) to monitor and supervise the activities of the reporting agencies;
(d) to give directions to the reporting agencies to take preventive steps to prevent financing of terrorist activities and proliferation of weapons of mass destructions (WMD);
(e) to monitor the compliance of the reporting agencies and to carry out on-site inspection of the reporting agencies for carrying out any purpose of this Act; and
(f) to provide training to the officers and employees of the reporting agencies for the purpose of identification of suspicious transactions and prevention of financing of terrorist activities.
(2) Bangladesh Bank, on identification of a reporting agency or any of its customers as being involved in a suspicious transaction connected to financing of terrorist activities, shall inform the same to the police or the appropriate law enforcement agency and provide all necessary cooperation to facilitate their inquiries and investigations into the matter.
(3) If the offence is committed in another country or the trial of an offence is pending in another country, Bangladesh Bank shall take steps to seize the accounts of any person or entity upon request of the foreign state or pursuant to any international, regional or bilateral agreement, United Nations conventions ratified by the Government of Bangladesh or respective resolutions adopted by the United Nations Security Council.
(4) The fund seized under sub-section (3) shall be subject to disposal by the concerned court or pursuant to the concerned agreements, conventions or resolutions adopted by the United Nations Security Council.
(5) The power and responsibilities of Bangladesh Bank under the provisions of this Act shall be exercised by Bangladesh Financial Intelligence Unit (BFIU), and if Bangladesh Financial Intelligence Unit requests to provide with any information under this Act, all the governmental, semi-governmental or autonomous bodies, or any other relevant institutions or organizations shall, on such request or, as the case may be, spontaneously provide it with such information
(6) Bangladesh Financial Intelligence Unit shall, on request or, as the cases may be, spontaneously provide the financial intelligence units of other countries or any other similar foreign counterparts with any information relating to terrorist activities or financing of terrorist activities.
(7) For the interest of investigation relating to financing of terrorist activities, the law enforcement agencies shall have the right to access any document or file of any bank under the following conditions, namely:- (a) according to an order passed by a competent court or special tribunal; or (b) with the approval of the Bangladesh Bank.
(8) If any reporting agency fails to comply with the directions issued by Bangladesh Bank under this section or knowingly provides any wrong or false information or statement, the said reporting

agency shall be liable to pay a fine, determined and directed by Bangladesh Bank, not exceeding taka 25 (twenty five) lac, and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

(9) If any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank according to sub-section (8), Bangladesh Bank may recover the amount from the reporting agency by debiting its accounts maintained in any other bank or financial institution or in Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

Section 16 (3), (4) and (5) of ATA, 2009

(3) If any reporting agency fails to comply with the provision under sub-section (1), the said reporting agency shall be liable to pay a fine, determined and directed by Bangladesh Bank, not exceeding taka 25 (twenty five) lac and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

(4) If the Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of any reporting organization fails to comply with the provision of sub-section (2), the Chairman of the Board of Directors, or the Chief Executive Officer, as the case may be, shall be liable to pay a fine, determined and directed by Bangladesh Bank, not exceeding taka 25 (twenty five) lac, and Bangladesh Bank may remove the said person from his office or, as the case may be, shall inform the competent authority about the subject matter to take appropriate action against the person.

(5) If any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank under sub-section (3), or if the Chairman of the Board of Directors, or the Chief Executive Officer, by whatever name called, fails to pay or does not pay any fine imposed by Bangladesh Bank under sub-section (4), Bangladesh Bank may recover the amount from the reporting agency or from the account of the concerned person by debiting any account maintained by him in any bank or financial institution or in Bangladesh Bank, and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

Section 20A (1) (j) of ATA, 2009

to issue directions, from time to time, to the reporting agencies by Bangladesh Financial Intelligence Unit for proper implementation of this section.

Section 20A (5) of ATA, 2009

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

A.8 Financial Action Task Force (FATF)

The pace of international activity in the anti-money laundering (AML) field accelerated in 1989 when the Group of Seven nations launched the Financial Action Task Force (FATF) at its annual economic summit in Paris. With France serving as its first chair, this multinational group started working toward a coordinated effort against international money laundering. Originally referred to as the G-7 Financial Action Task Force, today FATF serves as the vanguard in promulgating AML guidance to governmental bodies around the globe. The International Monetary Fund (IMF) and the World Bank also offer important perspectives to the field. FATF has brought significant changes to the ways that Banks and businesses around the world conduct their affairs. It also has brought about changes in laws and in governmental operations. The intergovernmental body is based at the Organization for Economic Cooperation and Development (OECD) in Paris, where it has its own secretariat.

A.8.1 FATF Objectives

FATF's stated objectives are to "set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Starting with its own members, the FATF monitors countries' progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and counter-measures; and, promotes the adoption and implementation of the FATF Recommendations globally."

FATF fulfills these objectives by focusing on several important tasks, which include the following.

a) **Spreading the AML message worldwide:** The group promotes the establishment of a global AML and anti-terrorist financing network based on expansion of its membership, the development of regional AML bodies in various parts of the world and cooperation with other international organizations.

b) Monitoring implementation of the FATF Recommendations among its members.

In 2011, FATF concluded its third round of mutual evaluations of all its members. The process began in 2004. For its fourth round of mutual evaluations, which started in 2014, it adopted a new approach for assessing technical compliance with the Recommendations and assessing if a member's AML/CFT system is effective.

The new Methodology, which was released in 2013, is informed by the experience of FATF, FATF-style regional bodies (FSRBs), the International Monetary Fund (IMF) and the World Bank in conducting assessments of compliance with earlier versions of the FATF Recommendations. Collectively, the technical compliance and effectiveness assessments provide an integrated analysis of the extent to which the country is compliant with the FATF Recommendations and how successful it is in maintaining a strong AML/CFT system. It focuses on the following:

(a) Technical Compliance Assessment: Evaluates the specific requirements of the FATF Recommendations, including how a member relates them to its relevant legal and institutional framework, and the powers and procedures of its competent authorities. The focus is on the fundamental building blocks of an AML/CFT system. For each Recommendation, assessors reach a conclusion about whether a country complies with the FATF standard. The result is a rating of five possible levels of technical compliance.

- Compliant
- Largely compliant
- Partially compliant
- Non-compliant
- Not applicable

(b) Effectiveness Assessment: Seeks to assess the adequacy of a member's implementation of the FATF Recommendations and identifies the extent to which a member achieves a defined set of outcomes that are central to a robust AML/CFT system. The focus is on the extent to which the legal and institutional framework of the member is producing the expected results. For the purposes of the 2013 Methodology, FATF defines effectiveness as "the extent to which the defined outcomes are achieved." Effectiveness is evaluated on the basis of 11 Immediate Outcomes (IO).

1. Money laundering/terrorist financing (ML/TF) risks are known and actions coordinated to combat or thwart the proliferation of ML/TF.
2. International cooperation provides actionable information to use against criminals.

3. Supervisors regulate financial institutions and nonBank financial institutions (NBFIs) and their risk-based AML/CFT programs.
4. Financial institutions and NBFIs apply preventative measures and report suspicious transactions.
5. Legal persons are not misused for ML/TF and beneficial ownership information is avail- able to authorities.
6. Financial intelligence information is used by authorities in money laundering and terrorist financing investigations.
7. Money laundering offenses are investigated and criminally prosecuted, and sanctions are imposed.
8. Proceeds of crime are confiscated.
9. Terrorist financing offenses are investigated and criminally prosecuted, and sanctions are imposed.
10. Terrorists and terrorist organizations are prevented from raising, moving and using money and are not permitted to abuse nonprofit organizations (NPOs).
11. Persons and organizations involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using money.

Each of the 11 Immediate Outcomes (IO) represents a key goal of an effective AML/CFT system. They also feed into the three Intermediate Outcomes that represent major thematic goals of AML/CFT measures.

01. Policy, cooperation and coordination to mitigate money laundering and terrorist financing.
02. Prevention of proceeds of crime entering into the financial system and reporting of such when they do.
03. Detection and disruption of of ML/TF threats. For each individual Immediate Outcome, assessors reach conclusions about the extent to which a country is (or is not) effective and provide an effectiveness rating based on the extent to which the core issues and characteristics are addressed.

    - High level of effectiveness
    - Substantial level of effectiveness
    - Moderate level of effectiveness

- Low level of effectiveness

If a country has not reached a high level of effectiveness, then assessors give reasons why it fell below the standard and recommend measures the country should take to improve its ability to achieve the outcome.

FATF does not have the power to impose fines or penalties against recalcitrant member-nations. However, in 1996, FATF launched a policy for dealing with nations that fail to comply with the FATF Recommendations that it describes as "a graduated approach aimed at enhancing peer pressure." This graduated approach ranges from requiring the country to deliver a progress report at plenary meetings to suspension of membership.

c) Reviewing money laundering trends and countermeasures.

Faced with a financial system that has few geographic limitations, operates around the clock in every time zone and maintains the pace of the global electronic highway, criminals are constantly searching for new points of vulnerability and adjusting their laundering techniques to respond to countermeasures introduced by FATF members and other countries. As such, FATF members are continually gathering information on money laundering trends to ensure the organization's Recommendations remain up to date.

Since its establishment, FATF has focused its work on three main activities:

1. Standard setting,
2. Ensuring effective compliance with the standards,
3. Identifying money laundering and terrorist financing threats.

These activities will remain at the core of FATF's work for the remainder of the mandate. Going forward, FATF will build on the work and respond to new and emerging threats, such as proliferation financing and vulnerabilities in new technologies that could destabilize the international financial system.

A.8.2 FATF 40 Recommendations

A key element of FATF's efforts is its detailed list of appropriate standards for countries to implement. These measures are set out in the 40 Recommendations, which were first issued in 1990 and revised in 1996, 2003 and 2012. FATF has also issued various Interpretative Notes designed to clarify the application of specific Recommendations and to provide additional guidance.

After the events of September 11, 2001, FATF adopted and published the FATF IX Special Recommendations on terrorist financing. The first eight Special Recommendations were adopted

on October 31, 2001, and the ninth on October 22, 2004. The 2012 revisions combined the IX Special Recommendations into the 40 Recommendations.

FATF's Recommendations have become the world's blueprint for effective national and international AML and CFT-related controls. The IMF and the World Bank have recognized the FATF Recommendations as the international standard for combating money laundering and terrorist financing. In 2002, the IMF, the World Bank and FATF agreed to a common methodology to assess compliance with the FATF Recommendations.

The 40 Recommendations provide a complete set of countermeasures against money laundering and terrorist financing, covering

- The identification of risks and development of appropriate policies;
- The criminal justice system and law enforcement;
- The financial system and its regulation;
- The transparency of legal persons and arrangements; and
- International cooperation.

FATF recognizes that because countries have different legal and financial systems, they cannot use identical measures to fight money laundering and terrorist financing. The Recommendations set minimum standards of action for countries to implement according to their particular circumstances and constitutional frameworks. With its 2012 revision, FATF introduced the risk assessment as the first recommendation, underscoring that assessing risk is the first step in combating money laundering and terrorist financing.

With its 2003 revisions of the 40 Recommendations, the FATF expanded the reach of its global blue- print for cracking down on illicit movements of funds. It introduced substantial changes intended to strengthen measures to combat money laundering and terrorist financing, which established further enhanced standards by which countries can better combat money laundering and terrorist financing.

The most important changes made to the Recommendations in 2003 were as follows.

- Expanded coverage to include terrorist financing
- Widened the categories of business that should be covered by national laws, including real estate agents, precious metals dealers, accountants, lawyers and trust services providers
- Specified compliance procedures on issues such as customer identification and due diligence, including enhanced identification measures for higher risk customers and transactions

- Adopted a clearer definition of money laundering predicate offenses
- Encouraged prohibition of so-called shell Banks, typically set up in offshore secrecy havens and consisting of little more than nameplates and mailboxes, and urged improved transparency of legal persons and arrangements
- Included stronger safeguards, notably regarding international cooperation in, for example, terrorist financing investigations.

In 2012, the Recommendations were revised again, incorporating the IX Special Recommendations on terrorist financing into the 40 Recommendations. The most important changes in this revision were

Group	Topic	Recommendations
I	**AML/CFT Policies and Coordination** • Assessing risks and applying a risk-based approach • National cooperation and coordination	1–2
II	**Money Laundering and Confiscation** • Money laundering offenses • Confiscation and provisional measures	3–4
III	**Terrorist Financing and Financing of Proliferation** • Terrorist financing offenses • Targeted financial sanctions related to terrorism and terrorist financing • Targeted financial sanctions related to proliferation • Non profit organizations	5–8
IV	**Financial and Non financial Institution Preventative Measures** • Financial institution secrecy laws • Customer due diligence and record-keeping • Additional measures for specific customers and activities • Reliance, controls and financial groups • Reporting of suspicious transactions • Designated nonfinancial businesses and professions	9–23
V	**Transparency and Beneficial Ownership of Legal Persons and Arrangements** • Transparency and beneficial ownership of legal persons	24–25

	• Transparency and beneficial ownership of legal arrangements	
VI	**Powers and Responsibilities of Competent Authorities and Other Institutional Measures** • Regulation and supervision • Operational and law enforcement • General requirements • Sanctions	26–35
VII	**International Cooperation** • International instruments • Mutual legal assistance • Mutual legal assistance regarding freezing and confiscation • Extradition • Other forms of international cooperation	36–40

Some highlights of the 2012 revision of the 40 Recommendations are as follows-

- **Risk-based approach:** Countries should start by identifying, assessing and understanding the money laundering and terrorist financing risks they face. Then they should take appropriate measures to mitigate the identified risks. The risk-based approach allows countries to allocate their limited resources in a targeted manner in line with their own particular circumstances in order to increase the efficiency of preventative measures. Financial institutions should also use the risk-based approach to identify and mitigate the risks they face.

- **Designated categories of offenses:** The Recommendations specify crimes, called "designated categories of offenses," that should serve as money laundering predicates (i.e. crimes that offenders attempt to conceal through financial subterfuge that should constitute precursory offenses to money laundering). Countries should also put in place provisions to allow for the confiscation of the proceeds of crime or otherwise prevent criminals from having access to their criminal proceeds.

- **Terrorist financing and financing of proliferation**: Countries should criminalize terrorist financing, including the financing of terrorist acts, organizations and individual terrorists, even if no terrorist activity can be directly attributed to the provision of financing. Countries should impose sanction regimes that will allow them to freeze the assets of persons designated by the United Nations Security Council for involvement in terrorism or the proliferation of weapons of mass destruction. Countries should also

establish sufficient controls to mitigate the misuse of nonprofit organizations to provide support to terrorists.

- **Knowledge and criminal liability:** The Recommendations include the concept that knowledge required for the offense of money laundering may be inferred from objective factual circum- stances. This is similar to what is known in some countries as "willful blindness," or deliberate avoidance of knowledge of the facts. In addition, the Recommendations urge that criminal liability—or civil or administrative liability, where criminal liability is not possible—should apply to legal persons as well.

- **Customer due diligence (CDD) measures:** Financial institutions should conduct customer due diligence when they

— establish business relations;

— carry out an occasional transaction or a wire transfer above the specified threshold;

— have a suspicion of money laundering or terrorist financing; and

— have doubts about the veracity or adequacy of previously obtained customer identification information.

Financial institutions must, using a risk-based approach

— identify the customer and verify that customer's identity using reliable, independent source documents, data or information. Establishing accounts in anonymous or obviously fictitious names should be prohibited;

— take reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include understanding the ownership and control structure of the customer;

— understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship;

— conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken in the course of that relationship to ensure that the transactions are consistent with the institution's knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds;

— maintain records of the above customer information as well as all transactions to enable them to comply with requests from competent authorities;

— rely on other parties to conduct customer due diligence in certain circumstances; however,

the relying institution remains liable for compliance with completing the required customer due diligence; and

— establish group-wide AML program for financial groups.

- **Additional customer due diligence on specific customers and activities:** Some customer types and activities pose heightened risks, especially the following.

— **Politically exposed persons (PEPs):** Appropriate steps must be taken to identify PEPs, including obtaining senior management approval of such business relationships, taking measures to establish the sources of wealth and funds and conducting ongoing monitoring.

— **Cross-border correspondent Banking:** Appropriate steps must be taken to understand the respondent institution's business, reputation, supervision and AML controls; obtain management approval of such relationships; document the responsibilities of each institution; mitigate risks associated with payable-through accounts and ensure accounts are not established for shell Banks.

— **Money or value transfer services (MVTS):** Countries should ensure that MVTS are licensed or registered and subject to appropriate AML requirements.

— **New technologies:** Countries and financial institutions should assess the risks associated with the development of new products, business practices, delivery mechanisms and technology. Financial institutions should assess these risks prior to launching new products; they should also take appropriate measures to mitigate the risks identified. It also includes Virtual Asset (VA) and Virtual Asset Service Provides (VASPS).

— **Wire transfers:** Countries should require financial institutions to obtain and send required and accurate originator, intermediary and beneficiary information with wires. Financial institutions should monitor wires for incomplete information and take appropriate measures. They should also monitor wires for those involving parties designated by the United Nations Security Council and take freezing actions or otherwise prohibit the transactions from occurring.

- **Suspicious transaction and/or activity reporting:** Financial institutions must report to the appropriate financial intelligence unit when they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing. The financial institutions and the employees reporting such suspicions should be protected from liability for reporting and should be prohibited from disclosing that they have reported such activity.

- **Expanded coverage of industries:** The Recommendations expand the fight against money laundering by adding new nonfinancial businesses and professions to the roster of financial institutions that are the usual focus of AML efforts. Expanding the scope of AML scrutiny is a key area where many governments have been aiming their AML arsenal in response to an increased flow of illicit money. These designated nonfinancial businesses and professions (DNFBPs) include

  — casinos when customers engage in financial transactions equal to or above a designated threshold. At a minimum, casinos should be licensed; authorities should prevent criminals from participating in casino operations and should supervise casinos to ensure compliance with requirements to combat money laundering and terrorist financing;

  — real estate agents when they are involved in transactions for clients concerning buying and selling properties;

  — dealers in precious metals and stones when they engage in any cash transaction with a customer at or above a designated threshold;

  — lawyers, notaries and independent legal professionals and accountants when they prepare or carry out transactions for clients concerning buying and selling real estate; managing client money, securities or other assets; establishing or managing Bank, savings or securities accounts; organizing contributions for the creation or management of companies; creating, operating or managing legal persons or arrangements and buying and selling businesses; and

  — trust and company service providers when they prepare or carry out transactions for a client concerning certain activities (e.g., when acting as a formation agent of legal persons, acting as a director or secretary of a company, acting as a trustee of an express trust or acting as a nominee shareholder for another person).

  FATF also designated specific thresholds that trigger AML scrutiny. For example, the threshold that financial institutions should monitor for occasional customers is $15,000; for casinos, including internet casinos, it is $3,000; and for dealers in precious metals, when engaged in any cash transaction, it is $15,000.

- **Transparency and beneficial ownership of legal persons and arrangements:** Countries should take appropriate measures to prevent the misuse of legal persons for money laundering or terrorist financing, including ensuring information about the beneficial ownership and control of such legal persons is available to competent authorities, particularly with regard to legal persons who can issue bearer shares or have nominee shareholders or directors.

- **Powers and responsibilities of competent authorities:** Countries should oversee financial institutions to ensure they are implementing the FATF Recommendations and are not owned by or controlled by criminals. The supervisors should be given sufficient resources and powers to effectively oversee financial institutions within their jurisdictions. Designated nonfinancial businesses and people should be subject to oversight as well when they engage in certain financial activities. Countries should establish financial intelligence units and provide law enforcement and investigative authorities with sufficient resources and powers to investigate money laundering and terrorist financing and to seize or freeze criminal proceeds where found. Countries should implement measures to detect the physical cross-border movement of currency and bearer-negotiable instruments. The authorities should provide meaningful statistics, guidance and feedback on AML/CFT systems.
- **International cooperation:** Several Recommendations deal with strengthening international cooperation. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in money laundering and terrorist financing investigations, freezing and confiscation of criminal proceeds, extradition and in other matters. Countries should ratify United Nations conventions against significant crimes and terrorism.

A.8.3 FATF Members and Observers

FATF currently comprises 37 member jurisdictions and 2 regional organizations, representing most major financial centers in all parts of the globe.

A.8.4 Non-Cooperative Countries and territories (NCCTs)

Since its inception, FATF has had a practice of "naming and shaming" countries that it determines maintain inadequate anti-money laundering controls or are not cooperating in the global AML/ CFT efforts. For years, FATF was engaged in an initiative to identify non cooperative countries and territories (NCCTs) in the global fight against money laundering. It developed a process to seek out critical weaknesses in specific jurisdictions' anti-money laundering systems that obstruct international cooperation in this area. On February 14, 2000, FATF published an initial report on non-cooperative countries and territories that set out the 25 criteria that help identify relevant detrimental rules and practices and that are consistent with the 40 Recommendations.

The goal of the NCCT process was to reduce the vulnerability of the financial system to money laundering by ensuring that all financial centers adopt and implement measures for the prevention, detection and punishment of money laundering according to internationally

recognized standards. The next step in the NCCT initiative was the publication in June 2000 of the first review identifying 15 NCCTs. The NCCT process ultimately involved 24 jurisdictions, including up to 19 jurisdictions at one time, until the jurisdictions eventually took the necessary steps to get off the list. The NCCT list was replaced by a new process when FATF started identifying jurisdictions with deficiencies in their AML/CFT regimes. This new FATF process was in response to the G-20 countries' efforts to publicly identify high-risk jurisdictions and to issue regular updates on jurisdictions with strategic deficiencies. Today, FATF identifies these jurisdictions in two public documents issued three times a year.

A.8.5 High-risk and other monitored jurisdictions

The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents that are issued three times a year. The FATF's process to publicly list countries with weak AML/CFT regimes has proved effective. As of October 2018, the FATF has reviewed over 80 countries and publicly identified 68 of them. Of these 55 have since made the necessary reforms to address their AML/CFT weaknesses and have been removed from the process. High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. This list is often externally referred to as the "black list". Currently Democratic People's Republic of Korea (DPRK) and Iran fall under the high-risk Criteria. On the other hand, Albania, Bahamas, Barbados, Botswana, Cambodia, Ghana, Iceland, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen and Zimbabwe falls under the Jurisdictions with strategic deficiencies as on February 2020.

FATF's Public Statement identifies

- Countries or jurisdictions with strategic deficiencies that are so serious that FATF calls on its members and non-members to apply counter-measures; and
- Countries or jurisdictions for which the FATF calls on its members to apply enhanced due diligence measures proportionate to the risks arising from the deficiencies associated with the country.

Improving Global AML/CFT Compliance: Ongoing Process identifies countries or jurisdictions with strategic weaknesses in AML/CFT measures but that have provided a high-level commitment to an action plan developed with the FATF.

- FATF encourages its members to consider the strategic deficiencies identified within these jurisdictions.
- If a country fails to make sufficient or timely progress, FATF can increase its pressure on the country to make meaningful progress by moving it to the Public Statement.
- The document also provides information on jurisdictions no longer subject to FATF's ongoing global AML/CFT compliance process. Typically, a country is identified to have made significant progress in improving its AML/CFT regime when it establishes a legal and regulatory framework to meet its commitments in its action plan regarding the previously identified strategic deficiencies. However, the country must continue to work with the appropriate FATF-style regional body on addressing the items noted in its mutual evaluation report.

A.8.6 FATF-Style Regional Bodies

There are nine FATF-style regional bodies (FSRBs) that have similar form and functions to those of FATF. They are also considered FATF associate members. In setting standards, FATF depends on input from the FSRBs as much as from its own members; however, FATF remains the only standard-setting body.

The following high-level principles apply for both FATF and FSRBs.

- **Role:** FSRBs play an essential role in identifying and addressing AML/CFT technical assistance needs for their individual members. In those FSRBs that carry out this coordination work, technical assistance necessarily complements mutual evaluation and follow-up processes by helping jurisdictions to implement FATF standards.
- **Autonomy:** FATF and FSRBs are free-standing organizations that share the common goals of combating money laundering and the financing of terrorism and proliferation and of fostering effective AML/CFT systems.
- **Reciprocity:** FATF and FSRBs operate on the basis of (mutual or joint or common) recognition of their work, which implies that FSRBs and FATF put in place similar mechanisms for effective participation and involvement in each other's activities.

Because FATF and FSRBs are part of a larger whole and the success or failure of one organization can have an effect on all organizations, protection of the FATF brand is in the common interest of both FATF and FSRBs. Many FATF member countries are also members of the nine FSRBs.

i) Asia/Pacific Group on Money Laundering (APG)

ii) Caribbean Financial Action Task Force (CFATF)

iii) Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL, formerly PC-R-EV)

iv) Eurasian Group (EAG)

v) Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

vi) Financial Action Task Force of Latin America (GAFILAT) (formerly known as Financial Action Task Force on Money Laundering in South America (GAFISUD)

vii) Intergovernmental Action Group against Money Laundering in West Africa (GIABA)

viii) Middle East and North Africa Financial Action Task Force (MENAFATF)

ix) Task Force on Money Laundering in Central Africa (GABAC)

A.8.7 ASIA/PACIFIC GROUP ON MONEY LAUNDERING (APG)

The APG, an autonomous regional anti-money laundering body, was established in February 1997 at the Fourth Asia/Pacific Money Laundering Symposium in Bangkok with 13 founding members, where it adopted its Terms of Reference. Bangladesh is the founding member of APG. Currently APG has 41 member Countries/Jurisdictions.

The Terms of Reference were substantially revised in July 2012 to recognize that the FATF's revised 40 Recommendations constituted the new international standards on combating money laundering and the financing of terrorism and proliferation. The Terms included a commitment that APG members would implement these recommendations according to their particular cultural values and constitutional frameworks. It also said that to ensure a global approach member of the APG would work closely with FATF.

- Provides a focus for cooperative AML/CFT efforts in the Asia/Pacific region;
- provides a forum in which
  - regional issues can be discussed and experiences shared, and
  - operational cooperation among member jurisdictions is encouraged;
- facilitates the adoption and implementation by member jurisdictions of internationally accepted AML/CFT measures;
- enables regional and jurisdictional factors to be taken into account in the implementation of international AML/CFT measures;
- encourages jurisdictions to implement AML/CFT initiatives, including more effective mutual

legal assistance; and

- Coordinates and provides practical support, where possible, to member and observer jurisdictions in the region, when requested.

The APG is voluntary and cooperative in nature. The work done by the APG and its procedures are decided by mutual agreement among its members. The group was established by agreement among its members and is autonomous. It is not derived from an international treaty and is not part of any international organization.

The APG also uses similar mechanisms to those used by FATF to monitor and facilitate progress. The APG and FATF have reciprocal rights of attendance at each other's meetings, as well as reciprocal sharing of documents. However, the APG, as with other autonomous AML bodies, determines its own policies and practices. It is not a precondition for participation in the APG that AML/CFT laws already be enacted.

The APG has seen its membership grow from its original 13 founding members in 1997 to 41 members as of July 2015. APG members include Afghanistan, Australia, Bangladesh, Bhutan, the Kingdom of Brunei Darussalam, Cambodia, Canada, China, the Cook Islands, Fiji, Hong Kong (China), India, Indonesia, the Republic of Korea (South Korea), Japan, Lao People's Democratic Republic, Macao (China), Malaysia, Maldives, The Marshall Islands, Mongolia, Myanmar, Nauru, Nepal, New Zealand, Niue, Pakistan, Palau, Papua New Guinea, The Philippines, Samoa, Singapore, Solomon Islands, Sri Lanka, Chinese Taipei, Thailand, Timor Leste, Tonga, the United States of America, Vanuatu and Vietnam.

The APG Secretariat is headquartered in Sydney, Australia. The APG has a permanent and a rotating Co-Chair. The permanent chair is held by Australia, as host and supporting member jurisdiction of the Secretariat, and the rotating chair is appointed for a two-year term by the membership. Head of BFIU served as rotating co-chair of APG during 2018-2020.

A.8.8 Egmont Group of FIUs

In 1995, a number of national financial intelligence units (FIUs) began working together in an informal organization known as the Egmont Group (named for the location of the first meeting, the Egmont-Arenberg Palace in Brussels). The goal of the group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field. At present Egmont Group is a united body of 168 Financial Intelligence Units (FIUs)**.** The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF). This is especially relevant as FIUs are uniquely positioned to cooperate and support national and international efforts to counter terrorist financing and are the

trusted gateway for sharing financial information domestically and internationally in accordance with global Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) standards.

The Egmont Group continues to support the efforts of its international partners and other stakeholders to give effect to the resolutions and statements by the United Nations Security Council, the Financial Action Task Force (FATF) and the G20 Finance Ministers. The Egmont Group is able to add value to the work of member FIUs by improving the understanding of ML/TF risks amongst its stakeholders. The organization is able to draw upon operational experience to inform policy considerations; including AML/CFT implementation and AML/CFT reforms. The Egmont Group is the operational arm of the international AML/CFT apparatus.

The Egmont Group recognizes sharing of financial intelligence is of paramount importance and has become the cornerstone of the international efforts to counter ML/TF. Financial Intelligence Units (FIUs) around the world are obliged by international AML/CFT standards to exchange information and engage in international cooperation. As an international financial intelligence forum, the Egmont Group both facilitates and prompts this amongst its member FIUs. BFIU has achieved the membership of Egmont Group in July, 2013.

A.9 National Coordination Committee (NCC) on AML& CFT

For preventing money laundering and combating financing of terrorism through policy formulation, overseeing the activities of relevant stockholders and coordinating the national AML & CFT effort Bangladesh established National Coordination Committee (NCC) in 2010. Composition of NCC is-

Honorable Minister, Ministry of Finance	-	Convenor
Chairman, Anti-Corruption Commission	-	Member
Principal Secretary, Prime Minister's Office	-	Member
Attorney General for Bangladesh	-	Member
Governor, Bangladesh Bank	-	Member
Secretary, Finance Division, Ministry of Finance	-	Member
Secretary, Bank & Financial Institution Division, Ministry of Finance	-	Member
Secretary, Legislative and Parliamentary Affairs Division, Ministry of Law, Justice and Parliamentary Affairs	-	Member
Secretary, Ministry of Home Affairs	-	Member
Secretary, Ministry of Foreign Affairs	-	Member
Secretary, Ministry of Housing and Public Works	-	Member
Secretary, Ministry of Commerce	-	Member
Chairman, National Board of Revenue	-	Member

Chairman, Securities and Exchange Commission - Member

Head of BFIU - Member Secretary

(2) **The power and functions of the National Coordination Committee. -** The power and functions of the National Coordination Committee shall be as follows:

(a) formulating nationally important policies for preventing money laundering and terrorist financing;

(b) providing necessary guidance to all concerned in implementing the policies made;

(c) ensuring coordination among different Ministries or Agencies;

(d) reviewing the position of Bangladesh in complying international standards for anti-money laundering and combating financing of terrorism, and ensuring compliance of the standards;

(e) forming different working committee from time to time for special purpose and approving terms of reference of the committee and giving guidance to implement the terms of reference;

(f) collecting any information or report related to money laundering and terrorist financing from any relevant Ministry, Division, Agency or Institute and making necessary decision on that basis;

(g) taking any initiative and making decision as considered by the Committee; and

(h) the Committee can co-opt any related individual.

(3) The Committee shall meet at least twice in a year and the Convener of this Committee may ask for meeting as and when necessary.

(4) BFIU will provide secretarial assistance to the Committee.

A. 10 Central and Divisional Task Force on AML & CFT

To prevent money laundering, smuggling of money/asset and illegal hundi activities, two-layered task forces i.e. the Central Task Force and Divisional Task Force have been formed in 2002 and restructured in 2017. The Head of BFIU is the convener of the Central Task Force whereas the Director of BFIU serves as its member secretary. The organizations having representative in the Central Task Force include-

- National Board of Revenue (NBR),
- Anti-Corruption Commission (ACC),
- Bangladesh Securities and Exchange Commission (BSEC),
- Department of Cooperatives,
- Insurance Development and Regulatory Authority (IDRA),
- NGO Affairs Bureau (NGOAB),

- Department of Narcotics Control (DNC),
- Registrar of Joint Stock Companies and Firms (RJSC),
- Police Headquarters,
- Dhaka Metropolitan Police (DMP),
- Criminal Investigation Department (CID) and
- supervision-related departments of Bangladesh Bank
- 8 (eight) representatives from scheduled banks,
- 2 (two) representatives from financial institutions,
- 2 (two) representatives capital market intermediaries,
- 2 (two) representatives non-government organizations (NGOs),
- 2 (two) representatives insurance companies and
- 2 (two) representatives cooperative societies

The Central Task Force works to coordinate the activities of different investigative agencies, law enforcement agencies, prudential regulators of reporting organizations and the BFIU. It is mandated to convene quarterly meetings to discuss the progress achieved in implementing its goals.

Functions of Divisional Taskforce:

- Coordination with the activities of the divisional Law Enforcement Agencies, Investigating agencies, Regulatory Authorities of the Reporting Organizations (ROs) and BFIU.
- Reviewing progress of divisional activities related to AML/CFT by different stakeholders
- Reviewing progress of actions about the reported incidents including the smuggling of money, currency, gold and other valuable items, Child and Human Trafficking, Trafficking etc.
- Taking initiatives to identify and eradicate the barrier of implementing the AML/CFT activities.

Chattogram, Khulna, Maymensing, Rajshahi, Sylhet Rangpur and Barisal Divisional Taskforces are headed by the respective office Heads of the divisional offices of Bangladesh Bank. The followings are the members of the Divisional Task Force:

1) The Head, Concerned Divisional Office of Bangladesh Bank,
2) Representative, office of Divisional Commissioner,
3) Representative, Divisional/District Office of Anti Corruption Commission,
4) Representative, Divisional Office/Commissionarate of Bangladesh Customs;
5) Representative, Divisional Office/Commissionarate of Income Tax,
6) Representative, the Department of Social Service,
7) Representative, the Department of Cooperative,
8) Representative, the RJSC,

9) Representative, DNC,
10) Representative, Special Branch of Bangladesh Police,
11) Representative, Metropolitan Police,
12) Representative, CID,
13) Manager of Sonal Bank PLC,
14) Manager of Rupali Bank Ltd,
15) Manager of Agrani Bank Ltd.,
16) Manager of Janata Bank Ltd,
17) Manager, Bangladesh Krishi Bank Ltd/Rajshahi Krishi Unnayan Bank Ltd.
18) Four (04) Representatives from the Commercial Banks nominated by the respective Divisional Office of Bangladesh Bank
19) One (01) Representative from the Financial Institutions nominated by the respective Divisional Office of Bangladesh Bank
20) One (01) Representative from the NGOs nominated by the respective Divisional Office of Bangladesh Bank

Functions of Divisional Taskforce:

- Coordination with the activities of the divisional Law Enforcement Agencies, Investigating agencies, Regulatory Authorities of the Reporting Organizations (ROs) and Bangladesh Bank.
- Reviewing progress of divisional activities related to AML/CFT by different stakeholders
- Taking initiatives to identify and eradicate the barrier of implementing the AML/CFT activities.

Sample Questions

Case: A company, M Agro Ltd. received govt. cash incentives of BDT 100.00 million against potato export valuing around BDT 500.00 million to Malaysia. The cash incentives were then layered using some other affiliated companies of M Agro such as F Telecom, T Media, Z Outfit, S Logistics, Z Fashion House etc. and later withdrawn the entire amount in cash. But no physical existence of those companies, including M Agro Ltd. was found during on-site verification. Furthermore, discrepancy was found in the line of business of M Agro Ltd. and the foreign importer companies. It was found that, the owner of the company Mr. Amin got citizenship of Antigua and the UAE under investment quota though he had no permission from Bangladesh Bank to invest in foreign country. It was assumed that, he might be smuggled money abroad through hundi for such investment. On the other hand, lapses on the side of ABC Bank Ltd. in performing CDD and KYC procedures for opening the bank accounts of the suspected companies were found.

Sample Question:

1) What is financial crime? What are the common forms of Financial Crime? Which are the main stakeholders of countering financial crimes in Bangladesh?
2) What is money laundering? Define money laundering as per MLPA, 2012. What additional elements of ML are in MLPA, 2012?
3) A government employee named Mr. X took 50 lac BDT as bribe from a person in exchange of providing service. Then he kept 25 lac BDT in a safe place of his house and gave the rest to his brother in law, Mr. Y deposited the money in his own bank account in the bank HP Bank Ltd.
    a. Is it falls under money laundering? Give reason for your answer.
    b. In the above scenario, who will be charged for money laundering and why?
    c. What due diligence measures should be taken by the bank HP Bank Ltd?
4) What are the stages of money laundering? Is it necessary to follow all the stages to commit ML Offences? Explain with example.
5) What is smuggling of money or asset? Elaborate your answer in line with MLPA, 2012. What is the difference between smuggling of money or asset and money laundering?
6) What is predicate offence? Which agencies are empowered to investigate money laundering cases?
7) What is BFIU? What are the main functions and responsibilities of BFIU as per MLPA & ATA?
8) Write down the penalty provision for tipping off and providing false information to BFIU by a Reporting Organization (RO).
9) What is FATF? Which seven broad areas are covered under FATF Recommendations? What do you understand by non-cooperative countries and territories (NCCTs)?
10) How many FATF Style Regional Bodies (FSRBs) are there? What is APG?
11) What Egmont Group? What are their functions in AML/CFT?
12) What are the roles and responsibilities of National Coordination Committee (NCC)? Write down the structure of Central and Divisional Taskforce.

Module B: Financial Crime in the Key Functional Areas of Banking

B.1 Financial Crime in General Banking

Banking is the inevitable part of an economy and plays a major contribution towards socio-economic development of a country. The sector is considered as life blood of the economy as well. As one of the most important sectors of the financial system, it forms the core of the money market and plays very dynamic role in mobilizing resources for productive investments in a country, which in turn contributes to economic development. An efficient and stable banking system is the prerequisite for over all development of the country.

Because of their diversified products and complex nature of transaction, banks bear some inherent vulnerabilities and risks of money laundering and terrorist financing. The second National Risk Assessment (NRA) of Bangladesh has identified banks as the most vulnerable sector of ML&TF which stated that 'as the principal gateway to financial system, banks face high probability of being threatened by criminals attempting to launder illicit fund.'

Economic and financial crimes are global problems today especially different forms of asset misappropriations and cybercrimes became grave concerns both at operational and policy levels. According to the most recent Global Economic Crime Survey (2016) of the Pricewaterhouse Coopers (PwC), more than one in three organizations report being victimized by economic crime; and close to half the organizations surveyed believe that local law enforcement is not adequately resourced to investigate economic crime, leaving the responsibility for fighting economic crime on other organizations.

Any bank is likely to become vulnerable to financial crimes involving various parties - customers, employees, external organized crime groups or influential sections and those with whom banks has business dealings. Such activities are often associated with money laundering, embezzlement, evasion of sanction, and illegal transfer of funds for tax avoidance and financing terrorism. If the perpetrators get advantage of deficiency in bank management, the risks become even higher. Several drivers including globalization, the proliferation of banking channels, rising transaction volumes and technological advancements have introduced new opportunities for financial crimes. As the case of the banking sector of developed and developing economies, banking sector of Bangladesh is increasingly facing the difficulties of financial crimes. In spite of some notable improvement in the loan default status over the years, some banks have still been struggling with high volume of non-performing loans (NPL) when cyber frauds and other forms of sophisticated financial crimes are adding to the burdens of the banking sector.

B.1.1 Cheque related Frauds

Cheque related frauds are the most commonly experienced fraud incidences in Bangladesh. Cheque frauds are mostly committed through the alteration in the material parts of a cheque, such as, date, amount, signature. This type of fraud may also occur due to manipulation of chequebook.Fake cheque category is followed by signature forgery, amount manipulation, FDR fraud, cheque book fraud, etc.

Some of the most common methods of cheque fraud include:

- **Forgery**: This occurs when someone alters a check or creates a fake check using someone else's account information.
- **Paper hanging:** This occurs when an account holder fills out a check knowing they don't have the funds to cover it, then takes advantage of the "float" time between when the check is written and when it is deposited
- **Check kiting:** Similar to paper hanging, this occurs when a check is written from an account without sufficient funds, but the amount is added to the account before deposit to cover the missing funds.
- **Counterfeiting:** This occurs when someone creates a fake check that appears to be legitimate.
- **Chemical alterations:** This occurs when a fraudster erases the ink on a check using special chemicals, allowing them to write new fraudulent information.
- **Stolen checks:** This occurs when someone steals a check and alters the payee and/or amount before cashing or depositing it.
- **Check washing:** This occurs when someone erases the ink on a check and changes the payee and/or amount before cashing or depositing it.
- **Alteration of amount:** This occurs when someone alters the dollar amount on a check.
- **Post-dating:** This occurs when someone writes a check with a future date, in order to make the check appear to be valid later.

Check fraud can happen in a variety of ways, including through mail theft, online scams, and the use of skimmers at ATMs or point-of-sale terminals.

B.1.2 Loan Related Financial Crimes

Most of the loan related frauds are committed by creating loan in the name of non-existent borrowers or fake borrowers. Other loan frauds are related to documentation, fund diversion, collateral valuation, directed lending, fake title deed, change in loan limit and expiry date, etc. in

the context of banks are not generally maintained and reported, and are not recognized as financial crimes.

Loan related financial crime may happen in different of ways, like-

- Loan fraud or loan scam
- Loan scam related money laundering
- Loan or Credit banked money laundering

B.1.2.1 Credit backed money laundering

Credit backed money laundering (CBML) is defined as the process of disguising the proceeds of crime and moving value through the credit transactions or credit facilities in an attempt to legitimize their illicit origins. This method of money laundering involves 'cleaning' of money obtained from predicate offences to become visible to have been derived from legal activities. Under credit-backed money laundering, criminals borrow their own illicit money. It is usually executed through the creation of credit agreement between the criminal and a third party.

The common techniques which are used in CBML process are offshore corporations, front companies, shell companies, phantom mortgage, fund diversification, over valuation of primary securities, over valuation of collateral securities, using fictitious assets as security, accommodation bill, using beneficial owner, willful defaulter etc.

Case: Mr. A is a government officer purchased a duplex luxury apartment in exchange of BDT 5 (five) crore for his wife Ms. L. She borrowed BDT 3 crore from bank and NBFI for 10 (ten) years. Remaining BDT 2 corer is from encashment of her FDRs maintained in different banks. Source of those FRDs is gift from his father but his father was also a government officer. After six months Mr. A request bank and NBFI through phone and accordingly Ms. L applied to pay the loan amount in 2(two) years. Bank and NBFI re-fixed loan installment. It is assumed that corrupt money was disguised through this loan process and may be comingled legal money with processed of corruption.

Bangladesh faces numerous challenges to prevent CBML due to involvement of multiple parties in the credit processing. Skilled manpower is required to deal with credit related activities like borrower selection, assessment of the borrower's business; scrutiny of various documents related to primary and collateral securities, analysis of financial statements, legal formalities etc. In Bangladesh there are limited credit specialists who are able to understand and handle the credit dealings very well. Willful defaulters are another challenge. Lack of effective Management Information System (MIS) increases the risk of CBML. Lack of adequate customer due

diligence/enhanced due diligence (CDD/EDD) measures on the underlying credit facilities; collusion between credit approval authorities and the credit customers; Directors' involvement in credit operation, insider lending, weak compliance culture of Banks/NBFIs; weak corporate governance; hindrance of implementation of quick legal action against defaulters are also challenges for preventing credit backed money laundering.

B.1.2.2 Potential Red Flags: Credit Backed Money Laundering

Red flag means a potential signal that helps to financial entities to be careful about the clients' behavior and their nature of transactions whether the clients are involved in any form of money laundering. There are many red flags related to CBML but the following are the most common.

- Unwilling to submit required documents for credit facilities;
- using front and shell companies;
- loan repayments by third parties;
- loan proceeds used to purchase property in the name of a third party;
- formation of a new company in the name of employees;
- creation of forced loan without valid reason;
- customer requests to disburse loan by issuing cheques in favor of another bank/FIs/third parties;
- large cash transaction inconsistent with customer's business/profession;
- huge credit balance in the loan account;
- transfer of funds between irrelevant businesses;
- multiple online deposit/withdrawal from irrelevant locations;
- making loan decisions and then cancelling immediately and asking for refund of documents;
- adjustment of long terms loan like home loan within short time;
- customer suddenly pays off a large classified loan with no plausible explanation of source of funds;
- offering third party's property as collateral security;
- counterfeited documents submitted for credit facilities;
- frequently attempt to enjoy Excess Over Limit (EOL) facility;
- diversification of credit (fund) facility;
- willful defaulter;
- making pressure to enhance credit limit which is not viable according to the volume of business;
- willing to pay highest profit/ interest rate without any bargaining;

- purchase DD/PO or EFT/RTGS by using credit facilities to different parties who have no business relationship with the client;
- over valuation of primary security;
- over valuation of collateral security; frequently enjoying Secured Over Draft (SOD) facility against new high valued term deposits;
- proposal for credit facility for investment in luxurious products and antiques items;
- application for credit facility to investment in movable commodities like gold, diamond and gems;
- credit cardholder uses card for purchasing luxurious products frequently;
- excess amount deposited in credit card than outstanding amount and then claim the additional amount via cheque or Pay Order;
- loan secured by deposits or other readily marketable assets, such as securities.

B.1.2.3 Tactics to Prevent CBML

Applying Risk Based Approach (RBA) for credit customers, checking and verifying customers' background, nature of business, net worth, beneficial owner, analyzing of the purpose of the loan, conducting borrower due diligence (BDD),monitoring credit transaction profile (CTP), introducing three lines of defense, ensuring good corporate governance, strengthening institutional & regulatory frameworks, avoiding of undue influence at the approval stage of credit, arrangement of proper training and awareness among the bankers and the related parties may help to prevent CBML.

B.1.3 International trade related financial Crime

The international trade system is clearly subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist financiers. International trade related frauds may take different forms, such as, over invoicing, under invoicing, non-repatriation of export proceeds. As regards nature of international trade related frauds, approximately 50 percent of the total frauds of this nature are committed through fake documents and another 50 percent through fake foreign demand draft. In several instances, banks of the country have been facing tunes because of the non- performance or breach of contracts by the traders; however, these are not included in the data as crimes provided by the banks. Moreover, though money laundering instances in the context of Bangladesh are mainly trade based, banks do not report on the issue. These cases are generally unearthed by the competent authorities. Most common form of international trade related financial crime is trade based money laundering.

B.1.4 Trade Based Money Laundering

It is argued worldwide that almost 80 percent of the money laundering occurred trough international trade operation, which is generally known as 'Trade Based Money Laundering (TBML)'. The FATF has defined TBML as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trades-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

The basic techniques of trade-based money laundering include:

- Over- and under-invoicing of goods and services;
- Multiple invoicing of goods and services;
- Over- and under-shipments of goods and services; and
- Falsely described goods and service
- Phantom Shipment

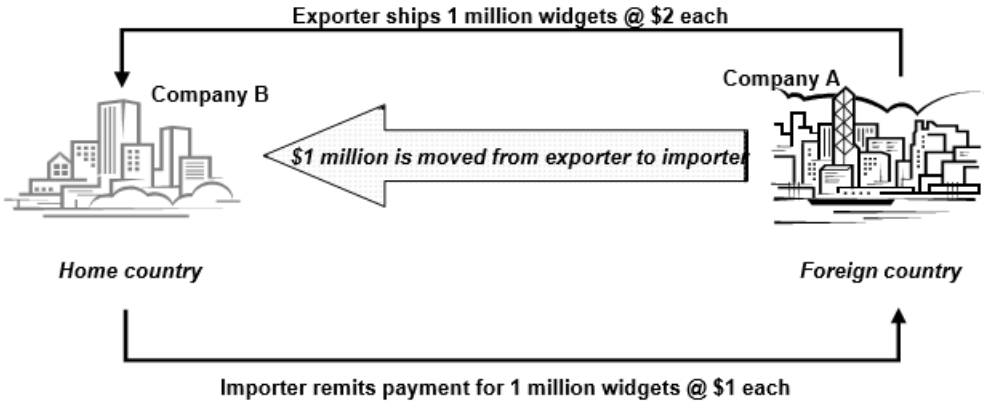
B.1.4.1 Over- and Under-Invoicing of Goods and Services

Money laundering through the over- and under-invoicing of goods and services, which is one of the oldest of fraudulently transferring value across borders, remains a common practice today. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

By invoicing the good or service at a price below the "fair market" price, the exporter is able to transfer value to the importer, as the payment for the good or service will be lower than the value that the importer receives when it is sold on the open market. Alternatively, by invoicing the good or service at a price above the fair market price, the exporter is able to receive value from the importer, as the payment for the good or service is higher than the value that the importer will receive when it is sold on the open market.

Over- and Under-Invoicing of Goods – An Example

Company A (a foreign exporter) ships 1 million widgets worth $2 each, but invoices Company B (a colluding domestic importer) for 1 million widgets at a price of only $1 each. Company B pays Company A for the goods by sending a wire transfer for $1 million. Company B then sells the widgets on the open market for $2 million and deposits the extra $1 million (the difference between the invoiced price and the "fair market" value) into a bank account to be disbursed according to Company A's instructions.



Alternatively, Company C (a domestic exporter) ships 1 million widgets worth $2 each, but invoices Company D (a colluding foreign importer) for 1 million widgets at a price of $3 each. Company D pays Company C for the goods by sending a wire transfer for $3 million. Company C then pays $2 million to its suppliers and deposits the remaining $1 million (the difference between the invoiced price and the "fair market" price) into a bank account to be disbursed according to Company D's instructions.

Source: FATF Study on Trade Based Money Laundering, 2006

B.1.4.2 Multiple Invoicing of Goods and Services

Another technique used to launder funds involves issuing more than one invoice for the same international trade transaction. By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions.

In addition, even if a case of multiple payments relating to the same shipment of goods or delivery of services is detected, there are a number of legitimate explanations for such situations including the amendment of payment terms, corrections to previous payment instructions or the payment of late fees. Unlike over- and under-invoicing, it should be noted that there is no need for the exporter or importer to misrepresent the price of the good or service on the commercial invoice.

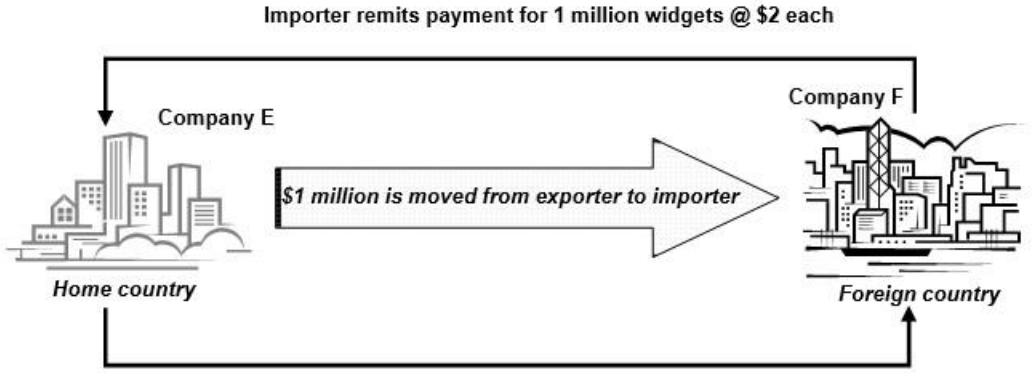
B.1.4.3 Over- and Under-Shipments of Goods and Services

In addition to manipulating export and import prices, a money launderer can overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with this so- called "phantom shipment" are routinely processed. Banks and

other financial institutions may unknowingly be involved in the provision of trade financing for these phantom shipments.

Over- and Under-Shipment of Goods – An Example

Company E (a domestic exporter) sells 1 million widgets to Company F (a colluding foreign importer) at a price of $2 each, but ships 1.5 million widgets. Company F pays Company E for the goods by sending a wire transfer for $2 million. Company F then sells the widgets on the open market for $3 million and deposits the extra $1 million (the difference between the invoiced quantity and the actual quantity) into a bank account to be disbursed according to Company E's instructions.



Alternatively, Company G (a foreign exporter) sells 1 million widgets to Company H (a colluding domestic importer) at a price of $2 each, but only ships 500,000 widgets. Company H pays Company G for the goods by sending a wire transfer for $2 million. Company G then pays $1 million to its suppliers and deposits the remaining $1 million (the difference between the invoiced quantity and the actual quantity) into a bank account to be disbursed according to Company H's instructions.

Source: FATF Study on Trade Based Money Laundering, 2006

B.1.4.4 Falsely Described Goods and Services

In addition to manipulating export and import prices, a money launderer can misrepresent the quality or type of a good or service. For example, an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs documents and what is actually shipped. The use of false descriptions can also be used in the trade in services, such as financial advice, consulting services and market research. In practice, the fair market value of these services can present additional valuation difficulties.

Falsely Described Goods – An Example

Company I (a domestic exporter) ships 1 million gold widgets worth $3 each to Company J (a colluding foreign importer), but invoices Company J for 1 million silver widgets worth $2 each. Company J pays Company I for the goods by sending a wire transfer for $2 million. Company J then sells the gold widgets on the open market for $3 million and deposits the extra $1 million (the difference between the invoice value and the actual value) into a bank account to be disbursed according to Company I's instructions.

Alternatively, Company K (a foreign exporter) ships 1 million bronze widgets worth $1 each to Company L (a colluding domestic importer), but invoices Company L for 1 million silver widgets worth $2 each. Company L pays Company K for the goods by sending a wire transfer of $2 million. Company K then pays $1 million to its suppliers and deposits the remaining $1 million (the difference between the invoiced value and the actual value) into a bank account to be disbursed according to Company L's instructions.

Source: FATF Study on Trade Based Money Laundering, 2006

B.1.4.5 Phantom Shipment

Without conducting any actual trade i.e export or import of goods and services fund may transfer from one jurisdiction to another jurisdiction by producing face shipping documents. It's generally happened within related parties. For this collaboration of exporter and importer as well as customs officials are essential.

[N.B Prevention of TBML is discussed in Module-C in line with TBML Guideline]

B.2 Handling Financial Crime by Banks

Under the provisions of the clause 23(1)(d) of Money Laundering Prevention Act, 2012 and the clause 15(1)(d) of Anti-Terrorism Act, 2009, instructions are issued for all the scheduled banks operating in Bangladesh to comply with Money Laundering Prevention Act, 2012 and Anti-Terrorism Act, 2009 and the related provisions of the rules issued under those acts.

B.2.3 Internal Control and Compliance Function of Banks in Preventing Financial Crime

With a goal of establishing an effective AML and CFT regime, it shall have to be ensured that the Internal Audit Department of the bank is equipped with enough manpower who have enough knowledge on the existing acts, rules and regulations, BFIU's instructions on preventing money laundering & terrorist financing and bank's own policies in this matter to review the Self Assessment Report received from the branches and to execute the Independent Testing Procedure appropriately. Internal Audit or Internal Control and Compliance (ICC) of a bank shall have an

important role for ensuring proper implementation of bank's AML & CFT Compliance Program. Every bank needs to ensure that ICC is equipped with enough manpower and autonomy to look after the prevention of ML&TF. The ICC has to oversee the implementation of the AML & CFT compliance program of the bank and has to review the 'Self Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately. To ensure the effectiveness of the AML&CFT compliance program, bank should assess the program regularly and look for new risk factors.

An institution's internal auditors 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 internal audit must-

- understand ML & TF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML/CFT Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML&CFT Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU or BB;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
    - the importance of the board and the senior management place on ongoing education, training and compliance,
    - employee accountability for ensuring AML&CFT compliance,
    - comprehensiveness of training, in view of specific risks of individual business lines,
    - training of personnel from all applicable areas of the bank,
    - frequency of training,
    - coverage of bank policies, procedures, processes and new rules and regulations,

- coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
- penalties for noncompliance and regulatory requirements.

Case and Sample Questions

Case: ABC Bank Ltd sanctioned BDT 150.00 million composite loans to an automobile company, Dx Automobile Ltd. taking land document as collateral. Though during the verification, the Panel lawyer, Surveyor and the loan approving branch initially declared the Mortgage and Power of Attorney Deed supplied by the customer as authentic, Internal Compliance Department found them as fictitious after several months of loan sanction. Furthermore, it was found that the property documents were provided by a third party mortgagor not the customer himself. Ultimately the loan became classified.

Sample Question:

1) Write down some common methods of cheque fraud.
2) What is credit backed money laundering? What measures a bank may take to prevent credit backed money laundering?
3) What is Trade Based Money laundering? Write down some methods of trade-based money laundering.
4) How an AML/CFT compliance structure of a bank should look like? Provide your answer in light with BFIU circular-26.
5) What is the necessity to establish an effective AML/CFT compliance structure in a bank?
6) Who is BAMLCO? Write down the responsibilities of BAMLCO on AML/CFT issues.
7) What is the composition of central compliance committee (CCC)? What responsibilities it has to scheduler for prevention of ML and TF.
8) Describe the qualification of a Chief Anti Money Laundering Compliance Officer (CAMLCO) of a bank. What are the roles and responsibilities of a CAMLCO?

Module C: Financial Crime Risk Assessment

C.1 Money Laundering and Terrorist Financing Risk Assessment Guidelines for the Banking Sector

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on anti-money laundering (AML) and combating terrorist financing (CTF) states that countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks. Rule 10 of MLPR 2019 states that every Reporting Organization-Financial Institution, considering the nature of business, products or services, country, geographical location etc., shall have to conduct periodic risk assessment which will be used to manage and control the ML/TF risk of the organization.

Money Laundering Prevention Act, 2012 empowers BFIU sufficiently to establish a sound and efficient AML&CFT regime. Every reporting agency has to comply with the instructions issued by BFIU under the power of Money Laundering Prevention Act (MLPA), 2012 and Anti-Terrorism Act (ATA), 2009 (including all amendments). With the empowerment of those Acts and Rules, BFIU has issued ML/TF Risk Assessment Guidelines for the Banks.

C.1.2 Requirement for Banks for Risk Assessment

(a) Assessing risk

Banks should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks for customers, countries or geographic areas, products, services and transactions or delivery channels. They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities.

(b) Risk management and mitigation

Banks should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures must be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

C.1.2.1 What is risk

Risk can be defined as the combination of the probability of an event and its consequences. In

simple term, risks can be seen as a combination of the chance that something may happen andthe degree of damage or loss that may result if it does occur.

C.1.2.2 What is risk management

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

C.1.2.3 which risks do banks need to manage

For the ML&TF aspects, BFIU expects a risk management practice to address two main risks: ***business risk and regulatory risk.***

C.1.3 Risk Management Framework

The banks 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 bank reasonably faces.

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

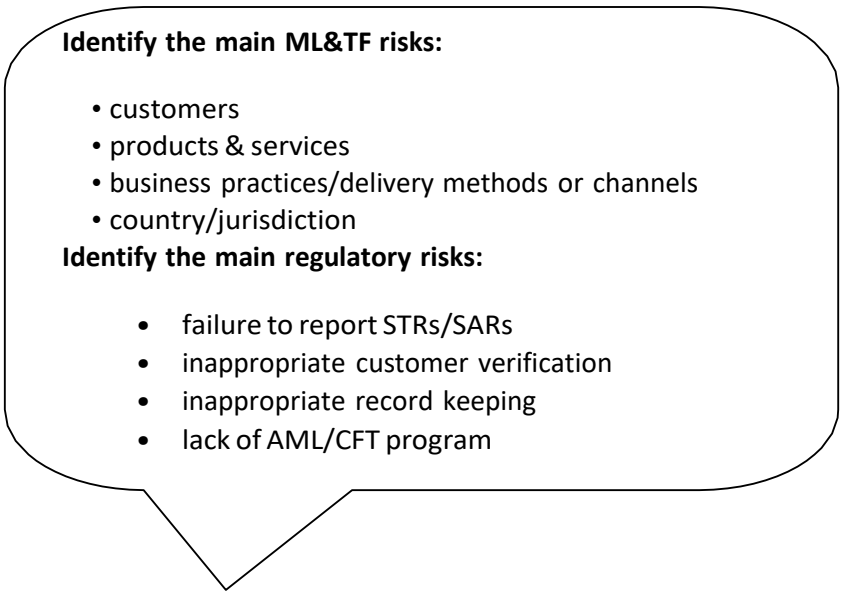
- Risk management contributes to the demonstrable achievement of objectives and improvement of performance, governance and reputation.
- Risk management is not a stand-alone activity that is separate from the main activities and processes of the bank. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning.
- Risk management helps decision makers making informed choices, prioritize actionsand 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 systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
- Risk management is based on the best available information.
- Risk management is aligned with the bank's external and internal context and risk profile.

- Risk management is transparent and inclusive.
- Risk management is dynamic, iterative and responsive to change.

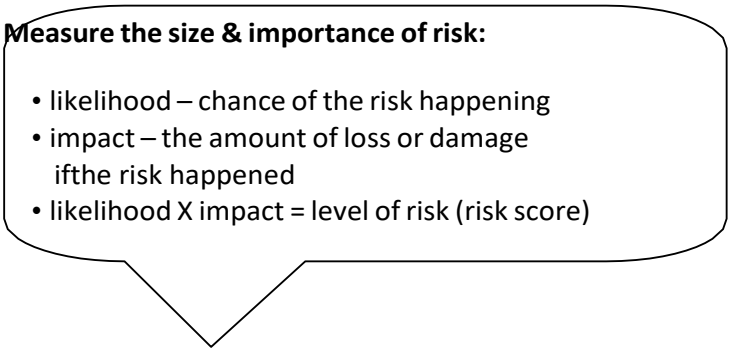
In assessing and mitigating ML&TF risk, the banks should consider a wide range of financial products and services which are associated with different ML/TF risks. These include, but are not limited to Retail banking, Corporate and investment banking, investment services, correspondent services etc.

The risk management framework at a glance:

(a) Risk identification:



(b) Risk assessment /evaluation



(c) Risk treatment

Manage the business risks:

- minimize and manage the risks
- apply strategies, policies and procedures

Manage the regulatory risks:

- put in place systems and controls
- carry out the risk plan and AML&CFT program

(d) Risk monitoring and review

Monitor and review the risk plan:

- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML&CFT program
- do internal audit or assessment
- do AML&CFT compliance report

C.1.4 The risk management process

(a) 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

Source: ML & TF Risk Assessment Guidelines for Banking Sector, 2015

The first step is to identify what ML&TF risks exist in a bank when providing designated services. Some examples of ML&TF risk associated with different banking activities:

- *Retail banking:* provision of services to cash-intensive businesses, volume of

transactions,high-value transactions, diversity of services.

- *Wealth management:* culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.
- *Investment banking:* layering and integration, transfer of assets between parties in exchangefor cash or other assets, global nature of markets.
- *Correspondent banking:* high value transactions, limited information about the remitter andsource of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

There are two risk types i.e. **Business risk and Regulatory risk.**

(i) Business risk

A bank must consider the risk posed by any element or any combination of the elements listed below:

01. Customers: followings are some indicators (but not limited to) to identify ML&TF risk arises from customers of a bank.

- a new customer
- a new customer who wants to carry out a large transaction
- a customer or a group of customers making lots of transactions to the same individual or group
- a customer who has a business which involves large amounts of cash
- a customer whose identification is difficult to check
- a customer who brings in large amounts of used notes and/or small denominations.
- customers conducting their business relationship or transactions in unusual circumstances, such as:
- significant and unexplained geographic distance between the institution and the location of the customer
- frequent and unexplained movement of accounts to different institutions
- frequent and unexplained movement of funds between institutions in various geographic locations
- a non- resident customer
- a corporate customer whose ownership structure is unusual and excessively complex

- customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates
- customers submit 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.

02. Products and services:

- private banking i.e., prioritized or privileged banking
- credit card
- anonymous transaction
- non face to face business relationship or transaction
- payment received from unknown or unrelated third parties
- any new product & service developed
- service to walk-in customers
- mobile banking.

03. Business practice/delivery methods or channels:

- direct to the customer
- online/internet
- phone
- fax
- email
- third-party agent or broker.

04. Country/jurisdiction:

- any country which is unidentified by credible sources as having significantlevel of corruption and criminal activity
- any country subject to economic or trade sanctions
- any country known to be a tax haven and unidentified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country
- any country unidentified by FATF or FSRBs as not having adequateAML&CFT system
- any country identified as destination of illicit financial flow

(ii) 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.

(b) Risk assessment:

Calculation of Risk Score

Measure the size & importance of risk:

- likelihood – chance of the risk happening
- impact – the amount of loss or damage ifthe risk happened
- likelihood X impact = level of risk (risk score)

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

Therefore, each risk element can be rated by:

- the chance of the risk happening – **'likelihood'**
- the amount of loss or damage if the risk happened – **'impact' (consequence)**.

LIKELIHOOD X IMPACT=Risk Level/Score

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 the entity can have as many as they believe are necessary.

Table: 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 bank and its business circumstances, be rated or looked at from the point of view of:

- how it may affect the business (if through not dealing with risks properly the bank suffers a financial loss from either a crime or through fines from BFIU or regulator)
- the risk that a particular transaction may result in the loss of life or property through aterrorist act
- the risk that a particular transaction may result in funds being used for any of the following: corruption and bribery, counterfeiting currency, counterfeiting deeds and documents, smuggling of goods/workers/immigrants, banking offences, narcotics offences, psychotropic substance offences, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud, forgery, extortion, smuggling of domestic and foreign currency, black marketing
- the risk that a particular transaction may cause suffering due to the financing of illegal drugs
- reputational risk – how it may affect the bank if it is found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being shunned by the community of customers

- how it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the business.

Three levels of impact are shown in Table 3, but the bank can have as many as they believeare necessary.

Table : Impact scale

Consequence	Impact – of an ML/TF risk
Major	Huge consequences – major damage or effect. Serious terrorist act orlarge-scale money laundering.
Moderate	Moderate level of money laundering or terrorism financing impact.
Minor	Minor or negligible consequences or effects.

- **Risk matrix and risk score**

Use the risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The riskscore may be used to aid decision making and help in deciding what action to take in view ofthe overall risk. How the risk score is derived can be seen from the risk matrix *(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 bank can have as many as they believe are necessary.

Figure 2: Risk matrix

Threat level for ML/TF risk

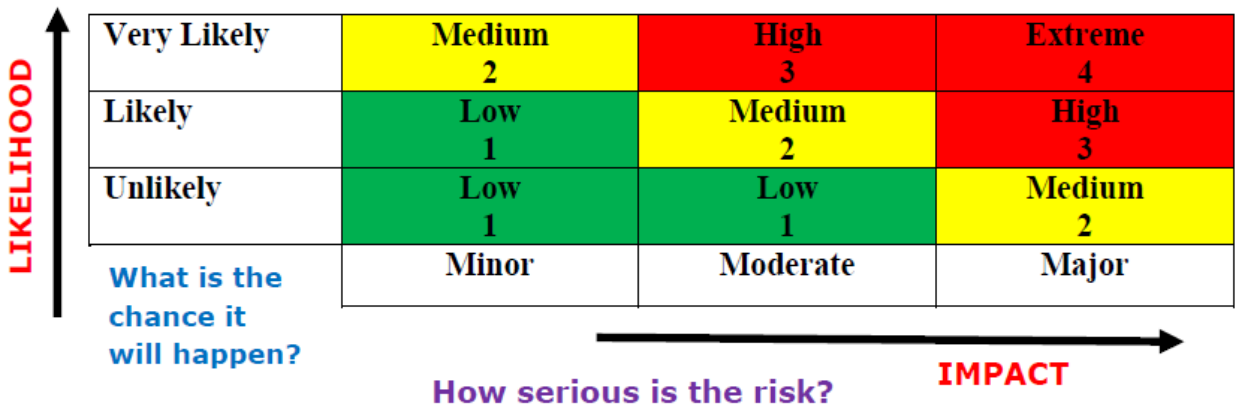


Table 4: Risk score table

Rating	Impact – of an ML&TF risk
4 Extreme	Risk almost sure to happen and/or to have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level.
3 High	Risk likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.
2 Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.
1 Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

Source: ML & TF Risk Assessment Guidelines for Banking Sector, 2015

- **Risk Assessment and Management Exercise:**

From the above discussion, the banks 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's outcomes of risks. All the exercises done by the banks would be calledtogether **"Risk Registrar"**.

(c) Risk Treatment

Manage the Business Risks:

- minimize and manage the risks
- apply strategies, policies and procedures

Manage the regulatory risks:

- Put in place systems and controls
- Carry out the risk plan and AML/CFT program

This stage is about identifying and testing methods to manage the risks the entity may have identified and assessed in the previous process. In doing this they will need to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk.

Examples of a risk reduction or treatment step are:

● setting transaction limits for high-risk products

● having a management approval process for higher-risk products

● process to place customers in different risk categories and apply different identification and verification methods

● not accepting customers who wish to transact with a high-risk country.

(d) Monitor and Review

Monitor & review the risk plan:

- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML&CFT program
- do internal audit or assessment
- do AML&CFT compliance report

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

Once documented, the entity should develop a method to check regularly on whether AML&CFT program is working correctly and well. If not, the entity needs to work out what needs to be improved and put changes in place. This will help keep the program effective and also meet the requirements of the AML&CFT Acts and respective Rules.

C.1.4.1 Additional tools to help risk assessment

The following tools or ideas can be useful in helping to manage risk. It can be included in theprevious risk assessment process so that the decisions are to be better informed.

(a) **Applying risk appetite to risk assessment**

Risk appetite is the amount of risk a bank is prepared to accept in pursuit of its business goals. Risk appetite can be an extra guide to the risk management strategy and can also helpdeal with risks. It is usually expressed as an acceptable/unacceptable level of risk. Some questions to ask are:

● What risks will the bank accept?

● What risks will the bank not accept?

● What risks will the bank treat on a case by case basis?

● What risks will the bank send to a higher level for a decision?

In a risk-based approach to AML&CFT the assessment of risk appetite is a judgment that must be made by the bank. 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

Source: ML & TF Risk Assessment Guidelines for Banking Sector, 2015

C.1.4.2 Risk tolerance

In addition to defining bank's risk appetite, the entity can also define a level of variation to how it manages that risk. This is called risk tolerance, and it provides some flexibility whilst still keeping to the risk framework that has been developed.

C.1.5 Risk Management: Strategies and Techniques

C.1.5.1 Risk Management Strategies

The banks may adopt the following components (where appropriate to the nature, size and complexity of its business), among others, as part of its risk management strategy:

a) reviews at senior management level of the bank's progress towards implementing statedML&TF risk management objectives

b) clearly defined management responsibilities and accountabilities regarding ML&TF riskmanagement

c) adequate staff resources to undertake functions associated with ML&TF risk management

d) specified staff reporting lines from ML&TF risk management system level to board or senior management level, with direct access to the board member(s) or senior manager(s) responsible for overseeing the system

e) procedural controls relevant to particular designated services

f) documentation of all ML&TF risk management policies

g) a system, whether technology based or manual, for monitoring the bank's compliance

with relevant controls

h) policies to resolve identified non-compliance

i) appropriate training program(s) for staff to develop expertise in the identification ofML&TF risk(s) across the bank's designated services

j) an effective information management system which should:

i) produce detailed and accurate financial, operational and compliance data relevant toML&TF risk management

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 banks

iv) allow the banks to identify, quantify, assess and monitor business activities relevant to ML&TF risk(s)

v) allow the banks to monitor the effectiveness of and compliance with its internalAML&CFT systems and procedures

vi) allow the banks to regularly assess the timeliness and relevance of informationgenerated, together with its adequacy, quality and accuracy.

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

C.1.5.2 Ongoing Risk Monitoring

A bank's ongoing monitoring of its risk management procedures and controls may also alert the bank 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 toML&TF risk(s)
e) changes in business functions which are not reflected in the AML&CFT program (forexample, the introduction of a new product or distribution channel)

f) failure to undertake independent review (at an appropriate level and frequency) of thecontent and application of the AML&CFT program

g) legislation incorrectly interpreted and applied in relation to a customer identificationprocedure

h) customer identification and monitoring systems, policies and procedures that fail to:

i) prompt, if appropriate, for further identification and/or verification when the ML&TF risk posed by a customer increase

ii) detect where a customer has not been sufficiently identified and prevent thecustomer from receiving the designated service

iii) take appropriate action where a customer provides insufficient or suspiciousinformation in relation to an identification check

iv) take appropriate action where the identification document provided is neither anoriginal nor a certified copy

v) recognize foreign identification documentation issued by a high-risk jurisdiction

vi) record comprehensive details of identification documents, for example, the date ofissue

vii) consult appropriate resources in order to identify high-risk customers

viii) identify when an expired or old identification document (for example, a driver's license) has been used

ix) collect any other name(s) by which the customer is known

i) lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers

j) lack of ability to consistently and correctly train staff and/or third parties, particularly inareas with high turnover in:

i) customer identification policies, procedures and systems

ii) identifying potential ML&TF risks

k) acceptance of documentation that may not be readily verifiable.

C.1.5.3 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:

i. 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 complexgiven the nature of the company's business

ii. 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

iii. Product, service, transaction or delivery channel risk factors

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

C.1.5.4 Lower risks Scenario

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

i. Customer risk factors

- Banks – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements

Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficialownership

- Public administrations or enterprises.

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

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

iii. **Country risk factors**

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

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

C.1.5.5 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.

C.1.5.6 Counter Measures for Risk

C.1.5.6.1 Enhanced due diligence measures

Banks 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, banks 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.), andupdating more regularly the identification data of customer and beneficial owner
- Obtaining and verifying additional information on the intended nature of the businessrelationship
- Obtaining and verifying information on the source of funds or source of wealth of thecustomer
- Obtaining and verifying information on the reasons for intended or performed transactions
- Obtaining and verifying the approval of senior management to commence or continuethe business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that needfurther examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

C.1.5.6.2 Simplified CDD measures

Where the risks of money laundering or terrorist financing are lower, the banks are allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishmentof the business relationship (e.g. if account transactions rise above a defined monetary threshold)
- Reducing the frequency of customer identification updates
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purposeand

nature from the type of transactions or business relationship established. Simplified CDD measures are not acceptable whenever there is a suspicion of moneylaundering or terrorist financing, or where specific higher-risk scenarios apply.

3.1.5.7 Ongoing due diligence

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

C.2 Identifying and Assessing Trade Based Money Laundering (TBML)

The international trade system is clearly subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist financiers. In part, these arise from the enormous volume of trade flows, which obscures individual transactions; the complexities associated with the use of multiple foreign exchange transactions and diverse trade financing arrangements; the commingling of legitimate and illicit funds; and the limited resources that most customs agencies have available to detect suspicious trade transactions.

Trade Based Money Laundering (TBML) was recognized by the Financial Action Task Force (FATF) in its landmark 2006 study as one of the three main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy. This method of money laundering (ML) is based upon abuse of trade transactions and their financing. The 2006 FATF Study highlighted the increasing attractiveness of TBML as a method for laundering funds, as controls on laundering of funds through misuse of the financial system (both formal and alternate) and through physical movement of cash (cash smuggling) become tighter.

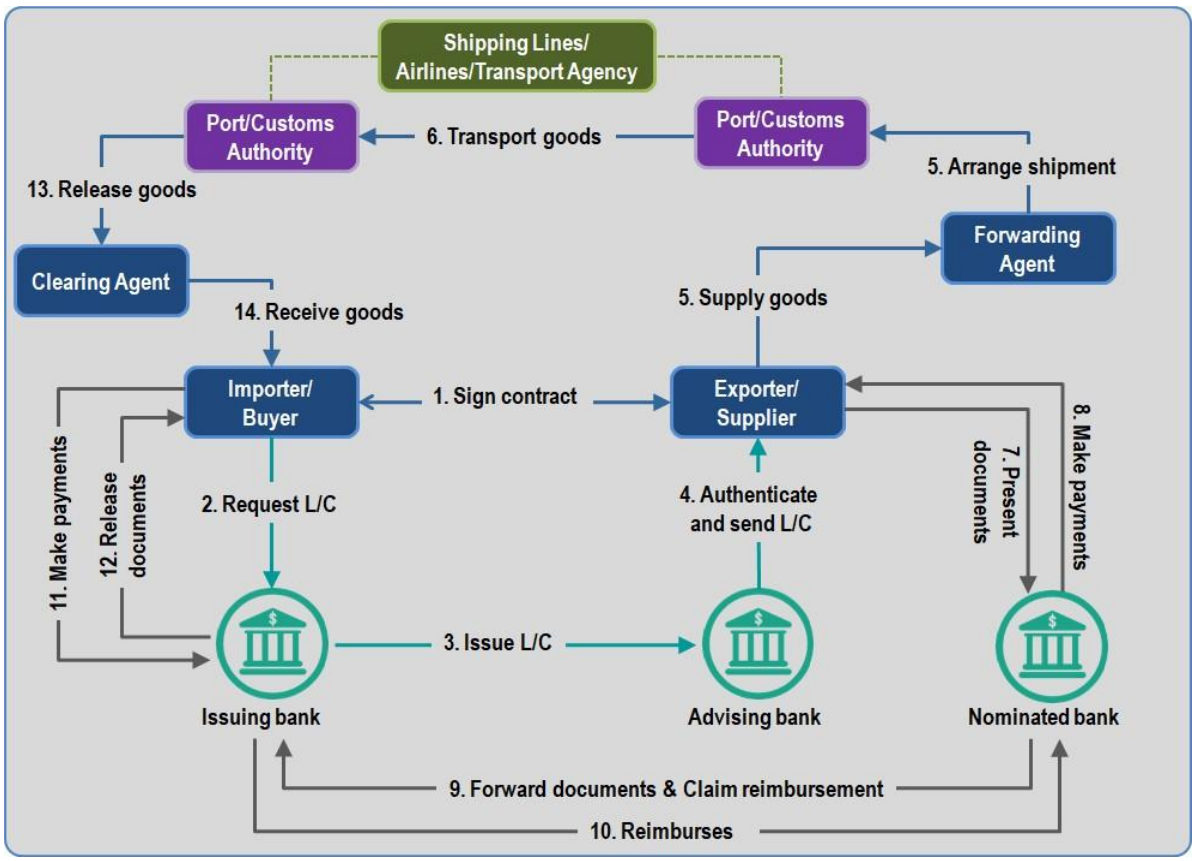
FATF, in its best practice paper in 2008, defined TBML as “the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origins or finance their activities”. Like many countries Bangladesh is also affected by trade-based money laundering and ensuing illicit outflow. Concerns in this area are almost unanimously agreed by all relevant agencies and authorities.

Recognizing Trade Based Money Laundering (TBML) as the riskiest area in money laundering, BFIU issued guidelines for Prevention of Trade Based Money Laundering for banks through BFIU Circular no. 24 on 10 December 2019. The guideline covers both TBML risk assessment and risk mitigation.

C.3 Guidelines for Prevention of TBML in Bangladesh

C.3.1 The process flow in a documentary credit

Among the trade payment methods mostly followed in Bangladesh are documentary credit and documentary collection. In a documentary credit process, the issuing banks have primary obligations in the transaction. The process flow is as under the Buyer (importer) and the seller (exporter) furnish sale/purchase contract



Source: Guidelines for Prevention of Trade Based Money Laundering, 2019

a) Among the trade payment methods mostly followed in Bangladesh are documentary credit and documentary collection. In a documentary credit process, the issuing banks have primary obligations in the transaction. The process flow is as under the Buyer (importer) and the seller (exporter) furnish sale/purchase contract.

b) The applicant (Buyer) requests the issuing bank to open documentary credit on account of the buyer.

c) The issuing Bank issues the credit in favor of the beneficiary and transmits through the advising bank (usually).

d) The advising bank advises the credit to the beneficiary (Seller).

e) The beneficiary ships the goods, prepares, collects & collates the requireddocuments under the credit and presents to the nominated bank (usually).

f) The nominated bank forwards documents to the issuing bank/confirming bank. Nominated bank can honour/negotiate documents i.e. make payments and claim re-imbursement if documents are in order as per LC terms.

g) Issuing bank on receipt of complying presentation and /or obtaining documents effects payment to the beneficiary and/or nominated bank, as the case may be.

h) The applicant releases documents from the issuing bank.

i) The applicant clears the goods from the customs through his appointed clearingagent.

C.3.2 Regulatory Framework in Combating TBML in Bangladesh

C.3.2.1 Money Laundering Prevention Act, 2012: As per section 2 (v) (ii) of Money Laundering Prevention Act, 2012 smuggling of money or property is money laundering while section 2

(a) of the Act defines "smuggling of money or property" as-

i) transfer or holding money or property outside the country in breach of the existinglaws in the country; or

ii) refrain from repatriating money or property from abroad in which Bangladesh has aninterest and was due to be repatriated; or

iii) not bringing into the country the actual dues from a foreign country, or paying toforeign country in excess of the actual dues;

It can be easily comprehended that in Bangladesh context, international trade is one of the avenues abusing which smuggling of money or property and illicit outflow can take place.

As per the Act, however, any person who commits or abets or conspires to commit the offense of money laundering is liable to be punished for minimum 4 years and maximum 12 years of imprisonment, in addition to that a fine equivalent to twice the value of the propertyinvolved in the offence or BDT 1 million whichever is higher shall be imposed. The punishment for an entity in this regard is a fine of not less than twice the value of the propertyor BDT 2 million whichever is higher; in addition to that license is also liable to be cancelled.

The law of the land, therefore, prohibits smuggling of money or property in the strictest term and provides stringent punishment for the offence. Despite such stringent legal provisions Banks may willingly or inadvertently become vulnerable to this offence.

Furthermore, Guidelines for Foreign Exchange Transactions (GFET) and Import Policy Order have made specific mandatory requirement for ensuring pricing competitiveness prior to any international trade transactions:

C.3.2.2 Import Policy Order 2015-2018: Chapter 2 "General Provisions for Import", Section 5(4) "Import at competitive rate":

a) Import shall be made at the most competitive rate and it is obligatory for the importers, at any time, to submit documents to Import Control Authority regarding the price paid or to be paid by them;

b) in case of import under Untied Commodity Aid in the private sector, goods shall be imported at the most competitive rate by obtaining quotations from at least three suppliers or indentors representing at least two source countries: Provided that this condition shall not apply for opening LC up to Tk. one lac; and

c) for import at the most competitive rate by the public sector importers, quotations have to be invited before opening letter of credit, and goods shall be imported at the most competitive price.

C.3.2.3 Guidelines for foreign Exchange transactions (GFET), 2018: volume-1Chapter 7, Para 20: Verification of import price etc.:

"Before opening of LC or issuing LCAF, the AD shall have to take usual and reasonable cautionary measures to ensure that both the exporter and importer are bona fide business person of the goods concerned, the exporting country is the usual exporter of the goods concerned and the price of the goods concerned is competitive in terms of prevailing price in the international market on the date of contract and/or similar imports in contemporary period. ADs are advised to verify the above, if needed, with the help of concerned Bangladesh Mission abroad."

C.3.2.4 Chapter 8, Para 7 "Certification of EXP forms by ADs":

(b) In order to avoid any loss of foreign exchange to the country, ADs shall not certify any EXP form unless they have satisfied themselves with regard to the followings: (iv) Bona fides of the buyers/consignees abroad and their credentials etc. where necessary, ADs should make discreet enquiries in this regard through their correspondents abroad etc., greater care should be taken particularly in cases of shipments against contract alone and shipments on CAD/DA basis. Where ADs doubt the bonafides and standing of the buyers/consignees abroad or whereowing to common interest or otherwise they suspect collusion with the intent of' delaying or avoiding repatriation of export proceeds ADs should report such cases promptly to Bangladesh Bank. Similarly, ADs should report to Bangladesh Bank cases where it comes to their knowledge that the exporters are directly or indirectly connected with or have any financial or other interest in the buyer/consignee abroad. Where felt necessary, discreet enquiry about the bonafides and credentials of the charter party should also be made in case the shipment is to be against a charter party Bill of Lading so as to avoid loss of cargo/foreignexchange

(c) These are only few examples of regulatory instructions. In fact, there are many other regulatory instructions relevant to combating TBML.

C.3.3 Scope of TBML in Bangladesh

Generally, criminals use trade finance to obscure the illegal movement of funds through misrepresentation of price, quality and/or quantity of goods and services. And to do this, in most cases, there might be collusion between the seller and the buyer. The collusion may well arise as both parties could be controlled by the same person/entity. The transfer of value in this way may be executed in a number of ways such as Over Invoicing, Under Invoicing, Multiple Invoicing, Short shipment, Over Shipment, Phantom Shipment, and Complicated Payment Structure, discount, price changes, freight charges or without making any payment at all etc. Bangladesh is not an exception in this regard. However, some of the vulnerabilities are given below.

C.3.3.1 Import Procedure and Some Avenues for TBML in Bangladesh

i. Import procedure in Bangladesh generally begins by obtaining an Importer Registration Certificate (IRC) from the Office of the Chief Controller of Import and Export (CCI&E) under the Importers, Exporters and Indentors (registration) Order, 1981. According to this Order, an importer can get one IRC for commercial and one for industrial import. Importers may take the opportunity to have more than one IRC to use one in TBML as throughout the import procedure and reporting of the transaction's importers are identified through IRCs not through their names. Moreover, family members of a trader having same business address may obtain IRCs and abuse them to commit TBML.

ii. Letter of Credit Authorization Form (LCAF) is mandatory for importer as it is the declaration of amount, value, HS code and the description of the goods as per Customs First Schedule and terms of import. After declaration of LCAF, importers are allowed to open/issue LC/Contract by the ADs. On the basis of the LC/Contract declaring on IMP by the importers ADs can sale/make payment of LC/Contract documents. Though importers are strictly prohibited from making payment in excess of LCAF value, sometimes abusing FC/ERQ accounts or other means, they pay more than the value of the LCAF or of Expired value and thus facilitate TBML.

iii. Major portion of imported goods are imported on CFR basis in Bangladesh where freight charges are invoiced to the importer. In some cases, it has been found that freight charges reached several times of the FOB value. In fact, freight and other charges can also be a medium of TBML.

iv. Value of goods to be imported can be medium of TBML as value can be quoted less than the actual price (Under invoicing) of the goods with a deliberate intention to evade import duties and taxes. Generally, most of the amount of under invoiced import is paid through hundi or hawala.

Evasion of taxes and duties i.e. custom related offenses is the predicate offence of ML in Bangladesh according to MLPA, 2012. On the other hand, capital machinery and raw materials (of which import duties are lower) can be imported quoting more than the actual price (Over invoicing) of goods as a medium of TBML.

v. Banks are responsible to make payment against the import documents if found inorder and no discrepancy arises. Yet, documents can be received directly by the importer and the goods can be released from the customs. In that case, banks may make payment based on the customs certified bill of entry (BE) submitted by the importer. This practice takes place while releasing goods with copy documents. TBML can occur in these situations as there are opportunities to fabricate the import documents and related BE by the malafide importer.

vi. Banks are permitted to make advance payment against import without prior approval of BB based on a repayment guarantee from a bank abroad. This guarantee is not needed for remittance up to USD 5,000 (and USD 25,000 from ERQ accounts). Moreover, fabricated/fake/false bank guarantee can create a scope of TBML through payment of advance remittance against import.

vii. After making payment against the goods to be imported, importers are liable either to import the goods or to bring back the amount remitted in proper banking channel (Article 4(3), FERA, 1947). BB marks out the duration of the process 4 months after the date of making payment. Failure to transport the goods within the prescribed duration makes the related Bill of Entry (BE) overdue and no importer can get any import facility (opening LC/making advance payment, or enhancement of existing LC/Contract value) from any bank in Bangladesh having overdue BE against any of its previous import without the prior approval of BB. Importers may take the opportunity to surrender the IRC (intended to avoid the import liability and also to be involved in TBML) against which BE is being overdue and get another IRC for a fresh start.

viii. The incidence of loss or damage of the goods-in-transit or before release as well as cancellation of shipment may be used as a medium of TBML. Compensation against the damaged goods or return of the remittance against cancelled shipment can be received from sources/third parties directly not related to the exporter of the goods. Again, loss of goods before release from the customs can be concocted (intended to evade tax and commit capital flight) to get the insurance claim and get waiver from submission of the BE.

ix. The ADs are allowed to open back-to-back (BTB) import LCs against export LCs operating under the bonded warehouse system, subject to observance of domestic value addition requirement. Misuse of the bonded warehouse facility (intended to evade tax) by selling the imported goods to the local market can also be an exampleof TMBL in import. Again, BTB LCs opened against arranged/fake master LCs can also be used in TBML where no export occurs

showing some 'valid' reasons though raw materials imported duly against the BTB LCs.

x. ADs are allowed to open deferred (Under Chapter 7, Para 33(a) of GFET, 2018), or usance basis L/C. As there are instances and vulnerabilities of abuse of suppliers' and buyers' credit, utmost care should be given to those payments where payments are settled through buyers' credit or suppliers' credit.

xi. Exporters are allowed to export on CMT (Cutting, Making and Trimming) basis as well as to import the raw materials on Free of Cost (FOC) basis. Since this FOC import does not require any bank endorsement and there is no matching of bill of entry with the value, customers can manipulate the FOC items.

xii. Import of non-physical goods (software and others) can be a medium of TBML as keeping track of import process of such non-physical goods is difficult for anyreporting/regulatory agency.

xiii. Import Policy Order allows actual users to import up to a certain limit (USD 7,000.00 per year) for their personal consumption. As AD banks have no control to monitor this limit through any system individuals might import through different ADs exceeding the limit and sell them commercially to the market illegally.

xiv. Consumers can purchase goods online by making payment through international credit or debit cards or unused portion of Travel Quota and later receive goods through courier. Criminal proceeds might be transferred through this online payment.

C.3.3.2 Export Procedure and Some Avenues for TBML in Bangladesh

i. Export procedure in Bangladesh generally starts with obtaining Exporter registration Certificate (ERC) from the CCI&E under the Importers, Exporters and Indentors (registration) Order, 1981. According to the order, an exporter can get only one ERC for export. Exporters may take the opportunity to have more than one ERC to use one in TBML, as throughout the export procedure and reporting of the transactions, exporters are identified through ERCs not through their names.

ii. Value of goods to be exported can be a medium of TBML as value can be quoted less than the actual price (under invoicing) of the goods intended to siphon money abroad.

iii. After shipment of the goods for export, exporters are liable to repatriate exportproceeds in full (Section 12 of FERA, 1947). BB marks out the duration of the repatriation of export proceeds within 4 months after the date of shipment. Failure to receive the full export proceeds within the prescribed duration makes the related Export Bill overdue. Exporter can be out of track having huge amount of overdue export bills intended to commit money laundering through export.

iv. Commission, brokerage fee or other trade charges to be paid to foreign importers/agents (of which up to 5% ADs can allow) may also sometimes be abused for TBML.

v. Payments in Foreign Exchange may be made through international cards (debit/credit/prepaid etc.) which are categorically mentioned in Chapter 19 of GFET, 2018. ADs should meticulously monitor the issuance and end-use of those cards.

vi. Partial drawing of export bill/Advance Receipt against export can be abused for TBML. It is the responsibility of the ADs to follow up each such case and to ensure that the balance amount is also realized within the prescribed period.

vii. Shutting out of a shipment by a particular vessel and re-shipment in another vessel should be checked. This is because there are opportunities of TBML as transshipment through one or more jurisdictions for no apparent economic reason is suspicious.

viii. The incidence of loss or damage of the exported goods in-transit or before release as well as cancellation of shipment (for which payment has not already been received) may be used as a medium of TBML. Compensation against the damaged goods can be received from other sources/third parties directly not related to the importer of the goods.

ix. Export of non-physical goods (software and others) can be a medium of TBML as keeping track of the export process of the non-physical goods is difficult for any reporting/regulatory agency.

x. Buying House Arrangement/Buyer Nominated Supplier Arrangement can be a medium of TBML. Shipment of goods can illicitly be delayed by the buying houses through 'arranged game' for getting discount on the exported value. Again, buyer nominated supplier can quote higher price for the raw materials and thus money laundering can take place.

xi. Transaction in large volume through other than banking channel such as exchange house etc. is vulnerable to TBML.

xii. In the name of export proceeds wage earners' remittance may be brought into Bangladesh to claim cash incentives.

xiii. Inward remittance may be brought from the countries where Bangladeshis have direct/indirect business and cash incentive may be claimed.

xiv. ADs are allowed to discount the usance bill (para 25, chapter 8). ADs should take utmost care while discounting or purchasing foreign documentary export bills.

C.3.3.3 Remittance of Royalty, Technical Assistance Fees etc.

Under Section 18 of Bangladesh Investment Development Authority Act, 2016, approved industrial

enterprises shall have to take approval from Bangladesh Investment Development Authority (BIDA) and other competent authorities for payment of royalty, technical know- how, operational service fees, management fees, technical assistance and franchise fees.

Vulnerabilities:

While making remittance of royalty and other technical fees, banks may expose them to money laundering by not conducting due diligence under the following conditions:

a) Ambiguous agreement/contract between local company and technical service provider;

b) Auditor's certificates regarding net remittable amount;

c) Suspicion remains about the genuineness of the papers (copies of the royalty/technical assistance agreements, documentary evidences); and

d) Lack of adequate due diligence on the underlying trade.

Adequate measures should be taken to combat TBML in this case and instructions contained in para 26, 27 & 28 of chapter 10 of GFET, 2018 should be followed meticulously when suchremittances are executed.

C.3.4 Some Avenues for TBML through OBUs, EPZs, EZs and PEZs in Bangladesh

Trade finance through OBUs and different mode of international trade practiced in the EPZs, EZs, PEZs are sometimes abused for TBML. As OBUs can borrow funds from banks and FIs from both home and abroad they are more vulnerable to TBML. It can provide finance facilities against purchase/supply order, corporate guarantee, personal guarantee of the directors of company etc. with borrowed fund. However, recovery of the fund may not be possible due to lack of verification of the authenticity of the documents, willful default of the borrowers and poor or biased customer risk assessment. In such cases Bangladeshi nationals can also siphon money if they have beneficial ownership or control on the company in whose favour the financing facilities are provided.

In case of companies in Special Economic Zones, directors' liabilities are limited by shares. When the company falls into trouble due to taking more exposure through more foreign/local loan or trade gap, they may transfer, sell or even wind up the company keeping the outstanding liabilities in Bangladesh. The situation arises sometimes that the company makes payment for import without entry of the goods, or export is done but the proceeds are not realized. Keeping these liabilities pending owners/directors transfer, sell or wind up the company and leave the country. Bankers should provide proper information to regulators in time before winding up of these companies. Bankers should apply enhanced due diligence while providing trade and other services to these

companies of Economic Zones.

In Bangladesh context letter of credit is safe compared to other mode of trade (such as Open Account, Cash in Advance etc.) in TBML perspective. However, it is also undeniable that TBML risk may arise under LC if the LC is between parent and affiliates or if the trade is just an arranged game. Because of this, TBML risk mitigation measures here need to be stringent, otherwise trade should be facilitated by banks through LC applying adequate due diligence only.

As banking sector of the country is more vulnerable to TBML, bankers should remain familiar with the different methods that may be abused for TBML. To get further insight, some case studies in Bangladesh context are discussed in Appendix A.

C.3.5 Key Challenges and Difficulties in Preventing Trade Based Money Laundering in Bangladesh

a) Price Verification for Financial Crime Control

As discussed in 2.3 according to Import Policy Order, importers are obligated to import goods at competitive prices. Banks are also advised in the GFET, 2018 to take usual and reasonable cautionary measures to ensure that the price of the goods concerned is competitive in terms of prevailing price in the international market on the date of contract and/or similar imports in contemporary period. They are also advised to verify the above, if needed, with the help of concerned Bangladesh Mission abroad. Due to lack of relevant business information, such as the terms of business relationship, volume discounting or specific quality, or feature, specifications of goods involved bankers have to be cautious in making meaningful determinations about the appropriateness of the unit price. Moreover, many products are not traded in public markets and their market prices are also not publicly available. Even where goods are publicly traded, the current prices may not reflect the agreed price used in any contract of sale or purchase and these details will not usually be available to the banks involved due to competitive sensitivity of such information.

b) Transfer Pricing

Transfer pricing is a related party transaction commonly used by transnational corporation as part of their financial and tax planning strategy. Multinational organizations use transfer pricing to shift taxable income from jurisdictions with relatively high tax rates to jurisdictions with relatively low tax rates to minimize income tax. Similar strategies are also employed in relation to import duties and value added tax. TBML can occur when international trade is abused for transfer pricing. This poses a significant challenge which needs to be overcome.

c) Limited Skilled Manpower

Performing the foreign exchange activities involves proper communication with the client, various

banks of the country as well as abroad. A single error may cost thousands of dollars. In Bangladesh there are limited skilled manpower who are able to understand and handle the foreign exchange dealings very well. As such, skill development through proper training is a must to address TBML risk.

d) Extreme Competition

Unhealthy competition is driving bankers to constantly hunt for aggressive business and profit target. Thus, working under pressure of such target combined with the fear of losing customers and presence of other competitor banks officials sometimes ignore minor trade related due diligence which makes the bank a victim to TBML. Unhealthy competition poses a challenge to combating TBML.

e) Absence of Co-ordination

Absence of coordination is also one of the major challenges in combating TBML. A coordinated Risk Management Unit/Division in combination of all concerned agencies may be formed to ensure co-ordination & concerted efforts. Besides, National Board of Revenue (specially the Valuations and Audit unit)/, Customs and Bangladesh Banks may also work to assess the value of the imported or exported goods/commodities/services. Arrangements may be in place so that customs authority and banks may be aware through mutual information sharing mechanism when there is abnormal increase in the number and value of LC of a particular company/firm etc., risky import of goods such as Reconditioned Capital Machinery, Software, Chemicals where complexity exists in determining price and description of the products, cases where importer and exporter are related, when import and export goods are inconsistent with the nature of trade of the customer, inconsistency in price exists, when an LC is frequently amended, where beneficiary desires payment in third country or party, when Bill of Lading does not mention container number, does not bear invoice number, where miscellaneous charges such as freight, lading charge etc are abnormal etc.

f) Absence of Management Information Systems (MIS) and a Central Data Base

Lack of MIS and a central data base or uniform price list of various commodities is also a hindrance to preventing under invoicing and over-invoicing by those engaged in trade operations.

g) Duty/Tax structure

At times, bankers disagree with the quoted price in the Proforma Invoice (PI), because they fail to match the given price which is sometimes far away from the actual price of the commodity in the international market. In some items of imports importers may quote higher price in line with customs' rate of duty even though the price may be less than the price mentioned in NBR's minimum price list[1]. Though there is no scope of tax/VAT evasion against such imports, it may be

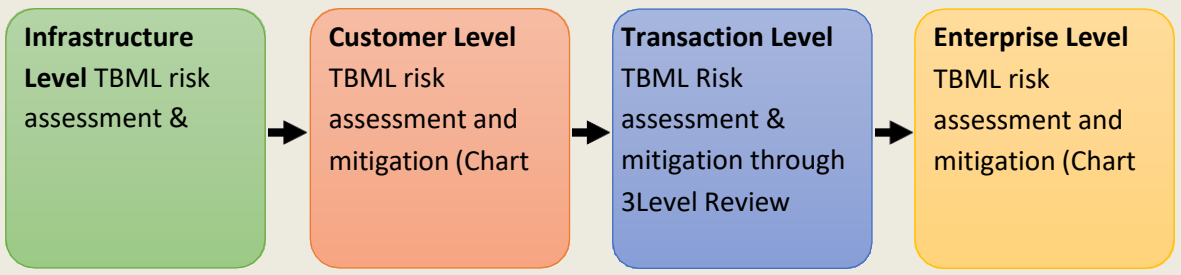
abused for TBML.

The Challenges and difficulties faced by the sector and the specific trend of trade-based money laundering in Bangladesh indicates the challenging task the banks have to accomplish to protect themselves from this financial crime. The next chapters, therefore, highlight the risk-based framework and trade controls that banks should establish to combat trade based money laundering effectively.

C.3.6 TBML Risk Assessment & Mitigation Mechanism

Trade based Money Laundering risk may arise and affect due to inadequate infrastructure of the bank, inaccurate assessment of the customer before on board, poor identification and handling of TBML alert while conducting trade transaction by the officials concerned and; overall for failure of the bank to address the risk at the enterprise or institute level. Hence all the banks are instructed to establish TBML risk assessment and mitigation at infrastructure level, customer level, transaction level and at enterprise level as shown in the flowchart below.

Chart 3.1: TBML Risk Assessment & Mitigation Mechanism



Source: Guidelines for Prevention of Trade Based Money Laundering, 2019

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

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

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

C.3.6.1 Infrastructure Level Risk Assessment

Banks should develop their own infrastructure for price verification, transaction monitoring and

screening in line with their exposure to international trade. The followings are indicative suggestions that banks should establish to combat trade-based money laundering:

- ✓ Standard Sanction screening process
- ✓ Standard for manual screening
- ✓ Own data base based on transactions
- ✓ Subscribe for publically available online commodity pricing website
- ✓ Vessel tracking system[2].

C.3.6.2 Customer Level TBML Risk Assessment and Mitigation Mechanism

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

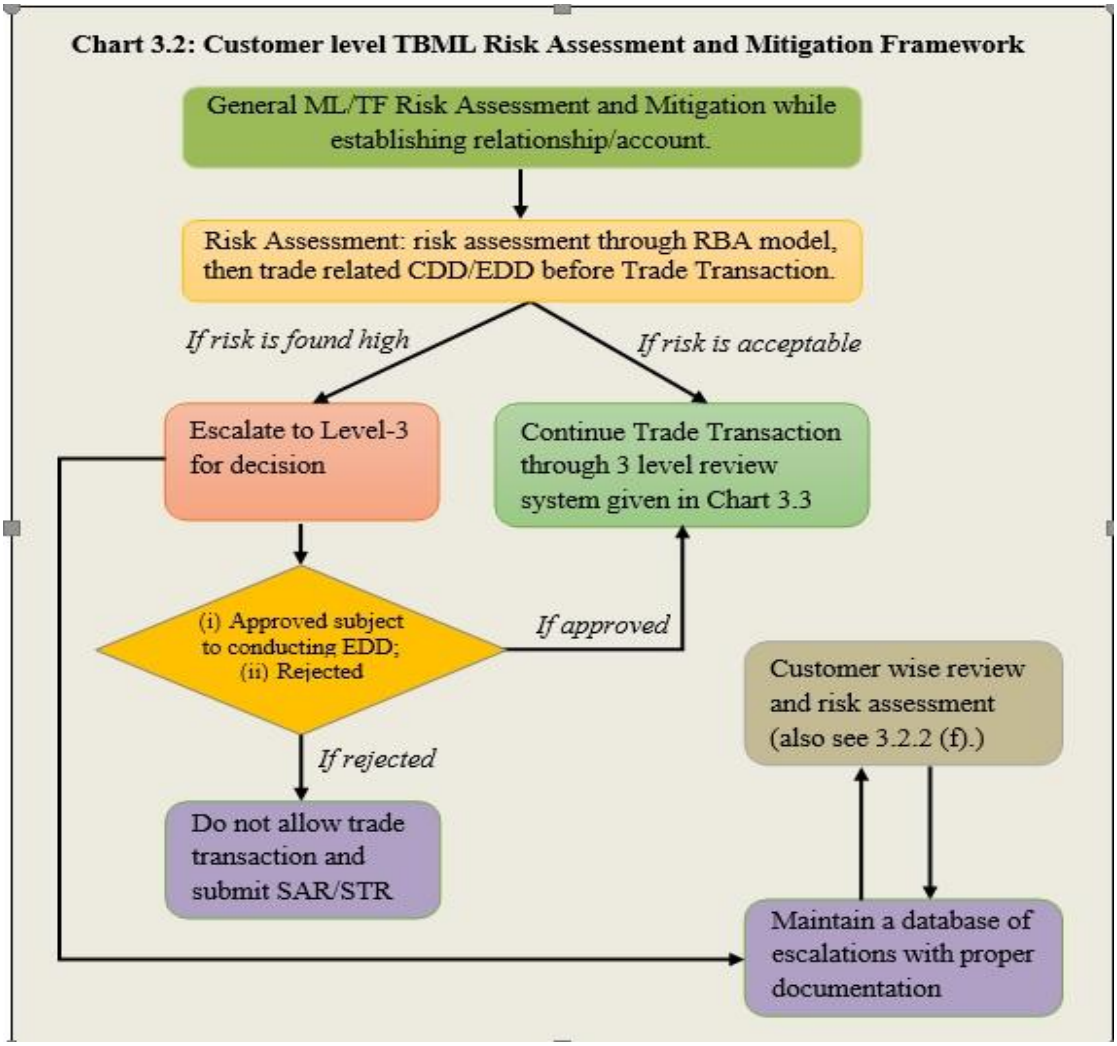
(b) **Risk Assessment related to Trade**: As in most cases there are some products and commodities, various delivery channels and jurisdictions through which TBML occurs, it is quite convenient to have a risk-based approach. Risk assessment should be done following the sample model given in Table 3.1 or any other suitable model developed by the bank (subject to vetting by BFIU) depending on their respective risk exposure and experience. Banks should design a standard format to collect the required information for this sample model. For fresh/new customers the assessment may be done on the projection submitted in the format by the customers and for the existing and old customers historical data may be chosen. It is also recommended that banks ensure independent evaluation/assessment of importers and exporters by their own staff and ensure/examine, to the extent practicable, the relationship between importers and exporters through third parties. Customer level risk assessment for newly onboarded tradecustomer is to be done before initiation of trade transactions. For existing tradecustomers, customer level risk assessment should be done as early as possible but shouldnot be later than next periodic review of KYC in pursuance with BFIU circular 19.

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

completion of CDD/EDD, the customer will be allowed to go for trade transaction. Details of requirements to conduct CDD/EDD has been described in section 3.2.2.2, which are not exhaustive rather indicatives.

(d) **Trade Transaction through 3 Level Review Systems**: When a customer is allowed for trade transaction, trade transaction will take place following Three Level Review System as mentioned in section 3.2.3

(e) **Maintaining a database of escalations with proper documentation:** A database should be established with customers assessed as high risk to facilitate yearly customer wise review and assessment.



Source: Guidelines for Prevention of Trade Based Money Laundering, 2019

(f) **Review and Assessment of Customers:** For high risk customers review and assessment frequency shall be one year, for medium risk customers this frequency shall be every three years and for low risk customers it shall be 5 years. The review system mentioned above in the Chart 3.2.2 will facilitate input for the enterprise wide risk assessment and assist banks to update TBML trend and typology and devise appropriate policy and strategy at the enterprise level.

C.3.6.2.1 Customer Level Risk Assessment

The framework as detailed below is a sample for guidance and reference only. Each and every bank may opt for qualitative and quantitative assessment (Q^2-method), should design their own feasible scoring model depending on their respective risk exposure and experience and get the model vetted by BFIU.

Table: Sample Risk Based Model for Trade Customers

SL	Risk Components	SL	Risk Parameters	Risk Score (0-3)[3]		Composite Risk Level
				Obtained score	Max score	$\frac{(\sum Obt.\_score) * 100}{\sum Max.\_score}$
1	**Trade Customer Demographic**	1	Business History [4]			
		2	Payment Behavior [5]			
		3	Adverse Media Report [6]			
		4	Law Suit Filed[7]			
		5	Others (if any)			
Sub Total=						
2	**Geographic locations of trade Transactions**	6	Jurisdiction[8] 1			
		7	Jurisdiction 2			
		8	Jurisdiction 3			
		9	Jurisdiction 4			
		10	Jurisdiction 5			
		11	Other Jurisdictions (if any)			
		12	Complexity			
Sub Total=						

SL	Risk Components	SL	Risk Parameters	Risk Score (0-3)[3]		Composite Risk Level
				Obtained score	Max score	$\frac{(\sum Obt.\_score) * 100}{\sum Max.\_score}$
3	**Products /services**	13	Food Grain			
		14	Industrial Raw Materials			
		15	Capital Machinery			
		16	Trading Goods			
		17	Service Import or Service Export			
		18	Defense-Goods[9]			
		19	Dual-Use Goods[10]			
		20	Other products (if any)			
		21	Multiple Products			
Sub Total=						
4	**Transactions Trend / History**	22	Value of trade transactions			
		23	Number of trade transactions			
		24	Number of escalated TBML Alerts			
		25	Number of STR			
Sub Total=						
Grand Total=				$\sum Obt.\_score$	$\sum Max.\_score$	

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

Source: Guidelines for Prevention of Trade Based Money Laundering, 2019

[3]'0' represents no risk, '1' represents low risk, '2' represents medium risk and '3' high risk.

[4]Business history of the customer, frequency of his/her trade default, his/her/its reputation in running business etc. within the period.

[5] Payment behavior of the customer.

[6] Adverse media report on the customer and/or the products he deals with and its impact or sensitivity.

[7] Law suits filed against the customer related to his/her trade.

[8] Jurisdiction with which the customer conducts import and export business, AML/CFT risk associated with the jurisdiction, FATF public document and other relevant lists etc.

[9]& 10 Consult Import Policy Order, website of World Customs Organizations and other reliable sources.

Relevant data such as on jurisdiction, products, services, value & number of trade transactions can be obtained from TTP. In assigning score banks should also take in to account the factors described in section C.3.3-C.3.4.

C.3.6.2.2 Trade Related CDD Requirements

Banks should conduct CDD in line with risk-based framework and consider the following requirements as suggested below. Banks may decide on whether the trade related CDD requirements will be performed at the time of establishing relationship/opening account with the customer along with conducting general CDD or separately before starting trade transaction.

1. Collection of required documents & information such as:
    a. Nature of business including major goods, services and jurisdictions the customer deals with;
    b. Usual delivery / transportation mode for goods or services;
    c. Major suppliers and buyers;
    d. Products and services to be utilized from the bank;
    e. Existing/anticipated account activities;
    f. Usual methods and terms of payment and settlement;
    g. Any observations/ratings on the customer by concerned departments of the bank;
    h. Any previous suspicious transaction/activity reports to BFIU;
    i. Other information from the relevant staff; and
    j. Trade Transaction Profile.
2. Verification of the documents & information mentioned in 1 above through reliable and

independent sources.

3. Ascertaining and verifying the identity of the beneficial owners of the trade customer.
4. Conducting enhance due diligence if required.
5. Record Keeping.
6. Understanding business, production capacity, end-use of goods, the principal counterparties, the countries where the counterparties are located and the goods or services that are exchanged, as well as the expected annual transaction volumes and flows to conduct Customer Due Diligence (CDD) for trade customers.
7. Updating CDD information in accordance with BFIU Circulars and ML&TF Risk Management Guidelines.
8. Maintaining customer wise trade transaction profile (TTP) including items of goods, value, volume, nature of business, and principal counterparty country etc. A sample is given at Appendix- C. TTP should be made available to Level 1, 2 & 3 so that they can easily check that a transaction is within the agreed profile of the customer. Until TTP is integrated within core banking system, it may remain offline outside of the core banking system. Level 2 shall conduct TTP review and decide on certain transactions escalated by Level 1. If necessary, Level 3 may also consult TTP while taking ultimate decision on transactions escalated by Level 2. Post facto review of TTP against trade transactions may be conducted at least annually to identify TBML Alerts.
9. The CDD processes are expected to include "feed-back loops" where a trigger event in a transaction or normal review process leads to new information or questions about a relationship. Objective behind updating of the CDD profile is to ensure that the information in the CDD profile is current. The reviews may also lead to the status of the relationship with the customer being escalated for decisions related to additional controls being applied or the exit of the customer.
10. Banks should develop their own process of "customer/transaction level risk assessment" based on their risk exposure.

C.3.6.3 Transaction Level TBML Risk Assessment & Mitigation through 3 Level Review System

Depending on TBML risks trade transactions shall be disambiguated at level 1 or shall require escalations to level 2 or level 3 before they are executed or rejected and reported to BFIU as STR/SAR. All three levels, their roles and responsibilities, escalation, review and disambiguation systems have been described below:

C.3.6.3.1 Level 1

Level 1 generally includes the transaction processors, i.e. maker, checker, authorizer, reviewer, verifier, designated officials.

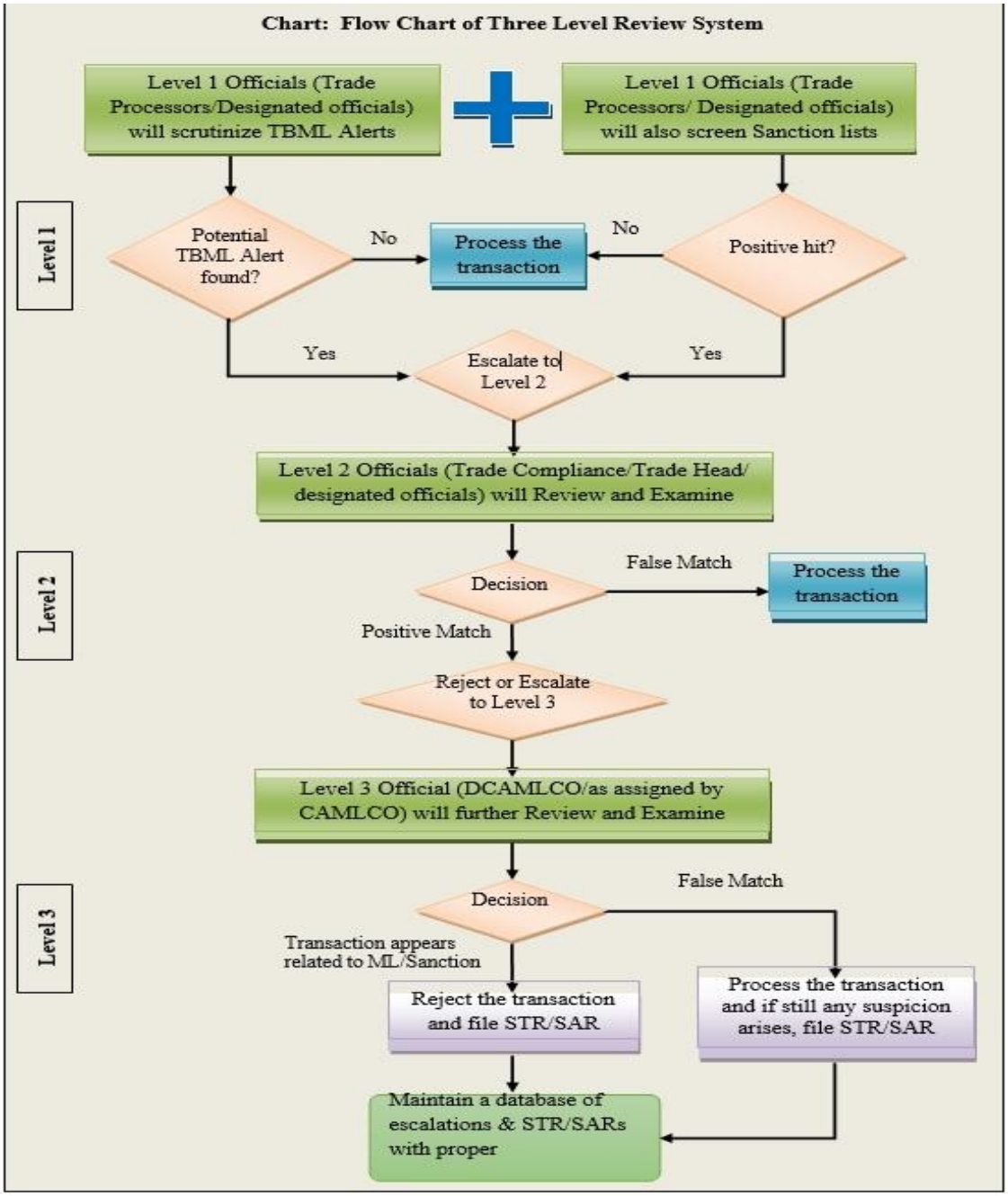
Roles and Responsibilities at Level 1

i. Ensure that the customer has a current, approved KYC record and TTP in place before processing transactions.
ii. Perform TBML Alert analysis and Sanction screening and execute transaction.
iii. Escalate TBML Alerts/Potential hits of the transactions to Level 2, whererequired.
iv. Escalate Suspicious Transactions/Activities to Level 2.
v. Keep record properly.

Level 1 Review, Disposition and Escalation Guidance

Every trade transaction should undergo TBML Alerts analysis and sanction screening. Initial TBML Alert analysis and screening should be completed at Level 1. The required elements of TBML Alert analysis and screening are set forth as below.

Maker or processor will review the transactions and identify relevant ML, TF, Sanction and TBML Alert and raise them to checker, reviewer, verifier, authorizer or designated officials who will further review the transactions and TBML Alerts. When needed, reviewer will examine through different channels i.e internet, telephone, email etc. to get more information related to the transaction for the disposition of those TBML Alerts with proper rationales and the mitigating factors. This TBML Alert analysis represents the minimum amount of due diligence required for each trade transaction before it may be executed. In addition, Level 1 officials should use their expertise and experience to evaluate each transaction on its merits and escalate any potential concerns to Level 2. If checker, authorizer**,** or designated officials cannot disambiguate or resolve the TBML Alert at level 1, he/she will escalate those TBML Alerts to Level 2. Level 1 disposition should be documented for periodic review.



Source: Guidelines for Prevention of Trade Based Money Laundering, 2019

Illustration 1:

Subject: AML concern ref. 123abc…., Applicant or Buyer: XYZ, Singapore, Consignee: PQR, Columbia, Goods shipped to: Columbia, Beneficiary: ABC Co. Ltd, Bangladesh, Applicant Bank: ABC Bank Ltd, Singapore, Value: USD 50,000.00 Goods: Handicrafts

This is an Export Bill in which the goods, "Handicrafts" is being shipped to Columbia.

The following TBML Alerts are identified:

1. Buyer is from Singapore; goods are consigned and shipped to Columbia.
2. High Risk Country: Columbia. (as referred to in *www.fatfgafi.org/countries/#high- risk*, for high-risk countries)
3. High Risk Goods: Handicrafts.

Resolution by Level-1:

1. Ok to process since Goods are shipped as per export contract.
2. Ok to process since Buyer has an agent in Columbia to sell the goods.
3. Ok to process since Bangladeshi exporter's line of business is to export handicrafts.

Illustration 2: From: Level 1 to: Level 2

Subject: AML concern ref. 123abc…., Applicant: XYZ Trading Co., Lagos, Nigeria, Beneficiary: ABC Co. Ltd, Bangladesh; Issuing Bank: ABC Bank Ltd, Nigeria, Value: USD 50,000.00

This is an export LC in which goods, "Sugarcane" is being shipped to Nigeria.

The followings are the TBML Alerts observed:

a. Goods are inconsistent with beneficiary's business line.

b. Port of loading not provided in the LC.

c. Price per unit of the sugarcane appears to be high.

d. High risk country: Nigeria.

After getting resolution/decision from Level 2, Level 1 will act accordingly.

C.3.6.3.2 Level 2

Level 2 generally includes officials with adequate expertise able to further analyze the merits of an escalation from Level 1 processor and the relevant suspicion itself. They are likely to require

extensive knowledge of trade-based money laundering risk and make appropriate use of third-party data sources[11] to verify key information. Level 2 officials may be trade compliance officer/Head of trade or designated officials. In any case, they should have adequate seniority and skill to conduct the role of level 2.

Roles and Responsibilities at Level 2

i. Review and examine the TBML Alerts raised by level 1.

ii. Review TTP on certain Alerts.

iii. Disambiguate with proper rationale and justification.

iv. Document properly.

Level 2 Review, Disposition and Escalation Guidance

All transactions that contain potential TBML Alerts and sanction hits and that cannot be resolved by Level1 processor should be escalated to Level 2.

Level 2 shall deeply analyze the alerts escalated to them and determine their merit. If they can easily resolve them with adequate justification they shall do so with documents and instruct Level 1 to allow the transaction, otherwise escalate to Level 3. However, if TBML risk appears very low to Level 2, yet for certain reasons they cannot resolve TBML Alerts, they may allow transactions escalating the Alert(s) to Level 3. If, after the transaction Level 3 finds the transaction suspicious, STR shall be submitted.

Illustration 1: From: Level 1 to: Level 2

Subject: AML concern ref. 123abc…., Applicant: XYZ Trading Co., Lagos, Nigeria, Beneficiary: ABC Co. Ltd, Bangladesh, Issuing Bank: ABC Bank Ltd in Nigeria, Value: USD 50,000.00

This is an export LC in which the goods, "Sugarcane" is being shipped to Nigeria.The following are the TBML Alerts observed:

a. Goods are inconsistent with beneficiary's business line.
b. Port of loading is not provided in the LC.
c. Price per unit of the Sugarcane appears to be high.
d. High risk country: Nigeria.

Resolution by Level 2:

a. D&B search on the beneficiary confirms that it is involved in the export and import of sugarcane and sugar products.
b. The amendment received from the issuing bank confirmed that the port of loading is Chattogram, Bangladesh.

c. Unit price provided is consistent with the current market price available online.
d. High risk country: Nigeria

Since applicant is registered in Nigeria and shipment is also made to Nigeria, it is ok to process the transaction. Level 2 shall instruct Level 1 to conduct the transaction.

Illustration 2:

Subject*: AML concern ref. 123abc…., against an import LC for importing 10 (ten) 1500cc Toyota Cars. Applicant: XYZ Automobile Co., Bangladesh, Beneficiary: ABC Co. Ltd, in Hong Kong. Issuing Bank: XY Bank Ltd, Value: USD 60,000.00*

While scrutinizing the documents TBML Alerts mentioned below have been identified by Level1 processors and escalated to Level 2:

1. Current market price of these 10 cars are $100,000.00 whereas the invoice shows it as $60,000.00 (price variance identified is $40,000.00)
2. Applicant and beneficiary are related parties.
3. High risk product is involved.

Further analysis and escalation by Level 2 to Level 3:

Designated Level 2 officers have further scrutinized these TBML Alerts and they could not disambiguate these TBML Alerts. As such they further escalated to Level 3 stating same alerts as mentioned by Level 1.

After getting resolution/decision from Level 3 they will inform Level 1 accordingly.

C.3.6.3.3 Level 3

Level 3 generally includes officials with vast experience and expertise on trade based money laundering process. Level 3 should be able to further assess the merits of an escalation from Level 2 officials. Level 3 generally includes DCAMLCO/officials as assigned by CAMLCO.

Roles and Responsibilities at Level 3

i. Conduct comprehensive review and examine the TBML Alerts raised by Level 2.
ii. Consult TTP if necessary.
iii. Disambiguate with proper rationale and justification.
iv. File STR/SAR where required.
v. Document properly.

Level 3 Review and Disposition Guidance

Level 3 shall complete a comprehensive review and determine if there are facts that reasonably mitigate the TBML Alerts associated with the transaction or if the transaction appears to be suspicious. If Level 3 identifies facts that reasonably mitigate each of the TBML Alerts associated with the transaction, then Level 3 shall explain and document the mitigating factors for each alert and allow the transaction to proceed.

If the TBML Alerts are not resolved and the activity or transaction remains suspicious, then Level 3 shall prepare a Suspicious Activity/Transaction Report.

Level 3 shall determine whether the activity or transaction in question should be permitted or rejected and whether the activity or transaction warrants a Suspicious Activity Report. If Level 3 is apparently satisfied with the available information, he/she may approve the transaction with a remark for further scrutiny or more information for complete satisfaction on post facto basis. Before submission of STR/SAR to BFIU, CAMLCO shall ensure compliance with due procedure, required data and documents in line with the instructions given in relevant BFIU circular.

All Level 2 and Level 3 escalation dispositions of TBML Alerts or screening hits should be properly documented.

Illustration 1:

Subject*: AML concern ref. 123abc….,against an import LC for importing 10 (ten) 1500cc Toyota Cars. Applicant: XYZ Automobile Co., Bangladesh, Beneficiary: ABC Co. Ltd, in Hong Kong. Issuing Bank: XY Bank Ltd, Value: USD 60,000.00*

While scrutinizing the documents, TBML Alerts mentioned below are identified by Level 1 processors and escalated` to Level 2:

1. Current market price of these 10 cars are $100,000.00 whereas the invoice shows it as $60,000.00 (price variance identified is $40,000.00)
2. Applicant and beneficiary are related parties.
3. High risk product is involved.

Further Examination and escalation by Level 2 to Level 3:

Designated Level 2 officers have further examined these TBML Alerts and they could not disambiguate these alerts. As such they further escalated to Level 3 with same rationales:

Level 3 designated official also examined the TBML Alerts and found that the alerts are valid and rejected the transaction with rationale given below:

- Under-invoicing is attempted through this LC application since the invoice price is quoted much below the fair or competitive market price. So, it is recommended to reject the transaction.

- Level 3 official filed an STR against this money laundering attempt by the importer in Bangladesh.

Illustration 2:

***Subject**: ML/TF concern ref. 123abc….,against an inward remittance to be processed as advance receipt against export through Advance Receipt Voucher (ARV) at the request of exporter ABC Co. Ltd, in Bangladesh. For Value: USD 15,000.00 buyer, XYZ Co. in China.*

TBML Alerts identified and escalated from Level 1 to Level 2 are described below:

1. Swift message does not mention purpose and there is no reference in the message toconnect this remittance with the advance payment. Only customer's instruction mentions that this is advance receipt for export.
2. The bonafides of buyer is not ensured.
3. Shipment date is unusually longer i.e 9 (nine) months, whereas goods are ready made garments that need maximum 4 months for shipment.
4. This exporter has also received more advance payments earlier against whichshipment has not yet been made.

Further examination and escalation by Level 2 to Level 3:

Designated Level 2 officers have reviewed these TBML Alerts and they further escalatedthese alerts to Level 3 with the same rationales as stated by Level 1 officials. Level 3 designated official also reviewed and examined the TBML Alerts and disambiguatedthese alerts with the rationales below:

1. Though swift message does not mention the purpose or reference, buyer is mentioned as same. Moreover, export contract shows the payment term as advance payment. Besides, exporter has declared the purpose as advance payment against export in the request letter. He also submitted the ARV and copy of the contract against this transaction.
2. Further examination shows that buyer is a trading company who also trades ready- made garments.
3. Some shipments may take longer period.

It is ok to go ahead with this transaction as the exporter has track record of shipment default after receiving advance payment. In this case advance payment of the customer should be released. However, if shipment is not done after reasonable time period and bank is not satisfied, bank should report to regulators. The sample review process as described above is not intended to be prescriptive. Banks should tailor their own review process to their particular needs.

C.3.6.4 Screening System

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

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

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

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

5) A combination of automated and manual controls will be relevant in the context of AML and counter-terrorist financing (CTF) efforts. Typically, the following elements are, but not limited to, checked via automated /manual procedure:
    i. Unit prices
    ii. Number of items shipped
    iii. Shipping marks
    iv. Trade term – often an Incoterms rule followed by a place
    v. Commercial contract
    vi. The documentary credit applications
    vii. The guarantee applications
    viii. The documents presented under import documentary credits
    ix. The documents presented under export documentary credits
    x. The documents presented under import documentary collections
    xi. The documents presented under export documentary collections
    xii. Guarantee demands

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

C.3.6.5 Price Verification

Banks should develop their own database and frame clear policies and procedures to guide trade processing staff in performing price checks. The policies should, at a minimum, mention the level of acceptable price variance and escalation procedures when significant price difference is identified. Provision of different threshold for different types of underlyinggoods and services may be allowed on the basis of periodic market price assessment. To enhance the effectiveness of the price checks, the process may be centralized or automated; otherwise care should be taken to ensure avoidance of any conflict of interest.

C.3.6.6 TBML Alerts

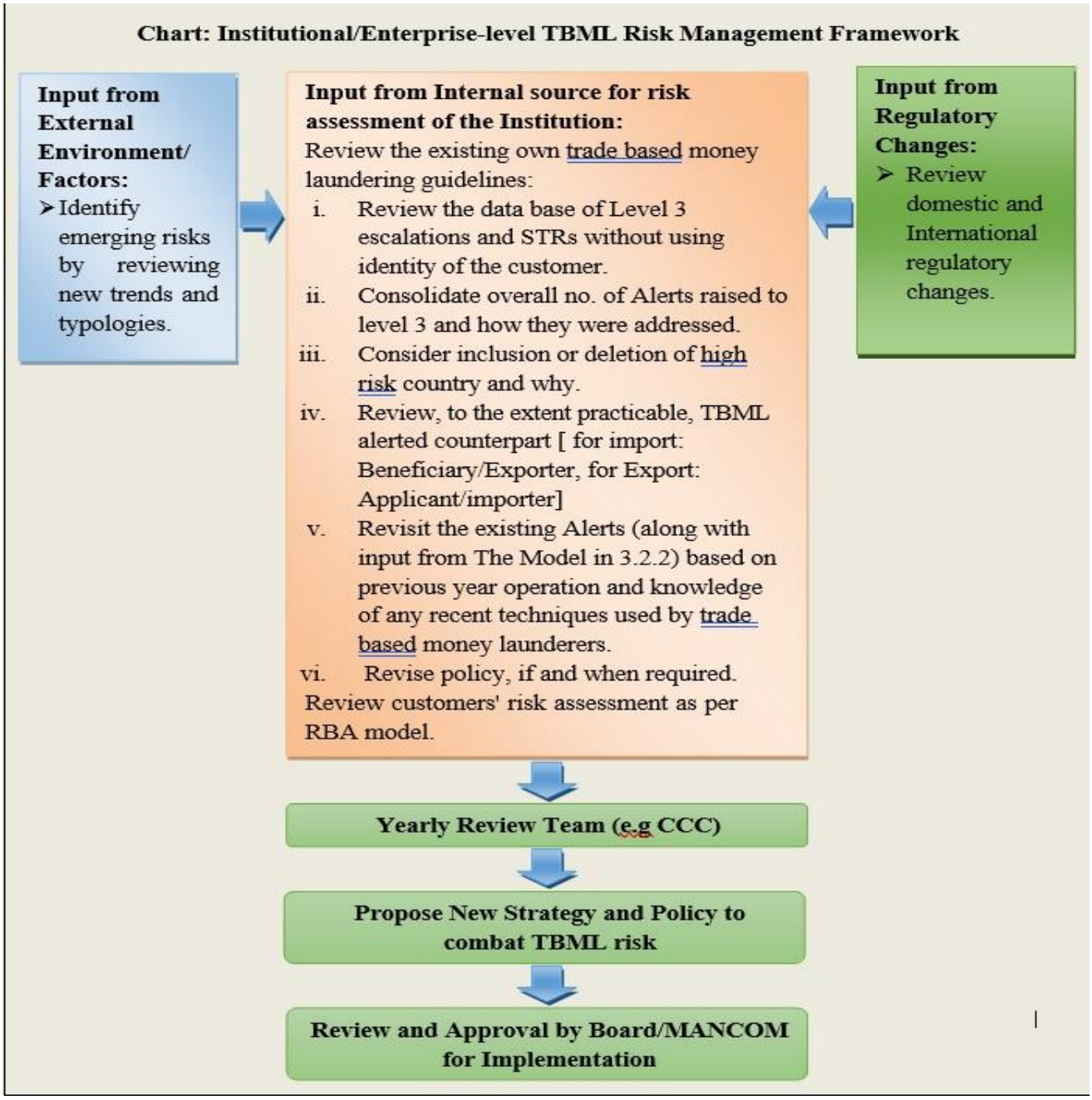
KYC process is the foundation on which the individual transaction should be evaluated/ examined for TBML Alerts. However, compliance checks carried out on the trade finance transactions are, to a large degree, Manual. This requires a structured risk-based approach to identify, escalate and examine unusual/suspicious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

C.3.7 Enterprise/Institute Wide TBML Risk Assessment and Mitigation

i. Ensure Enterprise wide TBML risk assessment.
ii. Review Policy Strategy depending on TBML risk assessment.
iii. Take into account gaps found through annual review as shown in 3.2.4.1
iv. Review new trend and typology related to TBML and include relevant ones forguidance.
v. Revisit TBML Alerts to mitigate the risks.

C.3.7.1 Enterprise/ Institutional Level Risk Management of Trade Based Money Laundering Framework

As an enterprise Bank shall assess its TBML risk exposure using holistic approach. In assessing enterprise level risk assessment, it shall obtain and use input from internal source, external sources and from review of international regulatory changes. The following diagram is a sample how, on the basis of assessment, institutional/enterprise- level risk management of trade-based money laundering and terrorist financing may work in abank:



Source: Guidelines for Prevention of Trade Based Money Laundering, 2019

C.3.7.2 Suspicious Transaction/Activity Reporting

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

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

C.4 FATF Blacklist and Gray List

The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents containing black list and grey list jurisdictions that are issued three times a year. As of June 2023, the FATF has reviewed over 125 countries and jurisdictions and publicly identified 98 of them. Of these 98, 72 have since made the necessary reforms to address their AML/CFT weaknesses and have been removed from the process.

C.4.1 High-Risk Jurisdictions subject to a Call for Action (i.e. "black list")

High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. This list is often externally referred to as the “black list”. Currently (as of 19 August 2023) the following jurisdictions are on the black list

1. *Democratic People's Republic of Korea (DPRK)* [unchanged since February 2020]
2. *Iran* [unchanged since February 2020]
3. *Myanmar*

C.4.2 Jurisdictions under Increased Monitoring (i.e. "grey list")

When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. **This list is often externally referred to as the *grey list*.** Jurisdictions under increased monitoring actively work with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring.

Countries that are on the grey list of FATF are Albania, Barbados, Burkina Faso, Cayman Islands, Democratic Republic of Congo, Gibraltar, Jamaica, Jordan, Mali, Mozambique, Panama, Philippines, Senegal, South Africa, South Sudan, Türkiye, UAE, and Uganda, Haiti, Nigeria, Syria, Tanzania and Yemen, Cameroon, Croatia and Vietnam.

Case and Sample Question:

Case: Mr. Alam is the Managing Director and his wife Mrs. Sultana is the Director of P Ceramics Ltd. P Ceramics Ltd. opened LC to import capital machinery valued USD 0.337 million from N Export Ltd & HK Group Ltd. H.S. Later it was found that Mr. Alam and Mrs Sultana are also hold 100 % and 50% share of N Export Ltd in China and HK Group Ltd. in Hong Kong respectively. On the other hand the HS code of the product mentioned in Commercial Invoice is found to be totally different from that of H.S. Code mentioned in the Bill of Entry. Even the price of the products appeared to be much higher even compare to price shown in Alibaba.com in 2023.

Sample Question:

1) What is risk assessment? How an AML/CFT risk management of a bank should be?
2) How a bank can assess and calculate the risk associated with product and service? Explain with example.
3) What is risk matrix and risk score? How a financial institution should treat risk? Write down some risk management strategies that a bank can take.
4) Write down the probable measure that a bank can take in higher risk scenario.
5) What are the Key Challenges and Difficulties in Preventing Trade Based Money Laundering in Bangladesh?
6) Discuss briefly about the trade based money laundering risk assessment and mitigation mechanism in a bank.
7) How a bank may assess the TBML risk associated with customer?
8) Write down the roles and responsibilities of bank during Transaction Level TBML Risk Assessment & Mitigation through 3 Level Review System.
9) What is vessel tracking? How a bank can mitigate risk of TBML through sanction screening?

Module D: Prevention, Detection and Reporting

D. 1 Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

D.1.1 Obligations under MLPA, 2012

The reporting organizations shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to Bangladesh Financial Intelligence Unit (BFIU).

D.1.2 Obligations under MLP Rules, 2019

The Bank shall identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data). The verification of identity of a customer or a beneficial owner should include a series of independent checks and inquiries and not rely only on documents provided by the customer or beneficial owner. The Bank shall verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person.

The Bank shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the Bank is satisfied that it knows who the beneficial owner is.

The Bank shall understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship. The Bank shall also conduct ongoing due diligence on the business relationship.

The Bank shall scrutinize the transactions undertaken by a customer throughout the relationship with the customer to ensure that the transactions are consistent with the nature, business and risk profile of the customer, including where necessary, with the source of funds.

D.1.3 Who are Customers:

In the money laundering and terrorist financing risk management, 'Customer' shall mean the following individual or entity:

1) Any individual or entity maintaining account or having business relationship with the bank;
2) Beneficial Owner of bank account or business relationship (for whom account is being operated directly or indirectly. This subject matter is elaborately discussed in Guidelines on Beneficial Ownership.);
3) Any professional intermediary (Lawyer, Legal Consultancy Firm, Chartered Accountant etc.), appointed to operate the account of any account holder, Trust or beneficial owner, within the existing legal framework;

4) Any individual or entity making high valued occasional transaction by a single transaction or any individual or entity related to a financial transaction that can cause reputational and any other risk to the organization (here high value transaction is defined as such transaction which seems to be unusual to the profession/profile of the relevant individual or entity); and
5) Any individual or entity defined by BFIU from time to time.

D.1.3.1 Know Your Customer (KYC)

In money laundering and terrorist financing risk management, the compliance of the following points shall have to be assured in obtaining and verifying customer's identity:

1) To open account of the customer, the prescribed account opening form issued by Banking Regulation and Policy Department (BRPD) of Bangladesh Bank has to be used. However, considering the convenience of applying modern technology, when necessary, the direction in this regard described in `*Guidelines on Electronic Know Your Customer (e-KYC)*' issued by BFIU should be taken into consideration. Hard copy of account opening form can be used if any inconvenience arises to open account using electronic system;

2) Complete and accurate information regarding customer's identification needs to be collected. Each bank should have thorough understanding of the purpose for account opening by the customer and need to verify the information or data related to customer identification in order to ensure that the banking channel might not be prone to the risk of money laundering and terrorist financing. To obtain or preserve such complete and accurate information, complete refers to the combination of all necessary information for verifying identification of the applicant or account holder and on the other hand, accurate refers to such complete information that's accuracy has been verified from reliable and independent sources.

3) If any other individual operates the account on behalf of a customer then, complete and accurate information of that individual need to be collected after being confirmed that the said individual is appropriately authorized.

4) In case of the account operated by Trustee and Professional intermediaries on behalf of a customer, complete and accurate information of everyone related to such intermediaries have to be collected after reviewing their legal status and determining its appropriateness; and

5) In the event of providing banking service to any Walk-in Customer (i.e– DD, TT, MT, Pay Order or online transaction etc.) directives mentioned in different paragraphs of this circular

need to be followed. In this regard, Walk-in-Customer refers to non-accountholder of the bank.

D.1.4 Customer Due Diligence-CDD:

Customer Due Diligence or CDD means ensuring customer (individual or entity) identity based on information, data and documents received from reliable and independent source, regular monitoring of the said information or data and transaction along with verifying the accuracy of the collected information or data and source of fund. It is to be noted that, obtaining customer information (KYC) properly and verifying these, is a part of CDD measures.

D.1.4.1Timing of CDD

Bank must apply CDD measures when it does any of the following:

- While establishing business relationships;
- While dealing with occasional/ walk-in customers
- While carrying out an occasional transaction;
- While suspecting money laundering or terrorist financing;
- While suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification;
- While allowing mandate and/ or hold mail facilities to customers;
- While re-activating of Dormant/ Inoperative Accounts;
- In other situations, /scenarios i.e. if there is any suspicion of money laundering/Terrorist financing activities or if there is any doubt about the veracity or adequacy of customer's profile.

D.1.5 List of Customers Forbidden to Open Account with:

- Proscribed Individuals, Groups and Entities declared/ listed by UNSCR (United Nations Security Council Resolutions) and/ or by Bangladesh Domestic Sanction List or those who are known for their association with such entities and persons, whether under the proscribed name or with a different name;
- Accounts in Anonymous or / Fictitious Name/Numbered accounts; Accounts in the Name of/ for Shell Banks/ Companies;
- Accounts of Government/ Semi Government/ Autonomous Body in personal/individual names;
- Accounts of NGO, NPO, Trusts, Co-operative Societies, Charities or like Customers in personal/ individual names;

- Accounts, where there are reasonable doubt or suspicion arises for the veracity of customer`s profile, or for the beneficial ownership of the account or for any Money Laundering / Terrorist Financing Activity (ies);
- Accounts, where customer does not provide the required information/ documents in relation to Bank`s mandatory CDD/ EDD measures; and/ or Bank is not satisfied with credentials of customers in terms of AML/CFT regime.

D.1.6 Politically Exposed Persons (PEPS) & Influential Persons (IPS)

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

 Foreign PEPs;

 Domestic PEPs (known as Influential Persons: IPs in Bangladesh) and

 Chief or similar high-ranking positions in an international organization.

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

D.1.6.1 Politically Exposed Persons (PEPs)

PEPs refer to "Individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials." AML & CFT Division should preserve data of such accounts at their end.

The following individuals of other foreign countries must always be classed as PEPs:

i. Heads and deputy heads of state or government;
ii. Senior members of ruling party;
iii. Ministers, deputy ministers and assistant ministers;
iv. Members of parliament and/or national legislatures;

v. Members of the governing bodies of major political parties;
vi. Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
vii. Heads of the armed forces, other high-ranking members of the armed forces and heads of the intelligence services;
viii. Heads of state-owned enterprises.

D.1.6.2 Influential Persons (IPs)

'Influential persons' refer to, "Individuals who are or have been entrusted with prominent public functions in Bangladesh, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials." **AML & CFT Division** should preserve the list of accounts, approval records as well as monitor the transactions at their end.

The following individuals must always be classed as Influential persons:

- Heads and deputy heads of state or government;
- Senior members of ruling party;
- Ministers, state ministers and deputy ministers;
- Members of parliament and/or national legislatures;
- Members of the governing bodies of major political parties;
- Secretary, Additional secretary, joint secretary in the ministries;
- Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Governors, deputy governors, executive directors and general managers of central Bank;
- Heads of the armed forces, other high-ranking members of the armed forces and heads of the intelligence services;
- Heads of state-owned enterprises;
- Members of the governing bodies of local political parties;
- Ambassadors, chargés d'affaires or other senior diplomats;
- City mayors or heads of municipalities who exercise genuine political or economic power;
- Board members of state-owned enterprises of national political or economic importance.

D.1.6.3 Chief executive of any international organization or any top level official

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the boards or equivalent functions." The heads of international organizations and agencies that exercise genuine political or economic influence (e.g. the United Nations, the International Monetary Fund,

the World Bank, the World Trade Organization, The International Labor Organization) must always be classed as this category. AML & CFT Division should preserve the list of accounts, approval records as well as monitor the transactions at their end.

D.1.6.4 Close Associate of a PEP/IP

An individual who is known to have joint beneficial ownership or control of legal entities or legal arrangements, or any other close business relations with the PEP/IP; and an individual who has sole beneficial ownership or control of a legal entity or legal arrangement which is known to have been set up for the benefit of the PEP/IP.

In addition, it should include any person publicly or widely known to be a close business colleague of the PEP/IP, including personal advisors, consultants, lawyers, accountants, colleagues or the PEP's fellow shareholders and any person(s) that could potentially benefit significantly from close business associations with the PEP/IP. AML & CFT Division should preserve the list of accounts, approval records as well as monitor the transactions at their end.

D.1.6.5 Approval for PEP/IP Account Opening

Prior approval from CAMLCO is required for opening accounts of PEPs and IPs. These types of accounts can be treated as high risk accounts by default and therefore Enhanced Due Diligence (EDD) must be performed for opening and operating such accounts in relation to combat financing of terrorism.

Moreover, while opening account of close associate or family members of Politically Exposed Persons (PEPs defined by the BFIU Master circular 26 dated June 16, 2020, enhanced due diligence will have to be exercised. If the customer falls in such categories, then the account will automatically become a High Risk Account.

Following instructions will have to be followed to ensure Enhanced Due Diligence, while opening and operating the such accounts:

i. obtain senior management approval including concurrence from Chief Anti Money Laundering Compliance Officer (CAMLCO) for establishing business relationships with such customers;
ii. a risk management system will have to be introduced to identify risks associated with the opening and operating accounts of such customers;
iii. take reasonable measures to establish the source of wealth and source of funds;
iv. ongoing monitoring of the transactions have to be conducted; and
v. the Bank should observe all formalities as detailed in Policies for Foreign Exchange Transactions while opening accounts of nonresidents;

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

D.1.7 Bank's Policy on Dealing with Occasional/ Walk-In Customers

- Occasional or walk-in-customer means, "a person conducting occasional transactions and is not a customer having relationship with the Bank".
- Occasional transaction" or "walk-in-transaction" means a transaction carried by or on behalf of a person who is not a customer; having relationship with the Bank".
- While conducting transactions of such customers, branches should obtain copies of their Photo ID documents and/ or capture the information in the system, as per BFIU Policies and Bank's internal procedures.
- Any Transaction made by occasional/walk-in Customers above or equal to BDT 500000.00 shall be executed prior obtaining CDD measures.
- Transaction above BDT 50,000 but below BDT 500,000 shall be executed upon obtaining Valid photo ID of the applicant/sender/withdrawer/beneficiary and contact details such as Name, address, telephone number etc.
- Transaction upto BDT 50,000 shall be executed upon obtaining contact details such as Name, address, telephone number etc of the applicant/sender/withdrawer/beneficiary.

D.1.8 Management of Legacy Accounts

Legacy accounts refer those accounts opened prior to 30 April, 2002 and yet to update KYC procedures. These legacy accounts should be treated as "Dormant". No withdrawal should be permitted in those accounts; however, deposit can be permitted. These accounts will be fully functional only after conducting proper CDD measures. AML & CFT Division should preserve data of such accounts at their end.

D.1.9 Accounts/ Transactions where CDD measures are not completed

In case, where Bank is not able to satisfactorily complete the required CDD measures, account shall not be opened or service shall not be provided. Further, if CDD of any existing customer is found unsatisfactory, the relationship should be treated as high risk, and be reported as suspicious to AML & CFT Division for considering the filing of STR with BFIU, and/ or taking any other suitable action as per BFIU Circular No. 26.

D.1.10 Customer Identification

1. Customer identification is an essential element of KYC standards. For proper identification a customer includes the following:

- the person or entity that maintains an account with the Bank or those on whose behalf an account is maintained (i.e. beneficial owners);

- Any person or entity connected with a occasional transaction of single high value, single transaction Occasional transaction or who can pose significant reputational and other risks to the Bank.
- The customer as defined by BFIU.

2. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for the concerned officers to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if an officer becomes aware at any time that it lacks sufficient information about an existing customer, he should take steps to ensure that all relevant information are obtained as quickly as possible.

D.1.10.1 What Constitutes a Person's Identity

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

- the physical identity (e.g. name, date of birth, TIN/Passport/NID number/Birth certificate, etc.); and
- the activity undertaken.

2. 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/National sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issue should be recorded.

3. 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 description required will depend on the concerned officer's own understanding of the applicant's business.

4. When commencing a business relationship, concerned officers should consider recording the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. Documentation about the nature of the applicant's business should also cover the origin of funds to be used during the relationship. For example, funds may be transferred from a Bank or the applicant's employer, or be the proceeds of a matured insurance Policy, etc.

5. Once account relationship has been established, reasonable steps should be taken by the concerned officer to ensure that descriptive information is kept up to date as opportunities arise. It is important to emphasize that the customer identification process do 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.

D.1.10.2 Individual Customers (Natural Persons)

1. Where verification of identity is required, the following information should be obtained from all individual applicants for opening accounts or other relationships, and should be independently verified by the concerned officer himself/herself:

- true name and/or names used;
- parent's names;
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of wealth or income;

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

- provision of a recent utility bill, tax assessment or Bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- checking the NID;
- checking the telephone directory;
- record of home/office visit.

The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.

3. The date and place of birth are important as identifier in support of the name, and are helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard. It is also helpful for residence/nationality to be ascertained to assist risk assessment procedures and to ensure that the Bank does not breach UN or other international sanctions.

4. Identification of documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.: -

i) Current valid passport;

ii) National Identity Card;

iii) Birth Registration Certificate; (with a recent valid photo ID)

5. 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, 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 the concerned officer is unfamiliar, either because of origin, format or language, he must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. The concerned officers should also be aware of the authenticity of passports.

6. Where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID card where there is no face-to-face contact, then a certified true copy should be obtained.

7. There is obviously a wide range of documents which might be provided as evidence of identity. It is for each concerned officer to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

8. In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders, not only the first named, should normally be verified in accordance with the procedures set out above.

9. Any subsequent change to the customer's name, address, or employment details of which the concerned officer 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.

10. File copies of supporting evidence should be retained. Where this is not possible, the relevant details should be recorded on the applicant's file. In case of one-off transactions, the details should be recorded in a manner which allows cross reference to transaction records. Such institutions may find it convenient to record identification details on a separate form to be retained with copies of any supporting material obtained.

11. 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.

D.1.10.3 Persons without Standard Identification Documentation

Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the farmers, elderly, the disabled,

students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous anti-money laundering procedures is recommended. Internal procedures must allow for this, and must provide appropriate advice to the concerned officer on how identity can be confirmed in these exceptional circumstances. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

D.1.10.4 Joint Accounts

In case of joint accounts, complete separate KYC/ CDD Form for each of the account holders has to be filled up. Further, also carry out other CDD measures (as applicable) on all of the joint account holders, as if each of them is individual customer of the Bank.

D.1.10.5 Partnerships and Unincorporated Businesses

- In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the Bank, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandatee from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.
- Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable) should also be obtained.
- An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

D.1.10.6 Corporate Bodies and other Entities (Legal Persons)

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company’s assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a “brass plate company” where the controlling principals cannot be identified.

The following documents should normally be obtained from companies:

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

- Certified true 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 20% 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.

D.1.10.7 Accounts of NGO/ NPO/ Trust/ Society/ Club/ Association/ Charitable/ Religious Organizations:

- The account should be opened in the name of relevant NGO/NPO/Trust/ Society/ Club/ Association/ Charitable/ Religious Organizations (as the case may be), as per title given in the constituent documents of the entity.
- The individuals who are authorized to operate these accounts and members of their governing body/ Management Committee/ Board of Trustees should also be subject to EDD. Branches should ensure that these persons are not affiliated with any proscribed/ banned individual/ group/ entity, whether under the same name or different names.
- In case of advertisements through newspapers or any other media, especially when Bank account number is mentioned for donations, branches should ensure that the title of the account is the same as that of the entity soliciting/ asking for donations. In case of any difference, immediate caution should be marked on such accounts, and the matter should be escalated to Chief Compliance Officer & CAMLCO in order to consider the case for filing of STR and/or take other actions as per law.
- Personal accounts should not be allowed to be used for charity purposes/collection of donations.
- All existing relationships of NGOs/NPOs/Trust/ Society/ Club/ Association/ Charitable/ Religious Organizations should be reviewed and monitored to ensure that these organizations,

their authorized signatories, members of their governing body and the beneficial owners are not linked with any proscribed entities and persons, whether under the same name or a different name. In case of any positive match, branches should immediately report the same to CAMLCO & CCC for filing of STR and/or take other actions as per law.

- Besides above, following steps should be adopted while opening the accounts of NGOs, NPOs, Trusts/ Societies/ Clubs/ Associations/ Charitable/ Religious Organizations:
- Obtain Declaration from the Governing Body/ Board of Trustees/ Management Committee/ Sponsors on ultimate control, purpose and source of funds, etc.
- Obtain an undertaking from Governing Body/Board of Trustees/Management Committee /sponsors to inform the Bank about any change in control or ownership of entity during operation of the account
- Obtain a Resolution of the Governing Body/ Board of Trustees/ Management Committee of the entity for opening & operating the Account
- Obtain a fresh Resolution of the Governing Body/ Board of Trustees/ Management Committee of the entity in case of change in person(s) authorized to operate the account
- To ascertain the physical existence of entity, branches should conduct the physical verifications of the same, and document the results thereof by attaching a visit report with Account Opening Documents.
- Complete the prescribed EDD Form of the account properly & attach the same with Account Opening Documents.
- Obtain concurrence from the CAMLCO to open the account. Before approving such accounts, Respective Branch should:
    - Review all the required documents to ensure that the same are in line with Account Opening Documents checklist.
    - Seek legal opinion from Bank's Legal Department from legal perspectives.
    - Upon receipt of satisfactory response from the panel lawyer, obtain AML clearance from AML & CFT Division.

D.1.10.8 Government Account:

- Government account should not be opened in personal name of the government official.
- The government account, which is to be operated by an officer of government, should be opened only on production of especial resolution/ authority from the concerned administrative department duly endorsed by the Ministry of Finance Government.

- In case of Autonomous Entities and Armed Forces including their allied offices, account can be opened on the basis of especial resolution/ authority from the concerned administrative department or highest executive committee/management committee of that entity duly endorsed by their respective unit of finance.

D.1.10.9 Powers of Attorney / Mandates to Operate Accounts

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third-party mandates.

D.1.10.10 Dormant Accounts

- For dormant accounts, branches may allow credit/deposit entries without requiring activations. However, debit transactions/ withdrawals shall not be allowed until the account holder requests for activation and produces an attested copy of his/her NID, if already not available, and branch is satisfied with the KYC/ CDD profile of customer.

- However, in case of transactions e.g. debits under the recovery of loans and markup etc. any permissible Bank charges, government duties or levies and instruction issued under any law or from the court will not be subject to the debit or withdrawal restriction.

D.1.11 Timing and Duration of Verification

- The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed.
- However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority.
- This authority should not be delegated, and should 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 in itself suspicious.

D.1.11.1 Verification of Source of Funds

Branches should collect and verify the document supporting source of fund of the person at the time of establishing any business relationship or while conducting CDD. The document could include present employment identity, letter of introduction, salary certificate, pension book,

financial statement, income tax return, business document or any other document that could satisfy the Bank.

D.1.11.2 Verification of Address

Branches should verify the address of the person at the time of establishing any business relationship or while conducting CDD. This could be done through the physical verification by the Bank or by standard mail or courier service correspondence. The Bank could collect any other document (recent utility bill mentioning the name and address of the customer) up its satisfaction.

Verification of the information obtained must be based on reliable and independent sources – which might either be a document or documents produced by the customer, or electronically by the Bank, or by a combination of both. Where business is conducted face-to-face, branches should see originals of any documents involved in the verification.

D.1.11.3 Completeness and Accuracy

Bank is required to be certain about the customer's identity and underlying purpose of establishing relationship with the Bank, and should collect sufficient information up to its satisfaction. "Satisfaction of the Bank" means satisfaction of the appropriate authority that is necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

It is an obligation for the Bank to maintain complete and accurate information of its customer and person acting on behalf of a customer. **'Complete'** refers to combination of all information for verifying the identity of the person or entity. For example: name and detail address of the person, profession, source of funds, Passport/National Identity Card/Birth Registration Certificate/ acceptable ID card with photo, phone/ mobile number etc. **'Accurate'** refers to such complete information that has been verified for accuracy.

KYC procedures refer knowing a customer physically and financially. This means to conduct an effective KYC, it is essential to accumulate complete and accurate information about the prospective customer.

The verification procedures establishing the identity of a prospective customer should basically be the same whatever type of account or service is required. It would be best to obtain the identification documents from the prospective customer which is the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity, so verification will generally be a cumulative process. The overriding principle is that every Bank must know who their customers are, and have the necessary documentary evidences to verify this.

Where the Bank is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, unable to identify the beneficial owner taking reasonable measures, unable to obtain information on the purpose and intended nature of the

business relationship, BANK 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.

D.1.12 Ongoing CDD measures (Review and update)

Bank must take necessary measures to review and update the KYC of the customer after a certain interval. This procedure shall have to be conducted in **every five (5) years** in case of low risk customers. Furthermore, this procedure shall have to be conducted in **every year** in case of high risk customers. But, Banks should update the changes in any information on the KYC as soon as Bank gets to be informed. Moreover, BANK shall update KYC information anytime if there is any particular necessity realized. Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay.

D.1.13 CDD for Beneficial Owners

Bank should apply CDD obligations for the beneficial owners of the accounts before or during the course of establishing a business relationship or conducting occasional transactions. In doing so, Banks should put in place appropriate measures to indentify beneficial owner. Banks, upon its own satisfaction ensure CDD of beneficial ownership by collecting information and documents from independent and reliable sources that includes publicly available information, information from customer or information from other reliable sources. Banks should consider following aspects while identifying beneficial ownership includes: Beneficial owner refers to the natural person(s) who ultimately owns, controls or influences a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

Note: It is required to conduct CDD of settler, trustee, protector or any person with similar status or any beneficiary or class of beneficiaries who have hold effective control on trust, in case of identification of beneficial ownership of a legal arrangement.

- Any natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted;
- Any person (whether acting alone or together) who has controlling interest or ownership interest on a customer who might be legal entity or legal arrangements. Where there is any doubt identifying controlling interest, the Banks should consider other means to determine controlling interest or ownership of a legal entity or arrangements. In addition to that, Bank should also consider reasonable measures to verify the identity of the relevant natural persons who hold any senior management position;

- Any person or entity who has controlling or 20% or above share holding within any legal entity.
- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercises control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) should consider for other types of legal arrangements.

Where, a natural or legal persons who holds controlling interest, listed on a stock exchange and subjects to disclosure requirements or majority owned subsidiaries of such listed companies may exempted from identifying or verifying beneficial ownership requirements.

D.1.14 Simplified Customer Due Diligence:

Bank may take easier watchful measures for "Low Risk" accounts that opened for "Financial Inclusion (student account, farmers account)" & other "No Frill Account" purpose**.**

D.1.15 Enhanced Due Diligence measures

Bank must conduct Enhanced CDD measures, when necessary, in addition to normal CDD measures. Bank must conduct Enhanced Due Diligence (EDD) under the following circumstances:

1 Individuals or legal entities scored with high risk;

2 Individuals who are identified as politically exposed persons (PEPs), influential persons (IPs) and chief executives or top-level officials of any international organization;

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

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

Enhanced DD measures includes-

- Obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet etc.) and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the purpose of the account, source of funds or source of wealth of the customer.

- In applicable ground, obtaining concurrence from CAMLCO
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship when applicable.
- Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- Making aware the concerned Bank officials about the risk level of the customer.

D.1.16 Walk-In/ One off Customers

Banks must collect complete and correct information while serving Walk-in customer, i.e. a customer without having account. Banks should know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT.

Banks have to collect complete and accurate information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposits, Banks should identify sources of funds as well.

While establishing transaction up to Tk. 50,000/- by the "Walk-in Customer", Bank must collect applicant/sender and beneficial/ receiver name & address along with applicant/sender's telephone number.

While establishing transaction above Tk. 50,000/- but below Tk. 500,000/-, Bank must collect applicant/sender/ depositor/ withdrawer photo ID with name & address**,** telephone number.

While establishing transaction of Tk. 500,000/ or more "occasional transactions" including wire transfer by walk in customer, the Branch must prepare full KYC.

D.1.17 Non Face-to-Face Customers

Bank should assess money laundering and terrorist financing risks while providing service to non face to face customers and shall develop the Policy and techniques to mitigate the risks, as well as will review that time to time. 'Non face to face customer' refers to "the customer who opens and operates his account by agent of the Bank or by his own professional representative without having physical presence at the Bank branch".

D.1.18 Non-Completion of CDD/EDD:

1. In case of non completion of CDD due to either non cooperation/unwillingness of the customer or if the collected information/documents are not dependable, i.e., if the identity cannot be verified to complete CDD, the Bank shall take the following actions:
    a) Bank shall not open account of such customer and shall close such existing account, if needed.

b) Closure of such existing account requires prior approval from higher management and prior notice to the customer explaining reasons for closing of such account(s).
c) Branch will submit such accounts report to AML & CFT DIVISION on a monthly basis
d) Suspicious Activity Report may be submitted for such customers.

D.1.19 CDD Measures For PEP's/IPs/Chief Executives or top Level Officials of any International Organization

The Bank needs to identify whether any of their customer is a PEPs/IPs/ Chief Executives or top Level Officials of any International Organization. Once identified the Bank needs to apply enhanced CDD measures. Moreover, they need to perform the following-

(a) The Bank has adopted the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a PEP;
(b) obtain senior managements' approval and concurrence from CAMLCO before establishing such business relationship;
(c) take reasonable measures to establish the source of fund of a PEP's account;
(d) monitor their transactions in a regular basis; and
(e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Financial Intelligence Unit (BFIU) under this act have to be complied accordingly

D.1.20 CDD Measures for Close Family Members and Close Associates of PEPs

Bank need to identify whether any of their customer is a family member or close associates of a PEP, IP or CEO or top level officials of any international organization. Once identified Banks need to apply enhanced CDD measures. Moreover, they need to perform the following-

(a) Bank has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a family member or close associates of a PEP, obtain senior managements' approval and concurrence from CAMLCO before establishing such business relationship;
(b) take reasonable measures to establish the source of fund of the account of a family member or close associates of a PEP
(c) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Financial Intelligence Unit (BFIU) under this act have to be complied accordingly.

D.1.21 Accounts for on boarding of NGOs, NPOs, Trusts, Charitable/ Religious / Entities

NGOs, NPOs, Trusts, Societies, Welfare/ Charitable/ Religious organizations/ Associations, etc. hold the peculiar nature of organizational structures/ control/ operational activities, due to which, these entities are always viewed as vulnerable to be used for money laundering / terrorist financing

(ML/TF) activities; and hence, the Banks in terms of BB directives/ industry best practices are required to be more careful/ vigilant and exercise exhaustive/ enhanced due diligence measures while dealing with such organizations/ associations.

D.1.22 Accounts of landlords/Property Owners

- Obtain appropriate proof of land holding e.g., Land revenue receipt, or any other acceptable land holding evidence/ verifiable information (as much as possible)
- In addition to above, obtain a self-declaration of customer for source & beneficial ownership of funds/ account duly approved by Branch Manager.
- Obtain additional information regarding the land holding records of customer, e.g. location, area, etc., (as much as possible).
- Further, if the account is classified as high risk, complete the prescribed EDD Form of the account.

D.1.23 Accounts of non-income generating persons (e.g. Housewife/ Student/Minor/ Widow)

- Obtain Self-declaration of customer for source and beneficial ownership of funds duly approved by Branch Manager.
- KYC of the funds providers, i.e., the beneficial owner-has to be completed.
- Further, if the account is classified as high risk, EDD may be prescribed.

D.1.23 Reviewing & updating of KYC Profiles

KYC document is a yardstick, which enables the Bank to have (the most likely) up-to-date information/ records of the customers. Know Your Customer (KYC) is not a onetime exercise; rather it is an ongoing process. Therefore, KYC of all business relations should be conducted, updated & revised on an on-going basis by considering the following:

- When & where warranted by the conduct of the account;
- As & when customer`s profile changes;
- On periodic basis as per internal Policies of the Bank as well as BFIU.

D.2 KYC & CDD for MFS customers

KYC, Transaction Monitoring, Reporting of STR & SAR, Monitoring of agents and distributors, NID Verification, and other issues of Mobile Financing Services Customers have to be ensured in the light of BFIU Master Circular- 20 and the subsequent circulars that will follow later on (related to MFS). Along with the full compliance of master circular no 20, the following issues need to be highly emphasized.

1. **KYC:** Mobile Banking Division will follow the instructions of BFIU Master Circular- 20 and the subsequent circular regarding this if any, to ensure proper KYC of the clients. New

uniform account opening form for individual customers has to be adopted as per instructions of BFIU.

2. **NID Verification:** Mobile Banking Division will continue NID verification for all new and existing clients through Bangladesh Election Commission portal.
3. **Update of Application Form:** Mobile Banking Division will update the My-Cash application form for Individual Customers in order to comply the requirements stated in the BFIU Master Circular- 20
4. **Implementation of any New Service or technology by Mobile Banking Division:**
5. In order to comply the requirements stated in the BFIU Master Circular- 20, Mobile Banking Division will inform the AML & CFT Division before the implementation of any new service or technology by MFS in order to verify the risk issues for that particular service or technology.
6. **Transaction Monitoring:** Mobile Banking Division must ensure Transaction Monitoring.

The nature of this monitoring will depend on the nature of the transactions. Possible areas to monitor could be:

- Transaction type and number of transactions
- Frequency and changes in amount
- Unusually large amounts
- Geographical origin/destination
- Changes in mobile numbers to transfer funds

D.3 KYC & CDD for Agent Banking Customers

Agent Banking means providing limited scale Banking and financial services to the underserved population through engaged agents under a valid agency agreement, rather than a teller/ cashier. It is the owner of an outlet who conducts Banking transactions on behalf of a Bank. Globally these retailers are being increasingly utilized as important distribution channels for financial inclusion. Bangladesh Bank has also decided to promote this complimentary channel to reach to the poor segment of the society as well as existing Bank customer with a range of financial services specially to geographically dispersed locations.

D.4 Transaction Monitoring Process

It is a regulatory obligation to pay special attention to all complex, unusually large Transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help the relevant authorities in inspection and investigation.

Branches are primarily responsible to monitor transactions carried out by customers. As a counter measure, AML & CFT Division of Bank also monitors customers' transactions. The following mechanisms should be followed to monitor customer's accounts/transactions

Bank will monitor the transactions to identify the "Structuring" according provision section 2(fa)(EI) of Money Laundering Prevention Act;2012. And also, Bank will follow the BFIU Circular no-26.

It is also applicable for both foreign currency transactions & electronic transfer.

At the time of monitoring Transaction, consider UNSCRs and the country that do not meet the international standards in combating Money laundering & Financing of terrorism or any mentionable limitation.

D.4.1 Transaction Monitoring by Branches

D.4.1.1 All Transaction Analysis Report

Large Transaction in the customer`s Accounts should be monitored on the basis of above system generated report by applying following threshold amounts; and further economic consideration/ justifications of the same should be duly enquired, properly recorded & retained at the respective branches.

Report 1: **Cash transaction report (CTR)** – Monthly: Cumulative deposit or withdrawal in a day in a single account of customer over BDT 10 lakh.

Report 2: **Transactions that Breached Customer's Profile:** All Transaction exceeding Transaction profile of the accounts declared by accountholder.

Report 3: **Exceptional Movement of Money Transfer:** All the high value Transactions i.e., transactions above BDT 5.00 Lakh that were in the form of account to account transfer, Clearing, BEFTN, RTGS shall be analyzed with the KYC, TP, Profession and sources of fund of the customer by the respective branches on daily basis and by the AML & CFT Division on monthly Basis.

D.4.1.2 What is to be considered while reviewing the reports?

While reviewing the transaction monitoring reports the reviewer should always keep in mind some checking parameters, exceptions of which may trigger suspicion and may need to make effort to look into the facts in details. Some checking parameters are as follows (not exhaustive):

- The transaction is not consistent with the declared profession/business of the customer
- The type of transaction is of not common/regular nature with the customer
- The transaction is showing unusual variation from the normal transaction pattern of the customer (comparing Statistical History of last one year.)

- The pattern suggests that the customer is structuring transaction to avoid reporting requirement (CTR).
- The geographic location where the transactions are taking place or from where these are being generated have no relevance to customer's business/profession.
- Frequent intercity transactions which are not relevant to the nature of the account. Remittance to various parties in different locations with whom no apparent business relationship is evident.
- Transactions seem suspicious having high activity and low balances in the account; or having large or rapid movements of funds.

Any deviation of the checking parameters might be considered intriguing and may require additional effort to look into details of the transaction(s). Reviewer may need to obtain justifiable explanation from the customer on such occasions as well.

D.4.1.3 What the reviewer should do

In the monitoring report the reviewer should ensure the following:

- The purpose of transaction should be mentioned as clearly as possible
- The reviewer should not use vague terms such as 'business', 'sales', "inward remittance' 'cash delivery', "collection", "ok", "called", "known to relationship officer/Branch, "media business" etc.
- The explanations should be meaningful and understandable to any reviewer/auditor
- Contact the customer (if required) to ascertain the actual reason.
- Check if the explanation provided by customer matches with the customer profile.

D.4.1.4 Remaining Vigilant on Transaction Monitoring

In addition to the exception reports based monitoring process, staffs of the Bank who have customer or account contact have a responsibility to be vigilant throughout the course of carrying out their duties, and to report any activity they may observe or become aware of that in their judgment, they deem to be potentially suspicious or inconsistent with their general knowledge of customer should report the same. One of the key areas where the Banks staffs should be especially vigilant is the point of transaction. Particular attention should be paid to cash, pay orders, Inter account fund transfer, Clearing cheque, inward remittances or collection activity, early client redemption or unexpected pre-payment of loan products. Branches are required to review the deviations/ breaches in customer`s Annual Account Turnover identified through system generated report (This report should be generated on monthly basis. Further to this effect, update/ revise KYC profiles of the same by obtaining and documenting the plausible justifications/ reasons thereof.

D.4.1.5 Back-end Monitoring by AML & CFT Division

AML & CFT Division shall analyze CTR and threshold based transactions to raise STR/SAR on behalf of Bank in additional diligence basis.

D.4.1.6 Adverse Media Report:

Branches/Centralized Operation of Account Opening shall go through the adverse news regarding individuals and entities in the daily Newspapers or in electronic Media and will check up the records of branches whether any mentioned persons/entities in the adverse media has been maintaining any account with our branches or not. If any such person/entity is found, it should be immediately reported to AML & CFT Division and branches shall also keep this news in a separate file with paper cutting/source. AML & CFT Division with co-operation of branch will investigate the issue and take necessary steps for the account. Even AML & CFT Division should also go through the adverse news and if found anything, this should be forwarded to all the branches.

D.4.2 Cash Transaction Report Procedure

Most of the Banks extracts CTR qualified transaction but every branch will review, analyze and preserve the monthly cash transaction report. If the branch does not have any such transaction, it should report it to the AML & CFT Division as 'There is no reportable CTR'. Simultaneously, branches need to identify whether there is any suspicious transaction reviewing the cash transactions. If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' to the AML & CFT Division. If no such transaction is identified, it needs to inform to the AML & CFT Division as 'No suspicious transaction has been found' while reporting the CTR. Besides, every branch needs to preserve its CTR analysis records in its own custody.

The AML & CFT Division needs to prepare the accumulated CTR received for its all branches. The AML & CFT Division must ensure the accuracy and timeliness while reporting to BFIU. Moreover it has to review all the cash transactions from the branches above the threshold and search for any suspicious transaction. If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' to the BFIU. AML & CFT Division has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR.

D.5 Detection and Reporting of Suspicious Transactions

D.5.1 Statutory Obligation for Reporting of Suspicious Transactions

As per section 25(1)(Gha) of the Money Laundering Prevention Act-2012 including amendments in 2015 obligates us to make a report to Bangladesh Financial Intelligence Unit (BFIU) where a suspicion arises that a money laundering offence has been or is being committed.

Once employees have reported their suspicions to the appropriate person in accordance with the proper internal reporting procedure, they have fully satisfied their statutory obligations.

D.5.2 Identification of STR/SAR

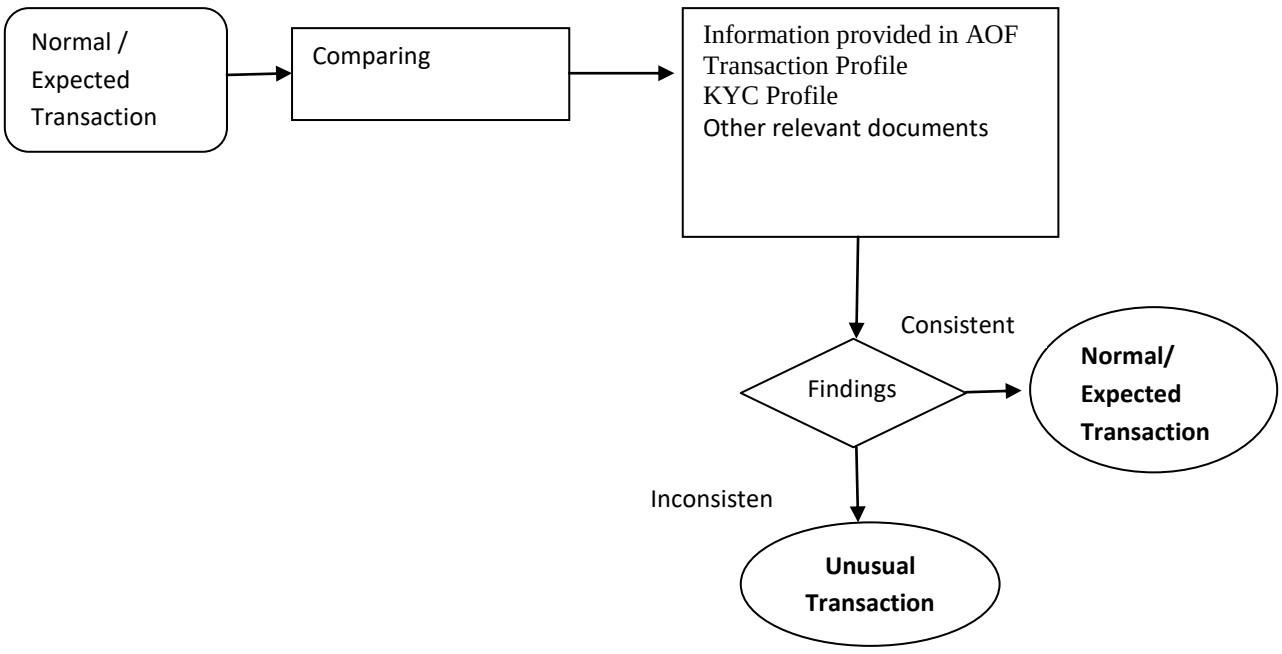
Identification of STR/SAR may be started identifying unusual transaction and activity. Such unusual transaction may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Generally the detection of something unusual may be sourced as follows:

- Comparing the KYC profile, if any inconsistency is found and there is no reasonable explanation;
- By monitoring customer transactions;
- By using red flag indicator.
- By analyzing the Non-performing loan & suit file accounts to identify any association with money laundering/Hundi/fake documents submitted by the customers/ fraud-forgery, if any.

A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

All suspicions reported to the AML & CFT Division shall be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rises to the suspicion. All internal enquiries made in relation to the report should also be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

The following chart shows the graphical presentation of identification of STR/SAR-



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

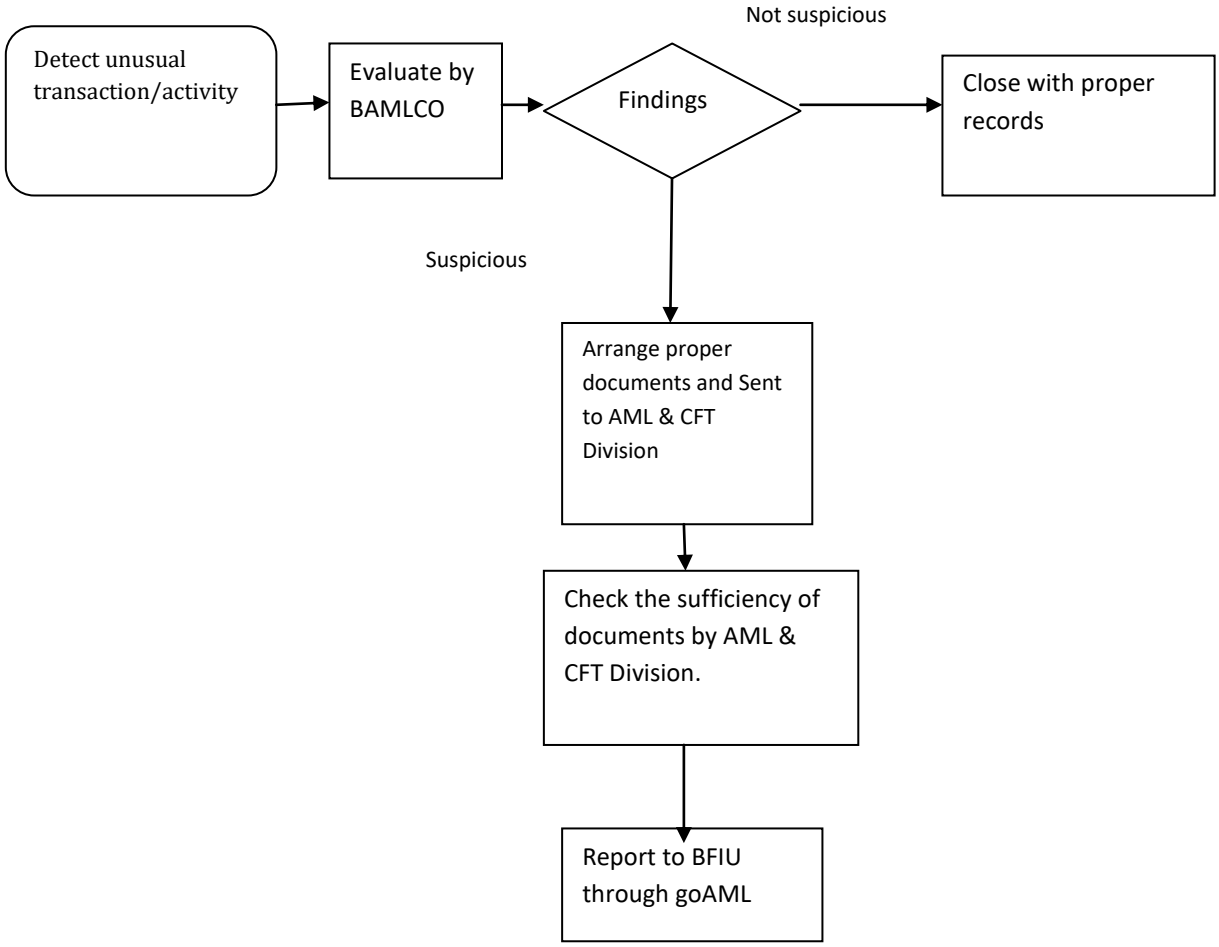
- **Identification:**

This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of Banks monitoring of unusual transactions may be automated, manually or both to detect unusual transactions or activities; Monitoring mechanisms should be more rigorous in high-risk areas of a Bank and supported by adequate information systems to alert management and other appropriate staffs of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should always be an ongoing activity.

- **Evaluation:**

This part must be in place at branch level and within AML & CFT Division. After identification of STR/SAR at branch level, BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. If BAMLCO is not satisfied, he should forward the report to AML & CFT Division Department. After receiving report from branch, AML & CFT Division should check the sufficiency of the required documents and checking whether it report previously or not. Every stages of evaluation (whether reported to BFIU or not), branch and AML & CFT Division should keep records with proper manner.

- **Disclosure:**



This is the final stage and Bank shall submit STRs/SARs to BFIU if it still looks suspicious.

D.6 AML & CFT Division's Obligations Regarding Self-Assessment and Independent Testing Procedure

Based on the received branch evaluation reports from the branches and submitted inspection/audit reports by the Internal Audit Department, the AML & CFT Division shall prepare a evaluation report on the inspected branches on a half yearly basis. In that report, the following topics, among others, must be included:

(a) Total number of branch and number of self assessment report received from the branches;

(b) The number of branches inspected/audited by the ICCD at the time of reporting and the status of the branches (branch wise score/rating);

(c) Same kinds of irregularities that have been seen in maximum number of branches according to the received self assessment report and measures taken by the AML & CFT Division to prevent those irregularities;

(d) The general and special irregularities mentioned in the report submitted by the ICCD and the measures taken by the AML & CFT Division to prevent those irregularities; and

(e) Measures to improve the ratings by ensuring the compliance activities of the branches that are rated as 'unsatisfactory' and 'marginal';

D.7 Record Keeping Procedure

D.7.1 Customer Information

In relation to the evidence of a customer's identity, Banks must keep a copy of or the references to, the evidence of the customer's identity obtained during the application of CDD measures. Where a Bank has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. A Bank may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. The date when the relationship with the customer ends is the date:

- an occasional transaction, or the last in a series of linked transactions, is carried out;
- the business relationship ended, i.e. the closing of the account or accounts.

D.7.2 Transactions

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the Bank's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed.

D.7.3 Internal and External Reports

Bank must make and retain:

- records of actions taken under the internal and external reporting requirements; and
- when the nominated officer has considered information or other material concerning possible money laundering but has not made a report to BFIU, a record of the other material that was considered.

In addition, copies of any STRs made to the BFIU should be retained in the branch and AML & CFT Division until further notice given by BFIU. Records of all internal and external reports should be retained for five years from the date the report was made.

Case and Sample Questions

Case: News was published that a member of parliament of Bangladesh, Mr. Haque was arrested with drugs by Malaysian Police. ABC Bank Ltd. found that Mr. Haque has been maintaining several accounts with the bank and so it lodged a Suspicious Activity Report (SAR) to BFIU. Another Bank, XYZ Bank Ltd found an account in the name of Mr. Khan where Mr. Haque is the nominee. But XYZ Bank Ltd did not take any action.

Sample Question

1) Who are customers? What KYC procedures need to take during on boarding a customer or providing banking service?
2) What is customer due diligence? Elaborate your answer with example. When a bank need to conduct customer due diligence?
3) What is PEPs and IPs? What measures should a bank need to take for business relationship with PEPs or IPs?
4) What is SDD? What CDD measures need to take for the following occasional transaction?
   (a) below 50.00 thousand,
   (b) above 50.00 thousand but below 5.00 lac BDT
   (a) above 5.00 lac BDT.

5) Who are beneficial owners? What measures a bank need to take if/when CDD cannot be performed?
6) What is Suspicious Transaction? Elaborate your answer in line with the definition provided in MLPA 2012 and ATA, 2009.
7) What is STR and SAR? How a bank can identify STR and SAR? Elaborate the process of identifying STR and SAR.
8) What is transaction monitoring? How transaction monitoring can help to identify STR?
9) What is CTR? Write down the procedure to submit CTR to BFIU? Why a bank should review the CTR?
10) What is self assessment and independent testing procedures (ITP)? Write down the roles and responsibilities of the branch, the AML/CFT division and the Internal Audit Department of a bank in carrying out self-assessment and ITP?

Module E: Sanctions, Anti-Bribery and Corruption

E.1 Sanctions

The UN Security Council imposes sanctions to maintain or restore international peace and security. The Office of Foreign Assets Control (OFAC), an agency of the United States Department of the Treasury, administers and enforces economic and trade sanctions against targeted countries, entities and individuals based on US foreign policy. There are also sanctions imposed by EU, UK, Australia etc. to attain country-specific objectives.

Sanctions are targeted multiple purposes, take different forms, and are generally regarded as an alternative to war. Sanctions commonly target addressing the challenges of terrorism, violation ofhuman rights, nuclear proliferation, destabilize regimes, military conflicts etc. Curtailing trades orforeign aids, restricting travels, freezing assets, and denying access to financial institutions are common activities executed as part of economic sanction measures. There are ample evidences thatthese sanctions produce significant economic impacts. Of the different sectors, financial and banking is the most vulnerable to risks associated with sanctions. In recent time, violation of sanctions (especially OFAC) resulted in serious financial and business losses for the financial companies.

UN sanctions lists are a crucial tool in maintaining international peace and security. These sanctions are diplomatic decisions enforced by the United Nations member states against states, entities, or individuals suspected of engaging in illegal activities that might harm national security interests, peace, and international law. For businesses, complying with UN regulations is essential to avoid legal measures and protect themselves from potential risks. In this article, we explore the different types of UN sanctions, countries on the UN financial sanctions list, and other sanctions lists such as the US Consolidated Sanctions List, OFAC Sanctions List, HM Treasury Sanctions List, and UK Sanctions etc.

E.1.1 Economic Sanctions

Economic sanctions are commercial and financial penalties applied by states or institutions against states, groups, or individuals. Economic sanctions are a form of coercion that attempts to get an actor to change its behavior through disruption in economic exchange. Sanctions can be intended to compel (an attempt to change an actor's behavior) or deterrence (an attempt to stop an actor from certain actions).

Sanctions can target an entire country or they can be more narrowly targeted at individuals or groups; this latter form of sanctions are sometimes called "smart sanctions" Prominent forms of

economic sanctions include trade barriers, asset freezes, travel bans, arms embargoes, and restrictions on financial transactions.

E.1.2 Various Types of Sanctions

Sanctions may be imposed by multilateral organization, regional organization or even by a single jurisdiction. Based on the imposer of sanction it can be three types, like-

- Multilateral Sanction i.e UN Sanctions
- Regional Sanction i.e EU Sanctions
- Unilateral Sanction i.e OFAC Sanctions

E.1.2.1 UN Sanctions

UN sanctions are a crucial tool used by the United Nations member states to maintain international peace and security. These sanctions are diplomatic decisions enforced against states, entities, or individuals suspected of engaging in illegal activities that might harm national security interests, peace, and international law. They are often used as a non-military approach to address threats to international peace and security, with the aim of encouraging the subject of the sanction to change their behavior or to constrain their ability to carry out harmful activities.

International sanctions typically involve the imposition of special restrictions on cultural, economic, trading, and diplomatic relationships with a particular country, designated individual, or organization. They may involve freezing assets, travel bans, and trade prohibitions on certain economic sectors, among other measures.

The impact of UN sanctions on businesses can be significant. It is essential for businesses to be aware of the sanctions in place and to detect whether their clients are subject to any sanctions. Failure to comply with AML regulations and to take the necessary steps to comply with sanctions may result in legal measures such as criminal and civil penalties, as well as reputational damage.

The Security Council can take action to maintain or restore international peace and security under Chapter VII of the United Nations Charter. Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force. Since 1966, the Security Council has established 31 sanctions regimes, in Southern Rhodesia, South Africa, the Former Yugoslavia (2), Haiti (2), Angola, Liberia (3), Eritrea/Ethiopia, Rwanda, Sierra Leone, Côte d'Ivoire, Iran, Somalia/Eritrea, ISIL (Da'esh) and Al-Qaida, Iraq (2), DRC, Sudan, Lebanon, DPRK, Libya (2), the Taliban, Guinea-Bissau, CAR, Yemen, South Sudan and Mali.

Security Council sanctions have taken a number of different forms, in pursuit of a variety of goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council has applied sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation.

Today, there are 15 ongoing sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counter-terrorism. Each regime is administered by a sanctions committee chaired by a non-permanent member of the Security Council.

UN Sanctioned Countries:

Central African Republic	Democratic Republic of Congo
Eritrea	Guinea-Bissau
Iran	Iraq
Lebanon	Libya
Mali	North Korea
Somalia	South Sudan
Sudan	Yemen

UN Sanctioned Organizations: Al Qaeda, ISIL and Taliban

As of 3 April 2023, there were over 256 individuals and entities listed in the UN Security Council Consolidated list.

E.1.2.2 EU Sanctions

Restrictive measures, or sanctions, are one of the EU's tools to promote the objectives of the Common Foreign and Security Policy (CFSP). These include safe-guarding the EU's values, its fundamental interests and security; consolidating and supporting democracy, the rule of law, human rights and the principles of international law; preserving peace; preventing conflicts and strengthening international security.

EU sanctions do not target a country or population, but are always targeted at specific policies or activities, the means to conduct them and those responsible for them. Moreover, the EU makes every effort to minimize adverse consequences for the civilian population or for non-sanctioned

activities or persons. They always form part of a wider, comprehensive policy approach involving political dialogue and complementary efforts. They are not punitive.

Restrictive measures imposed by the EU may target governments of third countries, or non-state entities (e.g. companies) and individuals (such as terrorist groups and terrorists). For a majority of sanctions regimes, measures are targeted at individuals and entities and consist of asset freezes and travel bans. The EU can also adopt sectoral measures, such as economic and financial measures (e.g. import and export restrictions, restrictions on banking services) or arms embargoes (prohibition on exporting goods set out in the EU`s common military list).

In addition to complying with UN sanctions, the EU may reinforce UN sanctions by applying stricter and additional measures (e.g. vis-à-vis DPRK). Furthermore, the EU may also decide to impose fully autonomous sanctions regimes (e.g. vis-à-vis Syria, Venezuela, Ukraine, Russia). Since February 2022, over 1500 new individuals and entities came under EU sanctions.

E.1.2.3 OFAC Sanctions

The US government, like most others, imposes economic and trade sanctions in pursuit of its foreign policy and national security goals against targeted foreign countries, regimes, terrorists, international narcotics traffickers, those engaged in activities relating to the proliferation of weapons of mass destruction (WMD) and those who pose other threats to US national security or economy. The United States has imposed two-thirds of the world's sanctions since the 1990s. Numerous American unilateral sanctions against various countries around the world have been criticized by different commentators. It has imposed economic sanctions on more than 20 countries since 1998.

Types of sanctions imposed by the United States

- bans on arms-related exports,
- controls over dual-use technology exports,
- restrictions on economic assistance, and
- financial restrictions such as:
    - requiring the United States to oppose loans by the World Bank and other international financial institutions,
    - diplomatic immunity waived, to allow families of terrorism victims to file for civil damages in U.S. courts,
    - tax credits for companies and individuals denied, for income earned in listed countries,

    - duty-free goods exemption suspended for imports from those countries,
    - authority to prohibit U.S. citizens from engaging in financial transactions with the government on the list, except by license from the U.S. government, and
    - prohibition of U.S. Defense Department contracts above $100,000 with companies controlled by countries on the list.
- Visa designations that prevent from entering the U.S.

The **Office of Foreign Assets Control** (**OFAC**) is a financial intelligence and enforcement agency of the U.S. Treasury Department. It administers and enforces economic and trade sanctions in support of U.S. national security and foreign policy objectives. Under Presidential national emergency powers, OFAC carries out its activities against foreign states as well as a variety of other organizations and individuals, like terrorist groups, deemed to be a threat to U.S. national security.

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury acts under Presidential national emergency powers, as well as the authority granted to it by specific legislation, basically to impose controls on transactions and freeze assets under US jurisdiction. OFAC administers and enforces these sanctions. Many of these sanctions are based on UNSC resolutions (binding on all countries) and other international mandates. Implementation of these sanctions also involves close cooperation of the US with other allied governments. The organization is also responsible for administering the specially designated nationals (SDN) List. The SDN list is a publication of OFAC which lists individuals and organizations with whom US citizens and permanent residents are prohibited from transacting and doing business. This SDN list differs from the list maintained pursuant to Section 314(a) of the USA PATRIOT Act, which contains information regarding individuals and organizations engaged in terrorist or money laundering activities.

Sometimes described as one of the "most powerful yet unknown" government agencies, OFAC was founded in 1950 and has the power to levy significant penalties against entities that defy its directives, including imposing fines, freezing assets, and barring parties from operating in the United States. In 2014, OFAC reached a record $963 million settlement with the French bank BNP Paribas, which was a portion of an $8.9 billion penalty imposed in relation to the case as a whole.

As of May 2023, USA had sanction in place against more than 3600 individuals, entities, vessels and aircrafts, according to Castellum.AI- a compliance screening company that maintain counts. In the context of Russia- Ukraine war, over 1300 entities, individuals etc. came under OFAC sanction.

E.1.2.4 Other Sanctions:

Several individual countries have sanction compliance related regulations that can be imposed on foreign countries, entries, or persons. For example, the Sanctions and Anti-Money Laundering Act 2018 allows the UK government to impose sanctions on a foreign country, entity,or individual for various reasons, such as human rights abuses, economic crime, terrorist activities,or violations of international law. Autonomous Sanctions Act 2011 allows the Australian government to impose sanctions programs on a foreign country to take it under sanctioned jurisdictions, also on entities or individuals for various reasons, such as human rights abuses, terrorist activities, or violations of international law.

E.1.2.5 Domestic Sanction

For the purpose of attaining the objective of the Anti-Terrorism Act, 2009, the government can ban/proscribe any individual/entity involved in terrorism activity. Under the provision of the said Act, the government, till the date, has proscribed the following 09 organizations and listed into the schedule of terrorist organizations:

SL	Name of Entity	Date of Proscription
1.	Shahadat-E-Al Hikma PartyBangladesh	09/02/2003
2.	Jagroto Muslim Janata Bangladesh(JMB)	23/02/2005
3.	Jamatul Mujahidin	23/02/2005
4.	Harkatul Jihad Al Islami	17/10/2005
5.	Hizbut Tahrir Bangladesh	22/10/2009
6.	Ansarullah Bangla Team	25/05/2015
7.	Ansar-Al-Islam	12/02/2017
8.	Allahr Dol	05/11/2019
9	Jama’yatul Ansar Fi’l Hindal Sharkiyah	09/08/2023

E.1.3 Impact of Sanctions:

In terms of implications and enforcement approaches, UN and OFAC sanctions are particularly prominent and different. As member countries UN sanctions are bindings to the member states, and are enforced through government entities. OFAC economic sanctions may not be formal or explicit obligation to the global economies, however, are complied with in most instances to avoidbusiness and reputation risks. OFAC's sanctions programs have a global reach due to the influenceof the USA financial system and the role of the USD in international transactions. In reality, financial

institutions and businesses must comply with OFAC regulations, and violations can result in substantial penalties and legal consequences.

Economic sanctions affect international trade by creating abstractions, relocation of sourcing and destinations, and risks and costs of transportations that have severe economic impacts. Suppose, trades in food and fertilizer are getting affected due to Russia-Ukraine war and the associated sanctions, and food supply related obstacles might harm global food security. Trade in crude oil and petroleum products is more complicated. But for countries with limited capacity and few resources, ignoring the problem could have severe economic consequences. In the new geopolitical world with more sanctions and export controls, the trading environment inevitably becomes more expensive and legalistic. To continue to trade in support of their economic development, emerging market economies are confronting true challenges.

As a member state, Bangladesh is required to comply with economic sanctions on countries, organizations and individuals imposed by the UN. Like other jurisdictions, Bangladesh is required to comply with economic sanction on countries, organizations and individuals imposed by the UN Security Council under Chapter VII of UN Charter. Other forms of economic sanctions (OFAC, EU, UK Australia etc.) from an individual country or country-groups are not legal or formal obligation of an economy like Bangladesh, however, it does not afford to deny these comprehensively being part of this interdependent and globalized business environment of the globe. Bangladesh has notbeen subjected to comprehensive USA sanctions, but specific individuals and entities have been targeted under OFAC sanction programs. Currently, seven (7) entities and seven (7) individuals are in the OFAC sanction list from Bangladesh. The significant impact of economic sanctions andespecially by UN and OFAC sanctions cannot be denied with their spillover effects on the economy.

Bangladesh attain remarkable development in terms of economic growth, trade and business development, and social development indicators. However, this progression might be stumbled if any sanction from the UN, OFAC or some other unilateral sanctions imposed upon an individual or entity in Bangladesh or violation by any bank in Bangladesh. As a participating country in global trade and finance, Bangladesh may be affected. Sanctions may create a spillover effects on the country's economy. Financial and banking sector may be affected by sanctions as secondary actor and/or may be implicated as the designated individuals and entities may have financial transactions with these entities. Moreover, the sanctions (especially OFAC) can affect the reputation of Bangladesh as a business destination, as investors and companies may hesitate to dobusiness with Bangladesh for fear of violating the sanctions. The sanctions can also undermine thecountry's efforts to attract foreign investment and diversify its export sector. Consequently, these sanctions are boosting financial institutions' operational costs, losing prevailing customers and impacting

customers' overall satisfaction. Recently, in the wake of Russia-Ukraine war, OFAC has imposed sanctions on various Russian individuals and institutions and Bangladeshi banks are facing various obstacles in facilitating cross-border trade transactions.

E.1.4 Regulatory Approach to Sanctions:

BFIU primary mandate is to prevent money laundering, terrorist financing, proliferation financing of weapons of mass destruction and other illicit financial activities; and BFIU plays the central role in ensuring compliance with UN sanctions and domestic proscription and enlistment.

Banks and financial institutions are amongst the key actor in sanction implementation, compliance and related reporting. In the process of implementing UNSCRs, banks are required to maintain and update the listed individuals and entities in electronic form; and to check at the website of United Nations (http://www.un.org/sc/committees/index.shtm) for updated list. BFIU offered instructions to implement Local Sanction List and United Nations Security Council Resolutions. According to section 10 of BFIU Circular-26 (dated 16/06/2020), banks must implement UNSCRs to prevent financing terrorism and weapons of mass destruction proliferation, and must establish a process approved by their Board of Directors to prevent and identify transactions related to these issues.

BFIU arranged workshops and several meeting with different banks for providing general and technological support in collaboration with successfully implemented banks. Instructions on bank officials' roles and responsibilities should be issued, reviewed periodically, and ensure compliance with instructions from the BFIU. Banks must promptly report any news on financing terrorism or weapons of mass destruction to the BFIU.

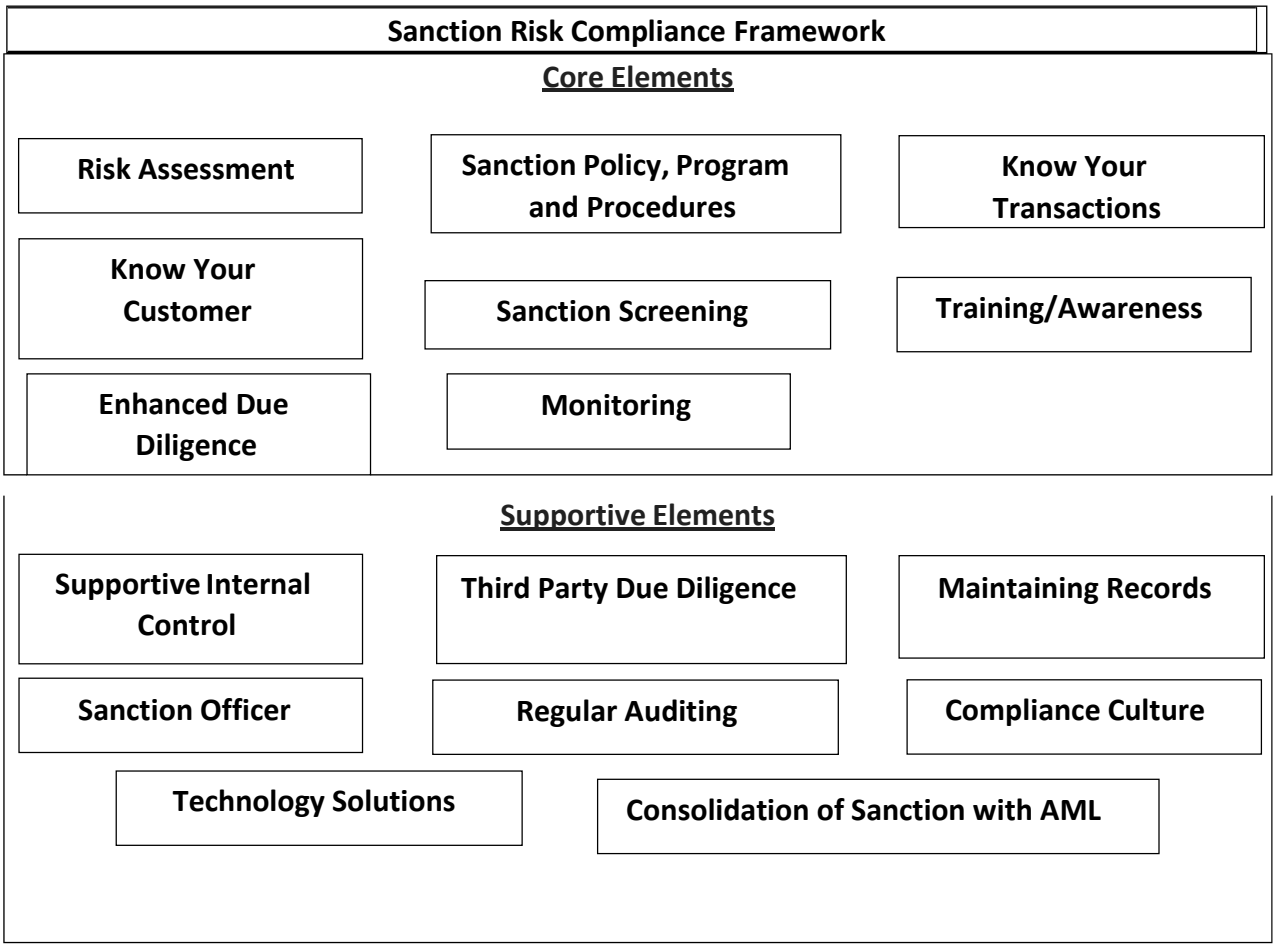
BFIU monitors the compliance of banks with sanctions regulations in a regular interval. It conducts periodic inspections and assessments to ensure that the necessary policies, procedures, and systems are in place to effectively implement sanctions measures. It also provides guidance, training, and capacity-building initiatives to financial institutions, regulators, and other stakeholders to enhance their understanding of sanctions regulations. This helps in promoting a culture of compliance and effective implementation of sanctions measures. It is important to note that BFIU's monitoring and supervising mechanism is carried out in collaboration with other relevant authorities, such as the Ministry of Foreign Affairs, regulatory bodies, and law enforcement agencies. This multi-agency approach ensures coordinated efforts in implementing and enforcingsanctions in Bangladesh.

E.1.5 Compliance with Sanctions and Minimizing Risks

Risks in sanctions compliance are potential threats or vulnerabilities that, if ignored or not properly handled, can lead to violations of sanctions and negatively affect an organization's reputation and business. FATF updated document (2023) recommended (as part of combating money laundering

and financiering of terrorism & proliferation) for taking care of sanction measures with the sub-titles 'Targeted financial sanctions related to terrorism and terrorist financing' and 'Targeted financial sanctions related to proliferation'[15] as required by the UN Security Council.

With the possibility of severe financial fines and reputational risk, no one wishes to be discoveredto have commercial links to a sanctioned firm. To ensure compliance with sanctions, organizationsmust adopt strategies that facilitate due diligence, risk management, and ongoing monitoring. Key elements of the Sanction Risk Compliance Strategies may be summarized as follows:



Senior management ensures that its compliance unit is delegated sufficient authority and autonomyto deploy its policies and procedures in a manner that effectively controls the organization's sanction risk. Conducting a risk assessment is the first step towards compliance with sanctions. Anentity must evaluate their business operations and assess the potential risks associated with their activities, including their customers, and partners. KYC is essential compliance strategies that involve verifying the identity of customers and must ensure that they are not doing business with individuals or entities that are sanctioned or restricted. Sanction Screening involves screening customers, suppliers, and transactions against various sanction lists. EDD is required to conduct a more detailed investigation of high-risk customers or transactions. For ensuring sanction compliance, entities must provide regular training and awareness programs to their employees to ensure they understand the importance of sanction compliance and their role in implementing it.

Moreover, it is crucial to implement effective monitoring systems to identify and prevent real-time prohibited transactions.

E.2.3 Sanctions Screening:

Sanctions Screening is an Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) control used to detect, prevent, and disrupt financial crime. Regulated businesses must conduct sanctions risk screening as a mandatory practice for effective sanctions compliance. This step is a crucial component of the Know Your Customer (KYC) process, which ensures thorough due diligence and risk mitigation. Banks must identify accounts or transactions held by listed or proscribed individuals or entities, review them when necessary, and retain records related to false positives. For better implementation, banks are instructed to use automated screening mechanism, either developed byown IT professionals domestically or by international vendors. As the reporting organization, banks need to run regular check on the given parameters, including transactional review, to verify, and in case of a match found shall immediately stop payment or transaction of funds, financial assets or economic resources. In such a situation, banks are required to report to the BFIU withinthe following working day with full particulars.

E.2 Anti-Bribery and Corruption (ABC)

Bribery and corruption are illegal and unethical practices that involve the exchange of money, gifts, or other favors in exchange for special treatment or favors. Bribery involves giving or receiving something of value to influence a person's actions or decisions, often in violation of the law or ethical standards. Corruption involves using power or authority for personal gain, often through illegal or unethical means.

Bribery and corruption are widespread problems that can have serious consequences for individuals, organizations, and societies as a whole. They can undermine the rule of law, distort competition, and erode public trust in government and institutions. In many cases, bribery and corruption can lead to economic and social inequality, as well as political instability and conflict.

E.2.1 Corruption

Transparency International defines corruption as the illegal and illicit enrichment of authorities in the government sector, whether politicians or civil employees, via the misuse of public power entrusted to them. IMF has defined corruption as the use of public office for private gain, or in other words, use of official position, rank or status by an office bearer for his own personal benefit. Examples of corrupt behavior would include: (a) bribery, (b) extortion, (c) fraud, (d) embezzlement, (e) nepotism, (f) cronyism, (g) appropriation of public assets and property for private use, and (h) influence peddling. Corruption may take the following forms:

- **Demand-Side Corruption** refers to accepting or soliciting unlawful reimbursement or unfair advantage, whereas providing such a payout or benefit is referred to as "supply-side corruption."
- **Conventional Corruption** is common among government personnel, regardless of rank and position. It occurs when they acquire an unfair advantage while disregarding the public's needs. "Petty" and "grand" corruption are examples of conventional corruption.
    - A few examples of the use of **Petty Corruption** include the payment of bribes to law enforcement officers, customs agents, medical professionals, and other government personnel. This category includes facilitation payments, sometimes called "grease" payments.
    - **Grand Corruption** results when elected officials and high-ranking government workers abuse the opportunities provided by their job with the government. Bribes given or received in connection with larger-scale government initiatives, such as construction and infrastructure projects, are increasingly common.
    - **Unconventional Corruption** occurs when a public official or member of the government does a specific action with the intent to benefit themselves personally rather than the general public**.** Because there isn't a direct exchange of products or services between the parties, the absence of a reciprocal connection is crucial. This kind of corruption comprises embezzlement, fraud, misappropriation, and breach of trust.

Most cases of corruption include kickbacks or bid-rigging tactics.

- **Kickback Schemes** can begin when an employee accepts a gift from a grateful business. The first gift is small and doesn't require anything in return; the next one is bigger, and eventually, the employee gets used to receiving gifts. The majority of kickback schemes require cooperation between a vendor partner and an employee who approves purchases. The employee accepts payment for the service and signs an invoice for overpriced or nonexistent goods. Alternatively, an inspector can receive payment for approving subpar products or poor workmanship.
- **Bid Rigging** is an illegal practice in which the parties involved plan to influence the result of a bidding process. Bid rigging is a kind of price manipulation and anti-competitive cooperation; when bidders work together, the bidding process is weakened and the rigging price may be higher than what would have happened in a free market bidding. Consumers and taxpayers might suffer as a result of bid rigging, having to pay higher pricing. People that participate get compensated for their work.

Although illicit economic activity exists in every country, it is more prevalent in those with high levels of corruption. Official macroeconomic data, which often only represent the formal sector of an economy, become inaccurate when trying to gauge economic performance or serve as a foundation for policy development and research. Because of significant illicit and unrecorded flows of services and goods across the border in a booming smuggling industry, official statistics on foreign trade, for instance, no longer accurately reflect a country's real quantity, or worth, of exports and imports.

E.2.2 Bribery

Bribery is the type of corruption most closely associated with corruption in general. Bribery is distinguished by its "quid pro quo" character. Bribery entails trade. It is simple to complicate the concept of bribery by adding words like "benefit to the bribe-giver" or "providing anything of worth." In truth, even if the items traded had little to no value, in the end, most people will view any transaction that satisfies the broad definition of corruption as a bribe.

In reality, even if the items traded eventually had little to no worth or were of little to no advantage to the bribe-giver, most people will still see any transaction that satisfies the broad definition of corruption as a bribe. Bribery may be defined simply as: "The abuse or misuse of authority or trust in a quid pro quo trade. This explanation incorporates the idea of exchange and works within the general definition."

The section 171B of Penal Code, 1860 describes bribery as-

(1) Whoever- (i) gives a gratification to any person with the object of inducing him or any other person to exercise any electoral right or of rewarding any person for having exercised any such right; or (ii) accepts either for himself or for any other person any gratification as a reward for exercising any such right or for inducing or attempting to induce any other person to exercise any such right, commits the offence of bribery:

(2) A person who offers, or agrees to give, or offers or attempts to procure, a gratification shall be deemed to give a gratification.

(3) A person who obtains or agrees to accept or attempts to obtain a gratification shall be deemed to accept a gratification, and a person who accepts a gratification as a motive for doing what he does not intend to do, or as a reward for doing what he has not done, shall be deemed to have accepted the gratification as a reward.

Section 171E of the said Penal Code includes the punishment of bribery as- whoever commits the offence of bribery shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both: Provided that bribery by treating shall be punished with fine only.

No one definition of what constitutes bribery is universally accepted. Still, all definitions concur that it involves someone in a position of trust behaving willingly and dishonestly in return for a financial benefit. It is unnecessary to trade money or any payment to receive the advantage. It can come in various shapes, such as costly gifts, hospitality, and other charges out of pocket, access to resources, or a favor done for a close friend, a family member, or a cause you believe in.

E.2.3 Corruption induced Money Laundering

Corruption and money laundering are intrinsically linked. Similar to other serious crimes, corruption offences, such as bribery and theft of public funds, are generally committed for the purpose of obtaining private gain. Money laundering is the process of concealing illicit gains that were generated from criminal activity. By successfully laundering the proceeds of a corruption offence, the illicit gains may be enjoyed without fear of being confiscated.

Combating money laundering is a cornerstone of the broader agenda to fight organized and serious crime by depriving criminals of ill-gotten gains and by prosecuting those who assist in the laundering of such ill-gotten gains. The FATF recognizes the link between corruption and money laundering, including how AML/CFT measures help combat corruption. This is why corruption issues are taken into account during the FATF mutual evaluation process which assesses countries' compliance with the FATF Recommendations. For example, the FATF considers how effectively AML/CFT measures are implemented in a country by considering the number of investigations, prosecutions and convictions for money laundering, and the amount of property confiscated in relation to money laundering or underlying predicate offences, including corruption and bribery (Recommendation 32). As well, the FATF considers whether the country can demonstrate that it has a solid framework of measures to prevent and combat corruption through respect for transparency, good governance principles, high ethical and professional requirements, and established a reasonably efficient court system to ensure that judicial decisions are properly enforced. These elements are important because significant weaknesses or shortcomings in these areas may impede effective implementation of the FATF Recommendations.

E.2.3.1 Initiatives of Bangladesh to fight Corruption and Money Laundering

Bangladesh signed and ratified the UNCAC in 2007. The country also signed the Convention against Transnational Organized Crime in 2011. To prevent corruption and other corrupt practices in the country and to conduct inquiry and investigation for other specific offences Anti-Corruption Commission (ACC) was formed through an act promulgated on 23 February 2004 that came into force on 9 May 2004. Anti-Corruption Commission (ACC) is an independent authority tasked with preventing, investigating and prosecuting corruption. The ACC was, in practice, the sole LEA responsible for investigating and prosecuting all ML cases until October 2015. Bangladesh has conducted National Risk Assessment (NRA) two times and a number of sector specific risk assessments. The 2015 NRA identified five high risk threat areas in which Corruption is one of them. The NRA identifies domestic proceeds as the predominant ML threat, with laundering of proceeds domestically and outside the country.

E.2.3.2 Counter Measures to Fight Corruption Induced Money Laundering

- **Safeguarding the Integrity in Public Sector**

Corruption flourishes in an environment where state officials and public sector employees misuse their positions for private gain. Effective implementation of the FATF Recommendations helps to safeguard the integrity of the public sector by ensuring that key government agencies involved in anti-money laundering and combating terrorist financing (such as the financial intelligence unit, law enforcement and prosecutorial authorities, supervisors and others) are adequately resourced and manned by staff of high integrity.

- **AML/CFT Compliance Measures in Private Sector**

Private sector institutions are an attractive venue for laundering the proceeds of corruption, particularly if they are owned or infiltrated by corrupt persons or have implemented weak AML/CFT measures. AML/CFT compliance measures help to protect designated financial institutions like the banks and other designated businesses and professions by requiring that their owners, controllers and employees are properly vetted, and they have adequate systems in place to comply with AML/CFT requirements.

Role of Top Management: Persons holding a significant controlling interest or management function in a designated private sector institution must be **vetted**. In the case of financial institutions, such vetting should use "**fit and proper**" criteria for directors and managers. This helps to prevent corrupt persons and other criminals from gaining control over a financial

institution.

Employee Screening: Institutions must **screen employees** to ensure high standards. This helps to prevent corrupt persons from infiltrating or otherwise criminally abusing a financial service provider.

Effective Internal Control System: The institutions must implement **internal control systems and audit functions** to ensure compliance with AML/CFT measures. This helps such institutions to detect when they are being abused by criminals and corrupt persons.

Monitoring and Supervision: The institutions must be subject to adequate **supervision and monitoring** by supervisory authorities (or self-regulatory organizations, in the case of lawyers, accountants, real estate agents, dealers in precious metals and stones, and trust and company service providers) with sufficient supervisory, inspection and sanctioning powers to ensure compliance with AML/CFT measures. Robust supervision and monitoring of the financial sector deters and facilitates the detection of corruption and other criminal activity.

Ensuring Transparency: Corruption is more likely to go unpunished in opaque circumstances where the proceeds of such crimes are laundered and cannot be traced back to the underlying corrupt activity, as is the case when the ownership of assets is obscured, and transactions and transfers leave incomplete (or no) audit trail. Effective implementation AML/CFT measures increase the transparency of the financial system by creating a reliable paper trail of business relationships, transactions, and discloses the true ownership and movement of assets.

Know Your Customer Process and Verification: Establishing business relationships or conducting transactions on behalf of customers, designated private sector institutions must **verify the identity of the customer**, any natural person on whose behalf a customer is acting, and any individuals who ultimately own or control customers that are legal persons (such as companies) or legal arrangements (such as trusts). Additional precautions must be taken when transactions are conducted through a third party or are not done face-to-face. These precautions increase transparency by making it difficult for corrupt persons to conduct business anonymously, or hide their business relationships and transactions behind other people, corporate structures, or complex legal arrangements.

Record Keeping: All customer identification, transaction and account records, and business correspondence must be kept, so that they can be made available to the authorities on a timely basis. Such **record keeping** measures ensure that there is a reliable paper trail the authorities can use to trace the proceeds of corruption, and use as evidence to prosecute corruption and other crimes.

Implementation of Risk Based Approach: Financial service providers must put in place appropriate risk management systems to determine whether a (potential) customer or the individual

who ultimately owns or controls the customer is a **politically exposed person** (PEP). When doing business with a PEP, financial service providers must take reasonable measures to determine the PEP's source of wealth and funds. Such measures increase the possibility of detecting instances where public officials and other persons who are (or have been) entrusted with prominent public functions in a foreign country — such as Heads of State, senior politicians, senior government judicial or military officials, senior executives of state-owned corporations and important political party officials—are abusing their positions for private gain

Detection of Suspicious Transaction: The institutions must conduct ongoing due diligence on all business relationships to ensure that the transactions being conducted are consistent with their knowledge of the customer, business and risk profile, and where necessary, the source of funds. Special attention must be given to any complex, unusual or large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose. Increased scrutiny must be given to high risk customers (such as foreign PEPs), jurisdictions, business relationships and transactions. This enables the detection of unusual or suspicious activity that might be related to corruption and which must be reported to the BFIU for further analysis and investigation.

Ensuring Transparency in the Financial Sector: The transparency of ownership makes difficult to hide the proceeds of corruption within a company or trust. Wire transfers are a fast way to move the proceeds of corruption elsewhere to obscure their source and must, therefore, be accompanied by accurate and meaningful information which identifies the person who sent the transaction. Likewise, cash or bearer negotiable instruments that are being moved across national borders either on one's person, through the mail, or in containerized cargo would also leave no paper trail and, therefore, must be declared or disclosed to the authorities. Transparent movement of assets makes it possible to trace the movement of corruption proceeds.

E.2.4 Anti-Corruption Commission (ACC)

To tackle the corruption problems the Government of Bangladesh established an independent Commission named Anti-Corruption Commission (ACC) to prevent corruption and other corrupt practices in the country and to conduct inquiry and investigation for other specific offenses and to enact other relevant matters by virtue of section 3 of Anti-Corruption Commission Act 2004 (ACCA 2004). In accordance with section 17 of the ACCA 2004 ACC may inquire and investigate any allegation of corruption on its own initiative, or upon an application filed by an aggrieved person or by any person on his/her behalf, file and conduct cases under this Act, carry out research on the prevention of corruption and submit recommendations to the President regarding the actions to be taken on the basis of the research findings, promote the values of honesty and integrity in order to prevent corruption and take measures to build up mass awareness against corruption,

arrange seminars, symposiums, workshops etc. on subjects falling within the jurisdiction of the commission.

E.2.4.1Main Provisions of Anti-Corruption Commission Act, 2004:

Establishment of Commission, etc. (Section 3)

1) After this law has come into force, the government shall as soon as possible through an official gazette notification establishes a commission named the Anti-Corruption Commission to meet the objectives of this law.

(2) This commission shall be independent and impartial.

Function of ACC (Section 17)

The Commission may discharge any or all of the following functions: -

(a) Inquiry and investigation into the offences set out in the schedule.

(b) File and conduct cases under this Act on the basis of investigation and inquiry under clause

(c) Inquire into any allegation of corruption on its own initiative, or upon an application filed by an aggrieved person or by any person on his/her behalf.

(d) Perform any duty entrusted to the commission by anti-corruption laws.

(e) Review the legally accepted measures for preventing corruption and submit recommendations to the President their effective implementation.

(f) Carry out research on the prevention of corruption and submit recommendations to the President regarding the actions to be taken on the basis of the research findings.

(g) Promote the values of honesty and integrity in order to prevent corruption and take measures to build up mass awareness against corruption.

(h) Arrange seminars, symposiums, workshops etc. on subjects falling within the jurisdiction of the commission.

(i) Identify the sources of different types of corruption existing in Bangladesh against the backdrop of the country's socio-economic conditions and present to the President any recommendations for appropriate action.

(j) Inquire into corruption, investigate, file cases and determine the process of approval by the commission in respect of such inquiry, investigation and filing of cases.

(k) Perform any other work considered necessary for the prevention of corruption.

Special powers of the Commission in respect of inquiry or investigation (Section 19)

(1) In respect of any inquiry or investigation into allegations of corruption the Commission shall have the following powers, namely: -

(a) Summons witnesses, ensure their appearance and interrogate them under oath.

(b) Discover and present any document.

(c) Take evidence under oath.

(d) Call for public records or its certified copies from any court office.

(e) Issue warrants for the interrogation of witnesses and the examination of documents.

(f) Any other matter required for realising and fulfilling the aims and objectives of this law.

Power of Investigation (Section 20)

(1) Notwithstanding anything in the Code of Criminal Procedure, corruption shall be the subject matter of investigation by the commission alone.

(2) The commission may through an official gazette notification empower a subordinate officer of the commission the power to investigate corruption under sub-section (1).

(3) For the purpose of investigation into offences under this law, an officer empowered under sub-section (2) shall have the power of an officer-in-charge of a police station.

(4) Besides the provisions of sub-sections (2) and (3), the commissioners shall also have the power to investigate any offence under this law.

Power of Arrest (Section 21)

Notwithstanding any other provision of this law, if any officer empowered by the commission has justifiable reasons to believe that a person in his/her name or in the name of others is the owner or in possession of moveable or immoveable property not compatible with known and declared sources of his/her income, then subject to the permission of the court the officer can arrest that person.

Declaration of properties (Section 26)

(1) If the commission is satisfied on the basis of its own information and after necessary investigation that any person or any other person on his behalf is in possession or has obtained ownership of property not consistent with his legal sources of income then the commission through an order in writing shall ask that person to submit a statement of assets and liabilities in the manner determined by the commission and to furnish any other information mentioned in that order.

(2) If any person -

(a) after having received an order mention in sub-section (1) fails to submit the written statement or furnish the information accordingly or submits any written statement or provides any information that is false or baseless or there are sufficient grounds to doubt their veracity or

(b) submits any book, account, record, declaration, return or any document under sub-section (1) or gives any statement that is false or baseless or there are sufficient grounds to doubt its veracity, then that person will be sentenced to a prison term of up to three (3) years or a fine or both. Possession of Property in Excess of Known Sources of Income (Section 27)

(1) If there are sufficient and reasonable grounds to believe that a person in his/her own name or any other person on his/her behalf is in possession and has obtained ownership of moveable or immoveable property through dishonest means and the property is not consistent with the known.

Case and Sample Questions

Case: XYZ Bank Ltd. established corresponding relationship with a North Korean Bank and intermediated several LCs on behalf of its customer to export garment products. The export proceed was later blocked by US government and the global banks cut off all the banking relationship with XYZ Bank Ltd.

Sample Question:

1) What is sanction screening? Describe different types of sanction. What are the impact and implications of sanction in the banking industry?
2) What if OFAC sanction? Whey Bangladeshi banks follow OFAC sanction?
3) What are the legal provisions for proscription of entity and enlistment of person for suspicion of terrorist activities? How many entities have been proscribed by Bangladesh Government till now?
4) What mitigations measures should a bank have to take to avoid the impact of sanction?
5) What is the relation between corruption and money laundering? Mention some red flag for identification of corruption induced money laundering.
6) What is ABC Policy? How a bank can apply ABC policy in its activities?

Module-F: Financial Crime Control (FCC) for New Technology

The Financial Action Task Force (FATF) defines "new technologies" as Innovative skills, methods, and processes that are used to achieve goals relating to the effective implementation of AMLCFT requirements or Innovative ways to use established technology-based processes to comply with AML/CFT obligations.

F.1 FCC Risk Associated with New Services and Technology

The FATF Recommendation 15 urges that the countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

VA and VASPs

FATF defined **"Virtual asset"** as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations; and

"Virtual asset service provider" as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currencies;
ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets; and
iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

F.2 FinTech Products

Financial Technology (FinTech) improves and automates financial services using new technologies. FinTech aims to compete with the traditional financial services method because technology has developed, and traditional methods are insufficient, so the financial sector needs FinTech and its solutions. It has developed the financial sector using mobile banking, mobile payment, cryptocurrency, and bitcoin technologies.

According to the Egmont Group of financial intelligence units, FinTech refers to entities that enable payments or transfers of value by using new or emerging technologies. Common examples of FinTech providing financial services include:

- Internet banking
- Mobile banking
- Digital or electronic money
- Money transfer platforms
- E-commerce platforms
- Non-face-to-face investments
- Crowd funding platforms etc.

FinTech service in the financial sector has provided undeniable convenience to the industry and customers, and FinTech is growing and developing day by day. It has transformed the modern financial landscape, harnessing global internet connectivity to deliver innovative new products and services and improve customer experiences. However, the benefits of fintech have been accompanied by considerable compliance risks as criminals use advances in technology to develop Fintech money laundering techniques and finance terrorist activities. In FinTech, money laundering is attractive for offenders because of the increase in the initiation of transactions in these systems, unlimited money flow, and the transaction of anonymous accounts facilitate money laundering for criminals. With the rise in digital money circulation, criminals continue their money laundering activities in this direction. Also, electronic anti-money laundering (transaction laundering) has started to replace traditional anti-money laundering. This case shows that FinTech is a potential target for money laundering criminal organizations. As a result of all these data, FinTech may be exposed to serious AML risks. So, to prevent AML/CTF and avoid criminal investigations, FinTech should use best practices and comply with regulations just like other ROs.

F.2.1 Fintech AML Risks

Money launderers have kept pace with advances in financial technology, developing new methodologies to exploit and avoid AML compliance measures. Accordingly, firms should be aware of the following types of fintech AML risks:

- **Customer identities:** Since fintech products and services are accessed over the internet, money launderers may take advantage of the anonymity benefits of online transactions, submitting incomplete, misleading, or false information in order to conceal their identities and avoid AML controls.

- **Transaction speeds:** The increasing speed of internet connections means that customers can complete transactions in seconds. Money launderers may exploit that speed by transferring large volumes of funds into and out of accounts or between different institutions quickly, outpacing the scrutiny of authorities.

- **Money-muling:** Money launderers may use third-parties to engage with fintech services on their behalf as a way to introduce illegal funds to the financial system. These so-called 'money mules' may be vulnerable members of society, such as the elderly or the disabled, or may have been coerced or incentivized to take part in the illegal activity.

- **Cross-border transactions:** Fintech services can be accessed anywhere and used to transfer funds between accounts located in different countries. Money launderers may exploit the cross-border connectivity of fintech services to transfer illegal funds to higher risk jurisdictions with fewer or less stringent AML controls than their accounts of origin.

- **Regulatory lag:** The novelty and innovation of fintech services often outpaces the ability of financial regulators to address illegal activity. Money launderers may be able to identify weaknesses and blind spots in regulation that authorities have not addressed, and use those opportunities to disguise illegal funds.

F 2.1 Mobile Financial Services (MFS)

Mobile Financial Services (MFS) is one of the finest FinTech innovations in the last decade-reshaping the financial service delivery models especially in the developing economies. It has enabled the financial service providers to include the bottom of the pyramid population into formal financial services which was otherwise impossible. MFS was launched in Bangladesh in 2011 and gained popularity within a short span of time. Total number of MFS accounts has crossed the fifty million mark in just six years making Bangladesh one of the fastest growing MFS markets in the world. It has brought revolutionary changes in local money transfer services where low income population is the main customer. Other services such as merchant payment and social benefit disbursement are gaining momentum in recent times. However, any financial services including MFS are not insulated from potential abuses for illicit purposes. Several typologies of abuse of MFS have been observed in MFS market. These are unique in nature compared to other financial services. Culprits are also innovating new techniques of fraud that make the task of regulators and

law enforcement agencies more challenging. Perpetrators have been seen to use this service to receive and transfer proceeds of crime anonymously.

There are several factors which are contributing for the abuse of m-money in Bangladesh. Agents acquire and register multiple SIM cards to conduct anonymous transaction (ATr) of the customers. Customers, having low academic qualification, find it difficult to navigate the mobile menu (in English language) required to conduct transaction. Customer acquisition based on previous falsely registered SIM along with lack of unique identification documents for all citizens and ID verification tools for the MFS providers; and inadequate monitoring mechanism for the agents are contributing heavily for the abuse of MFS.

F.2.2 Transaction Platform E-Wallet

E-wallet or Digital wallets enable users to link all their payment methods under a single account. The account stores funds, credit card numbers, and even cryptocurrencies and these wallets are accessible online through a smart phone or a website.

The main feature of e-wallets is that all information related to transactions is encrypted and tokenised. This enhances security and an individual's privacy but also leaves the merchants in vain as they cannot spot credit card scams.

F.2.2.1 The Risks of Money Laundering with Digital Wallets

eWallet firms pose a risk of money laundering and other crimes due to the anonymity provided by online financial services. Not only this but other aspects, such as the speed of transactions and lack of regulations from domestic and global authorities may also contribute to it. In detail, those risks involve:

- **Anonymity:** Sometimes digital wallet service providers may implement inadequate identity verification measures. Criminals take advantage of this to use services anonymously and fulfil their illicit intents. They use different tactics, such as proxies to open an account or even open many accounts for laundering money.
- **Transaction Obscurity:** Cybercriminals manipulate digital wallet services to conceal their efforts of laundering money. They either access multiple eWallet accounts from a single device to hide their identity or make many small transactions to conceal a handsome amount of transferred money. Digital wallets also offer to transfer money abroad to elude the attention of authorities.
- **Speed:** eWallet transactions occur quickly and in real-time just like many other digital financial services. This means that criminals can move illegal funds around quickly,

bypassing safeguards and investigations. Rapid transactions help criminals structure their transactions, using several transfers across many accounts, to conceal the illegal origin effectively.

- **Lack of Oversight:** Some countries do not have effective legislation in place to deal with eWallet issues. Scammers, who are on the hunt for such loopholes, take this opportunity and exploit regulatory blind spots to accomplish their illicit goals. Moreover, the lack of oversight facilitates criminals in transferring illegal funds to different countries by avoiding suspicious activity reporting rules and reporting thresholds.

F.2.2.2 Compliance with AML Regulations regarding e-wallet fraud

The Financial Action Task Force (FATF) sets out an Anti Money Laundering and Countering Terrorist Financing (AML/CFT) framework for the member states to implement in national legislation. This means that all the companies, including digital wallet service providers, have a legally obligated to conduct comprehensive risk assessments of their clients and modify their AML response proportionately. In practice, eWallets should include the below-mentioned measures to satisfy AML regulations:

- **Customer Due Diligence:** Digital wallets should conduct Customer Due Diligence (CDD) to verify Personally Identifiable Information (PII) like names, date of birth, address, etc. High-risk clients have to undergo Enhanced Due Diligence (EDD) under the risk-based approach.
- **Transaction Monitoring:** eWallet services must check their customers' transactions and identify any suspicious activity that shows money laundering. In case any suspicious activity is detected, the organisation must generate a Suspicious Activity Report (SAR) to notify the authorities promptly.
- **Screening and Monitoring:** Digital wallet firms must check that their customers do not appear in sanction lists, watch lists, and Politically Exposed Persons (PEPs) lists. Moreover, eWallet also monitor clients for negative social media stories or any related things that increase the risk of money laundering.

Digital wallet service providers should look out for the following **"red flag"** behaviors to improve AML compliance.

- Disparities or inconsistencies in client verification during account registration.
- Unusual patterns of transactions or those involving PEPs or high-risk customers.
- Rapid and frequent cash withdrawals transferred to digital wallets.
- Routine transfer of money to third-party accounts after depositing them to eWallets.

- Transactions that occur above or below the reporting thresholds.
- Several account registrations, transfers or deposits that seem connected.

F.2.3 E-Commerce Site and Market Place

E-commerce, short for electronic commerce, refers to the exchange of all types of goods, services, funds, or data over an electronic network, usually the internet. This type of business transaction can take place between businesses (B2B), businesses to consumers (B2C) and consumers to other consumers (C2C). E-commerce has revolutionized the way we shop and do business, making it easier and more convenient for consumers and companies to connect and transact. However, as with any technology-driven platform, e-commerce has also created new opportunities for criminal activity. Cybercriminals have found ways to exploit vulnerabilities in online transactions and leverage the anonymity and global reach of the internet to perpetrate a wide range of crimes, from (tax) fraud to money laundering. E-Commerce businesses can be exploited for criminal purposes in four major ways:

1) Committing fraud against the customer by failing to deliver goods or services.
2) Buying goods or services using stolen bank card data.
3) Creating e-commerce businesses as a front for illicit transactions (for example, to accept bank card payments for drugs).
4) Abusing online marketplaces to move criminally obtained funds (for example, through the sale of computer-generated books sold via Amazon)

Of these criminal modus operandi, the latter two present particular money-laundering and terrorist-financing (financial crime) threats because they involve consensual transactions that are intended to remain undetected. Despite their role in concealing criminal income, these phenomena remain poorly understood. For instance, there are multiple examples of criminal groups using e-commerce businesses to receive payments for illicit transactions – a criminal typology known as ‘transaction laundering.

E-commerce money laundering or transaction laundering is the process of leveraging e-commerce and merchant processing to create fictitious transactions that appear legitimate. These transactions may involve knowing or unknowing participants in the e-commerce ecosystem, a network of interconnected parties involved in the buying and selling of goods and services. Transactions may be facilitated by front companies that appear to sell legitimate goods and services but are set up by money launderers to provide cover for their illegitimate activities, pass-thru companies set up by third parties and used by one or more criminals, or funnel accounts in which payment processors may commingle legitimate and illegitimate transactions. They may involve the sale of fake or

contraband goods, the value of e-commerce transactions may be over-inflated, or the transactions may simply be nonexistent, a scheme sometimes referred to as ghost laundering. E-commerce has given rise to a variety of frauds that can have a significant impact on both consumers and businesses. Refund fraud is a common tactic used by fraudsters who are unable to receive goods or cash out using stolen credit cards. Another type of fraud is interception, where the fraudster places an order using a valid billing and shipping address, but then attempts to intercept the goods for themselves.

The other types of fraud that e-commerce face are-

- **Identity Theft**

Identity theft happens when a fraudster steals a person's identity information to make fraudulent purchases or transactions. Typically, the criminal obtains this information through phishing scams, hacking, or by purchasing it on the dark web. Once they access the victim's details, they can use them to open new accounts, make purchases, or commit other fraudulent activities. In the famous words of the notorious hacker Ngo Minh Hieu, who had stolen personal data from over 60% of Americans – "when a person loses their identity, they lose it forever."

- **Payment Fraud**

Another type of e-commerce fraud is payment fraud, where a cybercriminal uses stolen payment information or creates fake payment details to complete a purchase. For example, a fraudster may use a stolen credit card number to make a purchase or create a fake bank account or payment gateway to trick the seller into accepting the payment.

- **Chargeback Fraud**

Known as friendly fraud, chargebacks are also a common form of e-commerce fraud, where a customer disputes a charge with their bank or credit card company, claiming that they didn't authorize the transaction or that the product was not delivered as promised. To prevent double refunds, some e-commerce marketplaces may ask their users to close the dispute they opened and work with their bank to resolve the issue instead of making fraudulent chargeback claims.

These and other types of e-commerce fraud underscore the importance of vigilance and caution when engaging in online transactions. E-commerce is also being used as a tool for tax evasion. Several factors have led to e-commerce being recognized as a means for tax evasion. Among these factors is the challenge faced by tax authorities in tracking and monitoring e-commerce transactions, particularly those involving cross-border sales.

F.2.3.1 Red Flag Indicators

Several red flags can indicate fraud in e-commerce transactions. First, be wary of any sellers who demand payment through non-traceable methods such as wire transfers, gift cards, or crypto currency. These methods make it difficult to track the transaction and can be a red flag for fraud.

Second, be careful when bumping into sellers offering goods at prices significantly lower than market value. This can be a sign that the product is counterfeit or that the seller is attempting to scam the buyer by taking their money without delivering the product.

Third, check the reviews and feedback. If they have a high number of negative reviews, this may be a sign that they aren't a legitimate seller and that the buyer is likely to encounter issues with the transaction.

Finally, if the seller is unresponsive or refuses to provide information about the product or shipping, this can be a sign of fraudulent activity. Legitimate sellers will happily answer any questions or at least provide additional details about the item and the transaction.

F.2.3.2 Compliance Requirements regarding E-commerce Related Money Laundering

As ecommerce continues to grow in popularity, so will the threats it faces, from ecommerce fraud to money laundering. They no longer have the option of ignoring the dangers, hoping it won't affect them, as every business faces the real danger of becoming a victim. This is why the banks should take precaution and carry on ongoing monitoring of the transaction of e-commerce businesses.

- **Screening and Ongoing Monitoring**

Screening and ongoing monitoring can significantly aid e-commerce platforms in mitigating risks and preventing fraudulent activities in real-time. By regularly checking customer behavior, platforms can detect and flag suspicious users and automatically detect unusual patterns or high-risk customers. This enables e-commerce marketplaces to take action and deter fraud easier, no matter the stage of the relationship with the customer. Additionally, ongoing screening and monitoring can help e-commerce platforms maintain compliance with AML and other regulatory requirements, thus helping minimize legal risks and reputational damage.

- **Customer Due Diligence**

The banks need to compliance with the directions of the regulatory bodies and carry out proper due diligence in dealing business with the e-commerce businesses

- **Employee awareness and training**

Employees are one of the biggest elements in any institution, and they can help to fight against criminals and fraudsters. Educating and training them about recognizing signs and red flags connected with money laundering and what to do when they encounter it will significantly increase the chances to identify any fraudulent or suspicious activities.

F.3 Money Laundering in the New Payment Method (NPM)

Anonymity, high negotiability and utility of funds as well as global access to cash through ATMs are some of the major factors that can add to the attractiveness of NPMs for money launderers. Anonymity can be reached either "directly" by making use of truly anonymous products (i.e., without any customer identification) or "indirectly" by abusing personalized products (i.e., circumvention of verification measures by using fake or stolen identities, or using strawmen or nominees etc.). In a report titled 'Money Laundering Using New Payment Method', FATF has identified three main typologies related to the misuse of NPMs for money laundering and terrorist financing purposes which are as follows:

• Third party funding (including straw men and nominees).

• Exploitation of the non-face-to-face nature of NPM accounts.

• Complicit NPM providers or their employees

The money laundering (ML) and terrorist financing (TF) risks posed by NPMs can be effectively mitigated by several countermeasures taken by NPM service providers. Obviously, anonymity as a risk factor could be mitigated by implementing robust identification and verification procedures. But even in the absence of such procedures, the risk posed by an anonymous product can be effectively mitigated by other measures such as imposing value limits (i.e., limits on transaction amounts or frequency) or implementing strict monitoring systems. For this reason, all risk factors and risk mitigants should be taken into account when assessing the overall risk of a given individual NPM product or service

F.3.1 Prepaid Cards

In the twenty-first century, prepaid cards have become part and parcel of human life. It was first available in the 1990s, but it only recently gained mainstream popularity when people started using it to pay bills and online shop. Researchers suggest that the net worth of the prepaid cards market will grow to more than USD 3.1 Trillion by 2021. This volume makes prepaid cards interesting for criminals and prepaid card money laundering.

On the one hand, these prepaid cards have made the lives of consumers and the general masses very easy by making the bill payment and other payments easy. On the other hand, this technology has facilitated criminal fraud and prepaid card money laundering.

F.3.1.1 Money Laundering through Prepaid Cards

Prepaid cards facilitate users to buy any product from anywhere and from any outlet. They also assist them in sending the purchased product anywhere. They are using this facility to send and transfer illegal funds to different parts of the world. The criminals are using Prepaid cards in the placement, layering, and integration phases of money laundering.

F.3.1.1.1 Prepaid Card Money Laundering Stages

Prepaid cards are used by criminals in each of the money laundering stages, including placement, layering, and integration.

1) Placement

The criminals use their illegal funds to purchase a bulk of prepaid cards. They are also using them to clean their black money. They use their cards to buy products to introduce their money into the legal financial system. Hence, in this way, they clean their illegal black money. In addition, they are also transporting these cards from one country to another country to deceive scrutiny from the relevant authorities. These criminals are also using money mules to buy and sell these Prepaid cards to transport the illegal money from one place to other, even across the borders.

2) Layering

Layering is a crucial stage in money laundering. In this phase, the launderer uses their money to buy expensive items and resell them again. They do it many times to hide the origin and source of the funds. This step is called layering. The criminals also use prepaid cards to buy expensive items such as laptops and resell them to hide the source. In this way, the criminals are using prepaid cards as a currency.

3) Integration

This is the last stage in money laundering. In this phase, the launderer uses the illegal money to buy expensive items for themselves. In this way, criminals integrate illicit cash into the country's financial system. In this context, criminals use prepaid cards to buy legitimate goods and services such as expensive electronic items, drug manufacturing components, and insurance products.

F.3.1.2 Features That Make Prepaid Cards Prone to Money Laundering

Some of the main prepaid card features that criminals exploit to do money laundering and frauds are as under:

1) Anonymity

Unlike other credit card cards, prepaid cards do not require strict customers due to diligence verification and identification. The criminals are taking advantage of this feature. They are using it to buy goods and services to integrate illegal money into the financial system.

2) Global Reach

Using Prepaid cards, one can buy anything from anywhere at any time. This allows criminals to purchase goods and services using their illegal money from any part of the world. These prepaid cards can even be used to fund unlawful activity in any part of the world.

3) Portability

Transferring a bulk of the money from one part of the world to another part of the world is complex and even impossible. However, a small prepaid card is very easy to transport from one part of the world to other. So, criminals are using this card to send money across the border.

4) Funding Methods

The transaction history of the prepaid cards can be hidden easily. It is difficult to find out the source fund loaded into the card. Funds can be transferred to prepaid cards using different mediums such as phone and online banking.

F.3.1.3 Red Flags Indicators regarding Prepaid Cards

1. When a customer holds an excessive number of cards (according to program parameters)
2. An unwilling customer refuses to provide the information the CIP requires
3. Customers who present unusual or suspect identification documents that the financial institution is unable to validate
4. Customers who request that cards be shipped outside of the country
5. Tax identification numbers for customers with variations in their names may be used
6. In response to notification of mandatory reporting, a customer is reluctant to provide the information required or to proceed with the transaction

7. Coerce or attempt to coerce an employee of a bank to not file the required recordkeeping or reporting documents
8. Withdrawals in small amounts followed by large deposits in foreign currency
9. The use of multiple value loadings at different locations by the same Cardholder
10. An unusually large number of authorizations fail
11. Authorizations appearing on the card account but not associated with the transactions
12. When transactions occur simultaneously in multiple states or countries
13. Transactions that occur at the same time and for the same amount week after week
14. Transactions that consistently occur outside of the Cardholder's area of residence
15. No logical explanation for transactions
16. Transactions that are out of character for the Cardholder
17. Multiple transactions slightly beneath reporting thresholds
18. Clients buying many Prepaid cards or making a bulk of transactions using prepaid cards are considered suspicious.
19. A single person holding multiple prepaid accounts also triggers a red flag.
20. Frequent loading of the prepaid card by a third party also reflects the suspicious transaction.
21. Loading funds more than the threshold is also questionable and need to be looked at it carefully.
22. Transferring funds soon after loading is also suspicious.
23. Abnormal purchasing power and pattern is also doubtful.
24. Sending prepaid cards to the recipient through an irrelevant person is also doubtful.
25. Prepaid card only using for cash withdrawal is also suspicious.

F.3.1.4 AML/CFT Due Diligence Measures

There are a number of measures in place to prevent and detect money laundering activities involving prepaid cards. Some of these measures include:

- Customer due diligence (CDD): Financial institutions are required to gather information about the customer and verify their identity to prevent anonymous usage of prepaid cards.
- Monitoring of transactions: Financial institutions continuously monitor transactions for unusual or suspicious activities, such as large transactions or transactions to high-risk countries.
- Reporting: Financial institutions are required to report suspicious transactions to BFIU.
- Sanction Screenign: Financial institutions use blocklists to prevent transactions with sanctioned individuals, entities, and countries.

- Enhanced Due Diligence (EDD): Financial institutions are required to perform enhanced due diligence on high-risk customers and transactions, such as those to high-risk countries.

By implementing these measures, financial institutions can help prevent and detect money laundering activities involving prepaid cards. However, it is important to note that money launderers are constantly finding new ways to evade these measures, so it is crucial for financial institutions to stay vigilant and continuously update their AML procedures.

F.3.2 Mobile Banking

Mobile money systems can be abused to launder money in a similar way to bank accounts. A person can easily and quickly set up multiple different accounts under their own or false names and transfer money between them to throw investigators off the track. Bangladesh is playing a flagship role in leveraging mobile financial services to provide access to formal financial services to vulnerable segments of the society such as the rural poor, women and Forcibly Displaced Persons (FDPs). However, like many other countries, Bangladesh is also experiencing misuse of Mobile Financial Services (MFS) for criminal purposes that can deter broader financial inclusion. Early detection of potential risks and vulnerabilities are essential for timely intervention.

F.3.3 Internet based Services

Criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. As the Internet becomes more and more a worldwide phenomenon, commercial websites and Internet payment systems are potentially subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist group. The Internet opened up the world of e-commerce and led to the development of various types of Internet-based payment services which emerged in the late 1990s to intermediate between online buyers and sellers (P2B) and for personal transfers (P2P) transactions. During the last decade, financial institutions and retailers have continued to develop electronic payment instruments which use the Internet and are available to a wide range of consumers. Internet-based payment services provide mechanisms for customers to access, via the Internet, pre-funded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which also hold accounts with the same provider. The recipient then redeems the value from the issuer by making payments or withdrawing the funds. Withdrawals occur by transferring the funds to a regular bank account, a prepaid card, or another money or value transfer service. While typically customers hold funds in pre-paid accounts, customers are not required to do so. When the account needs to be funded, this can happen with a debit from a bank account or payment card account, or supplied via another funding source as needed.

Many Internet-based payment services use a variety of business models. These services are referred to as digital wallets, digital currencies, virtual currencies, or electronic money. Internet- based payment services can vary significantly in their functionality, structure and procedures. Services may allow individuals to transfer to any individual or business subscribed to the service, or they may limit transactions to a particular merchant or online environment. Internet-based payment services may also be interconnected with other payment methods such as prepaid cards.

Another common form of Internet-based payment service is digital currency providers that sell a digital representation of precious metals online. These service providers sell virtual gold or silver at market prices, claiming to hold actual precious metals on behalf of the customer.

Pre-funded accounts that consumers use for online auction payments are among the most dominant Internet-based payment services. Recipients may or may not be required to register with the payment service provider to receive a funds transfer. Customers may pre-fund an Internet- based payment account using a regular bank account. The funds in the Internet-based payment account can be used for transfers to other customers of the same provider, or transferred back to the customer's regular bank account.

Internet-based payment services may also be associated with online gambling or virtual worlds for which only a proprietary form of currency can be used to conduct transactions. Participants hold the proxy currency in an account, using the funds for transactions with the proprietor, other participants or retailers in the closed online environment. Recipients of the proprietary currency can exchange it for their national currency on exiting the environment.

Sample Questions:

1) What are the requirements of FATF under Recommesntion-15 for new technology? Define VA and VASPs.
2) Mention some common new technology based financial product and ML&TF risk associated with those products.
3) Write down the vulnerabilities of e-commerce sites in money laundering. Mention some red flags related with e-commerce business.
4) Why the new payment methods are very prone to money laundering. Explain with example.
5) Mention some features pre-paid card those may be helpful for money laundering.
6) How money laundering using prepaid card can be identified? Explain with some red flags and examples>

Module-G: Compliance

G.1 Concept of Compliance

In a general sense, compliance *means abiding by a set of rules.* AML/CFT Compliance in the financial sector refers to the compliance where the financial institution adheres to the applicable rules, regulations and instructions set out by the regulatory bodies. This includes both country specific laws and requirements from the regulatory authorities as well as internal company directives. A range of tools and process can be implemented and used by an institution to bring about good compliance. They are designed to ensure that misconduct or violations can be detected, prevented or resolved at an early stage, ahead of any serious consequences such as criminal prosecution, fines or severe damage to a financial institution's reputation. AML/CFT compliance, when effectively implemented, mitigate the adverse effects of criminal economic activity and promote integrity and stability in financial markets.

FATF sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system and urges the countries to comply with them. In line with those standards, in reviewing the ML/TF risk and threats, the countries set AML/CFT related laws and regulations, establish AML/CFT mechanism and regulatory bodies to effectively combat the ML & TF.

G.2 Compliance Risk

Compliance risk is an organization's potential exposure to legal penalties, financial forfeiture and material loss, resulting from its failure to act in accordance with industry laws and regulations, internal policies or prescribed best practices. Compliance risk is also known as *integrity risk*.

Compliance with the AML/CFT regulations, international standards, instructions of BFIU, the central agency to combat money laundering and terrorist financing in Bangladesh, are very crucial for the banking sector to safeguard the integrity of financial systems and their business. Failure to comply with these regulations can have severe consequences for individuals, businesses, and financial institutions raises non-compliance risk in this sector.

Non-compliance with AML and CFT regulations carries severe consequences for individuals, businesses, and financial institutions. The legal, reputational, and financial repercussions can be debilitating, jeopardizing the very existence of non-compliant entities. It is imperative for organizations and individuals to understand and fulfil their obligations under these regulations to mitigate the risks associated with non-compliance. Adhering to AML and KYC requirements not

only ensures legal and ethical conduct but also helps maintain the integrity of the global financial system. Potential compliance risks in the financial sector are described briefly below:

- **Legal consequences**

Banks found to be failing to comply with AML and CFT regulations are at risk of substantial legal repercussions. Governments worldwide have established stringent laws and penalties to deter money laundering and ensure transparency in financial transactions. Entities found in violation of AML regulations may face hefty fines, civil or criminal charges, and reputational damage. In some jurisdictions, individuals responsible for non-compliance could even face imprisonment.

- **Reputational damage**

Failure to comply with AML and CFT regulations can result in severe reputational damage for businesses and individuals alike. In today's interconnected world, news of non-compliance spreads rapidly, eroding trust and confidence in the firm involved. The public, stakeholders, and clients may perceive non-compliant entities as untrustworthy, leading to a loss of business relationships, customers, and opportunities.

- **Financial losses**

Non-compliance can lead to significant financial losses for businesses. Regulatory authorities have the power to impose substantial fines and penalties, often amounting to millions or even billions of dollars. Such financial burdens can strain the resources of organizations, leading to customer retention or acquisition issues, diminished profitability, and, in extreme cases, bankruptcy. Financial institutions may also face restrictions on their operations or be barred from certain markets due to non-compliance.

- **Restricted access to financial services**

AML and CFT regulations require financial institutions to adhere to strict due diligence measures. Failure to comply with these requirements can result in restricted access to financial services, including banking facilities, payment processing, and investment opportunities. Entities found to be non-compliant may face account closures, transaction limitations, or even being blacklisted by other financial institutions, effectively cutting them off from the mainstream financial system.

- **International sanctions**

Non-compliance with AML and CFT regulations can trigger international sanctions and restrictions. Global regulatory bodies actively collaborate across borders to combat money

laundering and terrorist financing, and, as such, entities found to be non-compliant may face restrictions on cross-border transactions, freezes on assets, and limitations on trade activities. These sanctions can have far-reaching effects on an entity's operations and ability to conduct business globally.

- **Loss of regulatory trust and increased scrutiny**

Persistent non-compliance with AML and CFT regulations can result in a loss of trust from regulatory bodies. This loss of trust leads to increased scrutiny and monitoring by authorities, who may impose stricter reporting requirements, audits, and inspections. Financial institutions found to have systemic non-compliance may be subject to enhanced supervision, such as on-site examinations or the appointment of external auditors. This heightened regulatory scrutiny can disrupt normal business operations and increase compliance costs.

G.2.1 Compliance Risk Management

Compliance risk management is the process of identifying, assessing and mitigating potential losses that may arise from an financial institutions' noncompliance with laws, regulations, standards, and both internal and external policies and procedures. It is a continuous process that involves tracking changes in the regulatory environment to ensure an organization's compliance is up to date.

G.2.2 Identifying and Managing Compliance Risk

A key concept of compliance risk management is the risk assessment process, which includes identifying and evaluating the potential risks that threaten an organization's ability to ensure it is compliant with laws and regulations. Risk assessment can include reviewing information sources, such as reports from the institution's management and from regulatory bodies, BFIU as well as identifying data and information that is already available to the organization.

Following a compliance risk assessment, a bank can determine its level of compliance to reveal what changes need to be made for improvement. A bank uses this information to create and implement a compliance risk management strategy that helps ensure it is in compliance with laws. For example, the assessment might reveal that a bank requires to providing AML/CFT training to its employee to raise awareness among them and for better compliance with BFIU's instruction. Then they can address this weakness by arranging training programs for its employees.

Six key steps to help banks adapt right risk management to the ever-changing criminal and regulatory landscape

One, Conduct a risk assessment based on the bank's products, services, geographies and clients to better understand the threat environment.

Two, Integrate the efforts of various disciplines involved in financial crime prevention across the organization to identify synergies and overlaps in people, processes and technologies; this will help reduce redundancies and streamline processes.

Three, Improve the availability and quality of data to support real-time transaction monitoring and advanced analytics.

Four, Apply advanced analytics to gain a holistic view of threats and the entities that cause them; this will help uncover complex and subtle threats, as well as emerging ones, early and effectively.

Five, Nurture a culture of high ethics and integrity by setting accountability standards, establishing controls and policies, working closely with regulators and increasing employee awareness.

Six, Actively participate in the industry-wide initiatives undertaken to mitigate risk and improve compliance.

Source: Continzent, 2016

G.2.2.1 Assessing Risk-Risk Based Approach

The banks shall have to follow Risk Based Approach in determining and assessing compliance risk. Every bank shall assess its risk relating to money laundering and terrorist financing periodically following the instruction of 'ML/TF Risk Assessment Guidelines for Banking Sector' issued by BFIU. Nature of business, customer, product or service, country and geographical position etc. shall be considered at the time assessing such risk. The aforesaid Risk Assessment Report shall be used in preventing money laundering and terrorist financing risk of the bank.

Bank shall have to take Enhanced Due Diligence (EDD) measures for high risk identified in the Risk Assessment Report on money laundering, terrorist and terrorist financing.

Bank can take Simplified Due Diligence (SDD) measures for low risk or similar indicator of low risk identified in the Risk Assessment Report on money laundering, terrorist and terrorist financing.

Every bank shall take necessary Due Diligence measures in line with the risk, importance and relevance of existing customer. Apart from this, bank shall fix the time for taking or reviewing Due Diligence measures for existing customer considering the time when the Due Diligence measures was taken and what kind of or what amount of information was collected previously.

G.2.3 Assessing Inherent and Residual Risk

G.2.3.1 What is Inherent Risk?

Inherent risk is the level of risk associated with a product, customer, channel, or country without any mitigation controls in place. This means that inherent risk is the level of risk any organization faces if does not implement any measures to prevent money laundering and terrorism financing.

The inherent risk is determined based on various factors, such as the nature of the product or service the organization offer, customer's background, the channel used to deliver the product or service, and the country of origin. By assessing these factors, the organization can determine the level of risk associated with each area of the business and develop appropriate risk mitigation measures. For example, if any bank offers a high-value loan product, this may pose a higher inherent risk of money laundering than a low-value savings account. Similarly, customers from high-risk jurisdictions or with a history of financial crimes pose a higher inherent risk than those with a clean financial record.

Understanding inherent risk is crucial for developing effective risk mitigation measures to prevent financial crimes. By identifying the level of inherent risk associated with each area of the business, the reporting organization need to implement appropriate measures to manage those risks effectively. This will help the business from being exploited by criminals and comply with regulatory requirements.

G.2.3.1.1 Mitigation Controls for Inherent Risk

Mitigation controls are an essential part of an effective ML/TF risk management program. They are measures that an RO need to implement to reduce the risk of money laundering and terrorism financing in its business or organization. Mitigation controls are policies, procedures, and systems designed to detect and prevent financial crimes. There are several types of mitigation controls. Here are some examples:

- Know Your Customer (KYC) procedures: This involves verifying the identity of customers and understanding their business activities to assess the potential for money laundering or terrorism financing.

- Enhanced due diligence: This involves collecting more detailed information about high-risk customers or transactions to assess their potential for money laundering or terrorism financing.
- Transaction monitoring: This involves reviewing transactions for suspicious activity and unusual patterns, such as large or frequent transactions.
- Staff training: This involves educating staff on the risks associated with money laundering and terrorism financing, as well as how to identify and report suspicious activity.
- Customer screening involves screening customers against sanctions lists and other databases to identify any links to money laundering or terrorism financing.

Implementing these types of mitigation controls can help reducing the risk of money laundering and terrorism financing in your business or organization. They can also help to comply with regulatory requirements and protect your reputation. Regular review and updating of the mitigation controls need to be ensured so that they remain effective and up-to-date with any changes in business or industry.

G.2.3.2 What is residual risk?

Residual risk is the level of risk that remains after implementing mitigation controls. It is calculated by subtracting the effectiveness of the mitigation controls from the inherent risk. This means that residual risk is the level of risk that an organization is willing to accept after putting in place measures to prevent money laundering and terrorism financing.

Thus, a classic residual risk formula might look something like this:

Residual risk = inherent risk - impact of risk controls

As an example, consider a risk analysis of a ransomware outbreak in a specific business unit. The organization concludes that, in a perfect storm scenario, the inherent risk associated with the outbreak -- i.e., the risk present without any controls or other countermeasures applied or implemented -- could be $5 million. With new malware detection and prevention controls, as well as an additional emphasis on backups and redundancy, the organization estimates that recovery from ransomware is possible in almost all cases without paying a ransom and waiting for decryption. The cost of all solutions and controls is $3 million.

The residual risk formula would then look like this:

Residual risk = $5 million (inherent risk) - $3 million (impact of risk controls)

In this case, the residual, or leftover, risk is roughly $2 million.

Calculating residual risk is essential for determining whether the mitigation controls that have implemented are effective. If the residual risk is too high, the organization needs to implement additional mitigation controls or adjust the existing controls to reduce the level of risk.

For example, if the inherent risk associated with a high-value loan product is high, then a bank may implement enhanced due diligence and transaction monitoring as mitigation controls. After implementing these controls, the bank needs to calculate the residual risk and find that it is still high. This may indicate that the bank's mitigation controls are not effective enough, and it needs to implement additional measures to manage the risk effectively.

G.2.3.2.1 Managing Residual Risk

For any residual risk present, organizations can do the following:

- **Nothing.** Assuming the residual risk is below the acceptable level of risk in any endeavor, organizations can simply accept that the implemented controls have proven effective *enough* to reduce the risk to an acceptable level.
- **Update or increase controls implemented.** In the case that residual risk is still above an acceptable risk level, new or modified controls and processes may be needed to reduce the inherent risk to a level that is deemed acceptable.
- **Evaluate controls vs. mitigation costs to make a decision.** In the case where the residual risk is still beyond the acceptable level of risk and the cost of the needed controls and countermeasures is too high, organizations may need to accept the risk, regardless of what residual risk remains.

In general, when addressing residual risk, organizations should follow the following steps:

1. Identify relevant governance, ML & TF risk and AML/CFT compliance requirements
2. Determine the strengths and weaknesses of the organization's AML/CFT compliance and internal control framework.
3. Acknowledge existing risks.
4. Define the organization's risk appetite.
5. Identify available options for offsetting unacceptable residual risks.

G.3 Compliance Policies and Governance

The Compliance Policy aims at managing compliance risk and also oversees its implementation besides ensuring that compliance issues are resolved effectively and expeditiously with the assistance of compliance Committee and Compliance Officers. Each bank shall have a compliance

policy in place approved by the board of directors (BOD) The main objective of a bank's compliance policy should cover-

- To introduce, standards and procedures relating to compliance functions, which are in line with international and national practices.
- To propagate Compliance Function as an integral part of Governance, Internal Control and Risk Management Process.
- To enlighten all constituents for initiating preventive measures for mitigating compliance risk. To prevent Material Financial Loss or Loss to Reputation, which Bank may suffer owing to failure to comply with Laws, Regulations, Rules, Relating to Regulatory Organizations; Standards and Code of Conducts applicable to Banking Activity.
- To Frame bank-wide compliance functions, which would help Senior Management and the Board of Directors in recognizing the legal and reputation risks in the Bank which required to be monitored for mitigating compliance risk.
- To introduce a healthy compliance culture within the organization so that compliance functions are effectively complied with.

The compliance function is an integral part of governance of a bank in consonance with the internal control. The significance of compliance function lies in identifying, evaluating and addressing legal and reputational risks. It has to ensure strict observance of all statutory guidelines issued by BFIU and Bangladesh Bank.

G.3.1 Regulatory Compliance

Regulatory compliance describes the goal that an institution aspires to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations. Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls.

On the initiative of BFIU, self-assessment and independent testing procedure system were introduced for banks to assess their own AML/CFT compliance. Side by side, Bangladesh Bank (BB) has also been monitoring the same through the process called system check inspection.

As per the instruction of the BB, banks must have a risk management unit to take care of different risks of the banking operation. Various risk related guidelines are available in Bangladesh that includes discussion on issues related to risk management especially operational risk management in banks. These guidelines are mostly issued by Bangladesh Bank. Some of the guidelines are Internal Control and Compliance (ICC), Self-Assessment of Anti-fraud Internal Controls, Guidance Note on Prevention of Money Laundering, Risk Management Guidelines for Banks, Guideline on

ICT Security, Guideline on Risk Based Capital Adequacy (RBCA), Credit Risk Management Guideline, Foreign Exchange Risk Management Guideline, Asset Liability Risk Management Guideline, Guidelines on Mobile Financial Services, Note Refund Regulations, Bank Deposit Insurance Scheme, etc. The objectives of these guidelines are to protect various internal and external frauds, to prevent different financial crime related to credit, foreign exchange, money laundering, IT security etc. Security of Information for banks has gained much importance and it is vital now to ensure that the risks are properly identified and managed. As noted by the BB, the guideline on ICT Security is to be used as a minimum requirement and as appropriate to the level of technology adoption of their operations.

G.3.2 AML & CFT Compliance Program

G.3.2.1 Introduction

National ML & TF risk assessment suggests that banking sector is one of the most vulnerable sectors for the ML & TF among the financial sectors due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership. Banks can play a vital role in preventing ML, TF & PF and in this regard, their roles and responsibilities are delineated in MLPA, 2012, ATA, 2009 and rules and instructions issued under this legal framework by BFIU. To prevent ML, TF & PF and to ensure the implementation of required provisions of Acts, Rules and directives of BFIU, every bank should develop and maintain an effective AML and CFT compliance program. This should cover at least senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

G.3.2.2 Components of AML & CFT Compliance Program

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

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

2. Internal policies, procedure and controls- it should include Bank's AML & CFT policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, self assessment, independent testing procedure, employee screening, record keeping and reporting to BFIU;

3. Compliance structure includes establishment of Central Compliance Committee (CCC), appointment of Chief Anti-money Laundering Compliance Officer (CAMLCO), Branch Anti-money Laundering Compliance Officer (BAMLCO);

4. Independent audit function- it includes the role and responsibilities of internal audit on AML & CFT compliance and external audit function;

5. Awareness building program includes training, workshop, seminar for banks employees, member of the board of directors, owners and above all for the customers on AML & CFT issues.

G.3.2.3 Development of Bank's AML & CFT Compliance Program

In developing its own AML & CFT compliance program, bank may consider any relevant document including relevant guidelines issued by BFIU. The bank should also consider all relevant laws, regulations, guidelines relating to AML & CFT and also the practices related to corporate governance. In drafting the compliance program, a bank should involve all its relevant departments or divisions like general banking, credit, foreign exchange, information technology, international division, alternative delivery channels, internal audit and compliance and above all central compliance unit. Their involvement should be documented or reflected in the compliance program. Proper attention should be given to the size and range of activities, complexity of operations, customer base, and use of technology, diversity of product, delivery channel, external linkage, geographic location and the output of ML & TF risk assessment of every bank. Banks can use Bengali and/or English language in drafting compliance program. If the compliance program developed in English then banks may develop a Bangla version of it to make it more communicative.

G.3.2.4 Communication of Compliance Program

Bank should communicate their compliance program immediately after the approval from the board of directors or from the highest authority to all of its employees, member of the board of the directors and other relevant stakeholders at home and abroad. The individual bank should select the proper channel that is the best suited to them to communicate with the compliance program. The bank also should upload the compliance program in their website for their customers or other stakeholders.

G.3.2.5 Role of Senior Management

For the purposes of preventing ML, TF & PF, senior management includes members of the board of directors of the bank, or the member of the highest management committee in absence of the board of directors and the Chief Executive Officer (CEO) or the Managing Director (MD) of the

bank. The role of senior management has been delineated in Anti Terrorism Act (ATA), 2009 and BFIU circular No-26 issued on 16 January 2020.

Obligations under ATA 2009: The Board of Directors, or in the absence of the Board of Directors, the Chief Executive of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by BFIU under section 15 of ATA, which are applicable to the reporting agency, have been complied with or not.

Obligations under BFIU Circular (Circular-26; dated- 16 June 2020): All banks must have their own policy manual that must conform international standards, laws and regulations in force in Bangladesh and instructions of BFIU on preventing money laundering and terrorist financing, and this policy manual must be approved by their Board of Directors or by the highest management committee, where applicable. This policy manual shall be communicated to all concerned persons. Banks shall conduct review of the policy manual from time to time and shall amend/change where necessary. The chief executive of the bank shall announce effective and specific commitment, give the necessary instructions to fulfill the commitments in preventing ML & TF to all the employees of all branches, agent offices, regional offices and the head office and shall ensure the implementation of the commitments. This statement of commitment shall be issued in every year. Statement of commitment of CEO or MD of a bank should include the followings-

- Banks policy or strategy to prevent ML, TF & PF; Emphasize on effective implementation of bank's AML & CFT compliance program;
- Clear indication of balance between business and compliance, risk and mitigating measures; Compliance is the responsibility of each employee during their normal course of assignment and ignorance shall not be considered as the excuse for non-compliance;
- Point of contact for clarification in case of any ambiguity arise; Consequences of non-compliance as per human resources (HR) policy of the bank.

In summary, the Board of Directors (BoD) or Highest Management committee (in absence of BoD) shall-approve AML & CFT compliance program and ensure its implementation; issue directives to ensure compliance with the instruction of BFIU issued under section 23 of MLPA 2012 and section 15 of ATA, 2009; take reasonable measures through analyzing self assessment report and independent testing report summary; understand ML & TF risk of the bank, take measures to mitigate those risk; CEO or/and MD shall issue statement of commitment to prevent ML, TF & PF in the bank; Ensure compliance of AML & CFT program; Allocate enough human and other logistics to effective implementation of AML & CFT compliance program. Senior management must convey a clear signal that the corporate culture is as concerned about its reputation as it is

about profits, marketing, and customer service. Senior management should take the report from the Central Compliance Committee (CCC) into consideration which will assess the operation and effectiveness of the bank's systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner. Senior management of a bank should adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the bank. Bank's HR Policy should include at least following issues for proper implementation of AML &CFT measures:

- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- Proper weight should be given in the annual performance evaluation of employees for extra ordinary preventive action vis a vis for non-compliance;
- Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;
- Other measures that shall be taken in case of non-compliance by the bank.

G.3.2.6 Policies and Procedures

An AML & CFT policy usually includes the 4 (four) key elements; they are –

- High level summary of key controls;
- Objective of the policy (e.g. to protect the reputation of the institution);
- Scope of the policy (A statement confirming that the AML/CFT policy applies to all areas of the business); and
- Waivers and exceptions- procedures for obtaining exemptions from any aspects of the policy should be carefully controlled; and Operational controls.

(a) Written AML & CFT Compliance Policy

At a minimum, the board of directors or the management committee of each bank must develop, administer, and maintain an AML & CFT compliance policy that ensures and monitors compliance with the Acts, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes. The written AML&CFT compliance policy at a minimum should establish clear responsibilities and accountabilities within their organizations to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the law. The Policies should be tailored to the bank and would have to be based upon an assessment of the money laundering and terrorist financing risks, taking into account the

bank's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering and terrorist financing. It should include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures should address its Know Your Customer ("KYC") policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transactions, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness. It should also include a description of the roles the AML&CFT Compliance Officers(s)/Committee and other appropriate personnel will play in monitoring compliance with and effectiveness of AML&CFT policies and procedures. It should develop and implement screening programs to ensure high standards when hiring employees. It should also implement standards for employees who consistently fail to perform in accordance with an AML&CFT framework. It should incorporate AML&CFT compliance into job descriptions and performance evaluations of appropriate personnel. It should have the arrangements for program continuity despite changes in management or employee composition or structure. The AML&CFT policies should be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing AML&CFT related rules and regulations or business. In addition the policy should emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and should set forth the consequence of non-compliance with the applicable laws and the institution's policy including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any bank with money laundering and terrorist financing activity.

(b) **Procedures**

The standard operating procedures are often designed at a lower level in the organization and modified as needed to reflect the changes in products, personnel and promotions, and other day to day operating procedures. The procedure will be more detailed than policies. Standard operating procedures translate policy into an acceptable and working practice. In addition to policies and procedures, there should also be a process to support and facilitate effective implementation of procedures and that should be reviewed and updated regularly.

G.3.2.7 Customer Acceptance Policy

Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place to set-up any kind of business relationship with the bank. A concrete Customer Acceptance Policy is very important so that inadequate understanding of a customer's background and purpose

for utilizing a bank account or any other banking product/service may not expose the Bank to a number of risks. The primary objectives of a Customer Acceptance Policy are –

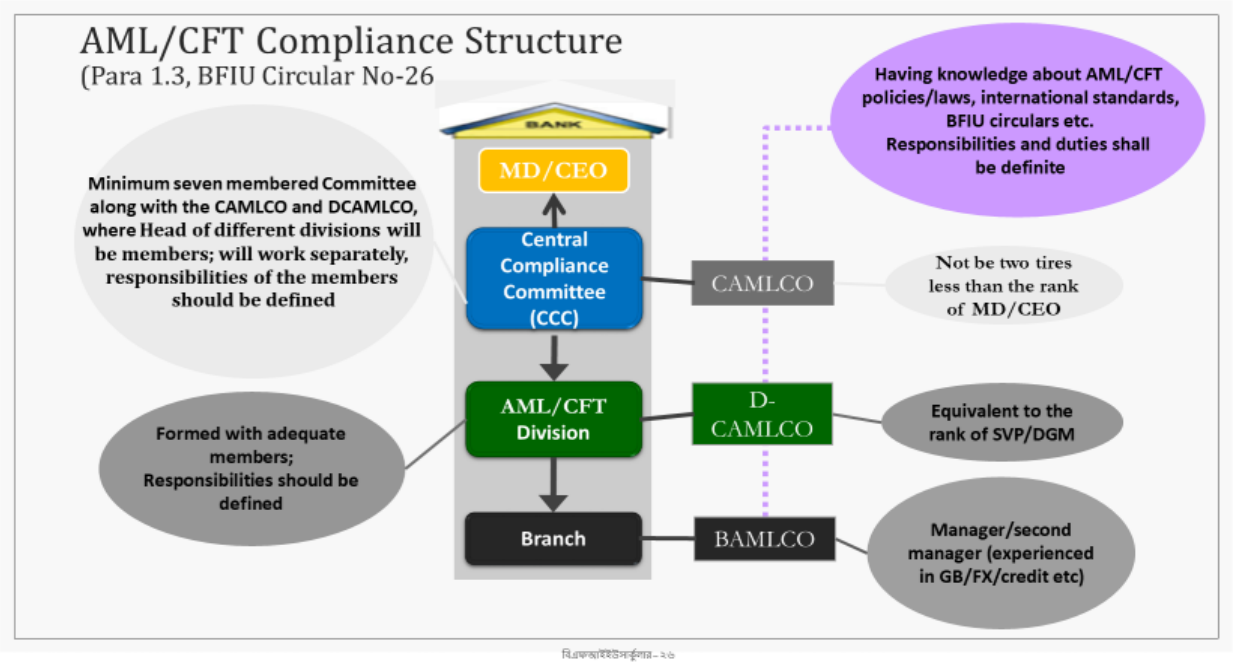
- to manage any risk that the services provided by the Bank may be exposed to;
- to prevent the Bank from being used, intentionally or unintentionally, for ML/TF purposes; and
- to identify customers who are likely to pose a higher than average risk.

The customer acceptance policy of bank should not be used against the disadvantaged people or the people who have not proper identification document. A customer acceptance policy should encourage the ultimate goal of transparent, accountable and inclusive financial system in Bangladesh. Banks need to ensure that they will accept only those customers whose appropriate identity is established by conducting due diligence to the risk profile of the client. Parameters of risk perception must be clearly defined in terms of 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 enable categorization of customers into different risk grade. Bank should not open an account where it is unable to apply appropriate customer due diligence measures i.e. if the bank is unable to verify the identity and/or obtain documents required as per with the risk categorization due to non cooperation of the customer bank will not open or allow withdrawal of money. Decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such decision. 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 banking 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. Necessary checks should be made before opening a new account so that the bank can ensure the identity of the customer does not match with any person with known criminal background or with proscribed entities such as individual terrorists or terrorist organizations etc. Customer acceptance policy of a bank must include-

- No account in anonymous or fictitious name or account only with numbers shall be opened;
- No banking relationship shall be established with a Shell Bank; and
- No account in the name of any person or entity listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance adopted under Chapter VII of the Carter of UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government shall be opened or operated.

G.3 Compliance Structure of a Bank

Compliance structure of a bank is an organizational setup that deals with AML & CFT compliance of the bank and the reporting procedure. This includes- Central Compliance Committee (CCC), Anti Money Laundering and Terrorism Financing Department, Branch Anti-Money Laundering Compliance Officer (BAMLCO).



G.3.1 Central Compliance Committee

To keep the banking sector free from the risks related to Money Laundering & Terrorist Financing and for the effective/proper compliance of all existing acts, rules and issued instructions by BFIU time to time, every bank should set up a Central Compliance Committee (CCC) that will be directly monitored by the Managing Director or the Chief Executive Officer of the bank. The central compliance unit must be headed by a high official, who will be known as the Chief Anti Money Laundering Compliance Officer (CAMLCO). In this case, designation of the 'Higher Official' shall not be lower than two steps from the Managing Director/Chief Executive Officer of the bank. In case of foreign bank, the said 'Higher Official' must be a member of Top Management Committee. Before assigning the CAMLCO to other duties of the bank, the management has to ensure that the AML & CFT activities of the bank will not be hampered.

G.3.1.1 Formation of CCC

Central Compliance Committee shall be comprised of at least 7 members; where the head or higher officials from different departments of the bank (e.g: Human Resource Division, Credit Division, Retail and Corporate Banking Division, Foreign Exchange Division, Operation Division, Card Division, IT Division etc or similar divisions) including CAMLCO and DCAMLCO will be the

members. But, any official from Internal Audit Department cannot be the member of Central Compliance Committee. The Central Compliance Committee and the Internal Audit division shall perform the anti money laundering and combating terrorist financing related responsibilities bestowed on them as two completely separate entities. Central Compliance Committee shall arrange at least 4(four) meetings annually on quarterly basis. However, the committee can convene any meeting at any time when necessary. In that meeting, after assessing overall compliance status of the bank on anti-money laundering and combating terrorist financing, the committee shall take necessary decision and provide instructions to be followed.

G.3.1.2 Authorities and Responsibilities of the CCC

Central Compliance Committee shall formulate organizational strategy and program to prevent money laundering and terrorist financing in accordance with the own policy of the bank and will evaluate the same from time to time. Under the supervision of the Central Compliance Committee and the CAMLCO, 'Anti-Money Laundering and Terrorist Financing Department' will ensure the implementation of the program annually on the prevention of money laundering and terrorist financing. CCU is the prime mover of the bank for ensuring the compliance of AML & CFT measures. Its main responsibilities are to-

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

For shouldering these responsibilities bank authority may consider to give the following authority to CCC-

- appointment of BAMLCO and assign their specific job responsibilities;
- requisition of human resources and logistic supports for CCC
- make suggestion or administrative sanction for non-compliance by the employees.

The CCC shall arrange at least 4(four) meetings annually on quarterly basis. However, the committee can convene any meeting at any time when necessary. In that meeting, after assessing

overall compliance status of the bank on anti-money laundering and combating terrorist financing, the committee shall take necessary decision and provide instructions to be followed. The CCC shall submit Half-Yearly report (January-June, July-December), to the CEO and/or where necessary, to the Board of Directors for notification of and direction, containing the steps taken by the bank on combating Money Laundering and Terrorist Financing, its implementation progress and the recommendation in this regard. That report along with the instruction and opinion of Chief Executive Officer shall have to be presented then to the meeting of the Board of Directors or Higher Management Committee and a copy of the same report shall be submitted to BFIU within 2(two) months from the completion of half-year.

G.3.2 Duties and Responsibilities of CAMLCO

The CAMLCO is responsible for oversight of the bank's compliance with the regulatory requirements on systems and controls against money laundering and terrorist financing. CAMLCO should be able to act on his own authority.

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

G.3.3 Separation of CCU from Internal Control & Compliance (ICC)

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

G.3.4 Anti Money Laundering and Terrorism Financing Department/Division

To perform the secretarial duties of Central Compliance Committee and execute the activities for compliance on the prevention money laundering and terrorist financing, there shall be 'Anti-Money Laundering and Terrorist Financing Department' (whatever the name may be titled) with

adequate officials considering the number of branches, extent and periphery of business, number of customers and institutional risk etc. Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO) shall perform duties as the Head of the said department. Note that, an official no lower than the designation of 'Deputy General Manager' or 'Senior Vice President' can be appointed as DCAMLCO.

The CAMLCO and the DCAMLCO should have sound knowledge on existing laws, rules, instructions issued by BFIU from time to time and relevant international standards related to anti-money laundering and combating terrorist financing. Terms of reference of 'Anti Money Laundering and Terrorist Financing Department' and the duties and responsibilities of Central Compliance Committee, its members, the CAMLCO and the DCAMLCO shall have to be defined specifically.

As per the directives from Central Compliance Committee, 'Anti Money Laundering and Terrorist Financing Department' shall issue instructions to be followed by the branches; that will include the procedure for completing KYC, transaction monitoring arrangement, internal control arrangement and other policy and procedures to be followed to prevent money laundering and terrorist financing.

G.3.5 Compliance Program at Branch Level

Central Compliance Committee shall establish internal monitoring and control by nominating Compliance Officer at branch level. In this case, an experienced official on ML/TF issues shall be nominated as Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch. Note that, Branch Manager, second in command of the branch or experienced High Official of General Banking /Foreign Exchange/Credit Division etc. shall be nominated as BAMLCO. The BAMLCO shall have sound knowledge on anti money laundering and terrorist financing related existing acts, rules, instructions issued by BFIU and bank's own policy. Terms of reference and the roles and responsibilities of the BAMLCO shall have to be specified in his/her nomination letter.

The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and bank's own policies on preventing Money Laundering and Terrorist Financing. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her appointment letter. BAMLCO shall arrange AML & CFT meeting with other concerned important officials of the branch quarterly and shall take effective measures on the following matters after reviewing the compliance of the existing acts, rules and regulations, BFIU's instructions on preventing Money Laundering & Terrorist Financing:

- Know Your Customer,
- Transaction monitoring,

- Identifying and reporting of Suspicious Transactions,
- Record keeping,
- Training.

G.3.5.1 Authorities and Responsibilities of BAMLCO

For preventing ML, TF & PF in the branch, the BAMLCO should perform the following responsibilities:

- ensure that the KYC of all customers have done properly and for the new customer KYC is being done properly;
- ensure that the UN Security Council and domestic sanction list checked properly before opening of account and while making any international transaction;
- keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction;
- ensure regular transaction monitoring to find out any unusual transaction (In case of an automated bank, the bank should follow a triggering system against transaction profile or other suitable threshold. In case of a traditional bank, transaction should be examined at the end of day against transaction profile or other suitable threshold. Records of all transaction monitoring should be kept in the file);
- review cash transaction to find out any structuring;
- review of CTR to find out STR/SAR;
- ensure the checking of UN sanction list before making any foreign transaction;
- ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
- compile self-assessment of the branch regularly and arrange quarterly meeting regularly;
- accumulate the training records of branch officials and take initiatives including reporting to CCU, HR and training academy;
- ensure all the required information and document are submitted properly to CCC and any freeze order or stop payment order are implemented properly;
- follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
- ensure that the branch is maintaining AML & CFT files properly and record keeping is done
- ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB

G.3.6 Internal Control and Compliance

[NB. Discussed in Module-B]

G.3.6.1 Self-Assessment and Independent Testing Procedure (ITP)

With the goal of establishing an effective mechanism to prevent money laundering and terrorist financing, the Internal Audit Department of the bank has to be equipped with manpower who have sound knowledge on analyzing self-assessment reports received from branches and completing independent testing properly.

G.3.6.2 Responsibilities of the Branches

1) Every branch shall evaluate itself on half yearly basis based on the specified checklist for Self-Assessment as provided by BFIU.

2) Before finalizing the evaluation report, a meeting chaired by branch manager shall be conducted with the relevant officials. In that meeting, there shall be a discussion on the draft of branch evaluation report and if the issues identified accordingly cannot be resolved at branch level, it should be noted in the report and sent it to Internal Audit Department and Anti Money Laundering and Terrorist Financing Department to resolve them; and the progress of the recommendations for resolving the issues sent to Head Office shall be discussed in next quarterly meeting.

G.3.6.3 Responsibilities of Internal Audit Department:

1) Internal Audit Department shall verify the Branch Evaluation Reports and it shall arrange an inspection to the branch immediately if any risky issue is observed in any branch; and shall inform Anti Money Laundering and Terrorist Financing Department of this matter;

2) Internal Audit Department shall examine anti-money laundering and terrorist financing matters of the branch based on the specified checklist provided by BFIU for Independent Testing Procedures while conducting inspection/audit in different branches according to its own regular annual inspection/audit schedule; then it shall send a report determining its rating to the concerned branch. In addition to regular annual inspection/audit programs, Internal Audit Department shall conduct a separate inspection in at least 10% (ten percent) of the branches and examine anti money laundering and terrorist financing compliance issues of that branches based on the specified checklist for Independent Testing Procedures and shall formulate a report of the respective branch including its rating;

3) The Internal Audit Department shall send the copy of the report including rating of the inspected/audited branches to the Anti Money Laundering and Terrorist Financing Department; and

4) In case of the bank involved in agent banking business, Internal Audit Department shall conduct an inspection/audit on at least 5% (five percent) of the agents on yearly basis to review the compliance status of anti-money laundering and terrorist financing issues of the agents and shall send a copy of the report to Anti Money Laundering and Terrorist Financing Department.

G.3.6.4 Responsibilities of Anti Money Laundering and Terrorist Financing Department:

1) Based on the self-assessment report received from branches and inspection/audit reports submitted by Internal Audit Department, Anti Money Laundering and Terrorist Financing Department shall prepare a checklist-based evaluation report on the branches audited in that quarter. The report shall contain the following mandatory matters along with other issues:

    (a) Total number of branches and total number of self-assessment reports received from branches;

    (b) Number of branches inspected/audited by Internal Audit Department and the compliance status of the branch (based on the score received);

    (c) The report shall contain the measures taken by Anti Money Laundering and Terrorist Financing Department to prevent the irregularities mentioned in self-assessment reports that are similar in nature in many branches;

    (d) The report shall contain the general and exceptional irregularities described in the report submitted by Internal Audit Department and the measures taken by Anti Money Laundering and Terrorist Financing Department to prevent those irregularities; and

    (e) The report shall contain the measures taken to ensure compliance and improve rating of branches that are evaluated as "Unsatisfactory" and "Marginal" in the report received.

2) If any risky issue is identified in any branches after verifying the Self-Assessment Report received from branches then Anti Money Laundering and Terrorist Financing Department shall visit the branch immediately or arrange inspection through Internal Audit Department and bring this matter to the attention of appropriate authority.

G.3.7 External Auditor

External auditor may also plays an important role in reviewing the adequacy of AML & CFT controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External auditor would be risk-focus while developing their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits in its audit report.

Sample Questions:

1) What is compliance and compliance risk in a bank? How banks manage compliance risk?
2) What are the main responsibilities of Reporting Organization (ROs) as delineated in MLPA, 2012 and ATA, 2009?
3) What are the elements of a compliance program of a bank? Describe the role and responsibilities of senior management.
4) What is the compliance structure of a bank? Describe the relationship between Central Compliance Committee and Anti Money Laundering Department/Division of a bank.
5) Why AML&CFT compliance function should be independent from Internal Audit function?

List of References

Anti Terrorism Act, 2009 (Act No.16 of 2016) [Bangladesh Gazette dated 12 June 2013].

Anti Terrorism Rules, 2013 (S.R.O. No-30/Law/2019) [Bangladesh Gazette dated 09 November 2013].

Anti Corruption Commission Act, 2004 (Act No.5 of 2004) [Bangladesh Gazette dated 23 February 2004].

BFIU (2019), Guidelines for Beneficial Owner.

BFIU (2019), Guidelines on Suspicious Transaction Report for the Reporting Organization.

BFIU (2019), Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations.

BFIU (2019), Guidelines for Prevention of Trade Based Money Laundering (TBML)

BFIU (2019), Guidelines on Electronic Know Your Customer (e-KYC).

BFIU (2015), Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector.

FATF (2023), The FATF Standards.

FATF (2023), Methodology.

Jonathan E. Turner (2011), *Money Laundering Prevention*, John Wiley and Sons, Inc, Hoboken, New Jersey, USA.

John A Cassara (2020), *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails.*

Kevin Sullivan (2015), *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business Managers*, Apress, New York, USA.

Ministry of Foreign Affairs (2012), Bangladesh Government, Guidelines for Implementation of the UN Security Council Resolutions Concerning Targeted Financial Sanctions, Travel Ban, And Arms Embargo.

Money Laundering Prevention Act, 2012 (Act No.4 of 2012) [Bangladesh Gazette dated 20 February 2012].

Money Laundering Prevention Rules, 2019 (S.R.O. No-30/Law/2019) [Bangladesh Gazette dated 13 February 2019].

Nkechikwu Valerie and Azinge-Egbiri (2022), *Regulation and Combating Money Laundering and Terrorist Financing*, Routledge, Taylor & Francis Group, England.

Patrick Kabamba (2019), *Know Your Customer Policy*, Kindle.

Peter Gottschalk (2009), *Policing Financial Crime: Intelligence Strategy Implementation*, Brown Walker Press, Boca Raton, Florida, USA.

Sebastian Billot (2020), *Financial Crime Compliance*.

OFAC Sanctions, Retrieved from https://ofac.treasury.gov/#:~:text=OFAC%20administers%20a%20number%20of,policy%20and%20national%20security%20goals and https://ofac.treasury.gov/sanctions-programs-and-country-information.

UN Sanctions, Retrieved from https://www.un.org/securitycouncil/sanctions/information