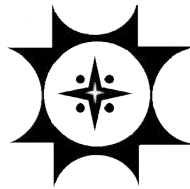


# **Risk Assessment and Management Guidelines on Money Laundering and Terrorist Financing**



**Sonali Bank Limited**

Money Laundering, Terrorism Financing  
Prevention and Vigilance Division  
Head Office, Dhaka.

**December, 2019**

## Preface

Banking is considered as life blood of an economy and it plays a vital role in socio-economic development of a country. Being the most important sectors of the financial system, it forms the money market and plays very dynamic role in mobilizing resources for productive sectors, which in turn contributes to economic development. So, an efficient and stable banking system is a must for overall development of a country like ours.

Money Laundering and Terrorist Financing (ML & TF) have been one of the major threats to the stability and the integrity of the banking system in recent times. So, Bangladesh Financial Intelligence Unit (BFIU) has instructed all scheduled banks operating in Bangladesh to identify, assess and take effective action to mitigate their ML & TF risks.

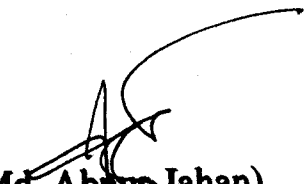
To comply with the requirement of BFIU, our Money Laundering, Terrorism Financing Prevention and Vigilance Division (MLTFPVD), with the direct supervision and guidelines of the bank's Central Compliance Committee (CCC), has updated existing guideline '**Risk Based Policy & Guidance on AML-CFT**' with the latest rules & regulations, policies & procedures, internationally practiced tools & techniques and suggestions & instructions of BFIU and renamed it as '**Risk Assessment and Management Guidelines on Money Laundering and Terrorist Financing**'.

I am very happy to know that, basic ideas regarding Money Laundering and Terrorist Financing, local and international major initiatives against ML & TF, ML-TF risks assessment and management etc. are initially covered in the guideline. Fundamental ideas of identifying, assessing and mitigating ML & TF risks that our branches may encounter in doing their day to day businesses are also described in it. We are aware that, ML & TF risks generally arise through/from our customers, product and services, business practices or delivery methods and jurisdictions or geographic location. Regulatory risks, i.e., non compliant with the requirements of MLPA 2012 (Amendment 2015), ATA 2009 (Amendment 2012 & 2013) and directives issued by BFIU may also arise due to inappropriate handling of them. How to assess risk level or evaluate risk score by blending likelihood and impact of the identified risks is illustrated and measures to be taken against them are also mentioned here.

Current policies and procedures as well as practices, compliance structure of the bank, customer acceptance policy, customer due diligence, transaction monitoring, reporting, training, record keeping etc. with regard to AML-CFT compliance are described in it. Trade Based Money Laundering (TBML) has become one of the main challenges in recent times for bankers, regulators, law enforcing agencies and country as a whole. A brief description of TBML is given in one chapter. However, concerned officials are advised to study more on it for the sake of themselves and institution.

My heartfelt thanks and gratitude goes to them, especially to the CAMLCO, all members of the CCC and officials of MLTFPVD, who have directly or indirectly been involved in formulation of this guideline. My thanks and gratefulness also extends to all members of the Board of Directors, Sonali Bank Limited for their kind approval of the same.

I hope, this guideline will enrich all officials of the bank with latest AML-CFT compliance issues. Moreover, this guideline will help domestic and foreign Banks and Financial Institutions, who have correspondent relationships with us, understand our AML-CFT related policies & procedures and know our corporate commitment in this regard. All branches (domestic & foreign), controlling offices including all Divisions of Head Office and subsidiaries of Sonali Bank Limited are advised to follow the guidelines strictly.



**(Md. Abius Jahan)**  
**CEO and Managing Director**  
**(Additional Charge)**

## Table of Contents

		Page
	<b>CHAPTER 01: Money Laundering &amp; Terrorist Financing</b>	<b>8-17</b>
1.1	Definition of Money Laundering	8
1.2	Stages of Money Laundering	10
1.3	Why Money Laundering is done	10
1.4	Definition of Terrorist Financing	11
1.5	Link between Money Laundering and Terrorist Financing	12
1.6	Why we must combat ML & TF	12
1.7	International Initiatives on ML & TF	14
1.8	National Initiatives on ML & TF	16
	<b>CHAPTER 02: ML &amp; TF Risk</b>	<b>18-20</b>
2.1	Obligation for ML&TF Risk Assessment and Management	18
2.2	Assessing risk	18
2.3	Risk Management and Mitigation	18
2.4	Definition of Risk	18
2.5	Risk Identification Methods	18
2.6	Objective	19
2.7	Risk Based Approach	19
2.8	Risk Identification	19
2.9	Risks that Need to be Managed	20
	<b>CHAPTER 03: Risk Management Framework</b>	<b>21-28</b>
3.1	Risk Management Principles	21
3.2	Risk Management Framework	21
3.3	Business risk	22
3.3.1	Customers	22
3.3.2	Products and Services	24
3.3.3	Business Practice/Delivery Methods or Channels	27
3.3.4	Country/Jurisdiction	27
3.4	Regulatory Risk	28
	<b>CHAPTER 04: Risk Assessment</b>	<b>29-32</b>
4.1	Calculation of Risk Score	29
4.2	Likelihood scale	29
4.3	Impact scale	29
4.4	Risk Matrix and Risk Score	30
4.5	Risk Matrix	31
4.6	Risk Score Table	31
4.7	Risk Register	32
	<b>CHAPTER 05: Risk Management</b>	<b>33-40</b>
5.1	Risk Management Component	33
5.2	Specific High Risk Elements and Recommendations for EDD	33

5.3	General High Risk Scenarios / Factors	35
5.4	General Low Risk Scenarios/ Factors	36
5.5	Situations that Require More Measures	37
5.6	Products and Services	38
5.7	Techniques of reducing risks against some Products and Services	38
5.8	Resort to Manage the Risks	40
	<b>CHAPTER 06: AML-CTF Compliance Structure</b>	<b>41-47</b>
6.1	Policy Manual and Management's Commitment	41
6.2	Compliance Structure for AML-CFT	41
6.3	Central Compliance Committee (CCC)	42
6.4	Authorities and Responsibilities of the CCC	43
6.5	Chief Anti Money Laundering Compliance Officer (CAMLCO)	43
6.5.1	Authorities and Responsibilities of CAMLCO	44
6.6	Branch Anti Money Laundering Compliance Officer (BAMLCO)	44
6.6.1	Responsibilities of Branch/BAMLCO	45
6.7	Responsibilities of GMO PO RO	47
	<b>CHAPTER 07: Policies &amp; Procedures</b>	<b>48-60</b>
7.1	Customer Acceptance Policy	48
7.2	Customer Due Diligence (CDD)	49
7.3	KYC Policies and Procedures	50
7.3.1	Implementation of KYC Policy	50
7.3.2	Walk-In/ One off Customers	51
7.3.3	Non Face to Face Customers	51
7.4	Politically Exposed Persons (PEPs)	51
7.5	Corresponding Banking	53
7.6	Wire Transfer	55
7.6.1	Cross-Border Wire Transfers	55
7.6.2	Domestic Wire Transfers	56
7.7	Duties of Ordering, Intermediary and Beneficiary Bank in Wire Transfer	56
7.8	CDD for Beneficial Owners	57
7.9	Management of Legacy Accounts	57
7.10	Prevention of Financing of Terrorism and Financing of Proliferation of WMD	58
7.11	Screening Different Sanction Lists	59
7.12	Flow-Chart for Implementation of TFS by Banks	60
7.13	Bank's Foreign Branches and Subsidiary Companies	60
	<b>CHAPTER 08: Transaction Monitoring</b>	<b>61-68</b>
8.1	Transaction Monitoring Process	61
8.2	Transaction Profile (TP)	62

8.3	Cash Transaction Report (CTR)	63
8.4	Suspicious Transaction Report (STR)	64
8.4.1	Why Reporting Unusual/Suspicious Transaction is Important	65
8.4.2	Techniques of identifying Suspicious Transaction/Accounts/Activities	65
8.4.3	Procedures and Steps of Reporting STR/SAR	67
8.4.4	Responsibilities after Reporting STR/SAR	68
	<b>CHAPTER 09: Self Assessment &amp; ITP</b>	<b>69-70</b>
9.1	Self Assessment Report and Independent Testing Procedures	69
9.2	Inspection and Audit Division's Obligation Regarding Self Assessment Report and Independent Testing Procedure	69
9.3	Central Compliance Committee's Obligation Regarding Self Assessment Report and Independent Testing Procedure	70
	<b>CHAPTER 10: Trade Based Money Laundering</b>	<b>71-73</b>
10.1	Trade Based Money Laundering (TBML)	71
10.2	Products and Services used in TBML	71
10.3	Parties Involved in Trade	71
10.4	Techniques used in TBML	72
10.5	Trade-Based Money Laundering Examples and Red Flags	72
10.6	Measures Needed to Curb Trade-Based Money Laundering	73
	<b>CHAPTER 11: Employee, Training &amp; Record Keeping</b>	<b>74-75</b>
11.1	Know Your Employee	74
11.2	Employee Screening	74
11.3	AML – CFT Training	75
11.4	Record Keeping	75
	<b>Annexure – A: RISK REGISTER</b>	<b>76-92</b>
	i. ML & TF Risk Register for Customers	76-81
	ii. Risk Register for Products & Services of SBL	82-85
	iii. Risk Register for Business Practices/Delivery Methods or Channels	86-87
	iv. Risk Register for Country/Jurisdiction	88-89
	v. Register for Regulatory Risk	90-92
	<b>Annexure – B: KYC Documentation</b>	<b>93-99</b>
	<b>Annexure – C: Red Flags Pointing to Money Laundering</b>	<b>100-102</b>
	<b>Annexure – D: AML-CFT Questionnaire for Correspondent Relationship</b>	<b>103-105</b>

## List of Abbreviations

<b>AML&amp;CFT</b>	<b>Anti-Money Laundering &amp; Combating the Financing of Terrorism</b>
<b>APG</b>	<b>Asia/Pacific Group on Money Laundering</b>
<b>ATA</b>	<b>Anti Terrorism Act</b>
<b>BAMLCO</b>	<b>Branch Anti Money Laundering Compliance Officer</b>
<b>BB</b>	<b>Bangladesh Bank</b>
<b>BFIU</b>	<b>Bangladesh Financial Intelligence Unit</b>
<b>CAMLCO</b>	<b>Chief Anti Money Laundering Compliance Officer</b>
<b>CCC</b>	<b>Central Compliance Committee</b>
<b>CDD</b>	<b>Customer Due Diligence</b>
<b>CTR</b>	<b>Cash Transaction Report</b>
<b>DNFBPs</b>	<b>Designated non-financial businesses and professions</b>
<b>EDD</b>	<b>Enhanced Due Diligence</b>
<b>FATF</b>	<b>Financial Actions Task Force</b>
<b>IPs</b>	<b>Influential Persons</b>
<b>KYC</b>	<b>Know Your Customer</b>
<b>KYE</b>	<b>Know Your Employee</b>
<b>ML</b>	<b>Money Laundering</b>
<b>MLPA</b>	<b>Money Laundering Prevention Act</b>
<b>MLPR</b>	<b>Money Laundering Prevention Rules</b>
<b>MLTFPVD</b>	<b>Money Laundering, Terrorism Financing Prevention and Vigilance Division</b>
<b>NCCT</b>	<b>Non-Cooperative Countries and Territories</b>
<b>OFAC</b>	<b>Office of Foreign Assets Control</b>
<b>PEPs</b>	<b>Politically Exposed Persons</b>
<b>RO-FI</b>	<b>Reporting Organizations-Financial Institutions</b>
<b>SAR</b>	<b>Suspicious Activity Report</b>
<b>SBL</b>	<b>Sonali Bank Limited</b>
<b>STR</b>	<b>Suspicious Transaction Report</b>
<b>TF</b>	<b>Terrorist Financing</b>
<b>UNSCRs</b>	<b>United Nations Security Council Resolutions</b>
<b>WMD</b>	<b>Weapons of Mass Destruction</b>

## CHAPTER 01: Money Laundering & Terrorist Financing

### 1.1 Definition of Money Laundering:

Money laundering can be defined in a number of ways. But the fundamental concept of money laundering is the process by which proceeds from a criminal activity is disguised to conceal their illicit origins. Most countries adopted to the following definition which was delineated in the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

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

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

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

'Money laundering' means –

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



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

Money laundering is a criminal offence under section 4(1) of MLPA, 2012 and penalties for money laundering are-

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) lacks, whichever is greater.
2. In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favour of the State which directly or indirectly involved in or related with money laundering or any predicate offence.

3. Any entity which commits an offence under this section shall be punished with a fine of not less than twice of the value of the property or taka 20(twenty) lacks, whichever is greater and in addition to this the registration of the said entity shall be liable to be cancelled.

## **1.2 Stages of Money Laundering:**

Obviously there is no single way of laundering money or other property. It can range from the simple method of using it in the form in which it is acquired to highly complex schemes involving a web of international businesses and investments. Traditionally it has been accepted that the money laundering process comprises three stages:

1. **Placement:** Placement is the first stage of the money laundering process, in which illegal funds or assets are brought first into the financial system directly or indirectly.
2. **Layering:** Layering is the second stage of the money laundering process, in which illegal funds or assets are moved, dispersed and disguised to conceal their origin. Funds can be hidden in the financial system through a web of complicated transactions.
3. **Integration:** Integration is the third stage of the money laundering process, in which the illegal funds or assets are successfully cleansed and appeared legitimate in the financial system.

## **1.3 Why Money Laundering is done:**

- ✓ First, money represents the lifeblood of the organization/person that engages in criminal conduct for financial gain because it covers operating expenses and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.
- ✓ Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.
- ✓ Third, the proceeds from crime often becomes the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or, alternatively, make them look legitimate.

## 1.4 Definition of Terrorist Financing:

Terrorist financing can simply be defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF as follows:

1. If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
  - a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
  - b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.
2. For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b).

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

Section 7 of Anti Terrorism Act (ATA), 2009, defines terrorist financing and sets punishment as follows –

- 1) If any person or entity willingly, by any means, directly or indirectly, from legal or illegal source, supply, receive or manage money, service, material support or asset with the intention that full or part of the same-
  - a) Will be used to carry out terrorist activities; or
  - b) Will be used or in the knowledge that they are to be used to carry out any other act by a terrorist or terrorist entity;

then, the person or entity shall be liable to financing of terrorism.

- 2) For an act to constitute an offence set forth in the preceding paragraph 1, it shall not be necessary that the money, service or any material support were actually used or intended to be used to carry out terrorist activities or linked to a specific terrorist activity.

- 3) Any person who commits an offence of financing of terrorism shall be punished with imprisonment for a term of at least 4 (four) years but not exceeding 20 (twenty) 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) lacks, whichever is greater.
- 4) If any entity is convicted under the sub-section (1) of this Act, then-
  - a) Step may be taken to punish the entity as per section 18 and, in addition to that, a fine equivalent to the thrice of the value of the property involved in the offence or taka 50 (fifty) lacks, whichever is greater.
  - b) The chief of the entity- Chairman, Managing Director, Chief Executive, or whatever is called- shall be punished with imprisonment for a term of at least 4 (four) years but not exceeding 20 (twenty) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 20 (twenty) lacks, whichever is greater, if he/she is not able to prove that such offence has been occurred beyond his knowledge or he/she has taken all out measures to avoid occurrence of the offence .

### **1.5 Link between Money Laundering and Terrorist Financing:**

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

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

### **1.6 Why we must combat ML & TF:**

Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a vital process to make crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupted public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to

the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences resulted from ML & TF.

Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection activities more difficult. This loss of revenue generally means higher tax rates than would normally be the case if the untaxed proceeds of crime were legitimate. We also pay more taxes for public works expenditures inflated by corruption. And those of us who pay taxes pay more because of those who evade taxes. So we all experience higher costs of living than we would if financial crimes including money laundering were prevented.

Money laundering distorts assets and commodity prices and leads to misallocation of resources. For financial institutions it can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability and even systemic crisis. The loss of credibility and investor's confidence, that such crisis can bring, has the potential of destabilizing financial systems, particularly in smaller economies.

One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers often use front companies, which co-mingle the proceeds of illicit activity with legitimate funds, to hide the ill-gotten gains. These front companies have access to substantial illicit funds, allowing them to subsidize front company products and services at levels well below market rates. This makes it difficult, if not impossible, for legitimate business to compete against front companies with subsidized funding, a situation that can result in the crowding out of private sector business by criminal organizations.

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

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

A nation cannot afford to have its reputation and financial institutions tarnished by involvement with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions (FIs) and the underlying criminal activities like fraud, counterfeiting, narcotics trafficking, and corruption weaken the reputation and standing of any financial institution. Actions taken by FIs to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. A financial institution tainted by

money laundering accusations from regulators, law enforcement agencies, may lose their good market reputation and damage the reputation of the country. It is very difficult and requires significant resources to rectify a problem that could be prevented with proper program.

Besides its effect on macro level, ML & TF also affects individual financial institution. If a money launderer uses a financial institution for making his/her money legitimate, the business of that financial institution may hamper. If the money launderer withdraws his/her deposited money from an FI before maturity, the FI will face liquidity crisis if the amount is big enough. Moreover, if it is found that an FI was used for ML & TF activities, and it did not take proper action against that ML & TF as per the laws of the country, the FI will have to face legal risk. Finally, the reputation of an FI can also be heavily affected through its involvement with ML & TF activities.

It is generally recognized that effective efforts to combat ML, TF & PF cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies. Accordingly, in order to address the concerns and obligations of these three parties, these Guidance Notes are drawn up.

## **1.7 International Initiatives on ML & TF:**

As a result of increase trading of drugs and narcotics and increase in smuggling and use of funds earned illegally in different countries of the world including the USA and Europe, a negative impact on social and economic aspects of those countries was being made. Concerned countries were feeling necessity of taking initiatives to resist that situation. As a result, United States enacted, for the first time in 1986, Money Laundering Control Act.

The UN adopted the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) known as **Vienna Convention**, named after the city in which it was signed. The Vienna Convention deals primarily with provisions to fight the illicit drug trade and related law enforcement issues.

The Financial Action Task Force on Money Laundering (FATF) was formed in 1989 by G-7 countries in their annual meeting. It is an intergovernmental body. Main purpose of it is to develop and promote an international response to combat money laundering. FATF adopted a set of 40 recommendations to prevent money laundering. These Forty Recommendations constituted a comprehensive framework for AML and were designed for universal application by countries throughout the world. FATF expanded its mission by including 8 new recommendations on combating the financing of terrorism in 2001 and lifted it to (40+9)

recommendations by adding another one in 2005. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. FATF Plenary has again revised its recommendations in February 2012. The previous 40+9 Recommendations has been accumulated into 40 (forty) recommendations called the FATF Standards. Proliferation financing has been included in the new standards. Currently, 34 countries and territories and two regional organizations are members of the FATF and its Forty Recommendations was endorsed by more than 180 countries. International communities, including World Bank, IMF and relevant organizations, have also endorsed FATF's Forty Recommendations as the international standard for AML.

Besides, different regional organizations including APG (Asia Pacific Group on Money Laundering), CFATF (Caribbean Financial Action Task Force), and ESAAMLG (Eastern and Southern African Anti Money Laundering Group) have adopted different policies to prevent money laundering activities of terrorist individual, group or organizations.

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of 10 (ten) countries. The committee formulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank/financial institution supervisory issues including money laundering.

In 1995, a number of governmental units of different countries commonly known as Financial Intelligence Units (FIUs) began working together and formed the Egmont Group of FIUs (Egmont Group). Bangladesh became member of the group in 2013. The purpose of the group is to provide a forum for FIUs to improve support for each of their national AML programs and to coordinate AML-CFT initiatives. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs world-wide.

The Asia Pacific Group on Money Laundering (APG), founded in 1997 is an autonomous and collaborative international organization consisting of 41 members and a number of international and regional observers. Bangladesh is an important founding member of it. APG is the FATF style regional body (FSRB) for the Asia Pacific region. APG members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations of the FATF on Money Laundering and Terrorist Financing.

FATF adopted a process of identifying those jurisdictions that serve as obstacles to international cooperation in implementing its recommendations. The process used 25 criteria, which were consistent with 40+9 recommendations, to identify such non-cooperative countries and territories (NCCT) and place them on a publicly available list. NCCT was a process of black listing of non compliant country and hence it has a massive impact on respective country.

### **1.8 National Initiatives on ML & TF:**

Prevention of money laundering and terrorist financing has been recognized as a challenge for banks and financial institutions of the world. Our country along with other countries of the world is committed to prevent such acts.

Bangladesh is the first country in the South Asia that has enacted Money Laundering Prevention Act (MLPA) in 2002. To meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER) of Bangladesh that was adopted in 2009, Bangladesh has again enacted Money Laundering Prevention Act in February, 2012 repealing MLPA, 2009. MLPA, 2012 was again amended in 2015 and Money Laundering Prevention Rules, 2019 has been framed for effective implementation of the act.

Bangladesh also enacted Anti Terrorism Ordinance (ATO) in 2008 to combat terrorism and terrorist financing. Subsequently, ATO, 2008 has repealed by Anti-Terrorism Act (ATA), 2009 with the approval of the parliament. To address the gap identified by APG in the Mutual Evaluation Report (MER), some provisions of ATA 2009 have been amended in 2012 and 2013. Anti-Terrorism Rules, 2013 has also been promulgated to make the roles and responsibilities of related agencies clear, specially to provide specific guidance on the implementation procedure of the provisions of the UNSCRs.

Bangladesh has enacted Mutual Legal Assistance in Criminal Matters Act, 2012 to enhance international cooperation on ML & TF and other related offences. The Government also enacted Mutual Legal Assistance in Criminal Matters Rules, 2013 which mainly emphasize on the process of widest possible range of providing mutual legal assistance in relation to ML & TF and other associated offences.



The Government of Bangladesh has formed a central and 7 regional taskforces (Chittagong, Rajshahi, Bogra, Sylhet, Rangpur, Khulna and Barisal) on 27 January, 2002 to prevent illegal hundi activities, illicit flow of fund & money laundering in Bangladesh.

A National Coordination Committee (NCC) headed by the Honorable Finance Minister and a Working Committee (WC) headed by the Secretary of Bank and Financial Institutions Division of Ministry of Finance have been formed consisting representatives from all concerned Ministries, Agencies and regulatory authorities. Main tasks of these committees are to provide guidance for effective implementation of AML & CFT in the country.

As per the provision of MLPA, 2012 Bangladesh Financial Intelligence Unit (BFIU) has been established, abolishing Anti-Money Laundering Department (AMLDD) which was established in 2002 to work as the FIU of Bangladesh, as a national central agency to receive, analyze and disseminate STRs/SARs, CTRs and complaints. BFIU has been entrusted with the responsibility of exchanging information related to ML & TF with its foreign counterparts. The main objective of BFIU is to establish an effective system for prevention of money laundering, combating financing of terrorism and proliferation of weapons of mass destruction and it has been bestowed with operational independence. BFIU has also achieved the membership of Egmont Group in July, 2013.

## **CHAPTER 02: ML & TF Risk**

### **2.1 Obligation for ML&TF Risk Assessment and Management:**

Rule 21 of MLPR 2013 states that every Reporting Organization-Financial Institution (RO-FI) shall conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. Rule 21 also states that RO-FI shall utilize this risk assessment report after having vetted by BFIU.

### **2.2 Assessing risk:**

As a scheduled bank in Bangladesh, Sonali Bank Limited is required to take appropriate steps to identify and assess its money laundering and terrorist financing risks for customers, countries or geographic areas, products, services and transactions or delivery channels. It should document those assessments in order to be able to demonstrate its basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities such as BFIU, Bangladesh Bank.

### **2.3 Risk Management and Mitigation:**

Sonali Bank Limited is also required to have policies, controls and procedures that enable it to manage and mitigate effectively the risks that have been identified. It is 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 such as BFIU, Bangladesh Bank.

### **2.4 Definition of Risk:**

Risk is the combination of the probability of an event and its consequences. In simple term, it can be defined as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur. Consequences can range from positive to negative.

### **2.5 Risk Identification Methods:**

Risk identification methods can include:

- Evidence based methods, examples of which are check-lists and reviews of historical data.

- Systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions.
- Inductive reasoning techniques.

## **2.6 Objective:**

A well-developed risk assessment will assist in identifying the bank's AML-CFT risk profile. Understanding the risk profile enables the bank to apply appropriate risk management processes to the AML-CFT compliance program to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the bank's controls. The risk assessment should provide a comprehensive analysis of the AML-CFT risks in a concise and organized presentation.

## **2.7 Risk Based Approach:**

Bank should identify, assess and understand the money laundering and terrorist financing risks for the interest of the banks. Risks may be diversified and different according to the nature of accounts and transactions. Considering nature of risks proper measures are necessary to be taken. In this respect bankers should apply their own skills and techniques for eliminating or reducing risks of money laundering and terrorist financing.

## **2.8 Risk Identification:**

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

- 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 exchange for cash or other assets, global nature of markets.
- Correspondent banking: high value transactions, limited information about the remitter and source of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

## 2.9 Risks that Need to be Managed:

As per requirement of BFIU, Sonali Bank Limited needs to address two main risks for the ML & TR aspects. They are- (a) Business Risk and (b) Regulatory Risk.

(a) **Business risk** is the risk that our business may be used for ML&TF. So, we must assess the following risks in particular:

- customer risks
- products or services risks
- business practices and/or delivery method risks and
- country or jurisdictional risks.

(b) **Regulatory risk**, on the other hand, is associated with not meeting all obligations of banks under the Money Laundering Prevention Act, 2012 (including amendment, 2015), Anti Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two acts and instructions issued by BFIU.

Some regulatory obligations are –

- failure to report CTR and STR/SAR,
- unable or inappropriately verification of customers,
- lacking of AML&CFT program etc.

It is not realistic that Sonali Bank Limited can operate its daily activities in a completely ML&TF risk-free environment. So, we shall identify the ML&TF risk we face, and then work out the best ways to reduce and manage that risk.

## **CHAPTER 03: Risk Management Framework**

### **3.1 Risk Management Principles:**

For effective risk management, Sonali Bank Limited is following, at all levels, some principles which are given 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 actions and distinguish among alternative courses of action.
- Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
- A 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.

### **3.2 Risk Management Framework:**

Risk management framework of Sonali Bank Limited is consisting of:

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

- the types of customers;
- the nature, scale, diversity and complexity of our business;
- our target markets;
- the number of customers already identified as high risk;

- the jurisdictions SBL is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML/CFT controls and listed by FATF;
- the distribution channels, including the extent to which SBL deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;
- the internal audit and regulatory findings;
- the volume and size of its transactions, considering the usual activity of SBL and the profile of its customers.

(b) risk identification;

(c) risk assessment or evaluation; and

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

In identifying and assessing the ML/TF risk to which they are exposed, banks should consider a range of factors which may include business risk and regulatory risk.

### **3.3 Business risk:**

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

- Customers
- Products and services
- Business practices/delivery methods or channels
- Country and jurisdiction

Under these four groups, individual risk to SBL is determined.

#### **3.3.1 Customers:**

Sonali Bank Limited has a large banking network across the country in Bangladesh. It has various types of customers. Most of the customers of this bank are common people. Accounts and relationship with this bank are maintained by the rich people of the society as well as by the people of low income group of the country. For example, businessmen of all classes (including international traders), industrialists, Govt. and Non-Govt. employees, students, farmers, household persons, retail traders etc.

In case of customers, some are treated as high risk customer because of their unwillingness to pay due attention to all the rules and regulations of the bank. They want to apply their local and personal influences for doing banking activities.

In that case bank takes preventive measures for securing its interest. Customer Due Diligence (CDD) is properly maintained for these types of customers. Such as, source of fund, previous record and activities are considered. These accounts are treated as high risk account. Special monitoring systems are conducted for following accounts:

(1) Social influential person, (2) Foreign PEPs, (3) Large transaction, (4) Client's business activity which is beyond control, (5) Corporate customer whose ownership structure is unusual and exclusively complex.

When bank fails to take/ensure true identity with proper evidence & record of a customer, then the customer may be treated as High Risk. If Bank can not ensure source of fund against large transaction, then associated account may also be treated as high risk.

In this context, Sonali Bank Limited is alert for performing KYC Profile and taking true identity of customer. CDD are conducted for those types of customer. So, we treat these as medium or high risk account before account opening and during the transactions of account. As per guidelines of central bank and BFIU circular no. 19, dated 17/09/2017 of Bangladesh Financial Intelligence Unit, transaction monitoring and source of fund are ensured. So, the chances for happening any adverse situation or occurring ML–TF risk is almost low.

In case of opening account for the following nature of customers, concerned Branch has to take steps to gauge if the account will be opened or not. There are instructions at field level of the bank from Central Compliance Committee (CCC) that before opening any account, KYC and CDD procedure to be completed with proper data and information and related documents also to be taken from the customers. Otherwise, Branch should not open account. In this way bank tries to reduce the risk associated with the following:

01. a new customer
02. a new customer who wants to carry out a large transaction
03. a customer or a group of customers making lots of transactions to the same individual or group
04. a customer who has a business which involves large amounts of cash
05. a customer whose identification is difficult to check
06. a customer who brings in large amounts of used notes and/or small denominations.
07. a non- resident customer
08. a corporate customer whose ownership structure is unusual and excessively complex
09. customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates
10. 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
- 11. customer submits account documentation showing an unclear ownership structure
- 12. 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.

Serial no. 10, 11 & 12 will be treated as high risk account. Normally these types of accounts are discouraged/ not allowed to open in Sonali Bank Limited. If, somehow these types of accounts exist in our bank, the concerned branch of the bank has right to close the account after performing the formalities or may report Suspicious Transaction Report (STR) to Bangladesh Financial Intelligence Unit (BFIU).

### **3.3.2 Products and Services:**

Sonali Bank Limited has a very wide range of products and services. Few of them are given below:

- a. Savings Deposit
- b. Current Deposit
- c. Special Notice Deposit
- d. Sonali Bank Daily Profit Account
- e. Fixed Deposit (different term)
- f. Monthly Earning Scheme
- g. Monthly fixed deposit scheme (SDS, EDS, MDS, DBS, MES, MSS, SBS, SBDP, RSS, SBRSS, RDS etc)
- h. Non Resident Deposit Scheme
- i. School Banking
- j. Double/Triple Benefit Scheme
- k. Islamic Banking Deposits (MSA, AWCA, MSND, MSS, MHSS)
- l. Cash Credit (Hypo, Pledge)
- m. SOD (against deposit scheme)
- n. OD
- o. SME Finance
- p. Project Finance
- q. Lease Finance
- r. Bridge Finance
- s. Working Capital
- t. House Building Loan (General, Staff)
- u. International Trade Finance (Export, Import, Bill Purchase)
- v. Telegraphic Transfer (TT)
- w. Demand Draft (DD)
- x. Payment Order (PO)



- y. Online Transfer
- z. Debit Card
- aa. Credit Card
- bb. Utility Bill Payment
- cc. Govt. Allowances Payment

Among the accounts mentioned above, most of the products and services have very low level risk. We need to identify the associated risk at the very opening stages of the account. Prior to opening all sorts of accounts in our bank, KYC profile is performed with due diligence. Careful monitoring is conducted regularly for high risk accounts.

In case of fixed deposit products, threshold limit becomes fixed. These types of accounts may contain low risk, because sources of fund for these types of account are ensured through inquiry by the bank. If concerned officials of the bank are fully satisfied regarding source of fund and other relevant information of the client, such kind of account is permitted to open.

In case of monthly deposit account, account holders identity is ensured through performing KYC profile. So, there is also risk level of money laundering and terrorist financing but it seems also low. Because earning of account holder with proper evidence is to obtain before opening account.

In case of saving, current & special notice account, some procedures are also followed accordingly. Source of fund and destination of fund is monitored closely. In case of large cash deposit and fund transfer, there may have some medium and high risk considering the account holder's previous history and profession.

### **Foreign Trade:**

Sonali Bank Limited has been largely involved in foreign trade and business since long. In case of these businesses, past record, performance, license, credit report, etc. of the customer have to be seriously considered. Even if there is a chance to happen money laundering and terrorist financing, branch has to take some protective measures, especially against import and export business. In this regard, following measures or rules and regulations should be followed :

- a. Foreign Exchange Regulation Act, 1947 of Bangladesh.
- b. Products which will be imported or exported to be verified by renowned inspection company.
- c. In case of import, country of origin, carrier, vessel, port of shipment etc. need also to be verified before opening letter of credit (L/C) or approval contact to which sanction countries can't be related directly or indirectly with this business.
- d. Price level of goods are verified through HS Code.
- e. Quality and quantity is also verified by obtaining pre-shipment inspection report.

### **Foreign Exchange Business:**

In case of international trade & business, bank has to follow Foreign Exchange Regulation Act, 1947 of our country. Moreover, international rules also to be followed.

Usually foreign trade is performed through letter of credit (L/C) and contract. For export and import of goods and services, those systems need to be adopted. There may have chances for happening money laundering and terrorist financing through foreign trade and business.

Branch has to take various measures to protect money laundering & terrorist financing in this respect.

Before allowing for opening LC, branch needs to perform KYC profile, to prepare a credit report of the importer. These must have the previous performance, experience, political association, business, volume of transactions, cash flow and fund flow, net worth etc. also need to be considered for approval of LC opening.

Moreover, before shipment of goods, pre-shipment inspection certificate has to be taken along with other documents where it has to be mentioned name of goods, quantity and quality. To protect under invoicing in export and over invoicing in import, mis-declaration of goods, branch has to take some measures under the foreign trade rules. In case of price fixation as per rules of foreign trade, branch needs verifying the price using international mechanism or practice. There may have some variation which has to be taken into consideration. If branch cannot follow related rules properly, there may have high risk for money laundering and terrorist financing.

### **Foreign Remittance:**

There are two types of transfer of fund, such as a) Electronic fund transfer through account and b) Spot cash payment to Walk-in-customer.

To provide those types of services to the remitter and beneficiary of the remittance, Sonali Bank Limited has been maintaining corresponding banking relationships with other Bank and Financial Institutions (FIs). The persons or entities from where the money is sent, KYC, CDD of the related customers are conducted by the remitting FIs. After satisfaction about the remitter's information & verification, a particular amount is sent at our end. On the other hand, our branches have to open account of clients as per prevailing act of the land and BFIU guidelines. This provision has also to be followed in case of beneficial owner.

In case of spot cash payment, National ID, mobile number, declaration, etc. need to be obtained from the receiver when the amount is very low and involved mass people.

### **Loans and Advances:**

Sonali Bank Limited deals loans and advances in various nature and forms. There is a huge chance for occurring ML–TF risk in this field. Some customers may adopt illegal means for blending their dirty or illegal earned money with the amount of loans and advances granted for them. In this case, customers present worth is measured before sanctioning loans, past performance is considered, credit information report are taken form Bangladesh Bank, physical verification of business is conducted and local confidential report is also considered for determining the level of risk.

### **Diversification of Fund:**

Whether the sanctioned loans and advances are utilizing properly is verified at every phases of disbursement. In this case, client’s integrity is also considered. The chance for happening ML–FT risk is also considered at variation of loan amount, nature of business and location.

In respect of products, services against loans and advances, Branches of Sonali Bank Limited apply their prudence to identify client’s trend whether the fund is diverted or used otherwise.

### **3.3.3 Business Practice/Delivery Methods or Channels:**

While doing business with following practice/delivery methods or channels, Sonali Bank Limited determines individual risks to it arise from them:

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

### **3.3.4 Country/Jurisdiction:**

On the other hand, while doing business with following countries/jurisdictions, Sonali Bank Limited determines risks arise for respective country/jurisdictions:

- any country which is identified by credible sources as having significant level of corruption and criminal activity
- any country subject to economic or trade sanctions
- any country known to be a tax haven and identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country

- any country identified by FATF or its associates as not having adequate AML&CFT system
- any country identified as destination of illicit financial flow

### **3.4 Regulatory Risk**

This risk is associated with not meeting the requirements of the Money laundering Prevention Act, 2012 (including Amendment, 2015), Anti Terrorism Act, 2009 (including Amendment, 2012 & 2013) 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.

## CHAPTER 04: Risk Assessment:

To mitigate ML-TF risk in banks, every bank has to assess risks associated with ML & TF. On the other hand, for assessing risk, a simple and generic table with Risk Score and Treatment (Annexure-A) is used. Again, Risk Score can be found by blending Likelihood (the chance of the risk happening) and Impact (the amount of loss or damage if the risk happened).

This table can be used for each risk group in preparation for assessing and managing those risks: customers, products and services, business practices/delivery methods, country/jurisdiction and the regulatory risks.

### 4.1 Calculation of Risk Score:

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:

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

<b>LIKELIHOOD</b>	<b>X</b>	<b>IMPACT</b>	<b>=</b>	<b>RISK LEVEL/SCORE</b>
-------------------	----------	---------------	----------	-------------------------

### 4.2 Likelihood scale:

A likelihood scale refers to the potential of an ML&TF risk occurring in the business for the particular risk being assessed. Following three levels of risk can be considered:

Table: Likelihood Scale

Frequency	Likelihood of an ML&TF risk	Score
<b>Very likely</b>	<b>Almost certain: it will probably occur several times a year</b>	<b>3</b>
<b>Likely</b>	<b>High probability it will happen once a year</b>	<b>2</b>
<b>Unlikely</b>	<b>Unlikely, but not impossible</b>	<b>1</b>

### 4.3 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 be rated or looked at from the point of view of the following:

- a. how it may affect the business (if not dealing with risks properly the bank suffers a financial loss from either a crime or through fines from BFIU or regulator)
- b. the risk that a particular transaction may result in the loss of life or property through a terrorist act
- c. 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
- d. the risk that a particular transaction may cause suffering due to the financing of illegal drugs
- e. 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 rejected by the community of customers
- f. 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.

Following three levels of impact can be considered:

Consequence	Impact – of an ML/TF risk	Score
Major	Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.	3
Moderate	Moderate level of money laundering or terrorism financing impact.	2
Minor	Minor or negligible consequences or effects.	1

#### 4.4 Risk Matrix and Risk Score:

After assessing likelihood scale and impact scale, next step is to use a risk matrix to combine LIKELIHOOD and IMPACT for getting a risk score. The risk score may be used to aid decision making and help in deciding what types of monitoring, effort or action has to be taken in view of the overall risk. How the risk score is derived can be seen from the risk matrix and risk score table given below. 6 (six) levels of risk score are considered for Sonali Bank Limited.

#### 4.5 Risk Matrix:

<b>LIKELIHOOD</b> ↓	Very Likely (3)	3 = Medium	6 = High	9 = Extreme
	Likely (2)	2=Medium Low	4=Medium High	6 = High
	Unlikely (1)	1 = Low	2=Medium Low	3 = Medium
		Minor (1)	Moderate (2)	Major (3)
		<b>IMPACT</b> →		

#### 4.6 Risk Score Table:

Rating	Impact of an ML & TF risk	Treatment/Action
9 =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.	<ol style="list-style-type: none"> <li>1. Approval from higher authority</li> <li>2. Response to the risk seriously</li> <li>3. Higher effort and monitoring in addition to conducting proper CDD and EDD.</li> <li>4. Ensure reporting to CCC or BFIU</li> </ol>
6 = High	Risk very likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.	<ol style="list-style-type: none"> <li>1. Response to the risk seriously</li> <li>2. Higher effort and monitoring in addition to conducting proper CDD and EDD.</li> <li>3. Ensure reporting to CCC or BFIU</li> </ol>
4=Medium High	Risk likely to happen and/or to have moderate consequences. Response: Allow transaction if risk can be reduced.	<ol style="list-style-type: none"> <li>1. Response to the risk aptly</li> <li>2. Higher effort and monitoring in addition to conducting proper CDD and EDD.</li> <li>3. Report to CCC or BFIU if needed.</li> </ol>
3 =Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.	<ol style="list-style-type: none"> <li>1. Response to the risk fairly</li> <li>2. Proper effort and monitoring in addition to conducting CDD.</li> <li>3. Scrutinize before reporting to CCC or BFIU.</li> </ol>
2=Medium Low	Less possibility this could happen and/or have moderate consequences. Response: Go ahead with caution.	<ol style="list-style-type: none"> <li>1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)</li> </ol>
1 = Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.	<ol style="list-style-type: none"> <li>1. Simplified CDD (Name, Address, Mob/Phone number, NID, etc.)</li> </ol>

#### **4.7 Risk Register:**

As we have an idea as to how can calculate risk score by blending likelihood and impact as well as the risk matrix and risk score, now we need to prepare following 5 (five) ML-TF Risk Registers for Sonali Bank Limited mentioning necessary actions against the particular outcomes of risks:

- i. Risk Register for Customer
- ii. Risk Register for Products and Services
- iii. Risk Register for Business Practices/Delivery Methods/Channels
- iv. Risk Register for Country/Jurisdiction
- v. Risk Register for Regulatory Risk.

Branches are advised to exercise their prudence and experiences while assessing risk score/rating for individual customer, product or service, business practice or delivery methods, country or jurisdiction and regulatory risk associated with the branch. They can use given five risk registers as specimens (Annexure-A).



## CHAPTER 05: Risk Management

### 5.1 Risk Management Component:

After assessing every individual risk associated with any one or more of customer, products and services, business practice/delivery methods or channels and country or jurisdiction, bank is required to have proper risk management guidelines or procedures in place. Following few risk management components should be emphasized at branch level:

- a. Risk Management Strategy and Policy of the Bank
- b. Ongoing Risk Monitoring
- c. Higher and Lower Risk Scenarios
- d. Risk Variables
- e. Counter Measures for Risk (EDD, CDD, Simplified CDD, Transaction Monitoring, Reporting etc.)

### 5.2 Specific High Risk Elements and Recommendations for EDD:

Some of the relatively high risk elements identified by Sonali Bank Limited and recommended actions for CDD/EDD may be as under:

Sl. no	Customers	Recommendations for CDD/EDD
a)	NPOs/ NGOs/ Charities, Trusts, Clubs, Societies, and Associations etc	In relation to these customers, banks may: i) Obtain a declaration from Governing Body/Board of Trustees/Executive Committee/sponsors on ultimate control, purpose and source of funds etc; ii) Obtain an undertaking from Governing Body/Board of Trustees/Executive Committee /sponsors to inform the bank about any change of control or ownership during operation of the account; and iii) Obtain a fresh Resolution of the Governing Body/Executive Committee of the entity in case of change in person(s) authorized to operate the account.
b)	Housewife accounts	In relation to housewife accounts, banks may i) Obtain a self-declaration for source and beneficial ownership of funds; ii) Update details of funds providers, if any along with customer's profile; and iii) Identify and verify funds providers if monthly credit turnover exceeds an appropriate threshold to be decided by banks.

Sl. no	Customers	Recommendations for EDD
c)	Proprietorships and self employed individuals/ professionals	<p>In relation to these accounts following measures may be taken by banks :</p> <p>i) The business transactions in personal accounts of proprietors may only be permitted by linking it with account/business turnover. For example, such customers having monthly credit turnover of TK. 10 million or above may be required to open a separate account for business related transactions; and</p> <p>ii) In order to verify the physical existence of business or self-employment status, banks may conduct physical verification <b>within 05 working days</b> of the opening of account and document the results thereof on account opening form. In case of unsatisfactory verification, bank may consider <b>reporting it to BFIU</b> and/or may change risk profile, as appropriate.</p>
d)	Landlords	In relation to such customers, bank may apply any recommend methods for assessment of source of funds/income e.g. Passbook of landholding records etc.
e)	Online transactions	In relation to online transactions, bank should pay special attention to geographical factors/locations for movement funds.
f)	Cash	<p>In relation to cash transactions, banks may</p> <p>i) monitor cash transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and</p> <p>ii) Pay special attention on cash based transactions considering nature of deposit and withdrawal.</p>
g)	Wire Transfers	<p>In relation to wire transfers, banks may:</p> <p>i) monitor such transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and</p> <p>ii) Ensure that funds transfers which are out of character/ inconsistent with the history, pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per act and policy.</p>

### 5.3 General High Risk Scenarios / Factors:

Following High risk Scenarios/Factors with regard to Customers, Products & Services, Delivery Channels and Geographic Locations are to be considered:

Customers	Products and Delivery Channels	Geographic Locations
<ul style="list-style-type: none"> <li>• Non-resident customers</li> <li>• Correspondent banks' accounts</li> <li>• Customers with links to offshore tax havens</li> <li>• Customers in high-value items etc</li> <li>• High net worth customers with no clearly identifiable source of income</li> <li>• There is a doubt about the veracity or adequacy of available identification data on the customer</li> <li>• There is reason to believe that the customer has been refused banking facilities by another bank</li> <li>• Companies that have nominee shareholders or shares in bearer form</li> <li>• Legal persons or arrangements that are personal asset holding vehicles</li> </ul>	<ul style="list-style-type: none"> <li>• Non-face-to-face business relationships or transactions</li> <li>• Cash intensive or other forms of anonymous transactions</li> <li>• Payment received from unknown or un-associated third parties</li> </ul>	<ul style="list-style-type: none"> <li>• The jurisdictions which have been identified for inadequate AML/CFT measures by FATF or called for by FATF for taking counter-measures</li> <li>• Countries identified by credible sources such as mutual evaluations or detailed assessment reports, as having inadequate AML/CFT standards</li> <li>• Countries subject to sanctions, embargos, for example, the United Nations, OFAC list</li> <li>• Countries identified by credible sources as having significant levels of corruption, or other criminal activity</li> <li>• Countries or geographic areas identified by credible sources as providing funding or support for terrorism activities</li> </ul>

In respect of general high risk elements every branch of Sonali Bank Limited has to conduct EDD measures which are effective and commensurate to the level of risks. In particular, branch may increase the degree and nature of on-going monitoring of the business relationship in order to determine whether those transactions or activities appear unusual or suspicious. Examples of such EDD measures may include:

- a) Obtaining additional information on the customer (occupation, volume of assets, address) information;
- b) Reducing interval for updating and reviewing customer risk profile;

- c) Reducing interval for updating the identification data of customer and beneficial owner;
- d) Obtaining additional information on the intended nature of the business relationship;
- e) Obtaining information on the reasons for intended or performed transactions;
- f) Obtaining additional information on the sources of funds or sources of wealth of the customer;
- g) Obtaining the approvals of senior management to commence or continue the business relationship e.g. PEPs account;
- h) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
- i) Documentary evidence may be sought to support transaction where possible, e.g. Purchase of property etc.

#### **5.4 General Low Risk Scenarios/ Factors:**

There may be circumstances where the risk of money laundering or financing of terrorism may be low, for example where information on the identity of the customer and the beneficial ownership is publicly available. In such circumstances, and provided there has been an adequate analysis of the risk by the branches of the bank, SDD measures may be applied. Examples of such low risk scenarios/factors may include:

<p>Low risk factors for Customers</p>	<ul style="list-style-type: none"> <li>• A financial institution regulated/ supervised by the Bangladesh Bank;</li> <li>• A Non-Bank Finance Institution (NBFI) regulated/ supervised by Bangladesh Securities and Exchange Commission (BSEC) unless an entity is notified for application of the requirements;</li> <li>• A government entity;</li> <li>• A foreign government entity;</li> <li>• Public administrations or enterprises;</li> <li>• An entity listed on any stock exchange in Bangladesh; and</li> <li>• An entity listed on a stock exchange outside Bangladesh that is subject to regulatory disclosure requirements and its information is publically available.</li> </ul>
<p>Low risk factors for Products &amp; Services and Delivery Channels</p>	<ul style="list-style-type: none"> <li>• Basic Banking Accounts (BBA);</li> <li>• Low value accounts having monthly credit turnover below Tk. 50,000/-</li> <li>• Salary accounts of individuals subject to the condition that account is not used for other than salary purposes.</li> <li>• Pension accounts for direct credit of pensions.</li> <li>• Remittance cards restricted to receive inward remittances only, and</li> <li>• Other financial products or services that provide appropriately defined and limited services to certain types of customers so as to increase access to financial services.</li> </ul>

<p>Low risk factors for Geographic Locations</p>	<ul style="list-style-type: none"> <li>• Country identified by credible sources such as mutual evaluation or detailed assessment reports, as adequately complying with and having effectively implemented the FATF recommendations; and</li> <li>• Country identified by credible sources as having a low level of corruption, or other criminal activity.</li> </ul>
--	---

In respect of general low risk elements mentioned earlier, bank has to perform such SDD measures as it considers adequate to effectively establish the identity of the customer, a natural person appointed to act on behalf of the customer and any beneficial owner. The SDD measures should be in accordance with pre-defined criteria within AML/CFT policy of BFIU. It should have commensurate with the low risk factors e.g. the SDD measures could relate only to customer acceptance measures or to aspects of on-going monitoring. Examples of such SDD measures may include:

- a) Decreasing the frequency of customer identification updates;
- b) Reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable monetary threshold; and
- c) Not collecting specific information (no exemption shall be presumed in respect of minimum documents for carrying out specific measures to understand the purpose and intended nature of the business relationship, but intended purpose and nature of account may be ascertained from the relationship established or from the type of transactions).

## **5.5 Situations that Require More Measures:**

- a) When there is a suspicion of money laundering or financing of terrorism;
- b) There are no exceptions in reporting STR to BFIU within the provisions of AML-CFT Act.
- c) In case of certain high risk factors identified by the branches in its own internal risk assessment procedures or as per international standards viz-a-viz FATF recommendations etc.
- d) In relation to customers that are from or in jurisdictions which have been identified for inadequate AML/CFT measures by FATF or identified by the branches of bank itself having poor AML/CFT standards or otherwise identified by the Bangladesh Financial Intelligence Committee, Bangladesh Bank.

## **5.6 Products and Services:**

Certain products and services offered by Sonali Bank Limited may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive:

- Electronic funds payment services —automated clearing house (ACH) transactions, and automated teller machines (ATM).
- Electronic banking.
- Trust and asset management services.
- Monetary instruments. Monetary instruments in this context include official bank checks, cashier's checks, money orders, and traveler's checks.
- Foreign correspondent.
- Trade finance.
- Services provided to third party payment processors or senders.
- Foreign exchange.
- Special use or concentration accounts.
- Lending activities, particularly loans secured by cash collateral and marketable securities.
- Non deposit account services (e.g., non deposit investment products and insurance).
- Anonymous transaction.
- Non face to face business relationship or transaction.

## **5.7 Techniques of reducing risks against few Products and Services:**

### **1. Electronic fund transfer:**

- a. All the employees of the bank have to be trained regarding running electronic fund payment process.
- b. Trust worthiness of the employees involved in such job to be evaluated.
- c. Regular monitoring to be conducted.
- d. Transferring big amount from any account has to be ensured contacting the operator/account holder over phone or by any means.

### **2. Trade finance: (KYC profile to be completed relating all sorts of banking)**

- a. Nature of business to be ensured.
- b. Utilization of fund to be financed has to be ensured.
- c. Turn over of account has to be monitored regularly.
- d. Related copy of license and paper has to be kept in the bank / branch.
- e. Transaction of personal account and trade account has to be monitored.

f. If any deviation is found where there is no reasonable ground in conducting transaction, this has to be reported as Suspicious Transaction (STR) to the BFIU explaining reasons with necessary papers/documents.

### **3. Customers and Entities :**

Although any type of account is potentially vulnerable to money laundering or terrorist financing, by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of risk assessment process, it is essential that banks exercise judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk banks should consider other variables, such as services sought and geographic locations.

### **4. Geographic Locations:**

Identifying geographic locations that may pose a higher risk is essential to a bank's AML-CFT compliance program. Every branch has to understand and evaluate the specific risks associated with doing business in opening accounts for customer's form, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively. Higher-risk geographic locations can be either international or domestic. International higher-risk geographic locations generally include:

- Countries subject to UN and OFAC sanctions, including state sponsors of terrorism are very risky in dealing with. Lists of such countries, jurisdictions and governments are available on the OFAC or UN websites.
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing identified as non cooperative by international entities such as the Financial Action Task Force (FATF).
- There are some locations (districts) within the country, such as border area and where riot often occurs due to religious fanaticism

Every concern branch of Sonali Bank Limited has to complete this analysis by reviewing the level and trend of information pertaining to banking activities identified, for example:

- Funds transfers.
- Private banking.
- Monetary instrument sales.
- Foreign correspondent accounts.
- Branch locations.
- Domestic and international geographic locations of the bank's business area.

This information should be evaluated relative to such factors as the bank's total asset size, customer base, entities, products, services, and geographic locations. Bank should exercise caution if comparing information between banks and use their experience and insight when performing this analysis. Specifically, bank should avoid comparing the number of STR filed by a branch to those filed by another bank or branch in the same geographic location. Bank can and should use its knowledge of the risks associated with products, services, customers, entities, and geographic locations to help them determine the bank's AML risk profile.

## **5.8 Resort to Manage the Risks:**

1. All relevant information which is satisfactory for opening account or establishing relationship has to be taken.
2. The information relating to KYC (Know Your Customer) includes the following:
  - a. What the person/entity does.
  - b. To analyze previous record / information about the person / entity.
  - c. Source of earning to be ensured.
  - d. What sorts of profession/business against the source of fund is involved?
  - e. How long the profession is running of the customer?
  - f. What the reasons behind to give up the previous business/job/profession etc.
  - g. Size and volume of worth to be understood.
  - h. In support of identity regarding the above relevant documents/paper to be taken.
  - i. In case of all sorts of transactions TP (Transaction Profile) to be taken with a view to identifying suspicious transaction.



## CHAPTER 06: AML-CTF Compliance Structure

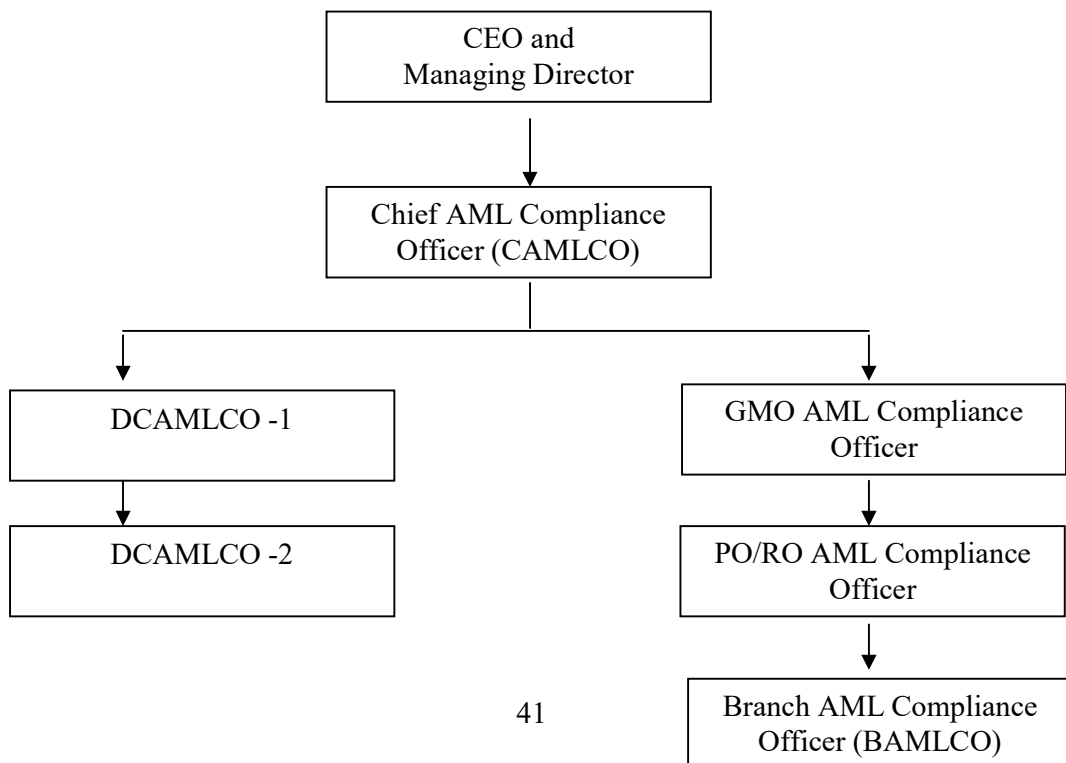
### 6.1 Policy Manual and Management's Commitment:

In order to prevent Money Laundering and Terrorist Financing, **Sonali Bank Limited** has issued its own policy manual conforming international standards, laws and regulations in force in Bangladesh and instructions of BFIU on preventing money laundering and terrorist financing, and this policy manual is approved by the Board of Directors (BoD) of the bank. This policy will be updated from time to time and at least biennially.

This policy manual is communicated to all concerned persons and offices. Bank conducts review of the policy manual from time to time and amends/modifies where necessary. Besides, with a view to keeping banks business and customer services safe and retaining bank's reputation high, The CEO and Managing Director of the bank announces effective and specific commitment, gives the necessary instructions to employees of all Branches, Regional Offices/Principal Offices (ROs/POs), General Manager's Offices (GMOs) and Head Office (HO) to fulfill the commitments in preventing ML & TF and shall ensure the implementation of the commitments. This statement of commitment is issued very outset of every year.

### 6.2 Compliance Structure for AML-CFT:

The Compliance structure of Sonali Bank Limited for the prevention of Money Laundering and Terrorist Financing is as follows:



### 6.3 Central Compliance Committee (CCC):

To keep the bank free from the risks related to Money Laundering & Terrorist Financing and for the effective compliance of all existing acts, rules, guidelines and instructions issued by BFIU time to time, Sonali Bank Limited has set up a Central Compliance Committee (CCC) which is directly accountable to the CEO and Managing Director of the bank. The CCC is headed by a Deputy Managing Director (DMD) who is also the Chief Anti Money Laundering Compliance Officer (CAMLCO) of the bank.

One Deputy General Manager and one Assistant General Manager are also nominated as the Deputy Chief Anti Money Laundering Compliance Officer-1 (DCAMLCO-1) and DCAMLCO-2 respectively. The CAMLCO, DCAMLCO-1 and DCAMLCO-2 are well conversant in existing acts, rules, regulations, instructions issued by BFIU from time to time and international standards on prevention of ML & TF.

The CCC of Sonali Bank Limited has been formed in banks Head Office comprising following executives:

Sl No.	Designation	Division	Position in the CCC
1	Deputy Managing Director and CAMLCO	-	President
2	General Manager	Money Laundering, Terrorism Financing Prevention & Vigilance Division (MLTFPVD)	Member
3	Deputy General Manager	Human Resource Development Division	Member
4	Deputy General Manager	Branches' Control Division (BCD)	Member
5	Deputy General Manager	Business Development Division (BDD)	Member
6	Deputy General Manager	General Advances Division (GAD)	Member
7	Deputy General Manager	Information Technology Division (Business IT)	Member
8	Deputy General Manager	Foreign Remittance Management Division	Member
9	Deputy General Manager	International Trade Finance Division	Member
10	Deputy General Manager	Treasury Management Division-2 (Mid & Back Office)	Member
11	Deputy General Manager	MLTFPVD	Member Secretary & DCAMLCO-1
12	Assistant General Manager	MLTFPVD	Member & DCAMLCO-2

All members of the CCC have enough knowledge on AML & CFT measures of Bangladesh including MLPA, ATA and rules and instructions issued by BFIU or Bangladesh Bank. Meeting of the CCC will be held in every three months and decision of the meeting should be conveyed to all Offices and Branches of the bank.

#### **6.4 Authorities and Responsibilities of the CCC:**

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

- develop banks policy, procedure and strategies in preventing ML, TF & PF;
- coordinate banks AML & CFT compliance initiatives;
- coordinate the ML & TF risk assessment of the bank and review thereon;
- present the compliance status with recommendations before the CEO & Managing Director on half yearly basis;
- forward STR 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 on AML & CFT to the employees of the bank;
- take required measures to submit information, report or documents to BFIU as per their requirement in time.

#### **6.5 Chief Anti Money Laundering Compliance Officer (CAMLCO):**

Sonali Bank Limited has designated one Deputy Managing Director (DMD) as the Chief Anti Money Laundering Compliance Officer (CAMLCO) at its head office and entrusted him with sufficient authority to implement and enforce AML&CFT policies, procedures and measures for the bank. He will report directly to the CEO & Managing Director. 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.

The CAMLCO, directly or through the CCC, is the central point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML&CFT program. If the CAMLCO is changed, Bank has to inform it to BFIU without delay. 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.

All staffs engaged in the bank at all levels must be made aware of the identity of the CAMLCO, his deputies (DCAMLCO-1 & DCAMLCO-2) and the staff and branch/unit level AML&CFT compliance officers, and the procedure to follow when making a suspicious transaction/activity report (STR/SAR). All relevant staffs must be aware of the chain through which suspicious transaction/activity reports should be passed to the CAMLCO.

### **6.5.1 Authorities and Responsibilities of CAMLCO:**

#### **Authorities-**

- CAMLCO should be able to act on his own authority;
- He/she should not take any permission or consultation from/with the CEO & MD before submission of STR/SAR and any document or information to BFIU;
- He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He/she must have access to any information of the bank;
- He/she shall ensure his/her continuing competence.

#### **Responsibilities-**

- 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 CEO & MD or BoD for proper functioning of CCC;
- CAMLCO shall review and update ML & TF risk assessment of the bank;
- Ensure that corrective actions have been taken by the bank to address the deficiency identified by the BFIU or Bangladesh Bank.

### **6.6 Branch Anti Money Laundering Compliance Officer (BAMLCO):**

For the implementation of all existing acts, rules, BFIU's instructions and bank's own policies on preventing Money Laundering & Terrorist Financing, every branch has to nominate an experienced official as Branch Anti Money Laundering Compliance Officer (BAMLCO). However, in a branch where branch incumbent is a General Manger, a Deputy General Manger of the General Banking section should be nominated as BAMLCO of the

Branch. Similarly, in a branch where branch incumbent is a Deputy General Manger, an Assistant General Manger of the General Banking section should be nominated as BAMLCO of the Branch. If branch incumbent is an Assistant General Manger, then a Senior Principal Officer (SPO) will be nominated as BAMLCO. On the other hand, if designation of the Branch Manager is SPO and below, he/she will be nominated BAMLCO by its controlling office (PO/RO).

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.

BAMLCO shall arrange AML & CFT meeting with other concerned and important officials of the branch on quarterly basis 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 or Activities (STR/SAR)
- Record keeping
- Training.

### **6.6.1 Responsibilities of a Branch/BAMLCO:**

For preventing ML, TF & PF in the branch, the Branch/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 Sanction List and Domestic Sanction List checked properly before opening a new account, while making any international transaction and providing any services to any Walk-in-Customer;
- keep information of 'Dormant Legacy Accounts' (which were opened before 30/04/2002 and could not maintain proper KYC) 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 or suspicious transaction. There will be a triggering system in CBS (Core Banking Solution) against transaction profile or other suitable threshold. Transactions should be

examined by the branch officials at the end of day to find out any unusual or suspicious transaction considering concerned customer's KYC and documents. Records of all transaction monitoring should be kept in a separate file);

- review cash transactions to find out any structuring;
- review CTR to find out STR therein, if any;
- ensure the checking of UN & Local Sanction List before making any foreign transaction;
- ensure that all the employees of the branch are well aware and capable of identifying any unusual transaction or any attempt of unusual transaction;
- compile Self Assessment Report of the branch regularly and arrange quarterly meeting regularly;
- accumulate the training records of branch officials and take initiatives including reporting to CCC, HRDD, HRMD and training institutes;
- ensure all the required information and document are submitted properly to CCC and any freeze order or stop payment order are implemented properly within stipulated time;
- 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 found, the BAMLCO should report an STR;
- ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements;
- ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.

## **6.7 Responsibilities of GMO, PO, RO:**

Head of the General Manager's Office (General Manager) will nominate through Office Order a Deputy General Manager (DGM) or at least an Assistant General Manager (AGM), if no DGM is available, of his office as the Anti Money Laundering Compliance Officer of the division (G-AMLCO). He/she will be liable to concerned GM with regard to AML/CFT. He/she will always be careful about implementation of AML/CFT related acts, rules and procedures. Head of Principal Office/Regional Office will act as the Anti Money Laundering Compliance Officer of his/her respective region (P/R-AMLCO). They will nominate BAMLCO of the branches under their jurisdictions; closely monitor whether Branch Incumbents/BAMLCOs are properly following AML/CFT related acts, rules and procedures; ensure the matter while inspecting the branches and take necessary measures to bring officials of the branches under AML/CFT related training/workshop.

## CHAPTER 07: Policies & Procedures

### 7.1 Customer Acceptance Policy:

Customer Acceptance Policy of Sonali Bank Limited is as follows:

- i. No relationship shall be established without ensuring correct and complete identification of customer and beneficial owner.
- ii. Banking services or transaction facilities are not allowed for the walk in customer without proper identification.
- iii. Source of income, nature of business, mode of transaction etc. are to be ensured.
- iv. Anonymous or fictitious or short named account, account with fake name or account only with numbers is not allowed for opening with the bank.
- v. UN, Domestic and other, (e.g. OFAC, EU, HMT), if need be, Sanction Lists have to be considered for screening prior to establishing a relationship or at the time of transactions.
- vi. No business relationship shall be established with Shell Bank (Shell bank means a bank that has no physical presence in the country which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.)
- vii. Risk gradation is needed to be considered at the time of opening account with the information of KYC–TP and other information of the client.
- viii. In case of opening account in the name of social elite / influential person necessary enhanced due diligence (EDD) is to be conducted.
- ix. High risk and PEPs customer's account has to be reviewed after every one year.
- x. Customer Due Diligence (CDD) has to be observed properly at the time of completing KYC Profile.
- xi. No relationship / business shall be established with terrorist person and terrorist organization.
- xii. Incoming and outgoing remittance has to be monitored with the information of applicant and beneficial owner.
- xiii. The regulations of Foreign Exchange Regulation Act, 1947 and various instructions issued by Bangladesh Bank under this Act shall be followed in case of opening any account of Non Resident Bangladeshi people.
- xiv. 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 Charter of UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government shall be opened or operated.
- xv. Instructions, issued by the BFIU from time to time, shall have to be followed.



## 7.2 Customer Due Diligence (CDD):

- Customer due diligence (CDD) means the procedures of transaction monitoring including KYC process based on the information, data and documents collected from reliable sources. Customer due diligence is always followed in case of establishing relationship by the bank. Necessary information has to be taken about the source of fund that the transactions are conducted by the customer. The correctness of papers/documents which are submitted by the client has also to be verified.
- Considering the risks, various steps described below shall be followed during CDD procedure:
  - a) while establishing relationship with the customer;
  - b) while conducting financial transaction with the existing customer;
  - c) when there is reasonable ground to suspect about the adequacy or of previously obtained customer identification data; and
  - d) if there is any kind of suspicion regarding Money Laundering or Terrorist Financing arises from a transaction.
- To be sure of the customer's identity and underlying purpose of establishing relationship with the bank, each branch shall collect adequate information up to its satisfaction. "Satisfaction of the bank" means satisfaction of the appropriate authority that necessary due diligence has been conducted considering the risks of the customers in light of existing directions.
- If a person operates an account on behalf of any customer, the concerned bank must satisfy itself that the person has due authorization to operate that account; and shall obtain correct and complete information of the person.
- In case of the accounts operated by trustee and professional intermediaries, after reviewing and being sure of the legal status and accuracy of information of the operators, correct and complete information of all concerned parties shall be collected.
- While establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering (such as the countries and territories enlisted in Financial Action Task Force's Non-cooperating Countries and Territories list), more cautionary Enhanced Due Diligence (EDD) shall have to be ensured.
- After confirming the identification of the beneficial owner, in relation to the satisfaction of themselves and based on the collected information from reliable sources, banks shall ensure the following matters:

- a) If a customer runs an account on behalf of other person on his own name, in that case, besides that customer, correct and complete information on the identity of that person shall have to be collected and preserved;
- b) The controller or the owner of the customer shall have to be identified;
- c) In case of company, the controlling shareholder and shareholder holding 20% or more shares shall be treated as the real beneficiary owner and correct and complete information on their identity shall have to be collected and preserved.

### **7.3 KYC (Know Your Customer) Policies and Procedures:**

Branches of Sonali Bank Limited has to conduct KYC policy prior to opening account or establishing relationship with customers. Complete identification and verification has to be conducted and necessary documents in this regard must be obtained. Uniform Account Opening Form has to be filled with correct and complete information about the customer. Documents in this regard must be obtained and authenticity of which should be ensured by the bank. The information and records is required to be up dated time to time or when deems to be necessary and minimum after **01 (one) year** for the high risk account/customer and **05 (five) years** for the low risk account/customer. Necessary detailed information about the beneficial owners is also required to be obtained and authenticity of the obtained information and records need to be verified by the bank.

#### **7.3.1 Implementation of KYC Policy:**

To implement KYC policy and customer's identification procedures, following data and information is required and need to be verified:

- a) Profession of customer.
- b) Nature of business / job.
- c) Present, permanent and professional address.
- d) Identity of the customer.
- e) Size of business
- f) Status and rank in job/service
- g) Length of business job/service.
- h) Source of wealth.
- i) Source of fund.
- j) Other related information as required by the bank.

### **7.3.2 Walk-In/ One off Customers:**

Branch should collect complete and correct information while serving Walk-in Customer, i.e. a customer without having account with this bank. Banks should know the source of fund and motive of transaction while issuing DD/TT/MT/PO/Online services. At least a copy of National ID (NID) should be obtained.

### **7.3.3 Non Face to Face Customers:**

‘Non face to face customer’ refers to “the customer who opens and operates his/her account by an agent of the bank or by his own professional representative (lawyer, accountant, etc.) without having physical presence at the bank branch”.

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 the same from time to time.

## **7.4 Politically Exposed Persons (PEPs):**

Sonali Bank Limited is required to undertake enhanced due diligence (EDD) for PEPs (as well as their family members and persons known to be close associates). Because, 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. However, these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatizing PEPs as such being involved in criminal activity.

PEPs have recently been categorized by FATF into 3 (three) criteria which include:

- (i) Foreign PEPs;
- (ii) Domestic PEPs (known as Influential Persons: IPs in Bangladesh) and
- (iii) Chief or similar high-ranking positions in an international organization.

Mentionable that, simply ‘PEPs’ generally refers to foreign PEPs and only foreign PEPs automatically should be treated as high risk. Banks are required to conduct Enhanced Due Diligence (EDD) for foreign PEPs. 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.

- (i) **Foreign PEPs:** Foreign PEPs refer to " Individuals who are or have been entrusted with prominent public functions of 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". These instructions will be applied to the family members (spouse, children and their spouses, parents) and close associates of such persons with whom the establishment of business relation may cause risks for reputation of this bank.

### **Responsibilities in case of Foreign PEPs:**

Along with CDD instructions, the following instructions are required to be followed for opening and operating foreign PEP's account with any branch of Sonali Bank Limited:

1. The concerned Branch should follow Risk Management Procedures to determine whether the beneficial owner of any account is PEPs or not.
2. As per proper approval of the higher authority of the bank, the relationship should be established with them.
3. Proper measures should be taken to know the source of assets and fund of the PEPs.
4. The account transaction of them should be monitored regularly.
5. Necessary compliance with Foreign Exchange Regulation Act, 1947 and the regulations of Bangladesh Bank for opening account by the non-resident shall be ensured.

The above mentioned instructions will also be necessary for family members (spouse, children and their spouses, parents) and the close associates of the PEPs.

### **(ii) Domestic PEPs/ Influential Persons (IPs):**

Domestic PEP or Influential Person (IP) refers to "Individuals who are or have been entrusted domestically with prominent public functions, for example head of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials".

Every branch has to assess the customers of branch whether the customers are locally or nationally influential person. If the customer is influential and seems to be in the high risk category, necessary EDD measures have to be taken for monitoring the transactions as per guidelines of BFIU. Accordingly, necessary information must be collected about the beneficial owner of the account.

### **Duties in case of Influential Persons (IPs):**

Concerned Branch of Sonali Bank Limited should determine whether the beneficial owner of the client and accounts are Influential Persons (IPs) or not. If the customer is an IP and seems to be in the high risk category, necessary EDD measures have to be taken for monitoring the transactions as per guidelines of BFIU. Accordingly, necessary information must be collected about family members (spouse, children and their spouses, parents) and the close associates or the beneficial owner of the account.

### **Who Are Politically Exposed Persons (PEPs)?**

Generally PEPs are following individuals (foreign and domestic individuals for foreign PEPs and domestic PEPs/IPs respectively) but not limited to:

- Heads of state or government, ministers and deputy or state ministers;
- Members of parliament or of similar legislative bodies;
- Members of the governing bodies of political parties (generally only apply to the national governing bodies where a member has significant executive power, eg. over the selection of candidates or distribution of significant party funds);
- Senior politicians
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, Charges d'affairs and high-ranking officers in the armed forces;
- Head or the senior executives or members of the administrative, management or supervisory bodies or State-owned enterprises;
- Chief, directors, deputy directors and members of the board or equivalent function of an international organizations

If a person, who is a PEP/IP is no longer entrusted with a prominent public function, that person should continue to be subject to risk-based EDD for a period of at least 12 months after the date he/she ceased to be entrusted with that public function.

**(iii) Chief or similar high-ranking position in an International Organization:**

Chiefs or similar high-ranking position in an International Organization refer to "Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management i.e. directors, deputy directors and members of the board or equivalent functions".

**Responsibilities in case of Chief or similar high-ranking position in an International Organization:**

Concerned Branch of Sonali Bank Limited should determine whether the beneficial owner of the client and accounts are Chief or similar high-ranking position in an International Organization or not. If the customer is a Chief or similar high-ranking position in an International Organization and seems to be in the high risk category, necessary EDD measures have to be taken for monitoring of the transactions as per guidelines of BFIU. Accordingly, necessary information must be collected about family members (spouse, children and their spouses, parents) and the close associates or the beneficial owner of the account.

**7.5 Corresponding Banking:**

‘Cross Border Correspondent banking’ shall refer to “providing banking services to another bank (respondent) by a bank (correspondent). These kinds of banking services shall refer to credit, deposit, collection, clearing, payment, cash management, international wire

transfer, drawing arrangement for demand draft or other similar services approved by the central bank.

While establishing and continuing Cross Border Correspondent Banking relationship, following instructions have to be maintained so that Sonali Bank Limited cannot be used in Money Laundering and Terrorist Financing:

1. Sonali Bank Limited will establish Cross Border Correspondent Banking relationship after being satisfied about the nature of the business of the correspondent or the respondent bank by collecting information through AML-CFT Questionnaire (Annexure-D) and as per BFIU circular no.19 dated 17 September, 2017.
2. Sonali Bank Limited will also obtain approval from its senior management before establishing and continuing any correspondent relationship.
3. Sonali Bank Limited must be sure about the effective supervision of that foreign bank by the relevant regulatory authority.
4. Sonali Bank Limited will not establish or maintain any correspondent relationship with any shell bank and not to establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank (Shell bank means a bank that has no physical presence in the country which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.)
5. Sonali Bank Limited should pay particular attention or conduct Enhanced Due Diligence while establishing or maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standards for the prevention of money laundering and terrorist financing (such as the countries and territories enlisted in High –Risk and Non- Cooperative Jurisdictions in the Financial Action Task Force’s Public Statement). Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained.
6. If any respondent bank (counterpart of SBL) allows **downstream (or, nested) correspondent banking**/direct transactions by their customers to transact business on their behalf (i.e. **payable through account**), the corresponding bank (SBL) must be sure about the appropriate CDD of the customer has done by the respondent bank

(counterpart of SBL). Moreover, it has to be ensured that collecting the information on CDD of the respective customer is possible by the respondent bank (counterpart of SBL) on request of the correspondent bank (SBL).

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

## **7.6 Wire Transfer:**

"**Wire transfer**" refers to such financial transactions that are carried out on behalf of an originator (person or institution) through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution.

### **7.6.1 Cross-Border Wire Transfers:**

(a) Under general or special consideration in case of threshold cross-border wire transfers of 1000 (one thousand) or above USD or equivalent foreign currency, full and accurate information of the originator has to be collected, preserved and sent to intermediary/beneficiary bank. In the said information, originator's account number or Unique Transaction Reference Number where there is no account number must be included so that the transaction can easily be traced out later. Besides, account number of the beneficiary or Unique Transaction Reference Number where there is no account number, must be included in the beneficiary's information so that the transaction can easily be traced out later.

(b) Furthermore, for transactions below the threshold limit, information, such as: name, address etc. and account number of originator and beneficiary or Unique Transaction Reference Number where there is no account number must be included so that the transaction can easily be traced out later.

(c) For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved.

(d) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file has to contain required and accurate originator information, and full beneficiary information. Moreover, account number of originator and beneficiary or Unique Transaction Reference Number where there is no account number must be included so that the transaction can easily be traced out later.

## **7.6.2 Domestic Wire Transfers:**

In case of threshold domestic wire transfers of at least 25000/- (twenty five thousands) BDT, full and accurate information of the originator has to be collected, preserved and sent to intermediary/beneficiary bank/institutions. Furthermore, for domestic wire transfers below the threshold full and meaningful originator information has to be preserved. For providing money of domestic wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved and instructions stipulated in 7.6.1 has to be followed, where necessary. In case of wire transfer by using debit or credit card (except buying goods and services), similar information as above has to be preserved in the payment related message/instructions.

## **7.7 Duties of Ordering, Intermediary and Beneficiary Bank in Wire Transfer:**

### **Ordering Bank:**

The ordering bank should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information. These information has to be preserved for minimum 5 (five) years. Furthermore, ordering bank will not do any wire transfer without following appropriate instructions described in 7.6.1 and 7.6.2.

### **Intermediary Bank:**

For cross-border and domestic wire transfers, any bank working as an intermediary between ordering bank and beneficiary bank, should ensure that all originator and beneficiary information that accompanies a wire transfer is retained. A record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution (or as necessary another intermediary financial institution).

An intermediary financial institution should have effective risk-based policies and procedures for determining reasonable measures to identify wire transfers that lack required originator information or required beneficiary information such as execution, rejection, or suspension of that wire transfer and the appropriate follow-up action. Such measures should be consistent with straight-through processing.

### **Beneficiary Bank:**

A beneficiary financial institution should initiate risk based procedure to identify wire transfers that lack required originator or required beneficiary information. In case of insufficient originator information concerned parties should collect those information through mutual communication or using any other means. During the payment to receiver/beneficiary, the bank should collect full and accurate information of receiver/beneficiary and should preserve those information for 5 (five) years.



An intermediary financial institution should have effective risk-based policies and procedures for determining reasonable measures to identify wire transfers that lack required originator information or required beneficiary information such as execution, rejection, or suspension of that wire transfer and the appropriate follow-up action. Such measures should be consistent with straight-through processing.

## **7.8 CDD for Beneficial Owners:**

Every branch of Sonali Bank Limited 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, branches should put in place appropriate measures to identify beneficial owner.

The definition of beneficial owner means the individual who –

- a) has effective control of a customer; or
- b) owns a prescribed threshold, 20% as per Bangladeshi regulation of the company or legal arrangements.

Identifying the beneficial ownership of a customer branches must apply three elements. Any one element or any combination of these three elements satisfies beneficial ownership. These elements are:

- a. who owns 20 or more percent of a company or legal arrangements
- b. who has effective control of the customer;
- c. the person on whose behalf a transaction is conducted

Branches, upon their 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 above mentioned aspects while identifying beneficial ownership.

## **7.9 Management of Legacy Accounts:**

Legacy accounts refer those accounts opened before 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. Central Compliance Committee should preserve data of such accounts at their end.

## **7.10 Prevention of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction:**

- Sonali Bank Limited shall establish a procedure by approval of Board of Directors for detection and prevention of financing of terrorism and financing of proliferation of weapons of mass destruction, shall issue instructions about the duties of Bank officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.
- If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, bank shall send the details of the accounts of any persons who are engaged in those activities to BFIU immediately.
- Sonali Bank Limited will preserve electronically the listed person or entity engaged in terrorism, financing of terrorism and financing of proliferation of weapons of mass destruction under different resolutions of United Nations Security Council and any person or banned entity listed by Bangladesh government.
- Sonali Bank Limited will monitor regularly whether there are any account or any transactions in the name of the listed person or entity engaged in terrorism, financing of terrorism and financing of proliferation of weapons of mass destruction under different resolutions of United Nations Security Council and any person or banned entity listed by Bangladesh government or individual or entity which are directly or indirectly controlled by them. If there are any account or any transactions in the name of the listed person or entity engaged in terrorism, financing of terrorism and financing of proliferation of weapons of mass destruction under different resolutions of United Nations Security Council and any person or banned entity listed by Bangladesh government or individual or entity which are directly or indirectly controlled by them, concerned branch shall stop payment or transaction immediately and inform the CCC with detail information of that account at the following day to forward the same to the BFIU.
- If the originator or beneficiary of wire transfer transaction is an individual or entity under the listed person or entity engaged in terrorism, financing of terrorism and financing of proliferation of weapons of mass destruction under different resolutions of United Nations Security Council and any person or banned entity listed by Bangladesh government, immediately after the identification, concerned branch will stop the transaction and inform the CCC with detail information of that account at the following day to forward the same to the BFIU.

- Whether there are any account of individual or entity, under the resolution 1373(2001) of United Nation Security Council, by the request of foreign government or foreign FIU or listed or banned by Bangladesh government under that resolution has to be monitored by Sonali Bank Limited and if necessary all transaction has to be reviewed. Immediately after the identification of any account of any listed individual or entity concerned branch will stop that transaction and inform the CCC with detail information of that account at the following day to forward the same to the BFIU.
- Before any international business transaction, every bank will review the transaction to identify whether the concerned parties of those transactions are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or banned by Bangladesh government. Immediately after the identification of any account of any listed individual or entity concerned branch will stop that transaction and inform the CCC with detail information of that account at the following day to forward the same to the BFIU.

## **7.11 Screening Different Sanction Lists:**

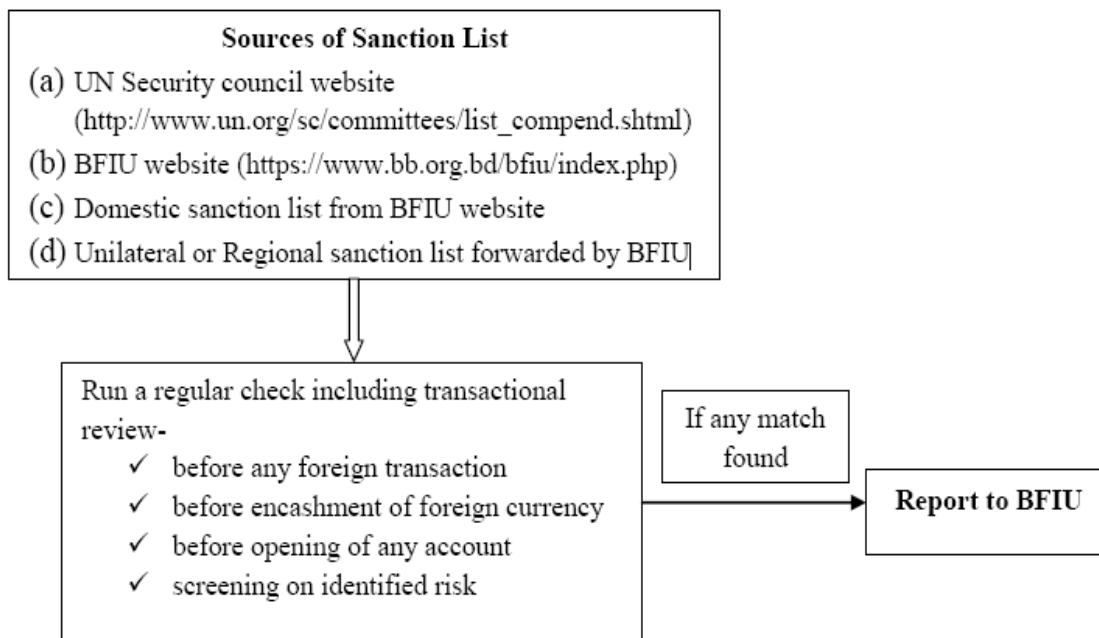
For effective implementation of Targeted Financial Sanctions (TFS) relating to TF & PF, SBL is required to have automated screening mechanism that could prohibit any listed individuals or entities to enter into its banking channel. To comply this requirement, SBL has introduced Screening Module with its CBS system so that branches can screen different Sanction Lists, such as, UN, OFAC, Local etc. automatically and can detect any listed individuals or entities prior to establishing any relationship with them and doing any wire transaction. Concerned officials of all branches shall ensure that screening has done before-

- a. Any international relationship or transaction.
- b. Opening any account or establishing relationship domestically.
- c. Doing any wire transfer.

For proper implementation of different sanction lists, every branch official of SBL must have enough knowledge about-

- a. legal obligation and consequences of non-compliance.
- b. sources of information.
- c. what to do and how to do with sanction list.
- d. transactional review.
- e. how to deal with 'false positives'.
- f. how to deal with actual match.
- g. how to deal with 'aggrieved person or entity'.
- h. how to exercise 'exemption' requirements.
- i. listing & de-listing process.

## 7.12 Flow-Chart for Implementation of TFS by Banks:



## 7.13 Bank's Foreign Branches and Subsidiary Companies:

In BFIU's Circular No. 19, dated 17.09.2017, responsibilities for bank's foreign branches and subsidiaries are mentioned as follows:

- (1) Every bank will ensure appropriate compliance of Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 as well as rules issued under aforementioned acts and instructions issued by BFIU from time to time in their foreign branches and subsidiary companies.
- (2) If foreign branches or subsidiary companies are unable to comply Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 as well as rules issued under aforementioned acts and instructions issued by BFIU from time to time appropriately for any reason, then BFIU must immediately be informed about the reason.

## **CHAPTER 08: Transaction Monitoring**

### **8.1 Transaction Monitoring Process:**

#### **a) Why Transaction Monitoring is Necessary:**

1. It helps the bank to analyze the trend, nature and volume of transactions.
2. Helps to emphasize complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern.
3. To identify the suspicious transaction as it is one of the legal obligations.
4. To prevent fraud and forgery.
5. To help the authority for making decision against account holder
6. To safe the bank from the risk arisen from unusual transaction.
7. Transaction of client is monitored on regular basis in order to identify suspicious transaction and account.
8. An effective system has been developed by Sonali Bank Limited to review the risk by maintaining a specific time interval; and according to the review, Enhanced Due Diligence has been maintained for accounts that are in high risk category.

#### **b) Transaction Monitoring Process:**

With a view to monitoring and identifying suspicious transaction, customer's source of income, nature of transactions, nature of profession, age, size of business, size of organization, nature of organization, and age of client's organizations, frequency of transactions, TP, etc. are necessary to be considered.

- The unusual and potentially suspicious activity is mainly accomplished by an ongoing transaction monitoring.
- Risk-based transaction monitoring for potential money laundering requires the development of risk models that identify the potential risks of money laundering and provide a means of ranking the risks in order to compare the risks with completed transactions.
- An appropriate transaction monitoring process compare the transaction's information against the identified risk, such as geographic location of transaction, the type of products and services being offered and the type of client engaging in the transaction with the different typologies for money laundering and other illicit activities to determine if a transaction is unusual or suspicious.

- This approach requires that a model exists that supports the identification of transactions that deviate from a standard model and allows a risk based review and analysis.
- Transaction monitoring is based on such a concept that provides Sonali Bank Limited with the necessary coverage for review of transaction.

## **8.2 Transaction Profile (TP):**

After opening an account of a person/organization, a declaration on Transaction Profile (TP) with regard to probable monthly transaction shall have to be collected from the customer. A specified TP Form is enclosed with the Uniform Account Opening Form. Cash deposit, cash withdrawal, transfer, foreign remittance, import /export income/expense and other monthly number of transaction, maximum amount of transaction, amount of total deposit or total withdrawal and source of transactional amount shall be written in the TP. Verification and monitoring of the same will be being conducted during transactions. After receiving TP, it shall have to be carefully verified whether Transaction Profile (TP) is consistent with information of the KYC (Know Your Customer) of the concerned customer. If any unusualness is found, Branch must be satisfied by questioning customer/representative of the customer about the matter.

In this case, it shall be carefully investigated whether the customer has concealed/hided any transaction or transaction related information. If it is to be believed after investigation that any type of suspicious transaction is being occurred, measure should be taken to report the same as STR (Suspicious Transaction Report) according to appropriate process. After reviewing the nature of the customer, the source of money in the account and the nature of transaction, bank should again collect the Transaction Profile along with the amendments in it from the customer by reviewing the transactions of the customer within 6 (six) months of establishing business relation and assessing the effectiveness with a logical consideration.

Main purpose of taking TP against continuous account is to identify whether any unusual or suspicious transaction is happening in any account. If transaction of the customer exceeds limit of the TP suddenly, normally transaction cannot be stopped. If customer is unable to satisfy (with information and evidence, where necessary) bankers about alarmed transaction of the account, STR can be filed against related account. TP shall be taken analyzing effectiveness of the customer's monthly income/real transaction of business. Unusual increase of TP limit will not be acceptable.

### 8.3 Cash Transaction Report (CTR):

It is mandatory for all banks and financial institutions to provide Bangladesh Financial Intelligence Unit (BFIU) with Cash Transaction Report (CTR) on monthly basis. As per Money Laundering Prevention Act, 2012 (including Amendment, 2015), Bangladesh Bank collects CTR to know about Cash Flow and preserves economic data/information, identifies and analyzes suspicious transactions of the accounts maintained with Banks and Financial Institutions.

Following instructions of BFIU have to be met for submitting CTR to BFIU:

1. CTR has to be provided for those accounts whose cash deposit/withdrawal (including Online, ATM and any other cash deposit or withdrawal) with a single or several transactions in a day is Taka 10.00 (Ten) Lac or above.
2. Monthly CTR must be submitted to the BFIU within 21<sup>st</sup> day of the following month through goAML.
3. No reportable account will be excluded from the reporting.
4. A list of branch wise number of transactions shall have to be attached.
5. Report with incomplete data/information will automatically be cancelled, i.e., it will be considered that no CTR has been submitted. Considering this, all necessary information need to be furnished with utmost care.
6. If there is no transaction to be reported as CTR, Branch must report to the Central Compliance Committee (CCC) as “**There is no reportable CTR**”.
7. Before submitting CTR, branches must review all cash transactions to identify whether there is any suspicious transaction. If any suspicious transaction is found, then Branch will separately submit it as ‘**Suspicious Transaction Report (STR)**’ to the CCC. If no such transaction is identified, Branch needs to inform the CCC as ‘**No suspicious transaction has been found**’ while reporting the CTR.
8. The CCC will centrally analyze all transactions to be reported as CTR in order to identify whether there is any suspicious transaction among them. If any suspicious transaction is found, the CCC will separately submit it as ‘**Suspicious Transaction Report**’ to the BFIU. If no suspicious transaction is identified, a certificate as ‘**No suspicious transaction has been found**’ signed by the CAMLCO must be attached on goAML Message Board.
9. The CCU must ensure the accuracy and time while reporting to the BFIU.
10. In case of cash deposit in accounts of govt. (different Ministries, Divisions), state owned organizations, semi government or autonomous bodies, there is no need to

submit CTR. However, in case of cash withdrawal from these accounts, CTR must be submitted as usual.

11. In case of inter-bank and inter-branch cash transactions, there is no need to submit CTR.
12. If no transaction is found to be reported as CTR in a particular month, BFIU must be informed with a certificate as “**No CTR is found**” through the Message Board of goAML web.
13. All Branches and controlling offices will preserve CTR information up to 5 (five) years from the month of submission to the BFIU.

#### **8.4 Suspicious Transaction Report (STR):**

According to Section 2(z) of Money Laundering Prevention Act, 2012 (Amendment, 2015)- “suspicious transaction” means such transactions –

- (i) which deviates from usual transactions;
- (ii) of which there is ground to suspect that,
  - (1) the property is the proceeds of an offence,
  - (2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;
- (iii) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit from time to time;

Section 2 (16) of Anti-Terrorism Act, 2009 (Amendment, 2012 & 2013) defines suspicious transaction as follows-

“suspicious transaction” means such transactions –

- (i) which deviates from usual transactions;
- (ii) which invokes presumption that,-
  - (a) it is the proceeds of an offence under this Act,
  - (b) it relates to financing of terrorist activities or a terrorist person or entity;
- (iii) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit from time to time;



On the other hand, as per Section 25(1)(d) of MLPA, 2012 and Section 2(16)(1) of ATA, 2009, if any doubtful transaction or attempt of such transaction as defined “suspicious transaction” under both the Acts is observed, the reporting organization (Bank) has to report the matter as “Suspicious Transaction Report (STR)” to the BFIU immediately on its own accord.

#### **8.4.1 Why Reporting Unusual/Suspicious Transaction is Important?**

Reporting unusual/suspicious transaction is important for the following reasons:

1. There is an obligation to report it under MLPA, 2012 and ATA-2009.
2. It helps bank to minimize its AML-CFT compliance risk.
3. It helps bank to retain its reputation at national and international level.
4. It protects the bank and bankers from the allegation of cooperating money launderers and terrorists.
5. It helps the authority to investigate activities of Money Laundering, Terrorist Financing and other financial scams.

#### **8.4.2 Techniques of identifying Suspicious Transaction/Accounts/Activities:**

AML-CFT compliance activities of any Bank/Financial Institution mostly depend on properly identifying and timely reporting unusual/ suspicious transactions of its customers by the employees of that Bank/FI. So, all officials of the bank must be active and vigilant in identifying suspicious transactions/activities.

Some (but not limited) remarkable signs/indications are given below that indicate accounts or transactions of accounts or activities of the customers are suspicious:

1. Customer’s unwillingness to provide correct and complete address.
2. Finding no genuineness of the address given by the customer.
3. Inconsistency between transaction and profession of the customer.
4. Frequent breach of TP declared by the customer
5. Frequent change of TP by the customer without visible change of income, profession or business.
6. Unwillingness to provide, if asked for, information of the transaction.
7. Informed about deposit of money earned from Predicate Offence.
8. Providing different information at different time by the customer.
9. Notice transactions inconsistency with the customer’s declared income.

10. Occurring huge transactions in the account but having few balances on end of the day.
11. Involvement with different high risk profession/ business.
12. Finding no specific and logical reason behind doing transactions at distant bank despite having banks at own area.
13. Finding inconsistency while verifying customer's said profession.
14. Doing cash transaction of big amount or many transactions of small amount by unknown persons.
15. Opening account at distance area from resident/office.
16. Deposit from different places by DD/TT/Online.
17. Frequently transferring fund to different places through DD/TT/Online for unknown reasons.
18. Frequently doing transactions by representatives instead of customer him/herself.
19. Without any reason, sudden repayment of bank loan prior to sanctioned time.
20. Frequently inviting officers/staffs of the bank for entertainment and trying to make intimacy with them.
21. Providing false statement in spite of having bank account with other Branch or Bank.
22. Relying on under invoicing in case of export and over invoicing in case of import.
23. Finding information on having direct or indirect involvement with terrorist group/ banned organization or helping them.
24. Involvement with illegal or banned profession/business.
25. Publication of adverse report on the customer or his/her business in any print or electronic media.
26. Frequently money receiving/sending from/to the border area.
27. Identify unusual transactions in CTR reported transactions.
28. Trying to hide, disguise, imply or avoid different matters.
29. Providing false address or providing address such a way that it cannot be verified whether the address is genuine or false.
30. In spite of using cheque or other instruments due to nature of the business, sudden cash deposit/withdrawal of unusual big amount.
31. Sudden increase of cash deposit without any logical reason and transfer of the same within a short period of time to the sector apparently not connected with the business or proprietor of the business.
32. Request for paying/receiving big amount of cash transferred to/from other Branch/Bank.
33. Showing interest in cash transaction avoiding normal nature of the account.

34. Existence of many accounts in different names of the clients organizations and showing abnormality in accumulated transactions of all accounts.
35. Operating many accounts in several banks beyond the notice of the bank but information of the other accounts is known to the bank because of repeated accumulation or transfer of the fund.
36. Frequently depositing big amount through other's cheque without any logical reason.
37. Getting one or more locker facilities from the bank suddenly, using the same frequently and keeping and taking sealed packets now and then.
38. Claiming export proceeds showing unacceptable cause.
39. Changing commodity price of imported goods by giving miss-declaration and avoiding custom duties.
40. Remitting money abroad against Letter of Credit (LC) showing fake documents before arrival of the goods in the country.
41. Exchanging foreign currencies without having Authorized Dealer or Money Changer License, or, doing illegal transactions instead of having License.
42. Submitting fake Bill of Entry.
43. Making Structuring transaction to evade CTR

### **8.4.3 Procedures and Steps of Reporting STR/SAR:**

In order to implement AML-CFT properly in the bank, identifying and reporting unusual/suspicious transaction/activity is very important.

Some features of processing STR are described below:

1. Concerned officer of the branch will report to the branch AML compliance officer (BAMLCO) about unusual transaction/activity and its type as soon as it is identified by him/her.
2. Branch Manager and BAMLCO will assess whether suspected transaction of the concerned account has any relation with Money Laundering or Terrorist Financing.
3. If they, following set procedures of AML-CFT, are confirmed about involvement of an account's transaction with Money Laundering or Terrorist Financing, s/he will have to report to the CCU of Head Office through Branch Manager. In this regard, duly filled up Form which was attached with Head Office Circular No. 27 dated 18.09.2008, attested photocopies of account opening form, KYC, TP and 2 (two) set Account Statement (for at least 1 year) of the concerned account and related other information will have to be enclosed along with reason for suspect. Confidentiality of

the matter has to be maintained in all respect. Normal transaction and behavior with the account holder will be continued.

4. Central Compliance Unit (CCU) will review/reexamine reports received from the branch. If they consider the same as reportable, they will confidentially report to the BFIU within 3 days of receipt along with related papers and information.
  1. Any sort of unusual or suspicious transaction has to be reported to the BFIU within the shortest possible time.
  2. For finding such type of transactions, branch needs to monitor transaction type, frequency of transaction, source of fund, unusually large amount, geographical location / origin, changes in account signatories, etc.
  3. If any suspicious transaction is identified by any officer of the branch, he/she has to inform it to the BAMLCO immediately in a written format.
  4. BAMLCO and branch Manager shall analyze the reported transaction or activity in an appropriate manner and preserve their observations on it in a written format without any delay. In this case, they should consider, among others, customer's profession, asset, source of income, purpose and nature of transaction, TP, behavior, linkage to ML-TF, etc.
  5. If the transaction or activity seems to be suspicious, it, along with all necessary supportive documents, i.e., AOF, KYC, TP, A/C Statement and other related documents, has to be sent to the CCC without delay.
  6. CCC shall review whether the reported suspicious transaction or activity has been reported in appropriate manner and with all necessary data, information and documents.
  7. The CCC shall report it, along with all supportive information, data and documents, to BFIU as Suspicious Transaction Report (STR) by using goAML web as per goAML manual.

#### **8.4.4 Responsibilities after Reporting STR/SAR:**

Attention is required to the following issues after reporting STR/SAR by the branch:

1. Transaction with the customer will be continued as usual till getting further instruction from the BFIU, law enforcing agencies or the court.
2. No information with this regard shall be leaked out to the customer.
3. If necessary, STR can be reported further against same account/customer after reporting earlier.
4. Branch shall preserve all information on the reported STR until further instruction is given by BFIU.

## **CHAPTER 09: Self Assessment & ITP**

### **9.1 Self Assessment Report and Independent Testing Procedures:**

According to the instructions of BFIU, branches of bank need to conduct the Self Assessment to evaluate them on a half yearly basis. On the other hand, independent audit shall be done by Inspection and Audit Division of the bank. Self Assessment and Independent Testing Procedures have to be done through a checklist that is circulated by BFIU circular no. 19, dated 17/09/2017 and our Head Office Circular No. 206, dated 03/10/2017. Before finalizing the evaluation report, there shall have to be a meeting presided over by the branch manager with all concerned officials of the branch. In the meeting, there shall be a discussion on the branch evaluation report; if the problems identified in that report can be solved at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations shall have to be jotted down. In the subsequent quarterly meetings on preventing money laundering and terrorist financing, the progress of the related matters should be discussed.

After the end of every half year, the branch evaluation report along with the measures taken by the branch in this regard and adopted recommendations regarding the issue should be submitted to the Inspection and Audit Division of the Head Office and the Central Compliance Committee (CCC) within the 15<sup>th</sup> day of the next month.

### **9.2 Inspection and Audit Division's Obligation Regarding Self Assessment Report and Independent Testing Procedure:**

The Audit and Inspection Division of the bank shall assess the branch evaluation report received from the branches and if there is any risky matter observed in any branch, it shall inspect the branch immediately and shall inform the matter to the CCC.

While executing inspection/audit activities in different branches according to its own regular yearly inspection/audit schedule, the Audit and Inspection Division should examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure. The Audit and Inspection Division should send a copy of the report with the rating of the branches inspected/audited by them to the CCC of the bank.

### **9.3 Central Compliance Committee's Obligation Regarding Self Assessment Report and Independent Testing Procedure:**

Based on the branches' evaluation reports received from the branches and inspection/audit reports submitted by the Audit and Inspection Division, the Central Compliance Committee shall prepare a checklist based evaluation reports on the inspected branches for the respective half year time. In that report, beside other, the following topics must be included:

- a) Total number of branches and number of self assessment reports received from the branches;
- b) The number of branches inspected/audited by the Audit and Inspection Division in the reporting period and the status of the branches (branch wise rating);
- c) Same kinds of irregularities that have been seen in maximum number of branches according to the self assessment report and measures taken by the CCC to prevent those irregularities;
- d) The general and special irregularities mentioned in the report submitted by the Internal Audit Department and the measures taken by the CCC to prevent those irregularities; and
- e) Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as 'unsatisfactory' or 'marginal' in the report.

## **CHAPTER 10: Trade Based Money Laundering**

### **10.1 Trade Based Money Laundering (TBML):**

Definition: In its 2006 study the Financial Action Task Force (FATF) defined trade based money laundering 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, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

### **10.2 Products and Services used in TBML:**

Trade related following Products and Services may be used in trade based money laundering:

- All types of Commercial Documentary Credits
- All types of Bank Guarantees
- All types of Standby LCs
- All types of Bills for Collections
- Open Account Transactions
- Cash in Advance
- All kinds of trade finance and payments
- Import and export of services and software.

So, bankers should be very much cautious and equipped with up-to-date knowledge and technology while dealing with aforesaid trade related products and services.

### **10.3 Parties Involved in Trade:**

Many parties are actively involved in international trade in various points and they differ from one country to another based on the local regulatory requirements involved in the process. However, importer and exporter are the primary parties of international trade and other parties are surrounding them in the process.

#### **1. Import related parties and their activities:**

- a) Buyer and seller furnishes sale/purchase contract.
- b) LC Opening Bank issues/opens the documentary letter of credit (LC) in favor of the importer.

- c) LC Advising Bank advises the LC to the exporter/supplier.
- d) Exporter/Supplier supplies the goods/services as per the terms agreed in the LC.
- e) Shipping Lines/Airlines/Transport Agency transports the goods from supplier's end to the buyer's end.
- f) Port Authority is the custodian of the imported goods till those are released properly.
- g) Customs Authority is responsible to assess and collect duties-taxes on the imported goods.
- h) Clearing Agent acts as the agent of importer to release the goods from the customs.
- i) Indenter is the agent of Supplier.

## **2. Export related parties and their activities:**

- a) Buyer and seller furnishes sale/purchase contract.
- b) LC Advising Bank advises the LC to the exporter/supplier.
- c) Importer/Buyer makes payment to the exporter as per the terms agreed in the LC.
- d) Forwarding Agent acts as the agent of exporter to arrange shipment of the goods.
- e) Shipping Lines/Airlines/Transport Agency transports the goods from supplier's end to the buyer's end.
- f) Port Authority is the custodian of the goods to be shipped for export properly.
- g) Customs Authority is responsible to assess and collect duties-taxes on the exported goods.
- h) LC Negotiating Bank negotiates the transport documents.
- i) Indenter is here the Agent of Buyer.

## **10.4 Techniques used in TBML:**

Following techniques, in general, are used in trade based money laundering:

- a. Over-invoicing in import and under-invoicing in export.
- b. Multiple invoicing of goods and services.
- c. Falsely described goods and services.
- d. Short shipment.
- e. Over shipment.
- f. Phantom shipment whereby the exporter does not ship any goods at all after payments had been made, particularly under confirmed letters of credit.
- g. Complicated payment structure.
- h. Transfer pricing.
- i. Discount

## **10.5 Trade-Based Money Laundering Examples and Red Flags:**

There are several red flags indicating potential TBML. According to the U.S. Immigration and Customs Enforcement (ICE), following are some of them:

- Payments to a vendor by unrelated third parties.
- False reporting, such as commodity misclassification, commodity over- or under-valuation.



- Repeated importation and exportation of the same high-value commodity, known as carousel transactions.
- Commodities being traded that do not match the business involved.
- Unusual shipping routes or transshipment points.
- Packaging inconsistent with the commodity or shipping method.
- Double-invoicing.
- There is reluctance or refusal on the part of the customer to give information, such as where the product is going.
- The products requested do not fit with the company's consistent line of business.
- The potential customer is unfamiliar with intended use of the product your company is selling.
- The product is incompatible with the purported shipping destination.
- The shipping route is abnormal.
- The final destination for the product is a freight-forwarding business.
- Customer prefers to pay cash even if they qualify for open credit terms.
- The customer's suggested payment method is inconsistent with the risk characteristics of the transaction.
- The transaction involves payment by cash, check, wire transfer, postal money orders, etc. from a third party with no obvious connection with the transaction.
- Letters of credit are frequently amended.
- Significant discrepancies in description, value, quality or quantity of goods are apparent on official documents (invoices, bills of lading, etc.).
- Numerous sole proprietorships or private limited companies are controlled by the same group of people.

## **10.6 Measures Needed to Curb Trade-Based Money Laundering:**

Money launderers are always well ahead of bankers in techniques. They also frequently change their techniques of money laundering. So every bank needs to look out present scenarios involving TBML and change its measures and policies in order to mitigate the same. In addition to primary requirements (e.g. KYC/CDD, EDD, Risk Grading, Transaction Monitoring etc.), following measures can be taken to mitigate this type of risk:

1. Price verification
2. Quality of goods testing
3. Quantity of goods testing
4. Use of advanced technology
5. Credit report of supplier/beneficiaries
6. Country of supplier/beneficiaries (Non-cooperative jurisdiction)
7. Shipping documents
8. Identifying and documenting vessel and cargo information including shipping routes, container, vessel types, etc.

## **CHAPTER 11: Employee, Training & Record Keeping**

### **11.1 Know Your Employee (KYE):**

Know Your Customer (KYC), an essential precaution, must be coupled with Know Your Employees (KYE). There are a lot of instances that highlight the involvement of employees in fraudulent transactions and in most cases in association with customers. This, therefore, brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables. Policies, procedures, job descriptions, internal controls, approval levels, levels of authority, compliance with personnel laws and regulations, code of conduct/ethics, accountability, dual control, and other deterrents should be firmly in place. And the auditor should be conversant with these and other requirements, and see that they are constantly and uniformly updated. Above all, KYE requirements should be included in the banks HR policy.

### **11.2 Employee Screening:**

Every bank is subject to ML & TF risk from its customers as well as from its employee in absence of proper risk mitigating measures. ML & TF risks arise from customers and its mitigating measures have been discussed in several chapters of this guideline. ML & TF risks arisen by or through bank's employees can be minimized if the bank follows fair recruitment procedure. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, Sonali Bank Limited has to follow the following measures (at least one from below):

- i. reference check
- ii. background check
- iii. screening through or clearance from Law Enforcement Agency
- iv. personal interviewing
- v. personal guarantee etc.

Before assigning an employee in a particular job or desk, branches or controlling offices (GMOs, POs/ROs) shall examine the consistency and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

### **11.3 AML – CFT Training:**

Training is conducted by Sonali Bank Staff College, 6 Training Institutes of SBL and Central Compliance Committee (CCC) for all the employees of the bank throughout the year. It is an ongoing program for the bank. Refresher training is also considered for the employees of the bank on AML–CFT related laws, rules, AML system or changes of existing AML related policies and practices.

### **11.4 Record Keeping:**

Necessary documents and papers for identification of customers and transactions of accounts are to be preserved minimum five (05) years from the date of closing relationship with the client. As per requirement of BFIU, under AML – CFT Act, bank may provide relevant documents to them if necessary for investigation & analysis.

**RISK REGISTER****i. ML & TF Risk Register for Customers**

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<b>A. Retail Banking Customer</b>					
1	A new customer	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
2	Walk-in customer (beneficiary is government/ semi government/ autonomous body/ bank & NBF)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
3	Walk-in customer ( beneficiary is other than government/ semi government/ autonomous body/ bank & NBF )	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
4	Non-resident customer (Bangladeshi)	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
5	A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
6	A customer making series of transactions to the same individual or entity	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
7	Customer involved in outsourcing business	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
8	Customer appears to do structuring to avoid reporting threshold	1	3	3	1. Response to the risk fairly 2. Proper effort and monitoring in addition to conducting CDD. 3. Scrutinize before reporting to CCC or BFIU.
9	Customer appears to have accounts with several banks in the same area	1	3	3	1. Response to the risk fairly 2. Proper effort and monitoring in addition to conducting CDD. 3. Scrutinize before reporting to CCC or BFIU.
10	Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
11	Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court	1	3	6	1. Response to the risk fairly 2. Proper effort and monitoring in addition to conducting CDD. 3. Scrutinize before reporting to CCC or BFIU.

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
12	Negative news about the customers' activities/ business in media or from other reliable sources	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
13	Customer is secretive and reluctant to meet in person	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
14	Customer is a mandate who is operating account on behalf of another person/ company.	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
15	Large deposits in the account of customer with low income	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
16	Customers about whom BFIU seeks information (individual)	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
17	A customer whose identification is difficult to check	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
18	Significant and unexplained geographic distance between the bank and the location of the customer	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
19	Customer is a foreigner	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
20	Customer is a minor	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
21	Customer is Housewife	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
22	Customers that are politically exposed persons (PEPs) or influential persons (IPs) or chief/senior officials of international organizations and their family members and close associates	3	3	9	1. Approval from higher authority 2. Response to the risk seriously 3. Higher effort and monitoring in addition to conducting proper CDD and EDD. 4. Ensure reporting to CCC or BFIU

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
23	Customer opens account in the name of his/her family member who intends to credit large amount of deposits	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
24	Customers doing significant volume of transactions with higher-risk geographic locations.	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
25	A customer who brings in large amounts of used notes and/or small denominations	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
26	Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
27	Customer is a money changer/courier service agent / travel agent	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
28	Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
29	Customer is involved in Manpower Export Business	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
30	Customer has been refused to provide banking facilities by another bank	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
31	Accounts opened before 30 April, 2002	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
32	Customers with complex accounting and huge transaction	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
33	Receipt of donor fund , fund from foreign source by micro finance institute (MFI)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
34	Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
<b>A. Wholesale Banking Customer</b>					
1	Entity customer having operations in multiple locations	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
2	Customers about whom BFIU seeks information (large corporate)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
3	Owner of the entity that are Influential Persons (IPs) and their family members and close associates	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
4	A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
5	A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
6	A customer whose identification is difficult to check.	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
7	Owner of the entity that are Politically Exposed Persons (PEPs) or chief / senior officials of International Organizations and their family members and close associates	3	3	9	1. Approval from higher authority 2. Response to the risk seriously 3. Higher effort and monitoring in addition to conducting proper CDD and EDD. 4. Ensure reporting to CCC or BFIU
8	Charities or NPOs (especially operating in less privileged areas).	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<b>B. Credit Card Customer</b>					
1	Customer who changes static data frequently	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
2	Credit Card customer	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
3	Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
4	Prepaid Card customer	1	1	1	1. Simplified CDD (Name, Address, Mob/Phone number, NID, etc.)
<b>C. International Trade Customer</b>					
1	A new customer (Outward remittance through SWIFT)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
2	A new customer (Import/ Export)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
3	A new customer (Inward remittance-through SWIFT )	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
4	A new customer who wants to carry out a large transaction (Import/ Export)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
5	A new customer who wants to carry out a large transaction (Inward/ outward remittance)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
6	A customer wants to conduct business beyond its line of business (import/ export/ remittance)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU



Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<b>C. International Trade Customer</b>					
7	Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
8	A new customer who wants to carry out a large transaction (Import/ Export)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
9	Correspondent Banks	3	3	9	1. Approval from higher authority 2. Response to the risk seriously 3. Higher effort and monitoring in addition to conducting proper CDD and EDD. 4. Ensure reporting to CCC or BFIU
10	Money services businesses (remittance houses, exchange houses)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU

ii. Risk Register for Products & Services (including All the Products & Services of SBL)

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<b>A. Retail Banking Product</b>					
1	Accounts for students where large amount of transactions are made (student file)	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
2	Gift Cheque	1	1	1	1. Simplified CDD (Name, Address, Mob/Phone number, NID, etc.)
3	Locker Service	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
4	Foreign currency endorsement in Passport	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
5	Large transaction in the account of under privileged people	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
6	FDR ( less than 2 million)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
7	FDR (2 million and above)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
8	Special scheme deposit accounts opened with big installment and small tenure	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
9	Multiple deposit scheme accounts opened by same customer in a branch	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
10	Multiple deposit scheme accounts opened by same customer from different location	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
11	Open DPS in the name of family member Or Installments paid from the account other than the customer's account	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
12	Stand alone DPS	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
13	Early encashment of FDR, special scheme etc.	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
14	Non face to face business relationship /transaction	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
15	Payment received from unrelated/un-associated third parties	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
<b>B. Retail Privilege Facilities</b>					
1	Pre- Approved Credit Card with BDT 3 lac limit	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
2	Enhanced ATM cash withdrawal Limit BDT 1 lac limit	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
<b>C. SME Banking Product</b>					
1	Want to open FDR where source of fund is not clear	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
2	Early encashment of FDR	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
3	Repayment of loan EMI from source that is not clear	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
4	Repayment of full loan amount before maturity	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
5	Loan amount utilized in sector other than the sector specified during availing the loan	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
6	In case of fixed asset financing, sale of asset purchased immediately after repayment of full loan amount	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
7	Source of fund used as security not clear at the time of availing loan	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
<b>D. Wholesale Banking Product</b>					
1	Development of new product & service of bank	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
2	Payment received from unrelated third parties	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
3	High Value FDR	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
4	Term loan, SOD (FO), SOD (G-work order), SOD (Garment), SOD (PO), Loan General, Lease finance, Packing Credit, BTB L/C	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
5	BG(bid bond), BG(PG), BG(APG)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
6	L/C subsequent term loan, DP L/C	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
7	C.C(H), SOD(G-Business), STL	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
8	OBU	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
9	Syndication Financing	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
<b>E. Credit Card</b>					
1	Supplementary Credit Card Issue	1	1	1	1. Simplified CDD (Name, Address, Mob/Phone number, NID, etc.)
2	Frequent use of Card Cheque	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
3	BEFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
4	Credit card issuance against ERQ and RFCD accounts	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
<b>F. International Trade</b>					
1	Line of business mismatch (import/ export/remittance)	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
2	Under/ Over invoicing (import/ export/ remittance)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
3	Retirement of import bills in cash (import/export/remittance)	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
4	Wire transfer	2	3	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
5	Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/ inward remittance)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.

### iii. Risk Register for Business Practices/Delivery Methods or Channels

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
1	Online (multiple small transaction through different branch)	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
2	BEFTN	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
3	BACH	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
4	IDBP	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
5	Mobile Banking	3	2	6	1. Response to the risk seriously 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Ensure reporting to CCC or BFIU
6	Third party agent or broker	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
<b>B. Credit Card</b>					
1	New Merchant sign up	1	3	3	1. Response to the risk fairly 2. Proper effort and monitoring in addition to conducting CDD. 3. Scrutinize before reporting to CCC or BFIU.
2	High volume transaction through POS	1	2	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
<b>C. Alternate Delivery Channel</b>					
1	Large amount withdrawn from ATMs	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
2	Larger amount transaction from different location and different time(mid night) through ATM	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)
3	Large amount of cash deposit in CDM	2	1	2	1. CDD (KYC, Standard ID Check, Sanction Screening, TP, Transaction Monitoring, Reporting, etc.)

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
4	Huge fund transfer through internet	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
5	Transaction Profile updated through Internet Banking	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
6	Customer to business transaction-Online Payment Gateway -Internet Banking	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
<b>D. International Trade</b>					
1	Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.
2	Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103) .	2	2	4	1. Response to the risk aptly 2. Higher effort and monitoring in addition to conducting proper CDD and EDD. 3. Report to CCC or BFIU if needed.

#### iv. Risk Register for Country/Jurisdiction

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
1	Import and export from/to sanction country	1	3	3	1. Follow FER Act, 1947 2. Follow all circulars and instructions of BFIU and BB 3. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
2	Transshipments, container, flag vessel etc. under global sanction	1	3	3	1. Follow FER Act, 1947 2. Follow all circulars and instructions of BFIU and BB 3. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
3	Establishing correspondent relationship with sanction bank and/or country	1	3	3	1. Follow instructions of BFIU in this regard 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
4	Establishing correspondent relationship with poor AML&CFT practice country	2	2	4	1. Follow instructions of BFIU in this regard 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
5	Customer belongs to higher-risk geographic locations such as High Intensity Financial Crime Areas	1	3	3	1. Follow instructions of BFIU in this regard 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
6	Customer belongs to 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.	1	3	3	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
7	Customer belongs to High Risk ranking countries of the Basel AML index.	1	3	3	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
8	Customer belongs to the countries identified by the bank as higher-risk because of its prior experiences or other factors.	2	2	4	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
9	Any country identified by FATF or FSRBs-(FATF style Regional Body) as not having adequate AML&CFT systems	1	3	3	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
10	Any bank that provide service to 'Shell Bank'	1	3	3	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.



Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
11	Any bank that allow payable through account	2	2	4	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
12	Any country identified as destination of illicit financial flow	1	3	3	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
13	Branches in a Border Area	2	3	6	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
14	Area identified as high risk in the NRA	2	3	6	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.
15	Countries subject to UN embargo/sanctions	1	3	3	1. Follow all circulars and instructions of BFIU 2. Ensure Screening of UN, Local, OFAC and other Sanction Lists.

### v. Register for Regulatory Risk

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
1	Not having AML/CFT guideline	1	3	3	Have two (one Bengali and one English) AML/CFT guidelines approved by the Board of Directors.
2	Not forming a Central Compliance Committee (CCC)	1	3	3	Formed a 11-member Central Compliance Committee (CCC) headed by CAMLCO.
3	Not having an AML&CFT Compliance Officer	1	3	3	One Deputy Managing Director is nominated as CAMLCO.
4	Not having Branch Anti Money Laundering Compliance Officer	1	3	3	Every Branch has a BAMLCO
5	Not having an AML&CFT program	1	3	3	An AML&CFT program is functioning.
6	No senior management commitment to comply with MLP and AT Act	1	3	3	Senior management is committed to comply with MLP and AT Act
7	Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	1	3	3	Ensure compliance of BFIU's circular, circular letter, instructions etc.
8	Unique account opening form not followed while opening account	1	3	3	Follow Unique Account Opening Form while opening account.
9	Non screening of new and existing customers against UNSCR Sanction and OFAC lists	1	3	3	Ensure screening of new and existing customers against UN, Local and OFAC Sanction lists.
10	Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	1	2	2	Strictly follow Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.
11	Complete and accurate information of customer not obtained	1	2	2	Ensure obtaining complete and accurate information of customer.
12	Failure to verify the identity proof document and address of the customer	1	2	2	Ensure verification of the identity proof document and address of the customer
13	Beneficial owner identification and verification not done properly	2	1	2	Ensure proper identification and verification of beneficial owner.
14	Customer Due Diligence (CDD) not practiced properly	1	2	2	Practice Customer Due Diligence (CDD) properly.
15	Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPs and influential person and senior official of international organization.)	1	3	3	Ensure performing Enhanced Due Diligence (EDD) for high risk customers such as PEPs, IPs, Senior Officials of MNCs etc.

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
16	Failure to complete KYC of customer including walk in customer	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
17	Failure to update TP and KYC of customer	2	2	4	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
18	Keep the legacy accounts operative without completing KYC	2	2	4	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
19	Failure to assess the ML & TF risk of a product or service before launching	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
20	Failure to complete the KYC of Correspondent Bank	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
21	Senior Management approval not obtained before entering into a Correspondent Banking relationship	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
22	Failure to comply with the instruction of BFIU by bank Foreign subsidiary	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
23	Failure to keep record properly	2	2	4	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
24	Failure to report complete and accurate CTR on time	2	2	4	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
25	Failure to review CTR	2	2	4	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
26	Failure to identify and monitor structuring	2	3	6	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
27	Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	2	3	6	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
28	Failure to conduct quarterly meeting properly	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
29	Failure to report suspicious transactions (STR)	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
30	Failure to conduct self assessment properly	2	2	4	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.

Sl No.	Risk	Likelihood	Impact	Risk Score	Treatment/Action
31	Failure to submit statement/ report to BFIU on time	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
32	Submit erroneous statement/ report to BFIU	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
33	Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
34	Not submitting accurate information or statement sought by BFIU or BB.	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
35	Not submitting required report to senior management regularly	1	3	3	Ensure submitting required report to senior management regularly.
36	Failure to rectify the objections raised by BFIU or bank inspection teams on time	2	2	4	Rectify the objections raised by BFIU or bank inspection teams on time
37	Failure to obtain information during wire transfer	2	2	4	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
38	Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
39	Failure to scrutinize staff properly	1	3	3	Strictly follow BFIU Circular No. 19, dated 17/09/2017 and other instructions.
40	Failure to circulate BFIU guidelines and circulars to branches	1	3	3	Ensure circulating BFIU guidelines and circulars to all branches and subsidiaries.
41	Inadequate training/ workshop arranged on AML & CFT	1	3	3	Arrange adequate training/ workshop on AML & CFT.
42	No independent audit function to test the AML program	1	3	3	Ensure independent audit function in the bank to test the AML program.

## KYC Documentation

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Individuals	<ul style="list-style-type: none"> <li>➤ Passport</li> <li>➤ National Id Card</li> <li>➤ Birth Registration Certificate (Printed copy, with seal &amp; signature from the Registrar)</li> <li>➤ Valid driving license (if any)</li> <li>➤ Credit Card (if any)</li> <li>➤ Any other documents that satisfy to the bank.</li> </ul> <p>NB: But in case of submitting the birth registration certificate, any other photo id (issued by a Government department or agency) of the person has to be supplied with it. If he does not have a photo id, then a certificate of identity by any renowned people has to be submitted according to the bank's requirement. That certificate must include a photo which is duly attested by the signing renowned person. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.</p>	<ul style="list-style-type: none"> <li>➤ Salary Certificate (for salaried person).</li> <li>➤ Employed ID (For ascertaining level of employment).</li> <li>➤ Self declaration acceptable to the bank. (commensurate with declared occupation)</li> <li>➤ Documents in support of beneficial owner's income (income of house wife, students etc.)</li> <li>➤ Trade License if the customer declared to be a business person</li> <li>➤ TIN (if any)</li> <li>➤ Documents of property sale. (if any)</li> <li>➤ Other Bank statement (if any)</li> <li>➤ Document of FDR encashment (if any)</li> <li>➤ Document of foreign remittance (if any fund comes from outside the country)</li> <li>➤ Document of retirement benefit.</li> <li>➤ Bank loan.</li> </ul>	<ul style="list-style-type: none"> <li>➤ Acknowledgement receipt of thanks letter through postal department.</li> <li>➤ Proof of delivery of thanks letter through courier.</li> <li>➤ Third party verification report.</li> <li>➤ Physical verification report of bank official</li> <li>➤ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name.</li> <li>➤ Residential address appearing on an official document prepared by a Government Agency</li> </ul>

Joint Accounts	<ul style="list-style-type: none"> <li>➤ Passport</li> <li>➤ National Id Card</li> <li>➤ Birth Registration Certificate (Printed copy, with seal &amp; signature from the Registrar)</li> <li>➤ Valid driving license (if any)</li> <li>➤ Credit Card (if any)</li> <li>➤ Any other documents (photo) that satisfy to the bank.</li> </ul>	<ul style="list-style-type: none"> <li>➤ Salary Certificate (for salaried person).</li> <li>➤ Employed ID (For ascertaining level of employment).</li> <li>➤ Self declaration acceptable to the bank. (commensurate with declared occupation)</li> <li>➤ Documents in support of beneficial owner's income (income of house wife, students etc.)</li> <li>➤ Trade License if the customer declared to be a business person</li> <li>➤ TIN (if any)</li> <li>➤ Documents of property sale. (if any)</li> <li>➤ Other Bank statement (if any)</li> <li>➤ Document of FDR encashment (if any)</li> <li>➤ Document of foreign remittance (if any fund comes from outside the country)</li> <li>➤ Document of retirement benefit.</li> <li>➤ Bank loan.</li> </ul>	<ul style="list-style-type: none"> <li>➤ Acknowledgement receipt of thanks letter through postal department.</li> <li>➤ Proof of delivery of thanks letter through courier.</li> <li>➤ Third party verification report.</li> <li>➤ Physical verification report of bank official</li> <li>➤ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name.</li> <li>➤ Residential address appearing on an official document prepared by a Government Agency</li> </ul>
Sole Proprietorships or Individuals doing business	<ul style="list-style-type: none"> <li>➤ Passport</li> <li>➤ National Id Card</li> <li>➤ Birth Registration Certificate (Printed copy, with seal &amp; signature from the Registrar)</li> <li>➤ Valid driving license (if any)</li> <li>➤ Credit Card (if any)</li> <li>➤ Rent receipt of the shop (if the shop is rental)</li> <li>➤ Ownership documents of the shop ( i.e purchase documents of the shop or inheritance documents)</li> <li>➤ Membership certificate of any association. (Chamber of comers, market association,</li> </ul>	<ul style="list-style-type: none"> <li>➤ Trade License</li> <li>➤ TIN</li> <li>➤ Self declaration acceptable to the bank. (commensurate with nature and volume of business)</li> <li>➤ Documents of property sale. (if injected any fund by selling personal property)</li> <li>➤ Other Bank statement (if any)</li> </ul>	<ul style="list-style-type: none"> <li>➤ Acknowledgement receipt of thanks letter through postal department.</li> <li>➤ Proof of delivery of thanks letter through courier.</li> <li>➤ Third party verification report.</li> <li>➤ Physical verification report of bank official</li> <li>➤ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name.</li> <li>➤ Residential address appearing on an official document prepared by</li> </ul>

	<p>trade association i.e.; Hardware association, cloth merchant association, hawker's association etc.</p> <ul style="list-style-type: none"> <li>➤ Any other documents that satisfy to the bank.</li> </ul>	<ul style="list-style-type: none"> <li>➤ Document of FDR encashment (if any fund injected by en-cashing personal FDR)</li> <li>➤ Document of foreign remittance (if any fund comes from outside the country)</li> <li>➤ Bank loan (if any)</li> <li>➤ Personal borrowing (if any)</li> </ul>	a Government Agency
Partnerships	<ul style="list-style-type: none"> <li>➤ Partnership deed/ partnership letter</li> <li>➤ Registered partnership deed (if registered)</li> <li>➤ Resolution of the partners, specifying operational guidelines/ instruction of the partnership account.</li> <li>➤ Passport of partners</li> <li>➤ National Id Card of partners</li> <li>➤ Birth Registration Certificate of partners (Printed copy, with seal &amp; signature from the Registrar)</li> <li>➤ Valid driving license of partners (if any)</li> <li>➤ Credit Card of partners (if any)</li> <li>➤ Rent receipt of the shop (if the shop is rental)</li> <li>➤ Ownership documents of the shop ( i.e. purchase documents of the shop or inheritance documents)</li> <li>➤ Membership certificate of any association. (Chamber of comers, market association, trade association i.e.; Hardware association, cloth merchant association, hawker's association ect.</li> <li>➤ Any other documents that satisfy to the bank.</li> </ul>	<ul style="list-style-type: none"> <li>➤ Trade License</li> <li>➤ TIN</li> <li>➤ Documents of property sale. (if injected any fund by selling personal property of a partner)</li> <li>➤ Other Bank statement (if any)</li> <li>➤ Document of FDR encashment (if any partner injected capital by enchasing Personal FDR)</li> <li>➤ Document of foreign remittance (if any fund comes from outside the country)</li> <li>➤ Bank loan</li> <li>➤ Personal Borrowing (if any)</li> </ul>	<ul style="list-style-type: none"> <li>➤ Acknowledgement receipt of thanks letter through postal department</li> <li>➤ Proof of delivery of thanks letter through courier.</li> <li>➤ Third party verification report.</li> <li>➤ Physical verification report of bank official</li> <li>➤ Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). The bill should be in the name of the applicant or his/her parent's name.</li> <li>➤ Residential address appearing on an official document prepared by a Government Agency</li> </ul>
Private Limited Companies	<ul style="list-style-type: none"> <li>➤ Passport of all the directors</li> <li>➤ National Id Card of all the directors</li> <li>➤ Certificate of incorporation</li> <li>➤ Memorandum and Articles of Association</li> <li>➤ List of directors</li> </ul>	<ul style="list-style-type: none"> <li>➤ A copy of last available financial statements duly authenticated by competent authority</li> <li>➤ Other Bank</li> </ul>	

	<ul style="list-style-type: none"> <li>➤ Resolution of the board of directors to open an account and identification of those who have authority to operate the account.</li> <li>➤ Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf.</li> <li>➤ Nature of the company's business</li> <li>➤ Expected monthly turnover</li> <li>➤ Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company.</li> </ul>	<ul style="list-style-type: none"> <li>statement</li> <li>➤ Trade License</li> <li>➤ TIN</li> <li>➤ VAT registration</li> <li>➤ Bank loan</li> </ul>	
Public Limited Companies	<ul style="list-style-type: none"> <li>➤ Passport of all the directors</li> <li>➤ National Id Card of all the directors</li> <li>➤ Certificate of incorporation</li> <li>➤ Memorandum and Articles of Association</li> <li>➤ Certificate of commencement of business</li> <li>➤ List of directors in form -XII</li> <li>➤ Resolution of the board of directors to open an account and identification of those who have authority to operate the account.</li> <li>➤ Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf.</li> <li>➤ Nature of the company's business</li> <li>➤ Expected monthly turnover</li> <li>➤ Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company.</li> </ul>	<ul style="list-style-type: none"> <li>➤ A copy of last available financial statements duly certified by a professional accountant</li> <li>➤ Other Bank statement (if any)</li> <li>➤ Trade License</li> <li>➤ TIN</li> <li>➤ Cash flow statement</li> <li>➤ VAT registration</li> <li>➤ Bank loan</li> <li>➤ Any other genuine source</li> </ul>	



Government-Owned entities	<ul style="list-style-type: none"> <li>➤ Statute of formation of the entity</li> <li>➤ Resolution of the board to open an account and identification of those who have authority to operate the account.</li> <li>➤ Passport of the operator (s)</li> <li>➤ National Id Card of the operator (s)</li> </ul>	N/A	N/A
NGO	<ul style="list-style-type: none"> <li>➤ National Id Card of the operator (s)</li> <li>➤ Passport of the operator (s)</li> <li>➤ Resolution of the board of directors to open an account and identification of those who have authority to operate the account.</li> <li>➤ Documents of nature of the NGO</li> <li>➤ Certificate of registration issued by competent authority</li> <li>➤ Bye-laws ( certified)</li> <li>➤ List of Management Committee/ Directors</li> </ul>	<ul style="list-style-type: none"> <li>➤ A copy of last available financial statements duly certified by a professional accountant.</li> <li>➤ Other Bank statement</li> <li>➤ TIN</li> <li>➤ Certificate of Grand / Aid</li> </ul>	
Charities or Religious Organisations	<ul style="list-style-type: none"> <li>➤ National Id Card of the operator (s)</li> <li>➤ Passport of the operator (s)</li> <li>➤ Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account.</li> <li>➤ Documents of nature of the Organisations</li> <li>➤ Certificate of registration issued by competent authority (if any)</li> <li>➤ Bye-laws ( certified)</li> <li>➤ List of Management Committee/ Directors</li> </ul>	<ul style="list-style-type: none"> <li>➤ A copy of last available financial statements duly certified by a professional accountant</li> <li>➤ Other Bank statement</li> <li>➤ Certificate of Grant / Aid/ donation</li> <li>➤ Any other legal source</li> </ul>	
Clubs or Societies	<ul style="list-style-type: none"> <li>➤ National Id Card of the operator (s)</li> <li>➤ Passport of the operator (s)</li> <li>➤ Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account.</li> <li>➤ Documents of nature of the Organisations</li> </ul>	<ul style="list-style-type: none"> <li>➤ A copy of last available financial statements duly certified by a professional (if registered)</li> <li>➤ Other Bank statement</li> <li>➤ Certificate of Grant / Aid</li> </ul>	

	<ul style="list-style-type: none"> <li>➤ Certificate of registration issued by competent authority (if any)</li> <li>➤ Bye-laws ( certified)</li> <li>➤ List of Management Committee/ Directors</li> </ul>	<ul style="list-style-type: none"> <li>➤ Subscription</li> <li>➤ If unregistered declaration of authorized person/body.</li> </ul>	
Trusts, Foundations or similar entities	<ul style="list-style-type: none"> <li>➤ National Id Card of the trustee (s)</li> <li>➤ Passport of the trustee (s)</li> <li>➤ Resolution of the Managing body of the Foundation/Association to open an account and identification of those who have authority to operate the account.</li> <li>➤ Certified true copy of the Trust Deed</li> <li>➤ Bye-laws ( certified)</li> <li>➤ Power of attorney allowing transaction in the account.</li> </ul>	<ul style="list-style-type: none"> <li>➤ A copy of last available financial statements duly certified by a professional (if registered)</li> <li>➤ Other Bank statement</li> <li>➤ Donation</li> </ul>	
Financial Institutions (NBF1)	<ul style="list-style-type: none"> <li>➤ Passport of all the directors</li> <li>➤ National Id Card of all the directors</li> <li>➤ Certificate of incorporation</li> <li>➤ Memorandum and Articles of Association</li> <li>➤ Certificate of commencement of business</li> <li>➤ List of directors in form -XII</li> <li>➤ Resolution of the board of directors to open an account and identification of those who have authority to operate the account.</li> <li>➤ Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf.</li> <li>➤ Nature of the company's business</li> <li>➤ Expected monthly turnover</li> <li>➤ Identity of beneficial owners, holding 20% interest or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time</li> </ul>	<ul style="list-style-type: none"> <li>➤ A copy of last available financial statements duly certified by a professional accountant.</li> <li>➤ Other Bank statement</li> <li>➤ Trade License</li> <li>➤ TIN</li> <li>➤ VAT registration</li> <li>➤ Cash flow statement</li> </ul>	

	employee , officer or director of the company.		
Embassies	<ul style="list-style-type: none"> <li>➤ Valid Passport with visa of the authorized official</li> <li>➤ Clearance of the foreign ministry</li> <li>➤ Other relevant documents in support of opening account</li> </ul>	N/A	

*Important - This is an example of documents that may be taken by a bank in case of establishing business relationship with its clients. But it is a mere example only, the bank should urge correct and accurate information that could satisfy the bank itself.*

### Red Flags pointing to Money Laundering

- ✓ The client cannot provide satisfactory evidence of identity.
- ✓ Situations where it is very difficult to verify customer information.
- ✓ Situations where the source of funds cannot be easily verified.
- ✓ Transactions in countries in which the parties are non-residents and their only purpose is a capital investment (they are not interested in living at the property they are buying).
- ✓ Frequent change of ownership of same property in unusually short time periods with no apparent business, economic or other legitimate reason and between related persons.
- ✓ Client wants to re-sell Property shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.
- ✓ Client wishes to form or purchase a company whose corporate objective is irrelevant to the client's normal profession or activities, without a reasonable explanation.
- ✓ The client sets up shell companies with nominee shareholders and/or directors.
- ✓ Client repeatedly changes Attorneys within a short period of time without any reasonable explanation.
- ✓ Client purchases property in names of other persons or uses different names on offers to purchase, closing documents and deposit receipts.
- ✓ Client deposits a large amount of cash with you to make payments which are outside of the client's profile.
- ✓ Client negotiates a purchase but wants to record a lower value on documents, paying the difference "under the table", (inadequate consideration).
- ✓ Client's documents such as identification, statement of income or employment details are provided by an intermediary who has no apparent reason to be involved, (the intermediary may be the real client).
- ✓ Transaction involves legal entities and there is no relationship seen between the transaction and the business activity of the buying company, or the company has no business activity.
- ✓ Client requests the firm to act as his agent in obtaining high sum bankers' drafts, cashiers' cheques and other cash equivalent or near cash monetary instruments or in making wire transfers to and from other banks or financial institutions, (anonymity).
- ✓ Divergence from the type, volume or frequency of transactions expected in the course of the business relationship.
- ✓ Client gives power of attorney to a non-relative to conduct large transactions (same as above).
- ✓ Use of letters of credit to move money between those countries, where such trade would not normally occur and / or is not consistent with the customer's usual business activity. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.
- ✓ The method of payment requested by the client appears inconsistent with the risk characteristics of the transaction. For example receipt of an advance payment for a shipment from a new seller in a high-risk jurisdiction.
- ✓ The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or that include changes in regard to the beneficiary or location of payment without any apparent reason.

- ✓ Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction of same business entity are indicators for TBML. In this regard the study of foreign exchange remittances may help detect the offence.
- ✓ The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities or sensitive / non co-operative jurisdictions.
- ✓ The commodity is transhipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
- ✓ Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense.
- ✓ Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- ✓ Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.
- ✓ Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management.

### **Red Flags pointing to Financing of Terrorism**

#### Behavioural Indicators:

- ✓ The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- ✓ Use of false corporations, including shell-companies.
- ✓ Inclusion of the individual or entity in the United Nations 1267 Sanctions list.
- ✓ Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
- ✓ Beneficial owner of the account not properly identified.
- ✓ Use of nominees, trusts, family members or third party accounts.
- ✓ Use of false identification.
- ✓ Abuse of non-profit organization.

#### Indicators linked to the financial transactions:

- ✓ The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
- ✓ The transaction is not economically justified considering the account holder's business or profession.
- ✓ A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
- ✓ Transactions which are inconsistent with the account's normal activity.
- ✓ Deposits were structured below the reporting requirements to avoid detection.
- ✓ Multiple cash deposits and withdrawals with suspicious references.
- ✓ Frequent domestic and international ATM activity.
- ✓ No business rationale or economic justification for the transaction.
- ✓ Unusual cash activity in foreign bank accounts.

- ✓ Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- ✓ Use of multiple, foreign bank accounts.

**ANTI-MONEY LAUNDERING & COMBATING FINANCING of TERRORISM  
QUESTIONNAIRE FOR CORRESPONDENT RELATIONSHIP**

**A. BASIC INFORMATION**

1. Name of Institution: \_\_\_\_\_
2. Registered Address: \_\_\_\_\_
3. Website Address: \_\_\_\_\_
4. Principal Business Activities: \_\_\_\_\_
5. Regulatory Authority: \_\_\_\_\_
6. Operational Status:
  - Does your Bank maintain a physical presence in the licensing country?  Yes /  No

**B. OWNERSHIP / MANAGEMENT**

7. Is your institution listed on any stock exchange?  Yes /  No  
If so, which stock exchange?

8. If "No" to Q7, please provide a list of the major shareholders holding more than 10% shares in your institution.

\_\_\_\_\_

\_\_\_\_\_

**C. ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CONTROLS**

If you answer "no" to any question, additional information can be supplied at the end of the questionnaire.

**I. General AML&CFT Policies, Practices and Procedures:**

9. Does your institution have in place policies and procedures approved by your institution's board or senior management to prevent Money Laundering and Combat Financing of Terrorism?  Yes /  No
10. Does your institution have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML/CFT framework?  Yes /  No
11. Has your institution developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions?  Yes /  No
12. Does your institution have a policy prohibiting accounts/relationships with shell banks? (*A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.*)  Yes /  No
13. Does your institution permit the opening of anonymous or numbered accounts by customers?  Yes /  No
14. Does your institution have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?  Yes /  No

15. Does your institution have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates? Yes / No

16. Does your institution have policies and procedures that require keeping all the records related to customer identification and their transactions?  Yes /  No  
If "Yes", for how long? \_\_\_\_\_

## II. Risk Assessment

17. Does your institution have a risk-based assessment of its customer base and their transactions?  Yes /  No

18. Does your institution determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?  Yes /  No

## III. Know Your Customer, Due Diligence and Enhanced Due Diligence

19. Has your institution implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?  Yes /  No

20. Does your institution have a requirement to collect information regarding its customers' business activities?  Yes /  No

21. Does your institution have a process to review and, where appropriate, update customer information relating to high risk client information?  Yes /  No

22. Does your institution have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?  Yes /  No

23. Does your institution complete a risk-based assessment to understand the normal and expected transactions of its customers?  Yes /  No

## IV. Reportable Transactions for Prevention and Detection of ML/TF

24. Does your institution have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?  Yes /  No

25. Where cash transaction reporting is mandatory, does your institution have procedures to identify transactions structured to avoid such obligations?  Yes /  No

26. Does your institution screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities or under the UN security Council Resolution?  Yes /  No



27. Does your institution have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?  Yes /  No

**IV. Transaction Monitoring**

28. Does your institution have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as travelers checks, money orders, etc?  Yes /  No

**V. AML Training**

29. Does your institution provide AML& CFT training to relevant employees of your organisation?  Yes /  No
30. Does your institution communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?  Yes /  No
31. Does your institution provide AML training to relevant third parties if they are employed to carry out some of the functions of your organisation?  Yes /  No

**Space for additional information:**

*(Please indicate which question the information is referring to.)*

.....

.....

**D. GENERAL**

32. Does the responses provided in this Declaration applies to the following entities:  Yes /  No
- Head Office and all domestic branches
  - Overseas branches
  - Domestic subsidiaries
  - Overseas subsidiaries

If the response to any of the above is ‘‘No’’, please provide a list of the branches and /or subsidiaries that are excluded, including the name of the institution, location and contact details.

I, the undersigned, confirm to the best of my knowledge that the information provided in this questionnaire is current, accurate and representative of the anti-money laundering and anti-terrorist financing policies and procedures that are established in my institution.

I also confirm that I am authorized to complete this questionnaire on behalf of my institution.

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Designation: \_\_\_\_\_

Date: \_\_\_\_\_

Contact No: \_\_\_\_\_

Email: \_\_\_\_\_