October 02, 2019

EXTRACT FROM THE MEETING MINUTES OF THE 260TH BOARD MEETING OF BRAC BANK LIMITED HELD ON MONDAY, SEPTEMBER 30, 2019 AT BOARD ROOM, ANIK TOWER (12TH FLOOR), 220/B TEJGAON- GULSHAN LINK ROAD, TEJGAON, DHAKA-1208, BANGLADESH.

Agenda 11: Approval memo on Revised Money Laundering & Terrorist Financing Risk Management Guidelines

Approval memo BBL/HO/RA/BM-260/2019/Agenda-11 dated September 30, 2019 regarding Approval memo on Revised Money Laundering & Terrorist Financing Risk Management Guidelines was tabled, discussed and noted.

Resolved that the Proposal is hereby approved as proposed in the memo.

Extract attested by,

Rais Uddin Ahmad
Company Secretary,
Head of Regulatory Affairs
And CAMLCO
Approval memo on Revised Money Laundering & Terrorist Financing Risk Management Guidelines

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>To facilitate the development of effective AML/CFT regime, the previous version of this policy combined the AML, CFT &amp; KYC/CAP procedures.</td>
<td>Revision incorporated more insights on CDD, EDD, KYC, reporting requirements and specific roles by stakeholders.</td>
</tr>
<tr>
<td>The policy was adopted to fulfill the requirements laid down by BFIU Circular No.10 dated December 28, 2014</td>
<td>This policy has been incorporated with modified requirements stated through BFIU Circular No.1p dated September 17, 2017 which replaced Circular 10.</td>
</tr>
<tr>
<td>The formation and responsibilities of Central Compliance Unit (CCC).</td>
<td>The more specific responsibilities of Central Compliance Committee (CCC) and its secretariat, Anti-Money Laundering Division in order to ensure proper implementation of strategic initiatives to combat ML, TF and PF.</td>
</tr>
<tr>
<td>General risk assessment process of client, products, delivery channels and geographic locations.</td>
<td>Directives to perform appropriate diligence in wire transfer transactions as per BFIU Circular No. 21: Amendment of Section 9 of BFIU Circular- 19 and enhanced due diligence (EDD) in correspondent banking relationships have been emphasized as per the BFIU Circular No.19 dated September 17, 2017. Considerations pertaining to risk assessment for customers, transaction, delivery channels, and locations have been modified as per requirement.</td>
</tr>
<tr>
<td>Brief directives on identification of ultimate beneficial ownership (UBO) of accounts.</td>
<td>A clause on verification of ultimate beneficial ownership (UBO) of the accounts has been incorporated in compliance to the International best practices focused by Fourth EU Money Laundering Directive, Section 325 and 326 of USA Patriot ACT, UK Money Laundering Regulations 2007 and FATF Recommendations 24 and 25.</td>
</tr>
</tbody>
</table>

BRAC Bank and its senior management are committed to combat money laundering, terrorist financing and proliferation financing in all its forms and manifestation. To facilitate the development of effective AML/CFT regime, a revised draft policy manual, combining of the AML, CFT & KYC/CAP policy, has been developed for BRAC Bank Limited, which is assumed to fulfill the requirements laid down by BFIU Circular No.19 dated September 17, 2017.

The revised policy is enclosed for the approval of the Board.

Rais Uddin Ahmad  
Company Secretary,  
Head of Regulatory Affairs & CAMLCO

Chowdhury Akhtar Asif  
Acting Managing Director & CRO
Money Laundering & Terrorist Financing
Risk Management Guidelines

BRAC BANK LIMITED
September 2019
**List of Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti Money Laundering/Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>AMLD</td>
<td>Anti Money Laundering Division</td>
</tr>
<tr>
<td>APG</td>
<td>Asia Pacific Group on Money Laundering</td>
</tr>
<tr>
<td>ATA</td>
<td>Anti-Terrorism Act</td>
</tr>
<tr>
<td>BAMLCO</td>
<td>Branch Anti Money Laundering Compliance Officer</td>
</tr>
<tr>
<td>BB</td>
<td>Bangladesh Bank</td>
</tr>
<tr>
<td>BBBL</td>
<td>BRAC Bank Limited</td>
</tr>
<tr>
<td>BDT</td>
<td>Bangladesh Taka</td>
</tr>
<tr>
<td>BFU</td>
<td>Bangladesh Financial Intelligence Unit</td>
</tr>
<tr>
<td>CAMLCO</td>
<td>Chief Anti Money Laundering Compliance Officer</td>
</tr>
<tr>
<td>CCC</td>
<td>Central Compliance Committee</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Due Diligence</td>
</tr>
<tr>
<td>CFT</td>
<td>Combating Financing of Terrorism</td>
</tr>
<tr>
<td>CTC</td>
<td>Counter Terrorism Committee</td>
</tr>
<tr>
<td>CTR</td>
<td>Cash Transaction Report</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Actions Task Force</td>
</tr>
<tr>
<td>FI</td>
<td>Financial Institution</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>FSRB</td>
<td>FATF Style Regional Body</td>
</tr>
<tr>
<td>GPML</td>
<td>Global program against Money Laundering</td>
</tr>
<tr>
<td>ICRG</td>
<td>International Cooperation and Review Group</td>
</tr>
<tr>
<td>IOSCO</td>
<td>International Organization of Securities Commissions</td>
</tr>
<tr>
<td>IAIS</td>
<td>International Association of Insurance Supervisors</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>MLPA</td>
<td>Money Laundering Prevention Act</td>
</tr>
<tr>
<td>NCC</td>
<td>National Coordination Committee</td>
</tr>
<tr>
<td>NCCT</td>
<td>Non-cooperating Countries and Territories</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Persons</td>
</tr>
<tr>
<td>PFWMDF</td>
<td>Proliferation of Weapons of Mass Destruction Financing</td>
</tr>
<tr>
<td>SAR</td>
<td>Suspicious Activity Report</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>TP</td>
<td>Transaction Profile</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNODC</td>
<td>UN Office of Drugs and Crime</td>
</tr>
<tr>
<td>UNSCR</td>
<td>United Nations Security Council Resolution</td>
</tr>
</tbody>
</table>
## CONTENTS

<table>
<thead>
<tr>
<th>Sl.</th>
<th>Chapter</th>
<th>Page no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EXECUTIVE SUMMARY</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>AN OVERVIEW OF MONEY LAUNDERING AND TERRORIST FINANCING</td>
<td>8-15</td>
</tr>
<tr>
<td>1.1</td>
<td>Introduction</td>
<td>8</td>
</tr>
<tr>
<td>1.2</td>
<td>General Provision</td>
<td>8</td>
</tr>
<tr>
<td>1.3</td>
<td>Purpose</td>
<td>9</td>
</tr>
<tr>
<td>1.4</td>
<td>Benefits of this Policy Manual</td>
<td>9</td>
</tr>
<tr>
<td>1.5</td>
<td>Defining money laundering</td>
<td>9</td>
</tr>
<tr>
<td>1.6</td>
<td>Stages of money laundering</td>
<td>10-11</td>
</tr>
<tr>
<td>1.7</td>
<td>Why money laundering is done</td>
<td>12</td>
</tr>
<tr>
<td>1.8</td>
<td>Defining terrorist financing</td>
<td>12-13</td>
</tr>
<tr>
<td>1.9</td>
<td>The link between money laundering and terrorist financing</td>
<td>13-14</td>
</tr>
<tr>
<td>1.10</td>
<td>Why we must combat ML &amp; TF</td>
<td>14-15</td>
</tr>
<tr>
<td>1.11</td>
<td>Targeted financial sanctions</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>VARIOUS TYPES/TECHNIQUES OF MONEY LAUNDERING AND TERRORIST FINANCING</td>
<td>16-23</td>
</tr>
<tr>
<td></td>
<td>Trade-Based Money Laundering &amp; terrorist financing (TBML &amp; TF):</td>
<td>16</td>
</tr>
<tr>
<td>2.1</td>
<td>Vulnerabilities of International Trade</td>
<td>16-17</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Basic Techniques of TBML/TF</td>
<td>17-19</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Assessment of Trade Finance Risks</td>
<td>19</td>
</tr>
<tr>
<td>2.1.3</td>
<td>Application of Controls</td>
<td>19</td>
</tr>
<tr>
<td>2.1.4</td>
<td>Key Controls of Letter of Credit (LCs) &amp; Bills for Collection (BCs)</td>
<td>19-20</td>
</tr>
<tr>
<td>2.1.5</td>
<td>CDD for Establishment of LC</td>
<td>20</td>
</tr>
<tr>
<td>2.1.6</td>
<td>EDD for Establishment of LC at Higher Risk Scenario</td>
<td>20-21</td>
</tr>
<tr>
<td>2.1.7</td>
<td>Best Practices to Combat TBML &amp; TF</td>
<td>21-22</td>
</tr>
<tr>
<td>2.1.8</td>
<td>Red Flags of Trade Based Money Laundering</td>
<td>22-23</td>
</tr>
<tr>
<td>2.1.9</td>
<td>Use of Alternative Remittance System</td>
<td>23</td>
</tr>
<tr>
<td>3</td>
<td>INTERNATIONAL INITIATIVES ON ML/TF</td>
<td>24-26</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>24</td>
</tr>
<tr>
<td>3.1</td>
<td>The United Nations</td>
<td>24-25</td>
</tr>
<tr>
<td>3.2</td>
<td>The Financial Action Task Force</td>
<td>25-26</td>
</tr>
<tr>
<td>3.3</td>
<td>Asia Pacific Group on Money Laundering (APG)</td>
<td>26</td>
</tr>
<tr>
<td>3.4</td>
<td>The Egmont group of financial intelligence units</td>
<td>26</td>
</tr>
<tr>
<td>3.5</td>
<td>The Basel committee on banking supervision</td>
<td>26</td>
</tr>
<tr>
<td>4</td>
<td>NATIONAL INITIATIVES ON ML/TF</td>
<td>27-28</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>27</td>
</tr>
<tr>
<td>4.1</td>
<td>Founding member of APG</td>
<td>27</td>
</tr>
<tr>
<td>4.2</td>
<td>Legal framework</td>
<td>27</td>
</tr>
<tr>
<td>4.3</td>
<td>Other various department and Committee</td>
<td>27</td>
</tr>
<tr>
<td>4.4</td>
<td>Risk based approach</td>
<td>28</td>
</tr>
<tr>
<td>5</td>
<td>AML &amp; CFT COMPLIANCE PROGRAM</td>
<td>29-31</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>29</td>
</tr>
<tr>
<td>5.2</td>
<td>Component of AML &amp; CFT compliance program</td>
<td>29</td>
</tr>
<tr>
<td>5.3</td>
<td>Compliance Program Development Of BRAC Bank</td>
<td>29</td>
</tr>
<tr>
<td>5.4</td>
<td>Communication of Compliance Program</td>
<td>30</td>
</tr>
<tr>
<td>5.5</td>
<td>Senior management role</td>
<td>30-31</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td><strong>COMPLIANCE STRUCTURE OF A BANK</strong></td>
<td><strong>32-36</strong></td>
</tr>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>32</td>
</tr>
<tr>
<td>6.2</td>
<td>Central Compliance Committee</td>
<td>32-33</td>
</tr>
<tr>
<td>6.3</td>
<td>Chief anti money laundering compliance officer (CAMLCO)</td>
<td>33-34</td>
</tr>
<tr>
<td>6.4</td>
<td>Appointment of CAMLCO &amp; Formation of CCC for Custodial Service</td>
<td>34</td>
</tr>
<tr>
<td>6.5</td>
<td>Branch anti money laundering compliance officer (BAMLCC)</td>
<td>34-35</td>
</tr>
<tr>
<td>6.6</td>
<td>AML &amp; NBR Affairs:</td>
<td>35</td>
</tr>
<tr>
<td>6.7</td>
<td>Internal control and compliance</td>
<td>35-36</td>
</tr>
<tr>
<td>6.8</td>
<td>External auditor</td>
<td>36</td>
</tr>
<tr>
<td><strong>7 &amp; 8</strong></td>
<td><strong>AML &amp; CFT POLICIES AND PROCEDURES of BRAC BANK LIMITED</strong></td>
<td><strong>37-60</strong></td>
</tr>
<tr>
<td><strong>7.0</strong></td>
<td><strong>POLICY</strong></td>
<td><strong>37-40</strong></td>
</tr>
<tr>
<td>7.1</td>
<td>Written AML &amp; CFT Compliance Policy</td>
<td>37</td>
</tr>
<tr>
<td>7.2</td>
<td>Customer Acceptance Policy</td>
<td>37-39</td>
</tr>
<tr>
<td>7.3</td>
<td>Oversight Policy On bkash</td>
<td>40</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td><strong>PROCEDURES</strong></td>
<td><strong>41-60</strong></td>
</tr>
<tr>
<td>8.1</td>
<td>Customer Due Diligence &amp; KYC Procedures</td>
<td>41</td>
</tr>
<tr>
<td>8.2</td>
<td>How to Perform CDD</td>
<td>41</td>
</tr>
<tr>
<td>8.3</td>
<td>Timing Of CDD</td>
<td>41-42</td>
</tr>
<tr>
<td>8.4</td>
<td>Customer Identity:</td>
<td>42-44</td>
</tr>
<tr>
<td>8.5</td>
<td>Verification of Address</td>
<td>44</td>
</tr>
<tr>
<td>8.6</td>
<td>Verification of Source of Fund/Occupation/Business Information</td>
<td>44-45</td>
</tr>
<tr>
<td>8.7</td>
<td>Introducer</td>
<td>45</td>
</tr>
<tr>
<td>8.8</td>
<td>Nominee</td>
<td>45</td>
</tr>
<tr>
<td>8.9</td>
<td>Corporate Bodies and Other Entities</td>
<td>45-48</td>
</tr>
<tr>
<td>8.10</td>
<td>Partnerships and Unincorporated Businesses</td>
<td>48</td>
</tr>
<tr>
<td>8.11</td>
<td>Internet or Online Based Customer</td>
<td>48</td>
</tr>
<tr>
<td>8.12</td>
<td>Correspondent Banking</td>
<td>48-49</td>
</tr>
<tr>
<td>8.13</td>
<td>Provision of Safe Custody and Safety Deposit Boxes</td>
<td>49</td>
</tr>
<tr>
<td>8.14</td>
<td>Walk-In / One off Customers/On-line transactions</td>
<td>49-50</td>
</tr>
<tr>
<td>8.15</td>
<td>Non Face-to-Face Customers</td>
<td>50</td>
</tr>
<tr>
<td>8.16</td>
<td>CDD for Beneficial Owners</td>
<td>50</td>
</tr>
<tr>
<td>8.17</td>
<td>Verification of Ultimate Beneficial Ownership (UBO)</td>
<td>50-52</td>
</tr>
<tr>
<td>8.18</td>
<td>Exception When Opening a Bank Account</td>
<td>52</td>
</tr>
<tr>
<td>8.19</td>
<td>In Case Where Conducting the CDD Measure is not Possible</td>
<td>52</td>
</tr>
<tr>
<td>8.20</td>
<td>Reliance On Third Party</td>
<td>52</td>
</tr>
<tr>
<td>8.21</td>
<td>Management of Legacy Accounts</td>
<td>53</td>
</tr>
<tr>
<td>8.22</td>
<td>Customer Unique Identification Code</td>
<td>53</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Pages</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>8.23</td>
<td>Politically Exposed Persons (PEPs), Influential Persons and Chief Executives or Top Level Officials of any International Organizations</td>
<td>54-58</td>
</tr>
<tr>
<td>8.24</td>
<td>KYC Procedure</td>
<td>58</td>
</tr>
<tr>
<td>8.25</td>
<td>KYC Profiling</td>
<td>58</td>
</tr>
<tr>
<td>8.26</td>
<td>Risk Categorization – Based on Activity/KYC Profile</td>
<td>58-59</td>
</tr>
<tr>
<td>8.27</td>
<td>Review and Update</td>
<td>59-60</td>
</tr>
<tr>
<td>9</td>
<td>TRANSACTION MONITORING PROCESS</td>
<td>61-67</td>
</tr>
<tr>
<td>9.2</td>
<td>Transaction Profile</td>
<td>61-62</td>
</tr>
<tr>
<td>9.3</td>
<td>On-going transaction monitoring by Branches</td>
<td>63-67</td>
</tr>
<tr>
<td>9.4</td>
<td>Monitoring of Structuring</td>
<td>67</td>
</tr>
<tr>
<td>10</td>
<td>REPORTING TO BFIU</td>
<td>68-75</td>
</tr>
<tr>
<td>10.2</td>
<td>Suspicious Transaction Reporting Procedures</td>
<td>68-71</td>
</tr>
<tr>
<td>10.3</td>
<td>Cash Transaction Report</td>
<td>71-73</td>
</tr>
<tr>
<td>10.4</td>
<td>Self-Assessment Report</td>
<td>73-74</td>
</tr>
<tr>
<td>10.5</td>
<td>Other Return Submission</td>
<td>75</td>
</tr>
<tr>
<td>11</td>
<td>RECRUITMENT, TRAINING AND AWARENESS</td>
<td>76-78</td>
</tr>
<tr>
<td>11.1</td>
<td>Employee Screening</td>
<td>76</td>
</tr>
<tr>
<td>11.2</td>
<td>Know Your Employee (KYE)</td>
<td>76</td>
</tr>
<tr>
<td>11.3</td>
<td>Education And Training Programs</td>
<td>76-77</td>
</tr>
<tr>
<td>11.4</td>
<td>Senior Management/Operations Supervisors</td>
<td>78</td>
</tr>
<tr>
<td>11.5</td>
<td>Customer Awareness</td>
<td>78</td>
</tr>
<tr>
<td>11.6</td>
<td>Awareness Of Mass People</td>
<td>78</td>
</tr>
<tr>
<td>11.7</td>
<td>Refresher Training</td>
<td>78</td>
</tr>
<tr>
<td>11.8</td>
<td>Job Specific Training</td>
<td>78</td>
</tr>
<tr>
<td>12</td>
<td>RECORD KEEPING</td>
<td>79-80</td>
</tr>
<tr>
<td>12.2</td>
<td>Legal Obligations</td>
<td>79</td>
</tr>
<tr>
<td>12.3</td>
<td>Records To Be Kept</td>
<td>79</td>
</tr>
<tr>
<td>12.4</td>
<td>Customer Information</td>
<td>79</td>
</tr>
<tr>
<td>12.5</td>
<td>Transactions</td>
<td>80</td>
</tr>
<tr>
<td>12.6</td>
<td>Internal And External Reports</td>
<td>80</td>
</tr>
<tr>
<td>12.7</td>
<td>Other Measures</td>
<td>80</td>
</tr>
<tr>
<td>12.8</td>
<td>Formats And Retrieval Of Records</td>
<td>80</td>
</tr>
<tr>
<td>13</td>
<td>TERRORIST FINANCING &amp; PROLIFERATION FINANCING</td>
<td>81-90</td>
</tr>
<tr>
<td>13.1</td>
<td>Introduction</td>
<td>81</td>
</tr>
<tr>
<td>13.2</td>
<td>Legal Obligations &amp; BFIU Circular</td>
<td>81</td>
</tr>
<tr>
<td>13.3</td>
<td>Necessity Of Funds By Terrorist</td>
<td>81</td>
</tr>
<tr>
<td>13.4</td>
<td>Sources Of Terrorist Financing</td>
<td>82</td>
</tr>
<tr>
<td>13.5</td>
<td>Movement Of Terrorist Fund</td>
<td>82-83</td>
</tr>
<tr>
<td>13.6</td>
<td>Proliferation Financing</td>
<td>83-87</td>
</tr>
<tr>
<td>13.7</td>
<td>Targeted Financial Sanctions</td>
<td>87-88</td>
</tr>
<tr>
<td>13.8</td>
<td>SANCTION Screening Mechanism At BRAC Bank</td>
<td>88-89</td>
</tr>
<tr>
<td>13.9</td>
<td>Role Of Banks In Preventing TF &amp; PF</td>
<td>89-90</td>
</tr>
<tr>
<td>10</td>
<td>CONCLUSION</td>
<td>90</td>
</tr>
</tbody>
</table>
### ANNEXURE

<table>
<thead>
<tr>
<th>Sl.</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annexure A</td>
<td>ML &amp; TF Risk Assessment Guideline</td>
</tr>
<tr>
<td>Annexure B</td>
<td>KYC DOCUMENTATION RED FLAGS POINTING TO ML/TF</td>
</tr>
<tr>
<td>Annexure C</td>
<td>RED FLAGS POINTING TO MONEY LAUNDERING</td>
</tr>
<tr>
<td>Annexure D</td>
<td>BRAC Bank Oversight Policy on bKash</td>
</tr>
<tr>
<td>Annexure E</td>
<td>SANCTION Screening Mechanism of BRAC Bank</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

In recent years, and especially since the events of September 11, 2001, worldwide efforts to combat money laundering and the financing of terrorism have assumed heightened importance. Money laundering and the financing of terrorism are global problems that not only threaten security, but also compromise the stability, transparency, and efficiency of financial systems, thus undermining economic prosperity. Such global threats of financing terrorism have led financial sector regulators and financial institutions to strengthen their vigilance in support of the efforts of governments to more easily detect attempts to finance terrorism and to minimize the possibility that their jurisdictions or institutions become involved.

BRAC Bank always acknowledge and support the increasing need for a partnership between government, regulators, law enforcement authorities, banks and the general public, both domestically and internationally, to work together to prevent the laundering of the proceeds of criminal activity and terrorism financing. The Board of Directors of BRAC Bank Ltd has considered the fight against financing of terrorism as a team effort and has drawn a policy which will assess the adequacy of the internal controls and procedures to counter terrorist financing. In addition to that, our Board of Directors and Senior Management are strongly committed to sustain high standards of identification and Customer Due Diligence (CDD) information across our entire customer base. BRAC Bank management also believe that on-going monitoring of transactions, training the employees, assisting the law enforcement authorities are as important as strong KYC controls. Accordingly, the bank has invested heavily - and is committed to continuing to do so - in transaction monitoring systems and operational processes to win the battle against money laundering and terrorist financing.

This is basically a new policy manual combining of the AML, CFT & KYC/CAP policy. This policy manual is adopted to fulfill the requirements laid down by BFIU Circular No. 19 dated September 17, 2017. In case of any ambiguity developed due to English version of the BB Circular, original Bangla test is to be considered. CAMLCO is the custodian of this policy manual and preserves the right to explain and clarify any ambiguity that arises from this policy manual.
1.1 INTRODUCTION

For most countries, money laundering and terrorist financing raise significant issues with regard to prevention, detection and prosecution. Sophisticated techniques used to launder money and finance terrorism add to the complexity of these issues. Bangladesh is no exception to this. BRAC Bank is committed to the highest standards of anti-money laundering (AML) compliance and requires management and employees to adhere to these standards to prevent use of our products and services for money laundering purposes. In recognition of the fact that financial institutions are particularly vulnerable to being used by money launderers, BRAC Bank Ltd has been at the forefront in the battle for prevention of money laundering and combating financing of terrorism (CFT). The Board of Directors of the Bank views Money Laundering Prevention as a part of Risk Management strategy and not simply as a stand-alone requirement that is being imposed by legislation. Money Laundering Prevention and Combating Financing of Terrorism are viewed as an integral part of the Bank’s business systems and needs.

This guideline is prepared based on:
1. Money Laundering & Terrorist Financing Risk Management Guidelines 2015 issued by Bangladesh Bank
3. All relevant laws, circulars and guidelines issued by Central Bank of Bangladesh
4. International best practices
5. BFIU-CIRCULAR-19, 2017
6. Money Laundering Rule prevention rules, 2019

1.2 GENERAL PROVISION:

This compliance manual will be effective upon reviewed by the CCC, MANCOM and subsequent approval from the Board of Directors. Accordingly, change of policy is to be approved by the Board of BRAC Bank Limited. However, MD’s approval suffices the changes of policy as recommended by CAMLCO, which to be ratified by Board of BBL during the next review of the policy manual.

All employees of the BRAC Bank Ltd need to comply with this manual and all relevant employees must be thoroughly familiar with and make use of the material contained in this manual. Sufficient copies of this manual will be distributed to all subsidiary companies of the Bank so that it will be readily available to all relevant employees.

CAMLCO is the authority to explain sense and sentiment of the policy. In case of any ambiguity developed due to English version of the BB Circular, original Bangla test is to be considered.

This document shall be kept updated by the AMLD of the bank under the supervision of the CAMLCO.

This document shall also be reviewed as and when required, while the time period between successive reviews shall not exceed three years.
1.3 PURPOSE:

The purpose of this guideline is to:

- Interpret the requirements of the relevant laws and regulations, and how these may be implemented in practice
- Enable bank in implementing an AML & CFT program appropriate to its business having regard to the business size, nature and complexity; and
- Design and implement the systems and controls necessary to mitigate the risks of the bank being used in connection with money laundering and the financing of terrorism

1.4 BENEFITS OF THIS POLICY MANUAL

This guideline is helpful to all concerns with respect to

- Enable us to increase awareness of anti-money laundering & combating financing of terrorism
- Help us to meet the regulatory requirements and international standards.
- Understand the consequences of non-compliance.
- Address the queries regarding the AML/ KYC/CDD procedures of the Bank.
- Operate various AML related monitoring & reporting procedures.

1.5 DEFINING MONEY LAUNDERING

Money Laundering can be defined in a number of ways. However, the fundamental concept of money laundering is the process by which proceeds of a criminal activity is disguised to conceal their illicit origins. However, it can be defined in a number of ways. 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 (9) 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 that the reporting requirement under this Act may also be avoided;
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) lac, 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 favor 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 the value of the property or taka 20(twenty) lac, whichever is greater and in addition to this, the registration of the said entity shall be liable to be cancelled.

1.6 STAGES OF MONEY LAUNDERING

Money laundering process begins after the predicate offences are committed and funds have been generated. The main objective of the money launderer is to transform 'dirty' money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation. Traditionally, it has been accepted that the money laundering process comprises three stages:

(1) Placement-

At this stage, illegal funds or assets are first brought into the financial system. This 'placement' makes the funds more liquid. For example, if cash is converted into a bank deposit, it becomes easier to transfer and manipulate.

(2) Layering-

Separating the proceeds of criminal activity from their source through the use of layers of financial transactions (multiple transfers of funds among financial institutions, early surrender of an annuity without regard to penalties, cash collateralized loans, L/Cs with false invoices/bills of lading, etc.) to disguise the origin of the funds, disrupt any audit trail, and provide anonymity. Launderers want to move funds around, changing both the form of the funds and their location in order to make it harder for law enforcement authorities to identify "dirty" money. At this stage, money launderers use multiple banks and accounts, act as intermediaries and transact through corporations and trusts.

(3) Integration-

Once the funds are layered and distanced from their origins, they are made available to criminals to use and control as apparently legitimate funds which is called 'integration'. The laundered funds are
Made available for activities such as investment in legitimate or illegitimate businesses, or spent to promote the criminal’s lifestyle.

How the 3 Stages are achieved...

Three common factors (3 C’s) identified in laundering operations are; the need to;
- Conceal (conceal the origin and true ownership)
- Control (maintain control of the proceeds)
- Change (change the form of the proceeds)

**Process of Money Laundering**

**SOURCES OF INCOME**
- Tax Crimes
- Fraud
- Embezzlement
- Drugs
- Theft
- Bribery
- Corruption

**PLACEMENT**
- GOAL
  - Deposit Criminal Proceeds in Financial System

  - Change of Currency
  - Change of Denomination
  - Transportation of Cash
  - Cash Deposits

**LAUNDERING**
- GOAL
  - Conceal the Criminal Origin of Proceeds

  - Wire Transfers
  - Withdrawals in Cash
  - Cash Deposits to Other Bank Accounts
  - Split and Merge Between Bank Accounts

**INTEGRATION**
- GOAL
  - Create an Apparent Legal Origin for Criminal Proceeds

  - Creating Fictitious Loans
  -Ignore/Sales, Capital Gains, Dividends, Contracts
  - Financial Statements
  - Disguise Ownership of Assets
  - Criminal Funds Used in Third Party Transactions

---

BRAC Bank Ltd
Page 11 of 123
1.7 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, the 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 of crime often become 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.

1.8 DEFINING 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 carryout:
   a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below 1; 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(1) 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(1) of Anti-Terrorism Act (ATA), 2009, defines terrorist financing as follows: If any person or entity willfully provides, receives, collects or makes arrangements for money, service or any other property, whether from legitimate or illegitimate source, by any means, directly or indirectly, with the intention that, it would, in full or in part, be used-
   a) to carry out terrorist activity;
   b) by a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.
Moreover, according to Anti-Terrorism Act (ATA), 2009 conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act. The penalties for the offences for money laundering are:

(1) In case of a TF offence made by a person, he/she shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or taka 10 (ten) lac, whichever is greater, may be imposed.

(2) In case of a TF offence made by an entity, the Government may list the entity in the Schedule or proscribe and list the entity in the Schedule, by notification in the official Gazette and in addition to that, a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is greater, may be imposed. Moreover, the head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20 (twenty) lac, whichever is greater, may be imposed unless he/she is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

1.9 THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

The techniques used to launder money are essentially the same as those used to conceal the sources of and uses for terrorist financing. 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.

<table>
<thead>
<tr>
<th>Difference between Money Laundering and Terrorist Financing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motivation</td>
</tr>
<tr>
<td>Source of Fund</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

BRAC Bank Ltd
1.10 WHY BRAC BANK 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 governments 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 work 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 activities 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 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.

Therefore, it is the responsibility of all BRAC Bank staff to be proactive and fight against money laundering and terrorist financing.

1.11 TARGETED FINANCIAL SANCTIONS

The term Targeted Financial Sanctions (TFS) means both asset freezing and prohibition to prevent funds on other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. This TFS is a smart solution to combat terrorism, terrorist financing and proliferation financing of weapons of mass destruction (WMD) by state actors or non-state actors from the UN Security Council. In contrast with the economic sanction on a jurisdiction, TFS is imposed on only suspected person or entities while innocent person or entities remain safe.

TFS related to terrorism and terrorist financing:
FATF recommendation 6 requires 'Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)'.

TFS related to Proliferation-
FATF recommendation 7 requires 'Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of The United Nations'.

ML & TF Risk Management Guidelines
VARIOUS TYPES/TECHNIQUES OF MONEY LAUNDERING AND TERRORIST FINANCING

2.1 TRADE-BASED MONEY LAUNDERING & TERRORIST FINANCING (TBML & TF):

The term "Trade-based Money Laundering and Financial Terrorism" refers to the process of disguising the proceeds of crime and moving its value through the use of trade transactions in an attempt to legitimize their illegal origins or finance by their activities.

Misuse of International trade system is one of the main methods by the criminals to integrate their proceeds into the formal economy. As evidence emerges that International trade is becoming a hub of heaven of dirty money.

Traditional Money Laundering are being done in Cash, Cheque, TC, Bond, Stock, Gold, Precious Metal, Wire transfer, Insurance policy, Casino Chips, Luxury Gods, Antiques, Art etc. But with the change of rapid global financial system, Money Laundering & Terrorist Financing activities evolve and transform quickly and which present new threats to our Banking system like Trade Based Money Laundering, Technology based Money Laundering and Proliferation Financing. So, Bank officials shall be aware of such techniques of Money Laundering & Terrorist Financing and keep them updated properly.

2.1.1 VULNERABILITIES OF INTERNATIONAL TRADE

The vulnerabilities of the international trade system are associated with:

- The enormous volume of trade flows, which obscure individual transactions and provide abundant opportunities for criminals/criminal organizations to transfer value across borders;
- The volume of trade not only has the potential to hide individual transactions, but makes oversight and enforcement difficult. Official regulation and monitoring of trade flows involve a range of agencies in Bangladesh and in overseas which add to the complexity of detecting TBML.
- The movement of goods through multiple transshipment points and third parties adds complexity to the money trail and enables criminals to distance themselves from the activity. Variable standards and controls in other jurisdictions can also assist criminals to embed TBML into a complicated chain of trade payments and shipments.
- The complexity associated with (often multiple) foreign exchange transactions and recourse to diverse financing arrangements;
- The additional complexity that can arise from the practice of commingling illicit funds with the cash flows of legitimate business;
- The limited resource of verification procedures or programs to exchange customs data between countries;
Most customs agencies have limited resources to detect illegal trade transactions;

- Generally, customs authority in Bangladesh inspects approximately 5 percent of all cargo shipments entering or leaving the country;
- Customs authority is more focused to collect customs duty than identifying suspicious trade transactions.

In this connection, all AD Branches & concerned Divisions of Head Office are advised to ensure Enhanced Due Diligence (EDD) and precautions in this matter – like various Sanctions, Red-flags, Trade data Tariff Schedule etc.

2.1.2 BASIC TECHNIQUES OF TBML/TF

The basic techniques of trade-based Money Laundering that we found in Bangladesh are:

- Price misrepresentation (Over-invoicing and Under-invoicing of goods and services);
- Multiple-invoicing of goods and services;
- Over-shipments and Under-shipments of goods and services;
- Falsey described goods and services;
- Cross Border Trade (through land port);
- Legitimate shipment of goods to transfer value between criminal groups.
- Disguising laundered funds as international consultancy service fees.
- Phantom or ghost shipments where the relevant paperwork is lodged with authorities, although the goods are not shipped.

A) Over-invoicing and Under-invoicing of goods and services:

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

i. Under-Invoicing in Export: By invoicing the good or service at a price below the "fair market" price, the exporter is able to transfer to the importer, as the payment for the goods or services will be lower than the value that the importer receives when it is sold in the open market.

ii. Under-Invoicing in Import: By the under invoicing of imported item the importer can evade the import duty and taxes. Foreign organization or its agents can use the importing country as dumping station. Multinational companies can use under invoiced import to create a monopoly market.

iii. Over-Invoicing in Export: By invoicing the good or service at a price above the fair market price, the exporter is able to receive value from the importer, as the payment for the goods and service is higher than the value that the importer will receive when it is sold in the open market. The exporter may also issue overpriced invoice to get some facilities that are provided by the Government like Cash Incentives, Subsidies etc. or to get CIP (Commercially Important Person) status or Export Trophy.
IV. Over-Invoicing in Import: By over invoicing of imported item the importer can transfer fund to the importing country. It happens generally in non-traditional items or low-taxed items. Besides this, motive of the importer is exercised through over invoiced imported items to transfer pricing, or to exploit local investors or to get the curb market premium.

B) Multiple-invoicing of goods and services:
Another technique is used to launder funds involves issuing more than one invoice for the same international trade transaction. By invoicing the same goods or services more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions. Generally, this type of technique is rarely used in Bangladesh.

C) Over-shipments and Under-shipments of goods and services:
In addition to manipulating export and import prices, a money launderer can also overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with this so-called “phantom shipment” are routinely processed. Banks and other financial institutions may unknowingly be involved in the provision of trade financing or these phantom shipments.

D) Deliberate obfuscation of the type of goods:
Parties may structure a transaction in a way to avoid altering any suspicion to FIs or to other third parties which become involved. This may simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it. This activity may or may not involve a degree of collusion between the parties involved and may be for a variety of reasons or purposes.

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

F) Phantom Shipping/Ghost Shipping:
A phantom shipping also known as a ghost shipping, is a shipping with no living crew aboard; it may be a ghostly vessel in folklore or fiction, such as the Flying Dutchman, or a real derelict found adrift
with its crew missing or dead under unknown circumstances. The term is sometimes used for ships that have been decommissioned but not yet scrapped.

g) Cross Border Trade (Through Land Port):

Bangladesh is surrounded by India on all sides except for a small border with Myanmar to the far southeast and by the Bay of Bengal to the south. There has been a substantial informal unrecorded trade across the India-Bangladesh land borders (2,429 miles). Much of this trade is quasi-legal and is best characterized as "informal" and the trade generally bypass Customs posts. India-Bangladesh informal trade is essentially one-way, from India to Bangladesh, leaving aside gold, silver and currency which is smuggled into India in part to pay for Indian goods.

2.1.3 ASSESSMENT OF TRADE FINANCE RISKS

As with the other lines of business, services and products, Bank shall apply a risk based approach to the assessment and management of risk in relation to trade finance. In this connection, BRAC Bank Ltd has developed general guidance on a Risk Based Approach named as "ML & TF Risk Assessment Guidelines (Annexure A)" which is considered relevant in the context of trade finance.

2.1.4 APPLICATION OF CONTROLS

Bank shall review trade transactions on an individual basis. Generally, transactions are examined for the application of the ICC rules referred to above and for the workability in terms of whether the conditions as documented conform with international standard banking practice as well as what is known of the customer. This review is used to examine the transaction not only for fraud but also for unusual and potentially suspicious activities. The complex paper based nature of these transactions provides a large amount of information about the parties, goods and services being transferred and involves scrutiny of relevant documents. Whilst certain elements of this process may be automated (e.g. screening of transactions against published lists of sanctioned entities) the overall process of reviewing trade documents by its nature cannot be successfully automated.

Such controls are relevant in the context of anti-money laundering and counter-terrorist financing efforts. The most effective means to identify terrorist involvement in trade finance transactions are for competent authorities to identify those individuals and organizations connected to terrorist activities and provide that information to Bank in a timely manner. Accordingly, trade finance controls screening part of the transactional information against lists of known or suspected terrorists issued by competent authorities having jurisdiction over the relevant FI are relevant in the context of anti-terrorist financing efforts.

2.1.5 KEY CONTROLS OF LETTER OF CREDIT (LCS) & BILLS FOR COLLECTION (BCS)

Due Diligence: Identifying and knowing the customer as well as exercise risk based checks in relation to parties who may not be customers. Given the range of meanings applied reference will be made as necessary to "appropriate due diligence" (which may consist of risk based checks only).
Reviewing: Bank shall be defined as any process (often not automated) to review relevant information in a transaction relating to the relevant parties involved, documentation presented and instructions received. As will also be described under the Risk Indicators section, certain information can and should be reviewed and checked before transactions are allowed to proceed.

Screening: Bank shall introduce an automated process to compare information against reference sources such as terrorist lists. Screening is normally undertaken at the same time as reviewing and prior to the completion of the specific activity subject to review. It may also be undertaken at the same time as, or as part of, due diligence.

Monitoring: Any activity to review completed or in progress transactions for the presence of unusual and potentially suspicious features. For trade transactions, it should be recognized that it is impossible to introduce any standard patterned techniques in relation to account/transactional monitoring processes or systems. This is due to the range of variations which are present even in normal trading patterns.

2.1.6 CDD FOR ESTABLISHMENT OF LC

- Apply Risk Based Approach to the assessment and management of risk.
- Ensure sanction screening (UN, OFAC, HM Treasury, EU, and Local List) before creation of MT700/MT103.
- Sanction Advice duly accepted by the client.
- Documentation/Mortgage formalities completed.
- Up to date Certificates/Licenses/Policies complying the latest Audit Observations. Clean CIB Report
- Factory Compliance
- Credit Ratings
- Environmental Risk ratings
- NOC on overdue Bill of Entry from previous Bank
- NOC on receiving down payment for default client: BF Bills liability to be adjusted within 6 months
- General Indemnity of the client
- Availing singly party exposure

This is not an exhaustive CDD because complexity of business, nature of risk and action plan may vary in case to case.

2.1.7 EDD FOR ESTABLISHMENT OF LC AT HIGHER RISK SCENARIO

An enhanced due diligence process shall be applied where Party/customer falls into a higher risk category or where the nature of their trade as disclosed during the standard due diligence process suggests that enhanced due diligence shall be prudent.

The enhanced due diligence shall be applied to understand the trade cycle, and gain assurance related to compliance with cross border customs or licensing regulations, physical controls over the traded goods and the legitimacy of payments flows. Some of the checks Bank shall undertake (not all of which may be applicable or available in each case) include:

BRAC Bank Ltd
• Make appropriate enquiries into the ownership and background of the other parties to
the transaction e.g., the beneficiary(ies), agents, shipping lines, taking further steps to
verify information or the identity of key individuals as the case demands;
• Seek information from the instructing party about the frequency of trade and the
quality of the business relationships existing between the parties to the transaction.
This should be documented to assist future due diligence;
• Check the transaction against warning notices from the external public sources, for
example the ICC's International Maritime Bureau;
• Refer the transaction to external agencies specializing in search ad validation
services in respect of bills of lading, shipping services and commodity prices, for
example the ICC Commercial Crime Services;
• Check details of the source of the goods;
• Check public source of information for prices of goods such as commodities—
where the contract price is significantly different from the market [say 25%] then
consider further investigation;
• Attend and record relationship meetings with the instructing party, visit
them by arrangement;
• For export letter of credit, refer details to other Group resources on the ground in
the country of origin, to seek corroboration
• Check into the verification of shipments after the UCP operation is over, drawn at
random from a sample of transactions, across a cross section of the bank's trade finance
clients. This may help to identify spurious transactions where buyers and sellers act in
collusion.

This may include third parties, (i.e. parties not associated with Bank) middlemen or traders
using back to back or transferable LCs to conclude offshore deals.

This is not an exhaustive EDD because complexity of business, nature of risk and action plan
may vary in case to case.

2.1.8 BEST PRACTICES TO COMBAT TBML & TF

a) Comparing domestic and foreign import/export data to detect discrepancies in the
Harmonized Tariff Schedule, country of origin, manufacturer, importer/exporter,
ultimate consignee, broker, unit price, commodity activity by the time period, and
port of import/export.

b) Capacity building and increased awareness of TBML to be achieved by enhancing the
focus on TBML through training programs. Developing capacity to identify anomalies
in data collected for trade transactions and in trade finance.

c) Analyzing financial information collected by the FIU to identify patterns of activity
involving the importation/ exportation of currency, deposits of currency in financial
institutions, reports of suspicious financial activities and the identity of parties of these
transactions.

d) Examining cargo movements through the comparison of import/export documentation
between two countries to verify that the data reported to one country's authorities
matches the data reported to other country’s authorities.
e) Examining domestic import data with an automated technique, such as Unit Price Analysis, to compare the average unit price for a particular commodity and identify traders who are importing commodities at a substantially higher or lower price than the world market.

f) Comparing information such as the origin, description and value of the goods, particulars of the consignee and consignor, and the route to shipment with intelligence information in existing data bases to detect any irregularities, targets or risk indicators.

g) Using statistical analysis methods, such as linear regression models, on trade data concerning individual, non-aggregated imports and exports.

h) Comparing export information with tax declarations to detect discrepancies.

i) Paying specific attention to trade transactions that display known red flag indicators of TBML/FT activity.

j) Cross-comparing known typologies of risk such as, those identified in the FATF typologies, report on Trade-based Money Laundering with trade data, information on cross-border money transfers associated with the payment of goods, intelligence, and tax and wealth information.

k) Taking appropriate follow-up action when anomalies and discrepancies in trade and financial transactions are identified. Depending on the circumstances, appropriate follow-up action could involve asking the trader for further explanation and supporting documents; auditing traders who have presented discrepancies to check the volume of their business, regularity of their operations, the kind of good exported, and connections with organized crime or any other illicit activity; and/or making the completed analysis available to the investigative authorities.

This not exhaustive because complexity of business, nature of risk and action plan may vary in case to case.

2.1.9 RED FLAGS OF TRADE BASED MONEY LAUNDERING

Trade Finance Department or any other concerned Department of the Bank shall always be aware of and monitor the following “Red Flag” indicators/situations to identify the trade based Money Laundering and Terrorist Financing activities:

- Significant discrepancies between the description of the commodity of the Bill of Lading and the Invoice.
- Significant discrepancies between the descriptions of goods on the Bill of Lading (or Invoice) and the actual goods shipped.
- Significant discrepancies between the values of the commodity reported on the invoice and the commodity’s fair market values.
- The size of the shipment appears to be inconsistent with the sale of the exporter or importer’s regular business activities.
- The type of commodity being shipped is designated as “high risk” for money laundering activities.
- The type of commodity being shipped appears to be inconsistent with the exporter or importer’s regular business activities.
• The shipment does not make economic sense.
• The commodity is being shipped to or from a jurisdiction designated as "high risk" for money laundering activities.
• The commodity is being trans-shipped through one or more jurisdictions for no apparent economic reason.
• The method of payment appears to be inconsistent with the risk characteristic of the transaction.
• The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction.
• The transaction involves the use of repeated amendment or frequently extended letters of credit.
• The transaction involves the use of fraud (or shell) companies.
• High-value, low-volume goods (e.g., consumer electronics), which have high turnover rates and present valuation difficulties.
• The use of a forty-feet container to transport a small amount of relatively low-value goods.
• The use of an advance payment for a shipment from a new supplier in a high-risk country.

This is not exhaustive because complexity of business, nature of risk may vary in case to case,

2.2 USE OF ALTERNATIVE REMITTANCE SYSTEM:

[Diagram of remittance process]

The US $10,000 debt stands between the bankers. It will be settled by future transactions or reciprocal remittances.
INTERNATIONAL INITIATIVES ON ML AND TF

3.1 INTRODUCTION
In response to the growing concern about money laundering and terrorist activities, the initiatives taken by international communities have acted on many fronts. This part of this Guideline discusses the various international organizations and their initiatives relating to AML/CFT. The details of the initiatives taken by the International Organizations worldwide are described below and BRAC bank must emphasize and should concentrate in implementing all these internal best practices.

3.2 THE UNITED NATIONS
The United Nations (UN) was the first international organization to undertake significant action to fight against money laundering on worldwide basis. In certain cases, the UN Security Council has the authority to bind all member countries through a Security Council Resolution, regardless of other actions on the part of an individual country.

3.2.1 THE VIENNA CONVENTION
Due to growing concern about the increased international drug trafficking and the tremendous amount of related money entering into financial system, 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.

3.2.2 THE PALERMO CONVENTION
In order to fight against internationally organized crimes, the UN adopted the International Convention against Transnational Organized Crime (2000), named after the city in which it was signed as Palermo Convention.

3.2.3 INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM
The financing of terrorism was an international concern prior to the attacks on the United States on 11 September, 2001. In response to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002 with 132 countries signing the convention and 112 countries ratifying it.

3.2.4 SECURITY COUNCIL RESOLUTION 1267 AND SUCCESSORS
The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the Sanctions Committee (now called the 1267 Committee).

3.2.5 SECURITY COUNCIL RESOLUTION 1373
Unlike an international convention, which requires signing, ratification, and recognition in local law by the UN member country to have the effect of law within that country, a Security Council Resolution was passed in response to a threat to international peace and security under Chapter VII of the UN Charter, is binding upon all UN member countries.

3.2.6 SECURITY COUNCIL RESOLUTION 1540
UNSCR 1540 (2004) imposes binding obligations on all States to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery, and establish appropriate domestic controls over related materials to prevent their illicit trafficking.
3.2.7 THE COUNTER-TERRORISM COMMITTEE
As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism.

3.2.8 COUNTER-TERRORISM IMPLEMENTATION TASK FORCE (CTITF)
The Counter-Terrorism Implementation Task Force (CTITF) was established by the Secretary-General in 2005 and endorsed by the General Assembly through the United Nations Global Counter-Terrorism Strategy, which was adopted by consensus in 2006. The mandate of the CTITF is to enhance coordination and coherence of counter-terrorism efforts of the United Nations system.

3.2.9 GLOBAL PROGRAM AGAINST MONEY LAUNDERING
The UN Global Program against Money Laundering (GPML) is within the UN Office of Drugs and Crime (UNODC). The GPML is a research and assistance project with the goal of increasing the effectiveness of international action against money laundering by offering technical expertise, training and advice to member countries upon request.

3.3 THE FINANCIAL ACTION TASK FORCE
The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. 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.

3.3.1 FATF NEW STANDARDS
FATF Plenary again revised its recommendations in February 2012. The previous 40+9 Recommendations was accumulated into 40 (forty) recommendations called the FATF Standards.

Summary of new FATF 40 Standards

<table>
<thead>
<tr>
<th>Group</th>
<th>Topic</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Policies and Coordination</td>
<td>1-2</td>
</tr>
<tr>
<td>2</td>
<td>Money Laundering and Confiscation</td>
<td>3-4</td>
</tr>
<tr>
<td>3</td>
<td>Terrorist Financing and Financing of Proliferation</td>
<td>5-8</td>
</tr>
<tr>
<td>3</td>
<td>Preventive Measures</td>
<td>9-23</td>
</tr>
<tr>
<td>4</td>
<td>Transparency and Beneficial Ownership of Legal Persons and Arrangements</td>
<td>24-25</td>
</tr>
<tr>
<td>5</td>
<td>Power and Responsibilities of Competent Authorities and Other</td>
<td>26-35</td>
</tr>
<tr>
<td>6</td>
<td>International Co-operation</td>
<td>36-40</td>
</tr>
</tbody>
</table>
3.3.2 THE NCCT LIST
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 (NCCTs) and place them on a publicly available list. NCCT was a process of blacklisting non-compliant countries. Considering its massive impact on respective country, the FATF introduced new implementation mechanism known as International Cooperation and Review Group (ICRG).

3.3.3 INTERNATIONAL COOPERATION AND REVIEW GROUP (ICRG)
The FATF has set up the International Co-operation Review Group (ICRG) as a new process that is designed to notably engage those jurisdictions which are ‘unwilling’ and pose a real risk to the international financial system. The ICRG process is designed to bind members of FATF and FATF Style Regional Body (FSRB) that show effective commitment to the standards against those that evade their international obligations.

3.4 ASIA PACIFIC GROUP ON MONEY LAUNDERING (APG)
The Asia Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 41 members and a number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units. APG is the FATF style regional body (FSRB) for the Asia Pacific region.

3.5 THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS
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), named after the location of its first meeting at the Egmont-Arenberg Palace in Brussels. 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 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.

3.6 THE BASEL COMMITTEE ON BANKING SUPERVISION
The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of 10 (ten) countries. Each country is represented by their central banks, or by the relevant authorities with formal responsibility for prudential supervision of banking where that authority is not the central bank. The committee has no formal international supervisory authority or force of law. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank/financial institution supervisory issues.
MAJOR NATIONAL AML & CFT INITIATIVES

4.1 INTRODUCTION
In line with international efforts, Bangladesh has also taken many initiatives to prevent money laundering and combating financing of terrorism and proliferation of weapons of mass destruction considering their severe effects on the country. BRAC Bank must comply with all relevant laws, regulations and instruction/circulars issued by Bangladesh government and Bangladesh Bank.

4.2 FOUNDING MEMBER OF APG
Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating in the annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region.

4.3 LEGAL FRAMEWORK
Bangladesh government has enacted required ML/TF laws to meet the national and international requirements. Necessary amendments of the law have been initiated from time to time.

**Practicing Laws in Bangladesh**

- **2002**: Prevention of Money Laundering Act (PMLA)– 2002 (e.f. April 30, 2002)
- **2008**: Prevention of Money Laundering Ordinance-2008 (e.f. April 15, 2008)
- **2008**: Anti-Terrorism Ordinance-2008 (e.f. April 15, 2008)
- **2009**: Prevention of Money Laundering Act – 2009 (e.f. April 15, 2008)
- **2009**: Anti-Terrorism Act – 2009 (e.f. April 15, 2008)
- **2012**: Prevention of Money Laundering Ordinance-2012 (e.f. January 16, 2012)
- **2012**: Prevention of Money Laundering Act 2012 (e.f. January 16, 2012)
- **2015**: Prevention of Money Laundering Amendment Act, 2015
- **Money Laundering Rule prevention rules, 2019**

4.4 OTHERVARIOUS DEPARTMENTS AND COMMITTEE:
A lot of initiatives on AML/CFT have been taken by Bangladesh Bank and the following departments and Committee have been formed to combat money laundering and terrorist financing:

1. ANTI MONEY LAUNDERING DEPARTMENT
2. BANGLADESH FINANCIAL INTELLIGENCE UNIT
3. NATIONAL COORDINATION COMMITTEE AND WORKING COMMITTEE
4. NATIONAL ML & TF RISK ASSESSMENT (NRA)
5. NATIONAL STRATEGY FOR PREVENTING ML AND TF
6. ANTI MILITANTS AND DR-RADICALIZATION COMMITTEE
7. MEMORANDUM OF UNDERSTANDING (MOU) BETWEEN ACC AND BFIU

Bangladesh Bank BFIU has achieved the membership of Egmont group in the Egmont plenary on July, 2013 in Sun City, South Africa. Through Egmont membership, BFIU has achieved access to a wider global platform and this will help to establish relationship with other FIUs of different countries to get benefits by exchanging views, experiences and information via Egmont Secure.
4.5 RISK BASED APPROACH

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on AML and CFT requires financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks. This requirement is reflected in the Money Laundering Prevention Rules (MLPR) 2013. 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 BFIIU.

BRAC Bank has developed Risk Assessment guidelines (see Risk Register in Annexure A) in line with BFIIU Circular letter no. 01/2015) for providing the basic ideas of identifying, assessing and mitigating ML & TF risks that banks may encounter in doing their businesses, vetted by Central Bank of Bangladesh.
AML & CFT COMPLIANCE PROGRAM OF BRAC BANK

5.1 Introduction
BRAC Bank Ltd is committed to prevent the use of its services and facilities for criminal purposes. This compliance program and the accompanying procedures are BRAC Bank's primary defense against money laundering, terrorist financing and other illegal activity. This compliance program is designed to help detect and prevent attempts to use BBL or any of its products and services for money laundering or other illegal activity. As a part of its efforts to deter and prevent ML and TF, BBL is committed to cooperate with regulators, prosecutors and other government authorities to achieve this goal. Adherence to all policies including this program is essential. Knowledge of and adherence to the processes described in this compliance program is a job requirement for those involved in any way with the acquisition and approval of clients, and subsequent provision of products and services or completion of transactions.

This compliance program of the BRAC Bank covers senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

5.2 COMPONENT OF AML & CFT COMPLIANCE PROGRAM
While developing the compliance program, BBL has paid special attention to the size and range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by the bank. The program includes:

1. Senior management role including their commitment to prevent ML, TF & PF;
2. Internal policies, procedure and controls- It includes Bank's AML & CFT policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, self-assessment, independent testing procedure, employee screening, record keeping and reporting to BFU;
3. Compliance structure includes establishment of Central Compliance Committee (CCC), Anti Money Laundering department, appointment of chief anti-money laundering compliance officer (CAMLCO) and Deputy CAMLCO, branch anti-money laundering compliance officer (BAMLCO);
4. Independent audit function - It includes the role and responsibilities of internal audit on AML & CFT compliance and external audit function;
5. Awareness building program includes training, workshop, seminar for banks employees, member of the board of directors, owners and above all for the customers on AML & CFT issues.

5.3 COMPLIANCE PROGRAM DEVELOPMENT OF BRAC BANK
In developing this AML & CFT compliance program, Bank has considered BFIU guideline ML and TF as a basis for it. The bank has also considered all relevant laws, regulations, guidelines relating to AML & CFT and also the practices related to corporate governance (refer to corporate governance policy). In drafting the compliance program, Bank has involved all its relevant stakeholders like business function, Credit, Foreign Exchange, ICC, Information technology, ADC, Operations, AMLD and CCC. Bank shall communicate the compliance program immediately after the approval from the board of directors to all of its employees, members of the board of the directors and other relevant stakeholders through email and BRAC Bank's dedicated server.
5.4 COMMUNICATION OF COMPLIANCE PROGRAM
The office of Company Secretary shall communicate this compliance program immediately after the approval from the Board/Highest authority to all of employees and other relevant stakeholders. The compliance manual shall also be available at the following location:

Location: Your PC/BBL Touch/IT Support/BBL Guideline

5.5 SENIOR MANAGEMENT ROLE
For the purposes of preventing ML, TF & PF, senior management include members of the board of directors of the bank, and Managing Director and CEO of the bank. However, as far as any written policy is concerned, it has to be approved by the Board. The Board of Directors shall approve and issue direction regarding the duties of BBL officials at all levels (ref: Under ATA Law 2009). ICC and AMLD shall update the board regarding any noncompliance under ML & TF compliance

Role of Senior Management
Board of Directors (BoD) shall-
- Approve AML & CFT compliance program and ensure its implementation through supervision; approve a separate yearly training plan for AML/CFT for BRAC Bank at the beginning of a year.
- Issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- Take reasonable measures through analyzing self-assessment report and independent testing report summary; On half yearly basis, MD & CEO shall review the reports submitted by AMLD of the bank and shall pass his/her observations in writing.
- Understand ML & TF risk of the bank, take measures to mitigate those risks;
- MD and CEO shall issue statement of commitment to prevent ML, TF & PF in the bank by 1st week of February each year;
- Ensure compliance of AML & CFT program;
- Allocate enough human and other logistics for effective implementation of AML & CFT compliance program.

Statement of Commitment of CEO or MD
As per Prevention of Money Laundering Policy of the Bank (BBL MLP Policy, page 02), Managing Director of the Bank declares a written commitment on AML/CFT measures at the beginning of each year addressing all the employees of the bank. The management commitment of Managing Director generally covers the following area:

- Banks policy or strategy to prevent ML, TF & PF;
- Procedures on effective implementation of bank's AML & CFT compliance program;
- Clear indication of balance between business and compliance, risk and mitigating measures;
- Compliance is the responsibility of each employee during their normal course of assignment
- and ignorance shall not be considered as the excuse for non-compliance; Point of contact for clarification in case of any ambiguity arises;

Senior management of the bank shall be accountable to ensure that the bank's policy, process and procedures towards AML & CFT are appropriately designed and implemented, and are
effectively operated to minimize the risk of the bank being used in connection with ML & TF. All high risk items on AML/CFT compliance ground identified in ICC audit/AML&D finding must be escalated to the senior management and subsequently to Board Audit Committee.

Senior management shall ensure the adequacy of the human and other resources devoted to AML & CFT. Senior management shall advice HR to include autonomy in the job description of the designated officials related to AML & CFT. For this, they may consult with CAMLCO of the bank for better input. Senior management shall take the report from the Central Compliance Committee (CCC) into consideration which will assess the operation and the effectiveness of the bank’s systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner.

Senior management shall advice HR for inclusion of AML & CFT compliance in their manual so that it helps senior management to adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the bank. Senior management shall also instruct HR to develop following issues for proper implementation of AML & CFT measures:

- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- Proper weight in the annual performance evaluation of employees for extra ordinary preventive action with regard to non-compliance;
- Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFU;

Senior management must be responsive of the level of money laundering and terrorist financing risk when the bank is exposed to and take a view whether the bank is equipped to mitigate that risk effectively; all high risk/PEPS/IP account must be escalated to senior management for approval (refer to KYC policy).
6.1 INTRODUCTION
BRAC Bank establishes clear lines of inter-accountability, responsibility and reporting. Compliance structure of AML/CFT compliance of BRAC Bank is as follows:

- Central Compliance Committee (CCC),
- Anti-Money Laundering Division (AMLD)
- Chief Anti-Money Laundering Compliance Officer (CAMLCO),
- Deputy CAMLCO
- Branch Anti-Money Laundering Compliance Officer (BAMLCO).

6.2 CENTRAL COMPLIANCE COMMITTEE
Bank has formed Central Compliance Committee (CCC) headed by CAMLCO in compliance with BFIU circular 19, dated 17-09-2017. The CCC acts under the supervision of Managing Director & CEO of the bank. As per regulatory requirement, the designations of CCC Members will be following:

- CAMLCO
- Deputy CAMLCO
- Head of Retail
- Head of Business Applications Management & Relations
- Head of Operation
- Head of Human Resources
- Head of Credit Administration
- Head of Corporate Banking

Members are selected as per prescribed criteria in BFIU circular 19, dated 17-09-2017. As per section 1.3[1(Ga)] of the circular, the primary responsibility of CCC would be to formulate organizational strategies to combat money laundering and financing of terrorism from the perspective of bank’s own policy and supervise the effective implementation of those strides through its official secretariat, Anti-Money Laundering Division. Section 1.3[1(Chha)] requires that members of CCC would meet at least quarterly (04 meetings yearly) to review the progress of implementation of AML/CFT activities and provide recommendations, as and when required. As per management decision, BRAC Bank will hold these meetings along with its meetings arranged for the Enterprise Risk Management Committee (ERMC) with a view to ensure maximum coverage while communicating AML & CFT issues with the stakeholders. The Central Compliance Committee will directly report to MD & CEO.

6.2.1 AUTHORITY & RESPONSIBILITY OF AMLD:
As per section 1.3[1(Ga)] of the circular, under the direct control and supervision of Deputy CAMLCO, AMLD is the prime mover of the bank for ensuring the compliance of AML & CFT measures and is supposed to operate as a secretariat of CCC. Its main responsibilities are to:

- Develop bank policies, procedures and strategies in preventing ML, TF & PF;
- Coordinate bank’s AML & CFT compliance initiatives;
- Coordinate the ML & TF risk assessment of the bank and review thereon;
- Present the compliance status with recommendations before the CEO or MD on half
yearly basis;

- Issue instructions for the branches, where transaction monitoring system, internal control system, policies and techniques will be included to prevent Money Laundering and Terrorist Financing,
- Forward STR/SAR and CTR to BFIU in time and in proper manner;
- Report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner;
- Impart training, workshop, seminar related to AML & CFT for the employee of the bank;
- Take required measures to submit information, report or documents in time.
- For shouldering these responsibilities bank authority may consider to give the following authority to AMLD—
  a. Appointment of BAMLCO and assign their specific job responsibilities;
  b. Requisition of human resources and logistic supports for AMLD;
  c. Make suggestion or administrative sanction for non-compliance by the employees.

The AMLD will report to BFIU without any delay in case of any account/business relationship found with any person/entity whose name/names appeared to the mass media (TV/News Paper) regarding ML, TF, PF or any predicate offences under MLPA, 2012. AMLD will ensure proper implementation of steps taken to combat money laundering and financing of terrorism on an annual basis maintaining coherence with the directives and guidelines provided by CCC, as instructed through section 1.3[1][Ga]].

For ensuring the independent audit function in the bank, AMLD has been kept separated from internal audit or compliance and control (ICC).

6.3 CHIEF ANTI MONEY LAUNDERING COMPLIANCE OFFICER (CAMLCO)
BRAC Bank has designated Mr. Rais Uddin Ahmad as Chief Anti Money Laundering Compliance Officer (CAMLCO) at its head office. Board has given sufficient authority to Mr. Rais at its 150th board meeting through BBL AML Policy (AML Policy page 09) to implement and enforce corporate wide AML&CFT policies, procedures and measures.

AUTHORITIES AND RESPONSIBILITIES OF CAMLCO

Authorities-
- All staff are required to follow the instruction issued by CAMLCO;
- CAMLCO shall not take any permission or consultation from/with the MD before submission of STR/SAR to BFIU;
- He shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He will access to any information of the bank as and when required;
- HR shall arrange training as required by CAMLCO.

Responsibilities-
- CAMLCO shall monitor overall AML & CFT activities of the bank; he will advise AMLD to carry out inspection on AML/CFT measures where required.
- Oversee the submission of STR/SAR or any document or information to BFIU in time; maintain the day-to-day operation of the bank's AML & CFT compliance;
- CAMLCO shall be liable to MD for proper functioning of AMLD;
- 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 BB.

BRAC Bank Ltd
6.4 APPOINTMENT OF CAMLCO & FORMATION OF AMLD FOR CUSTODIAL SERVICE:
BRAC Bank provides custodial services under the License of Security and Exchange Commission. Cash Management and Custodial Services under Corporate Banking Division look after the custodial service related issues. Addressing ML/TF issues is very important while providing custodial services. Therefore, appointment of CAMLCO and formation of AMLD under custodial service is also a regulatory obligation. Considering the structure of custodial service, existing AMLD and CAMLCO of the bank will work and look after custodial service related ML/TF issues.

6.5 BRANCH ANTI MONEY LAUNDERING COMPLIANCE OFFICER (BAMLCO)
As per section 1.3(5) of the circular, CCC is responsible to designate BAMLCOS for all the branches and business. As per the Policy, Branch Manager shall play the role of BAMLCO in BBL. As such, by dint of designation, each Branch Manager is BAMLCO for his/her Branch. Before appointing BAMLCO, Business and HR shall ensure that the BAMLCO has sufficient knowledge in the existing acts, rules and regulations, BFUI’s instructions and bank’s own policies on preventing Money Laundering and Terrorist Financing. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in his/her appointment letter.

For preventing ML, TF & FF in the branch, the BAMLCO should perform the following responsibilities:

- Ensure that the KYC of all customers have been done properly and for the new customers, KYC is being done properly;
- Ensure that the UN Security Council and domestic sanction list is checked properly before opening an account and while making any international transaction;
- Keep information of ‘dormant accounts’ and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFUI’s instruction;
- Ensure regular transaction monitoring to find out any unusual transaction (In case of an automated bank, the bank should follow a triggering system against transaction profile or other suitable threshold. In case of a traditional bank, transaction should be examined at the end of day against transaction profile or other suitable threshold. Records of all transaction monitoring should be kept in the file);
- Review cash transaction to find out any structuring;
- Review of CTR to find out STR/SAR;
- Ensure the checking of UN sanction list before making any foreign transaction;
- Ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
- Compile self-assessment of the branch regularly and arrange quarterly meeting regularly covering prevalent laws and circulars on AML and CFT, Instructions issued by BFUI from time to time as per section 1.3(6) of the circular;
- Accumulate the training records of branch officials and take initiatives including reporting to AMLD, HR and training academy;
- Ensure all the required information and documents are submitted properly to AMLD and any freeze order or stop payment order are implemented properly;
- Follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
- Ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements of chapter 7;
- Ensure that corrective actions have taken by the branch to address the deficiency
In BRAC Bank, BRANCH Manager of each branch will be designate as BAMLCO of the Branch

6.6 Anti-Money Laundering Division
Deputy CAMLCO shall lead the Anti-Money Laundering Division. There shall be a team under Deputy CAMLCO to facilitate and enforce operational activity of ML/TF related issues. Deputy CAMLCO shall be liable to CAMLCO and take advice in performing and discharging his duties and responsibilities. Deputy CAMLCO is authorized to communicate with BFII officials directly as required from time to time with regards to AML/CFT. Mode of communication may be over phone or mail or goAMl or fax or physical visitation etc.

6.7 INTERNAL CONTROL AND COMPLIANCE
Internal Control and Compliance division plays a vital role for ensuring implementation of bank's compliance program. Keeping this in mind and as per Bangladesh Bank prescribed ICC guideline, BRAC has formed an independent ICC department having sufficient authority from the Board of Directors of the bank. ICC is equipped with enough manpower and autonomy to look after the prevention of ML&TF. The ICC has to oversee the implementation of the AML & CFT compliance program of the bank and has to review the 'Self-Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

Internal auditors are resourced and enjoy a degree of independence within the organization. Therefore, before appointing/hiring an internal auditor, HR shall ensure that internal auditor

1. Have sufficient operational knowledge
2. Have sufficient knowledge on business, credit and foreign trade as per bank's requirement
3. Understand ML/TF risks
4. Have sufficient knowledge on KYC/CDD, EDD

The internal audit must-
• Examine the overall integrity and effectiveness of the AML/CFT Compliance Program;
• Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
• Determine personnel adherence to the bank's AML&GFT Compliance Program;
• Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
• Assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
• Communicate the findings to the board and/or senior management in a timely manner;
• Recommend corrective action to address the identified deficiencies;
• Track previously identified deficiencies and ensure corrections are made by the concerned person;
• Examine that corrective actions have been taken on deficiencies identified by the BFII or BB;
• Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
• Determine the effectiveness of existing training programs and materials

6.8 EXTERNAL AUDITOR
External auditor may also play an important role in reviewing the adequacy of AML & CFT controls by communicating their findings and recommendations to management via the
annual management letter, which accompanies the audit report. AMLD shall review the recommendations of external audit findings on AML/CFT matters and suggest preventive measures.
AML & CFT POLICIES AND PROCEDURES of BRAC BANK LIMITED

POLICIES

BRAC Bank Ltd always takes the lead in adopting the best practices recommended by regulators and international best practices. Accordingly, BRAC Bank has developed its own policy and procedures in line with regulatory requirement, law of the land and international best practices recommended.

In Pursuit to Global and Local laws, regulations, recommendations, and guidelines associated with AML & CFT, BRAC Bank Limited has put-in-place the following policy:

- Anti-Money Laundering Policy
- Combating Financing of Terrorism Policy
- Customer Acceptance/KYC Policy
- Oversight Policy (AML/CFT) on bKash

In broader terms, this policy provides commitment of the bank to reasonably ensure that banking business is conducted in conformity with the high ethical standards; and remain subservient to the laws of the land, related regulations/directives of BFIU including Central Bank of the country.

7.1 WRITTEN AML & CFT COMPLIANCE POLICY

BRAC Bank has developed a written AML policy for all of its stakeholders. The last updated AML Policy was approved at the 150th Board meeting held on November 26, 2012. This policy covers all the key aspects of AML/CFT compliance. The AML&CFT policies are reviewed regularly and kept updated by AMLD at least annually or when needed, based on any legal/regulatory or business/operational changes, such as additions or amendments to existing AML&CFT related rules and regulations or business.

AML Policy of BBL covers the following area

1. Basics on AML/CFT
2. Role of Senior Management
3. Clear roles and responsibility of BBL staff and segregation of duties
4. AML/CFT structure of BBL and Responsibility assignment
5. CDD/KYC principles
6. UNSCR screening
7. PEPS/PFA/IP account approving mechanism
8. Risk management
9. Transaction monitoring and reporting (STR)
10. Training of BBL staff
11. Record Keeping etc.

7.2 CUSTOMER ACCEPTANCE POLICY

Money Laundering Prevention Act 2012 requires all reporting agencies to maintain correct and detailed information with regard to the identity of its customers during the operation of their accounts.
Guiding Principle:

**Principle 1:** Do business with clients who are involved in legitimate business activities and whose income and wealth are derived from legitimate sources.

**Principle 2:** Record the identity, background and business of all customers; identify and know the beneficial owners of all relationships; and understand the business purposes to which BBL goods and services are used to serve.

**Principle 3:** From the information gathered, reasonably estimate the types and levels of the client's anticipated transactions, be alert to and regularly monitor the relationship in order to identify unusual or suspicious activity, and take appropriate action when questions of inconsistencies arise. The above basic principles should govern all BBL dealings with customers and prospective customers.

BRAC Bank has developed customer acceptance policy integrated with KYC policy (ref: KYC Policy 2013; Location: Your PC/BBL Touch/IT-Support/BBL guideline). The primary objectives are:

1. To manage any risk that the services provided by the Bank may be exposed to;
2. To prevent the Bank from being used, intentionally or unintentionally, for ML/TF purposes; and
3. To identify customers who are likely to pose a higher than average risk.

Detail discussions on Customer Acceptance Policy are described at latter part of this guideline.

Pursuant to above legal bindings, Sec. 5.3 of Guidance Notes on Prevention of Money Laundering issued by Bangladesh Bank and apropos to international standard, the Management of the bank has developed the Customer Acceptance Policy as under:

a. No account shall be opened in anonymous or fictitious name or numbered (A/C without Title).

b. No banking relationship should be established with a Shell Bank. "Shell bank" refers to such banks that are incorporated under jurisdiction where it has no branches or activities and which is not affiliated with a regulated financial group.

c. No account shall be opened or maintained in the name of individuals/entities who/which are listed in UNSCR or by the Government of Bangladesh as financier to terrorists group or terrorism.

d. Uniform A/C Opening Forms, KYC Profile Form and Transaction Profile Form developed in line with the guidelines of Bangladesh Bank should be properly filled in.

e. Customers' risk must be assessed as per parameters of risk perception as clearly defined in KYC Profile Form.

f. Documentation requirements and other information must be collected keeping in mind the instructions contained in BFIU Master Circular No. 19 dated September 17, 2017, the requirements of the AML Act-2012, the Anti-Terrorism Act(Amend)-2013 and other Circulars and guidelines issued by the BFIU, Bangladesh Bank from time to time.
g. The branch shall not open an account, where the bank is unable to apply appropriate customer due diligence measures i.e. the branch is unable to verify the identity and/or obtain documents required due to non-cooperation of the customer or non-reliability of the data/information furnished to the branch. But the branch must be careful to avoid unnecessary harassment of the customer.

h. If it becomes necessary to close an existing account due to non-cooperation of the customer in providing necessary documents/information required by law/regulatory authority or non-reliability of the information/documents furnished by the customer, the branch must be vigilant in doing so. For example, decision to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

i. In case of opening a Politically Exposed Person’s (PEP)/Influential Person’s account, the branch shall follow the instructions contained in BFIU Master Circular No. 19 dated September 17, 2017 and PEP related guidelines issued by BFIU. Opening of such types of account require prior approval from the senior management and will be classified as high risk and will be required very high level of monitoring.

j. At the time of opening new account the branch must take care to seek only such information from the customer which is relevant and is not intrusive. It is mentioned that the customer profile is a confidential document and the details contained therein shall not be divulged for any other purposes.

k. Source of funds, income or wealth and complete information on the actual or beneficial owners of the accounts or (for company account) the shareholder who control the company or holding 20% or more share of the account must be obtained and complete KYC at the time of opening of any account.

l. The branch will strive not to cause inconvenience to the general public, especially those who are financially or socially disadvantaged.

m. The branch will conduct necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

n. In case of establishing correspondent banking relationship, the branch/concerned department shall follow the guidelines as contained in BFIU Master Circular No. 19 dated September 17, 2017 and related guideline of BFIU meticulously.

o. The branch shall verify the identity of the customer using reliable sources, documents etc. but it must retain copies of all references, documents used to verify the identity of the customer.


q. The branches, where locker service facilities exist, will follow the identification procedure for their customers.
7.3 OVERSIGHT POLICY ON bKASH

Bangladesh Bank issued mobile banking license to bKash Limited as a subsidiary of BRAC Bank Limited to handle MFS within the broader concept of 'Financial Inclusion'. BRAC Bank Limited must ensure that bKash Limited is performing its activity following the MFS guidelines and directives issued by Bangladesh Bank (Central Bank of Bangladesh). Therefore, it becomes necessary for BRAC Bank Limited to have an oversight Policy in place on bKash Limited to ensure smooth operation of business, services and compliance issue of bKash Limited. Accordingly, BRAC Bank board approved an oversee policy in its 188th Board meeting dated August 24, 2015. The policy is enclosed with this guideline.

BRAC Bank Ltd
PROCEDURES

8.1 CUSTOMER DUE DILIGENCE & KYC PROCEDURES

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources. Bank should be able to demonstrate to their supervisory authority to put in place, implement adequate CDD measures considering the risks of money laundering and terrorist financing. Such risk sensitive CDD measures are based on:

a) Type of customers;
b) Business relationship with the customer;
c) Type of banking products; and
d) Transaction carried out by the customer.

The CDD obligations on banks under legislation and regulation are designed to make it more difficult to abuse the banking industry for ML/TF. Following laws/rules have directed the bank to comply with CDD measure:

1. Money Laundering Prevention Act 2012 with amendments
3. BFIU Master Circular No. 19 dated September 17, 2017

8.2 HOW TO PERFORM CDD

Section 25 of MLP Act 2012 states that all reporting institute are required to maintain complete and accurate information of their client and person acting on behalf of a customer

Completeness and Accuracy
‘Complete’ refers to combination of all information for verifying the identity of the person or entity. For example: name and detail address of the person, profession, source of funds, Passport/National Identity Card/Birth Registration Certificate/acceptable ID card with photo, phone/mobile number etc. ‘Accurate’ refers to such complete information that has been verified for accuracy.

Therefore, it is required for BRAC Bank to be certain about the customer’s identity and underlying purpose of establishing relationship with the bank, and must collect sufficient information up to its satisfaction. "Satisfaction of the bank" means satisfaction of the account opening approving officer that is necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

8.3 TIMING OF CDD

Officials involved with account opening/transaction must apply CDD measures when he/she does any of the following:
a) Establishing a business relationship;
b) Carrying out an occasional transaction;
c) Suspecting money laundering or terrorist financing; or
d) Suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification.

8.4 CUSTOMER IDENTITY:
Customer identification is an essential part of CDD measures. For the purposes of this Guidance Notes, a customer includes:

The person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);
- The beneficiaries of transactions conducted by professional intermediaries; and
- Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.
Whenever the opening of an account or business relationship is being considered, or a one-off transaction or series of linked transactions is to be undertaken, identification procedures must be followed. Identity must also be verified in all cases where money laundering is known, or suspected. Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken. Records must be maintained as set out in Chapter VII, and information should be updated or reviewed as appropriate.

8.4.1 WHAT CONSTITUTES A PERSON'S IDENTITY?

1. Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, body corporate, partnership, etc). For the purpose of this guideline, the two elements are:
   • The physical identity (e.g. name, date of birth, TIN/voter registration/passport/ID number, etc.); and
   • The activity undertaken.

2. Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non-money-laundering context, to avoid breaches of UN or other international/National sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issue should be recorded.

3. The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of description required will depend on the concerned officer's own understanding of the applicant's business.

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

4. Once account relationship has been established, reasonable steps should be taken by the concerned officer to ensure that descriptive information is kept up to date as opportunities arise. It is important to emphasize that the customer identification process do not end at the point of application. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector. It will also depend on the nature of the product or service being offered, and whether personal contact is maintained enabling file notes of discussion to be made or whether all contact with the customer is remote.

8.4.2 INDIVIDUAL CUSTOMERS:
Where verification of identity is required, the following information should be obtained from all individual applicants for opening accounts or other relationships, and should be independently verified by the concerned officer himself/herself:
• true name and/or names used;
• parent’s names;
• date of birth;
• current and permanent address;
• details of occupation/employment and sources of wealth or income;

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

The date and place of birth are important as identifier in support of the name, and are helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard. It is also helpful for residence/nationality to be ascertained to assist risk assessment procedures and to ensure that the Bank does not breach UN or other international financial sanctions. Identification of documents, either originals or certified copies, should be pre- signed and bear a photograph of the applicant.

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

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

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

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

5. Any subsequent change to the customer’s name, address, or employment details of which the concerned officer becomes aware should be recorded as part of the know your customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

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

A customer without standard identification documents: In case of opening account of socially or financially disadvantaged such as the elderly, the disabled, students and minors, a common sense approach without compromising sufficiently rigorous AML procedures is recommended. In exceptional cases, Employer provided ID card (bearing the photograph and signature of the applicant) acceptable to the bank, SSC/HSC Admit Card/Registration Card with photograph, Student ID (bearing the photograph and signature of the applicant) acceptable to the bank may be considered on satisfaction of the Branch Manager/Relationship Manager. However, in exceptional cases manager should take advice from CAMLCO or his designate.

Note: Without a valid NID card, special permission has to be taken from CAMLCO before opening any account.

8.5 VERIFICATION OF ADDRESS:
The client’s residential address and telephone number(s) must be recorded. Preferred means of validation of residence are as following:

a) Visit to residence documented by the preparation of a call report in which the dealing officer explains the basis upon which he/she concluded that the client uses the home visited as a place of residence

b) Residential address appearing on an official document prepared by a Government Agency supported by online verification from trusted site.

c) Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). If the bill is not in the name of applicant, then option d or e has to be exercised.

d) Sending a registered (welcome) letter to the address.

e) Contact Point Verification (CPV)

Proof of Address must match to any of the addresses (i.e. Present or Work address) stated in the Account Opening Form.

8.6 VERIFICATION OF SOURCE OF FUND/OCCUPATION/BUSINESS INFORMATION

The client’s occupation and position held, line of business (for business owners) along with the business/employer’s name, street address, and telephone number, must be recorded. In addition, branch should maintain records of cross reference of the allied or sister concerns or associated companies of the respective account (BRPD Cl 17, dated 07 November 2012). Branches should collect and verify the document supporting source of fund of the person at the
time of establishing any business relationship or while conducting CDD. The document could include present employment identity, salary certificate/copy/advice, pension book, financial statement, income tax return, business document or any other document that could satisfy the bank. The bank should request the person to produce E-TIN (Electronic Tax Identification Number) certificate which declares taxable income.

8.7 INTRODUCER
a) The Client would need an introduction from an introducer who has an A/C relationship with any of BBL branches for at least 6 months with satisfactory transaction history.
b) New accounts should be introduced by existing customers; if however staffs are introducing new account, they should personally know the customer or verify customer address personally.
c) No executive/PTE in sales channel is authorized to introduce customer’s account.
d) Dormant/Inactive account holders must not be allowed to introduce a new account holder.
e) Signature of the Introducer must be verified before opening of the account.
f) Relationship between introducer and account holder must be recorded.
g) For any newly opened branch, introduction by the branch staff may be accepted up to six month based on following conditions:
   1. Prior notification to BFIU would be required.
   2. Verification of ID including address would be required.

8.8 NOMINEE
a) Appointment of nominee is mandatory for opening an Account (individual + joint + proprietorship).
b) Photograph of nominee should be attested by the a/c holder.
c) The relationship between applicant and nominee should be acceptable to the bank.
d) No staff can become the nominee of an account holder (except parents, spouse, siblings, children)

8.9 CORPORATE BODIES AND OTHER ENTITIES
Particular steps should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The following documents should be obtained from companies:
I. Certified true copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
II. Certified true copy of the Memorandum and Articles of Association, or by-laws.
III. Copy of the board resolution to open the account relationship and the empowering authority for those who will operate the account;

IV. Details of the nature of the business, the purpose of relationship to be established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;

V. Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 20% interest or more or with principal control over the company’s assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;

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

VII. Copies of the list/register of directors.

The following persons (i.e. individuals or legal entities) must also be identified:

I. All of the directors who will be responsible for the operation of the account/transaction.

II. All the authorized signatories for the account/transaction.

III. All holders of powers of attorney to operate the account/transaction.

IV. The beneficial owner(s) of the company

V. The majority shareholders of a private limited company.

A letter issued by a corporate customer is acceptable in lieu of National ID/Passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again.

Additional information and copy of business permission from the appropriate authority should be obtained depending on the ownership, board formation, nature & purpose of opening the account.

a. Signatories / Intermediaries

When a client delegates discretion or authority, including a power of attorney, to a third party, or appoints an intermediary, the association between the party (ies) and the client should be explained. Signatories/Intermediaries who clearly exercise control/influence over the relationship should be profiled.
b. Business Information

The client must provide the business's address and telephone number on the application. In addition, the generic type of business must be recorded. This information and application must be retained on file.

c. Address

The client's full Business/Office address, Registered Address, Factory/Industry address along with telephone number(s) must be recorded.

d. Source of Wealth

Gathering and recording information relating to a client's source of wealth is another step to ensure that BBL does business only with clients who are involved in legitimate business activities and whose income and wealth are derived from legitimate sources.

e. Assessment of Source of Wealth Information

Sales/dealing staff must understand that the client/Key Party's source of wealth is consistent with his/her knowledge of the client's business activity and personal history. Source of wealth information must be reasonable in view of the nature of the relationship with the client.

f. Company not listed:

Concerned RM/Official must provide a visit report prior to opening such account. Visit report should cover the detail information on nature of business, product/service nature, area of business, who are target client of the company. RM/Official shall not proceed where he/she gets the sense that proposed company may defraud gullible people or business pattern is not supported ethically with our Bank's value.

8.9.1 COMPANY REGISTERED ABROAD

While establishing business relationships with company incorporated or registered abroad, bank should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh.

8.9.2 COMPANY NOT YET REGISTERED

Bank can open deposit account in the name of a Company which is yet to be registered. In that case, bank must collect Original NOC for Name (Name Release Letter / Certificate) from RISC; Draft Memorandum of Association & Article of Association; KYC of Entrepreneurs and
their capital (investment); Board Resolution regarding declaring name of the Chairman and Managing Director; Board Resolution of type of account to be opened, with which bank and authorized signatory(s) for the account and a resolution signed by all the entrepreneurs stating a Nominee to whom a Pay Order is to be issued if the company is not registered / fails to register (Ref: BRPD/policy -4/770 /2009-1508 dated May 19, 2012). However, Relationship Manager should take advice from CAMLC0 before opening such account.

8.10 PARTNERSHIPS AND UNINCORPORATED BUSINESSES
In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the bank, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

8.11 INTERNET OR ONLINE BASED CUSTOMER
Bank should not offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures. However, initial application forms could be completed on-line and then followed up with appropriate identification checks. These accounts should not be put into full operation until the standardized account opening provisions have been satisfied. Customers should also be educated about the use of internet banking and secrecy of the internet banking password.

8.12 CORRESPONDENT BANKING:
Special attention must be paid to correspondent banking business and enhanced due diligence must be implemented while opening and maintaining relationship. Bank should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant regulatory authority. Before providing correspondent banking service senior management approval must be obtained on being satisfied about the nature of the business of the respondent bank (BFIU Circular 10). KYC of all correspondence relationship must be kept by concerned department as per Bangladesh Bank directive.

While establishing and continuing correspondent banking relationship, the following drill should be observed so that banking system cannot be abused for the purpose of money laundering:
1. Before providing correspondent banking service senior management approval must be obtained on being satisfied about the nature of the business of the respondent bank through collection of information as per format of BFIU, Bangladesh Bank

2. Banks should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.

3. Banks should not establish or continue a correspondent banking relationship with any shell bank. [Here shell bank refers to such banks as are incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with a regulated financial group.]

4. Correspondent banking relationship shall not be established or continued with those respondent banks that established correspondent banking relationship or maintain account with a shell bank.

5. Banks should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries and territories enlisted in Financial Action Task Force’s Non-cooperating Countries and Territories list). Enhanced due diligence shall be required in such cases. Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.

6. Enhanced Due Diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customers to transact business on their behalf (i.e. payable through account)

7. PEPs involvement and downstream Correspondents to be checked.

The above instructions shall be applicable to the entire existing correspondent banking relationship.

8.13 PROVISION OF SAFE CUSTODY AND SAFETY DEPOSIT BOXES
Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that Financial Institutions will follow the identification procedures set out in these Guidance Notes. In addition, such facilities should only be made available to account holders.

8.14 WALK-IN/ONE OFF CUSTOMERS/ON-LINE TRANSACTIONS:
Branch must collect complete and correct information while serving Walk-in customer with a transaction BDT 50,000/= or above, i.e. a customer without having account. Banks should know the sources of fund and motive of transaction while issuing DD/PO or serving for
TT/MT. Branch shall collect complete and correct information/documents as per BFIU circular 19 of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit, banks should identify sources of funds as well.

Note: For online transaction of below 50,000 detailed information should be collected.

8.15 NON FACE-TO-FACE CUSTOMERS

‘Non face to face customer’ refers to “the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the bank branch”. The impersonal and borderless nature creates difficulty in customer identification and verification. So special attention shall be paid and verification of identity to be ensured. Before offering such facility bank must establish a separate procedure.

8.16 CDD FOR BENEFICIAL OWNERS

Bank should apply CDD obligations for the beneficial owners of the accounts before or during the course of establishing a business relationship or conducting occasional transactions. In doing so, banks should put in place appropriate measures to indentify beneficial owner. Banks, upon its own satisfaction shall ensure CDD of beneficial ownership by collecting information and documents from independent and reliable sources that include publicly available information, information from customer or information from other reliable sources. Banks should consider following aspects while identifying beneficial ownership include:

- Any natural person operating accounts on behalf of customer;
- Any person (whether acting alone or together) who has controlling interest or ownership interest on a customer who might be legal entity or legal arrangements. Where there is any doubt identifying controlling interest, the banks should consider other means to determine controlling interest or ownership of a legal entity or arrangements. In addition to that bank should also consider reasonable measures to verify the identity of the relevant natural person who holds senior management position;
- Any person or entity who has controlling or 20% or above shareholding within any or legal entity.
- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercises control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) should be considered for other types of legal arrangements.

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

8.17 EXCEPTION WHEN OPENING A BANK ACCOUNT

Establishing effective policy and processes to identify an ultimate beneficial owner (UBO) is essential in combating money laundering and terrorist financing. All UBOs should be identified, declared, verified (where applicable) for all new and changes to existing account holder accounts and financial services and products provided to occasional (walk-in) account holders. These procedures must require proper due diligence and may identify unusual transactions, and possibly report the suspicious transactions.

FATF defines UBOs as natural person(s) who ultimately owns or controls an account holder and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

(1) Reference to “ultimately owns or controls” and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

(2) This definition should also apply to a beneficial owner of a life or other investment schemes.
Money launderers, terrorists and sanctioned parties try to access the financial system by hiding their existence (i.e., true identity) during account opening and service request processes, through using individual or non-individual accounts opened by their association's or family members' names, or opening accounts for legal entities with complex ownership structure, or any other tactics to avoid detection.

Methods of Identification and Verification for UBOs

A. Possible UBOs of Common Types of Accountholders

<table>
<thead>
<tr>
<th>Accountholder Classification</th>
<th>Account Type</th>
<th>Possible UBO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adult Accountholder Account</td>
<td>Adult Accountholder Account</td>
<td>1. Third party</td>
</tr>
<tr>
<td>opened through Power of</td>
<td>1. Power of Attorney (POA) holder</td>
<td></td>
</tr>
<tr>
<td>Attorney (POA)</td>
<td>2. Third party</td>
<td></td>
</tr>
<tr>
<td>opened by Guardian</td>
<td>2. Third party</td>
<td>2. Directors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Authorized Signatory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Financial Control Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(FCO)</td>
</tr>
<tr>
<td>Non-Individuals</td>
<td>Corporate Account</td>
<td>5. Third party</td>
</tr>
<tr>
<td>Non-profit Organization/Charity Account</td>
<td>1. Shareholder &quot;if any&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Directors/trustee</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Authorized Signatory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Financial Control Officer (FCO)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Provider of material funds/allowances</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Third party</td>
<td></td>
</tr>
<tr>
<td>Mutual Fund</td>
<td>1. Provider of funds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Directors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Principal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Underwriter/Sponsor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Custodian</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Third party</td>
<td></td>
</tr>
<tr>
<td>Governmental/Official</td>
<td>1. Directors/trustees</td>
<td></td>
</tr>
<tr>
<td>Authorities</td>
<td>2. Authorized Signatory</td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td>3. Third party</td>
<td></td>
</tr>
</tbody>
</table>

B. The identification and verification process for UBOs should be performed during account opening, while updating KYC information, when obtaining banking services/products forms. Policy, procedures and processes must clearly ask the accountholder to declare the UBO, with imposing an obligation on the accountholder to update the FI, if the declared UBO is changed.

The following must be obtained, before providing the financial service, activating the account, or issuing banking self-services to the accountholder for individual and non-individual accounts:

1. Reason of having a third party as a UBO and the relationship between the accountholder and the declared UBO.
2. Full KYC documentation and information (full name, nationality, resident address, source of funds/wealth, etc.)
3. If the account holder is a citizen of the U.S., it is required that they complete the appropriate form, to comply with Foreign Account Tax Compliance Act (FATCA) requirements, for individual accounts only.

The methodology may differ between institutions and account holder types, but the UBO must be clearly identified and verified by the FI as an essential part of KYC requirements.

8.18 EXCEPTION WHEN OPENING A BANK ACCOUNT

The verification of the documents of account holder may take place after the account has been opened, provided that there are adequate safeguards in place to ensure that before verification has been completed:

a) The account is not closed;
b) Transaction is not carried out by or on behalf of the account holder (including any payment from the account to the account holder).

8.19 IN CASE WHERE CONDUCTING THE CDD MEASURE IS NOT POSSIBLE

If conducting the CDD measure becomes impossible because of the non-cooperating behavior of the customer or if the collected information seemed to be unreliable, that is, bank could not collect satisfactory information on customer identification and could not verify that, bank should take the following measures:

(a) Must not carry out a transaction with or for the customer through a bank account;
(b) Must not establish a business relationship or carry out an occasional transaction with the customer;
(c) Must terminate any existing business relationship with the customer;
(d) Must consider whether it ought to be making a report to the BFIU through an STR.

Branch shall consider whether an inability to apply CDD measures is caused by the customer. In this case, the BM should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the BM/RM should consider whether there are any circumstances which give grounds for making a report to BFIU.

If the AMLD concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be sent to the BFIU. The bank must then retain the funds until consent has been given to return the funds to the source from which they came.

If AMLD/relevant stakeholder conclude that there are no grounds for making a report, they will need to make a decision on the appropriate course of action. This may be retaining the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or returning the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

8.20 RELIANCE ON THIRD PARTY

Bank could rely on the third parties to perform the CDD measures with the prior permission of Bangladesh Bank which may include:

i) Identify and verify customer identity;
ii) Identify the beneficial ownership and control structure; and
iii) Identify the purpose and nature of the business relationship under the following criteria:

- A third party should immediately obtain necessary information related to i) - iii) as mentioned above;
- All necessary data and documents held with the third party must be available for the banks without any delay;
- Bank should verify that third party is regulated, supervised and monitored for, and has taken appropriate measures in compliance with CDD and record keeping requirements set out in this Guidelines.

BRAC Bank Ltd
8.21 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 withdrawals should be permitted in those accounts; however, deposits can be permitted. These accounts will be fully functional only after conducting proper CDD measures. AMLD should preserve data of such accounts at their end. BRAC Bank has managed all legacy accounts (1102 accounts) belong to Gulshan & Nawabpur branch suitably.

8.22 CUSTOMER UNIQUE IDENTIFICATION CODE
Branch must use unique identification code for any customer maintaining more than one account or availing more than one facilities. Such unique identification system could facilitate us to avoid redundancy, and saves time and resources. This mechanism also enables branches to monitor customer transactions effectively.
8.23 POLITICALLY EXPOSED PERSONS (PEPs), INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

All clients must be subject to an assessment to determine whether they are PEPs or Influential Persons or chief executives or top level officials of any international organization and their linked entities. These customers pose a higher risk of money laundering, bribery, corruption and reputational risk to the bank due to their current or former position of political power or influence, which makes them more vulnerable to corruption. Relationships with these customers may increase the risk to the bank due to the possibility of these individuals holding such positions may misuse their power and influence for personal gain or advantage or for the personal gain or advantage of their close family members and close associates. The person’s status (PEP's, Influential Persons and chief executives or top level officials of any international organization) itself does not incriminate individuals or entities. It does, however, put a prospective or existing client into a higher risk category.

8.23.1 DEFINITION OF PEPs
Politically Exposed Persons (PEPs) refer to “Individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.” The following individuals of other foreign countries must always be classed as PEPs:

i. Heads and deputy heads of state or government;
ii. Senior members of ruling party;
iii. Ministers, deputy ministers and assistant ministers;
iv. Members of parliament and/or national legislatures;
v. Members of the governing bodies of major political parties;
vi. Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
vii. Heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
viii. Heads of state-owned enterprises.

8.23.2 CDD MEASURES FOR PEP'S
Branch need to identify whether any of their customer is an IP. Once identified following instructions shall have to be followed to ensure Enhanced Due Diligence, while opening and operating the account:

- Identify risks associated with opening and operating the accounts of PEPs/ PFAs
- Obtain senior managements’ approval before establishing such business relationship;
- Documentation should be sufficient to demonstrate that the proposed account activity is consistent with the financial profile and legitimate source of wealth of the applicant
- Business should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

All instructions as detailed for PEPs shall equally apply if business relationship is established with

- The known members of the individual’s immediate family (i.e., spouse, parents, children, siblings, in-laws);
- Any known economic dependents of the individual;
• Any corporations, trusts or other entities in which the individual is known to have a beneficial or ownership interest or is known to use as a conduit;
• Any person who is in a position to conduct substantial transactions on behalf of the political figure, such as the holder of a power of attorney;
• All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

Approval Requirement: Accounts under PEPs as well as accounts for their principals may be accepted only with the prior written approval of the CAMLCO with recommendation from respective Business Head. Direct reports (i.e. Head of Branch Banking, Head of Sales etc) of the Business head can recommend for opening such report. However, email approval using BRAC Bank network only is acceptable.

8.23.3 DEFINITION OF INFLUENTIAL PERSONS

'Influential persons' refers to, "Individuals who are or have been entrusted with prominent public functions, 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."

The following individuals must always be classed as Influential persons:
(a) Heads and deputy heads of state or government;
(b) Senior members of ruling party;
(c) Ministers, state ministers and deputy ministers;
(d) Members of parliament and/or national legislatures;
(e) Members of the governing bodies of major political parties;
(f) Secretary, Additional secretary, joint secretary in the ministries;
(g) Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
(h) Governors, deputy governors, executive directors and general managers of central bank;
(i) Heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
(j) Heads of state-owned enterprises;
(k) Members of the governing bodies of local political parties;
(l) Ambassadors, chargés d’affaires or other senior diplomats;
(m) City mayors or heads of municipalities who exercise genuine political or economic power;
(n) Board members of state-owned enterprises of national political or economic importance.

Whether an individual is an influential person or not will depend on the prominence or importance of the function that he/she holds, and the level of corruption in the country, the reputation and personal links of the individual and whether he/she has any links to industries that are prone to corruption. If the individual does not hold sufficient influence to enable them to abuse his/her power for gain, they should not be classified as an influential person.

IP for these purposes, in short, is defined to include any person who, whether by election, appointment, military action, heredity, or other means.
### 8.23.4 CDD MEASURES FOR INFLUENTIAL PERSONS

Branch needs to identify whether any of their customer is an IP. Once identified, the following instructions shall have to be followed to ensure Enhanced Due Diligence, while opening and operating the account:

- Identify risks associated with opening and operating the accounts of PEPs/PFAs
- Obtain senior management's approval before establishing such business relationship;
- Documentation should be sufficient to demonstrate that the proposed account activity is consistent with the financial profile and legitimate source of wealth of the applicant
- Business should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

All instructions as detailed for IP shall equally apply if business relationship is established with:

- The known members of the individual’s immediate family (i.e., spouse, parents, children, siblings, in-laws);
- Any known economic dependents of the individual;
- Any corporations, trusts or other entities in which the individual is known to have a beneficial or ownership interest or is known to use as a conduit;
- Any person who is in a position to conduct substantial transactions on behalf of the political figure, such as the holder of a power of attorney.
- All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

Approval Requirement: Accounts under IPs as well as accounts for their principals may be accepted only with the prior written approval of the CAMLCO with recommendation from respective Business Head. Direct reports (i.e. Head of Branch Banking, Head of Sales etc) of the Business head can recommend for opening such report. However, email approval using BRAC Bank network only is acceptable.
8.23.5 DEFINITION OF CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

'Chief executive of any international organization or any top level official' refers 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 boards or equivalent functions." The heads of international organizations and agencies that exercise genuine political or economic influence (e.g. the United Nations, the International Monetary Fund, the World Bank, the World Trade Organization, the International Labor Organization) must always be classed as this category.

8.23.6 CDD MEASURES FOR CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

Branch need to identify whether any of their customer is a CEO or top level officials of any international organization. Once identified banks need to apply enhanced CDD. Moreover, they need to perform the following:
(a) Branch have to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a CEO or top level officials of any international organization;
(b) Obtain senior management's approval before establishing such business relationship;
(c) Take reasonable measures to establish the source of fund of the account of a CEO or top level officials of any international organization;
(d) Monitor their transactions in a regular basis; and
(e) All provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be compiled accordingly.

8.23.7 CLOSE FAMILY MEMBERS AND CLOSE ASSOCIATES OF PEPs, INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

In addition, close family members and close associates of these categories will also be classified as the same category. Close Family Members include:
(a) The PEP's/influential persons/chief executive of any international organization or any top level official's spouse (or any person considered as equivalent to the spouse);
(b) The PEP's/influential persons/chief executive of any international organization or any top level official's children and their spouses (or persons considered as equivalent to the spouses); and
(c) The PEP's/influential persons/chief executive of any international organization or any top level official's parents;

There may be exceptional circumstances where the individual should not be classified as a 'Close Family Member' of the PEP, such as estrangement, divorce etc. In such cases, the circumstances must be thoroughly investigated, examined and caution exercised.

In addition, where other family members such as the siblings, cousins, relatives by marriage of the PEP are deemed, by virtue of the nature of the relationship, to have a close relationship with the PEP, they should also be classified as PEPs.

A Close Associate of a PEP/Influential Person/Chief executive of any international organization or any top level official includes:
(a) An individual who is known to have joint beneficial ownership or control of legal entities or legal arrangements, or any other close business relations with the PEP; and
(b) An individual who has sole beneficial ownership or control of a legal entity or legal arrangement which is known to have been set up for the benefit of the PEP.

In addition, it should include any person publicly or widely known to be a close business colleague of the PEP, including personal advisors, consultants, lawyers, accountants, colleagues or the PEP's.
fellow shareholders and any person(s) that could potentially benefit significantly from close business associations with the PEP.

8.23.8 CDD MEASURES FOR CLOSE FAMILY MEMBERS AND CLOSE ASSOCIATES OF PEPS, INFLUENTIAL PERSONS AND CHIEF EXECUTIVES OR TOP LEVEL OFFICIALS OF ANY INTERNATIONAL ORGANIZATION

Branch needs to identify whether any of its customers are a family member or close associates of a PEP, IP or CEO or top level officials of any international organization. Once identified, branch needs to apply enhanced CDD measures. Moreover, they need to perform the same procedure for PEP/IP account.

8.24 KYC Procedure:

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

Each concerned officer is required to perform due diligence on all prospective clients prior to opening an account. This process is completed by fulfilling the documentation requirements (Account Application, Bank References, Source of funds and Identification for example).

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

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

8.25 KYC PROFILING:

KYC profile gives the basic information about the customer like, Name, Address, Tel/Fax Numbers, line of business, Annual sales. If the customer is a Public Figure, the account will become automatically a High Risk Account. The KYC Profile information will also include the observations of the Institution’s Staff/Officer when they visit the customer’s business place like, the business place is owned or rented, the type of clients visited, by what method is the client paid (cheque or cash). The Staff/Officer will record his observations and sign the KYC Profile form.

8.26 RISK CATEGORIZATION – BASED ON ACTIVITY/KYC PROFILE

When opening accounts, the concerned staff/Officer must assess the risk that the accounts could be used for “money laundering”, and must classify the accounts as either High Risk or Low Risk.

Following seven risk categories are scored using a scale of 1 to 5 for risk profiling:

- Occupation or nature of customer’s
- Business Net worth / sales turnover of the customer
- Mode of opening the account
ML & TF Risk Management Guidelines

- Expected value of monthly transactions
- Expected number of monthly transactions
- Expected value of monthly cash transactions
- Expected number of monthly cash transactions

The risk scoring of less than 14 indicates low risk and more than 14 would indicate high risk. The risk assessment scores are to be documented in the KYC Profile Form. However, branch may judgmentally override this automatic risk assessment to "High Risk" if it believes that there are appropriate reasons to the risk. This override decision must be documented (reasons why) and approved by the Branch Manager/Branch AML Compliance Officer.

8.26.1 APPROVAL PROCEDURES:
Accounts under 'High Risk' as well as accounts for their principals may be accepted only with the prior written approval of the CAMLCO with recommendation from respective Business Head. Direct reports [i.e. Head of Branch Banking, Head of Sales; Head of small SME etc] of the Business head can recommend for opening such account. However, email approval using BRAC Bank network only is acceptable.

8.27 REVIEW AND UPDATE:
Branch/Concerned business shall take necessary measures to review and update the KYC of the customer after a certain interval or at least as per BFIU instruction/circular.

Low Risk Account: This procedure shall have to be conducted in every five years in case of low risk customers.
High Risk Account: Furthermore, this procedure shall have to be conducted in every year in case of high risk customers.
General Conditions: But, branches shall update the changes in any information on the KYC as soon as bank gets to be informed. Moreover, branch may update KYC information anytime if there is any particular necessity to do so. Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay.

Any subsequent change to the customer's name, address, or employment details of which the business becomes aware should be recorded as part of the CDD process. Generally, this would be undertaken as part of good business practice and due diligence but also serves for prevention of money laundering and terrorist financing.

Branch/business should collect the announcement of customer about the Transaction Profile of customer account in the specified form. After reviewing the nature of the customer, the source of money in the account and the nature of transaction, branch 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.

Enhanced Due Diligence measures:
Banks should conduct Enhanced CDD measures, when necessary, in addition to normal CDD measures. Bank should conduct Enhanced Due Diligence (EDD) under the following circumstances:
- Individuals or legal entities scored with high risk;
- Individuals who are identified as politically exposed persons (peps), influential persons and chief executives or top level officials of any international organization;
• Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes;

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

Enhanced CDD measures include:

• Obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet, etc) and updating more regularly the identification data of customer and beneficial owner.

• Obtaining additional information on the intended nature of the business relationship.

• Obtaining information on the source of funds or source of wealth of the customer.

• Obtaining information on the reasons for intended or performed transactions.

• Obtaining the approval of senior management to commence or continue the business relationship when applicable.

• Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

• Making the concerned bank officials aware about the risk level of the customer.
TRANSACTION MONITORING PROCESS

On-going account transaction monitoring is an important element of AML/CFT program. It is a regulatory obligation to pay special attention to all complex, unusually large Transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help the relevant authorities in inspection and investigation.

Possible areas of monitoring that includes but not limited to the followings:

- Transaction type
- Transaction frequency
- Unusually large amounts
- Geographical origin/destination
- Changes in account signatories
- Large volume transaction
- Transaction inconsistent with the TP
- Transaction in High Risk Account
- Transaction in PEPs/IP account

9.2 TRANSACTION PROFILE:
TP is estimated transaction volume which acts as parameter of transaction to help for understanding/ascertaining the genuineness of actual transaction. The following steps and points should be noted while preparing transaction profiles:

- Take interview with the customer and request him/her to fill in the Transaction Profile Form as recommended by Bangladesh Bank. The main features of the Form for both deposit and withdrawal would be:
  - Various types of transactions (i.e. nature of transactions) · No. of transactions (monthly) · Maximum size (per transaction) · Total value (monthly)
- Before filling in, it has to be ensured by the Designated Officer that the customer's understanding is sufficient to fill the required cells of Transaction Profile Form.
- Assist customer in filling the Transaction Profile Form if any complexity arises.
- Officer must match the information mentioned in TP with all points covered in KYC guidelines. He has to establish normal resemblances between the two declared statements. Questions might be politely asked to customer for any noted discrepancy.
<table>
<thead>
<tr>
<th>Deposit Type</th>
<th>No. of Transactions</th>
<th>Highest Amount (for individual transaction)</th>
<th>Total Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash Deposit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(including online)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deposit through Transfer/Instrument</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deposit of Foreign Remittance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Borrowing from Export</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others (specify)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Probable Deposit</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What will be your total transaction per month?

Check the Relevance
9.3 ON-GOING TRANSACTION MONITORING BY BRANCHES

Following reports need to be generated at prescribed frequency to ensure effective monitoring.

a) Excessive Cash Movement Report: On a daily basis branch will generate a large value Cash Transaction Report and review the transaction pattern.

Note: daily CTR 7 lac & above for deposit transaction

- Branch prints out Daily Excessive Cash Movement Report (ECMR) on last working day
- Checks the account transactions from Finacle and analyses the source of cash deposit through annotation at the time of posting transaction
- Manually writes the annotation on the printed copy of Daily Cash Transaction Report with initial and date
- When reason/source of cash deposit does not match with the profession, calls the customer and collects the transaction reason
- Writes the outcome of the discussion with the customer on the Daily ECMR report and if suspicion arises, AMLD and BBL are informed through e-mail
- Branch Manager (BM)/ Customer Service Manager (CSM) signs with date on the ECMR and preserves the report for audit purpose.

b) EXCEPTION REPORT / TP BREACH REPORT:

On a monthly basis, branch will generate an Exception Report of customers whose transaction volume exceeded the transaction limit (more than 20%) mentioned in the transaction profile and will review the accounts. If, after confirming with the customer, the transaction trend continues, then the Account Officer will be responsible for documenting the reasons as to why the transaction profile has changed and should amend the TP & KYC profile accordingly.
BM/CSM downloads the TP breach report for the month and checks the excess transaction.

If the deviation is more than 20% with the given TP then writes down the specific reason on the TP breach report after consultation with the respective customer.

If any significant breach of TP is found, BA/MICO review the bank statement and if found suspicious invites customer to the branch to interview and check whether the transaction is genuine or not.

If the transaction seems to be genuine BM suggest customer to change TP proving supporting documents (if required) and BM updates the annotation "TP Updated on DD/MM/YY" in TP breach report.

If customer can not satisfy BM with explanation or if the customer do not show up, branch scrutinize transactions, account opening documents and raise STR and inform the same to AM/ID.
c) CTR (Cash Transaction Report): Cash transaction (deposit/withdrawal) for 10 lac taka or more in a day falls under CTR threshold. All such transactions are required to submit to Central Bank in softcopy. In case of cash deposit (regardless of amount in the Govt. accounts or accounts of the Govt. owned entities, CTR reporting is not required. But in case of cash withdrawal, such report is to be submitted as per prescribed CTR format. Before sending the report to BFIU and Bangladesh Bank, respective branch will review the transactions to detect suspicious transactions and if any suspicion arises, the branch will send the report to AMLD. Concerned department will prepare the report as per the format provided by the regulator.

d) Remittance Transaction Report: A system has been developed by the bank to monitor remittance transactions.
As per section 9 of BFIU Circular 19 Dated: 17-09-2017, wire transfer refers to financial transaction through which any bank of FI pays to the beneficiary (individual/organization) by assistance of any other bank or branch using electronic medium, upon request of the applicant (individual/organization).

We are required to ensure collection of the following information for all kinds of wire transfer according to BFIU Circular 19, Clause 9.1 and as follows:

1. **Cross-Border Wire Transfer:**
   It refers to the execution of electronic financial transaction between applicant and beneficiary from different countries. Chain of related transactions, for such applicant and beneficiary, at least one (01) transfer executed cross-border, is included under this as well.

   A. Transactions of USD 1,000 or above require banks-
      - To collect appropriate information regarding the applicant/originator (on whose request the wire transfer is going to be executed) and
      - To send the same to the intermediary/beneficiary bank.

   Transactions of amount below USD 1,000 require banks to preserve appropriate information regarding the applicant/originator only to detect the applicant late, if required.

   B. To collect information regarding the beneficiary while paying the beneficiary through cross-border wire transfer.

   C. To collect information regarding the applicant (along with account number) and all the beneficiaries in batch files in aspect of wire transfer to more than one beneficiaries upon request of a single applicant.

2. **Domestic Wire Transfer:**
   It refers to the execution of electronic financial transaction between applicant and beneficiary from a similar country. Chain of related transactions, for such applicant and beneficiary, having at least one (01) transfer executed cross-border, is included under this as well.

   A. Identification and verification of information regarding both the applicant and the beneficiary through effectively performing KYC and CDD (as per clause 3)

   B. 2(A) applies for domestic wire transfers with payment instructions through usage of debit/credit card (except purchasing of products/services)

   C. Above-mentioned instructions are not compulsory for wire transfer where beneficiary is government, semi-government or autonomous organization. Moreover, interbank wire transfers are also relieved of performing KYC, CDD as described in 2(A).

**Other Directions Regarding Wire Transfers:**

- Related guidelines, circulars issued by Bangladesh Bank are to be followed for such transactions.

- As per clause 2(3) of this circular, no transaction or relationship with any shell bank and as per clause 10, prevention of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction rules are to be followed in case of cross-border wire transfers.

**Duties of Ordering, Intermediary & Beneficiary Bank:**

1. **Ordering Bank:**
- Ensuring appropriate and complete information of the applicant (Name, Account number, Occupation, Purpose of Transaction)
- Ensuring meaningful information of the beneficiary (Name, Place, Purpose of Transaction)
- Preserving this information for at least five (05) years and provided upon request of entitled authorities, if required.

2. Intermediary Bank:
Bank working as an intermediary between the ordering and the beneficiary bank is subject to the following rules:
- Ensuring appropriate and complete information of the applicant and the beneficiary (Name, Account number, Occupation, Purpose of Transaction)
- Ensuring verification to detect data insufficiency (if exists) in the provided information of the applicant and the beneficiary.
- Preserving this information for at least five (05) years.
- Existence of Risk-based principles and policies of the intermediary bank for execution, holding on and required following-up for wire transfer, if data insufficiency in the provided information of the applicant and the beneficiary exists.

3. Beneficiary Bank:
- Having a risk-based procedure to verify the data sufficiency in the information of the applicant and the beneficiary.
- Verifying the provided information (if required) from inter-bank mutual relationships and other accessible sources.
- Collection information of the beneficiary while paying to the beneficiary and preserving the information for at least five (05) years.
- Existence of Risk-based principles and policies of the beneficiary bank for execution, holding on and required following-up for wire transfer, if data insufficiency in the provided information of the applicant and the beneficiary exists.

3.4 MONITORING OF STRUCTURING:
Structuring is a money laundering technique, which involves the slitting up of large cash deposit into a number of smaller deposit to evade the suspicious activity reporting requirement of the bank. Structuring can be done:

- Regular deposits of cash into accounts in amounts that fall below reporting threshold.
- Maintaining accounts at multiple bank branches with ill intention
- Using third parties to make deposits into single account or multiple accounts
- Purchasing instruments using cash

9.4.1 STRUCTURING IDENTIFICATION:
Branch shall generate the Excessive Cash Movement Report on daily basis. The report captures all single transactions above 7 (seven) lac. This report shall assist the concerned person to identify attempt of structuring by any customer.
REPORTING TO BFIU

Obligations under MLP Rules, 2013 & various instructions from BFIU, bank is obliged to send following reports to BFIU

1. Suspicious Transaction Report/Suspicious Activity Report
2. Cash Transaction Report
3. Self-Assessment & Independent Testing Procedure
4. Various AML return

10.2 SUSPICIOUS TRANSACTION REPORTING PROCEDURES:

10.2.1 SUSPICIOUS TRANSACTION

Will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account.

Account transactions or other activities which are not consistent with the due diligence file'

The bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible economic purpose of the transaction.

A transaction designed to evade any regulatory requirements under APPLICABLE LAW

Money Laundering Prevention Act, 2012 defines suspicious transaction as follows- 'suspicious transaction' means such transactions –

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

Anti-Terrorism Act, 2009 defines suspicious transaction as follows- 'suspicious transaction' means such transactions –

- Which are different from usual transactions;
- Which invoke presumption that,
  - it is the proceeds of an offence under this Act,
  - it relates to financing of terrorist activities or a terrorist person or entity;
- Which is any other transaction or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.

10.2.2 SUSPICIOUS TRANSACTION REPORT:

The final output of an AML & CFT compliance program is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the AML&CFT risk for banks. Therefore, it is necessary for the safety and soundness of the bank.
Usually, STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be of usual manner. Such report is to be submitted by banks to the competent authorities i.e. to BFUJ. Suspicion basically involves a personal and subjective assessment. The branch has to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

10.2.3 IDENTIFICATION OF STR/SAR
Identification of STR/SAR may start with identifying unusual transaction and activity. Such unusual transactions may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Generally, the detection of something unusual may be identified by:

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

A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious or not. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises. Annexure-C provides some red flag indicators for identifying STR/SAR related to ML & TF. All suspicions reported to the AMLD should be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the suspicion. All internal enquiries made in relation to the report should also be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

The following chart shows the graphical presentation of identification of STR/SAR-
As discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, banks should conduct the following 3 stages:

Identification:

STR/SAR can be identified by any staff of the Bank. However, frontline staff is more likely to identify suspicious transaction or activity in the account. This stage is very vital for STR/SAR reporting. For STR/SAR detection, Bank has developed the following reporting tools to monitor customer transaction and identify suspicious movement of transaction in to the account.

1. Daily Excessive Cash movement report (7 lac and above)
2. TP breach Report
3. Monthly CTR report

Evaluation:

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

Disclosure:
This is the final stage and banks should submit STR/SAR to BFIU if it still looks suspicious. A sample flowchart:
10.2.4 FEW IMPORTANT NOTES ON STR/SAR REPORTING:

- There is legal obligation under LAW (Section 25, MLP Act 2012) to disclose suspicious transactions and you may be personally liable for failure to report suspicion to relevant authority.
- Nobody can prevent you from filing a SAR.
- You can consult with your line manager but the decision to file a SAR should be yours, depending entirely on your suspicion.
- Disciplinary action can be taken if an employee willfully fails to report a very obvious suspicious activity.
- Disciplinary action will be taken against anybody including supervisors if they dissuade or prevent an employee from filing a SAR.
- No action will be taken against a person for filing a SAR even if it later turned out to be a genuine transaction, if the person acted in good faith without any mala-fide intent.
- Do not alert the customer about your suspicion or about filing of the SAR. (Putting hard holds on accounts can result in a tip-off). Tipping off is a punishable offence under Law.
- Once a SAR is filed, act as per the instructions of the CAMLCO or the authorities.
- CAMLCO is the only authority in the bank who is empowered to take a decision on a SAR, including external disclosure.

10.3 CASH TRANSACTION REPORT

Every branch will generate the monthly cash transaction report and send feedback to AMLD in due time. If the branch has not any such transaction, it should report it to the AMLD as 'There is no reportable CTR'. Simultaneously, branches need to identify whether there is any suspicious transaction while reviewing the cash transactions. If any suspicious transaction is found, the branch will submit it as 'Suspicous Transaction Report' to the AMLD. If no such transaction is identified, it needs to inform to the AMLD as 'No suspicious transaction has been found' while reporting the CTR. Besides, every branch needs to preserve its CTR in their own branch.
The AMLD needs to prepare the accumulated CTR received from its all branches. The AMLD must ensure the accuracy and timeliness while reporting to BFU. Moreover, it has to review all the cash transaction from the branches above the threshold and search for any suspicious transaction. If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' to the BFU. AMLD has to inform BFU through the message board of goAML web in case of no transaction is found to be reported as CTR. Moreover, AMLD must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFU.

CTR entails daily single or cumulative cash transaction above BDT 1 million in an account. The report generated on monthly basis.
10.4 SELF ASSESSMENT REPORT

Banking system in Bangladesh is mainly based on branch banking. The branches of the banks are in every corner of the country and they have an active role in stimulating the economic growth of the country. It is very difficult for the AMLD or ICC to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFJU has established a Self-Assessment Reporting system for the branches.

According to the instructions of BFJU, branches of bank need to conduct the Self-Assessment to evaluate them on a half yearly basis. Self-Assessment has to be done through a checklist that is
circulated by BFIU circular no. 19, dated 17 September, 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 that meeting, there shall be a discussion on the branch evaluation report; if the identified problems according to that report are possible to solve 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 Internal Audit Department or ICCD of the Head Office and the AMLD within the 15th of the next month.

10.4.1 INDEPENDENT TESTING PROCEDURE
The audit must be independent (i.e. performed by people not involved with the bank’s AML&CFT compliance). Audit is a kind of assessment of checking of a planned activity. Independent testing has to be done through a checklist that is circulated by BFIU circular no. 19; dated 17th September, 2017. The individuals conducting the audit should report directly to the board of directors/senior management. Audit function shall be done by the internal audit or ICC. At the same time, external auditors could be appointed (if possible) to review the adequacy of the program.

10.4.2 INTERNAL AUDIT DEPARTMENT'S OR ICC's OBLIGATIONS REGARDING SELF ASSESSMENT OR INDEPENDENT TESTING PROCEDURE
The Internal Audit Department shall assess the branch evaluation report received from the branches and if there is any risky matter identified in any branch, it shall inspect the branch immediately and shall inform the matter to the AMLD. While executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the Internal Audit Department should examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure. The Internal Audit Department should send a copy of the report with the rating of the branches inspected/audited by the Internal Audit Department to the AMLD of the bank.

10.4.3 AMLD’S OBLIGATIONS REGARDING SELF ASSESSMENT OR INDEPENDENT TESTING PROCEDURE
Based on the received branch evaluation reports from the branches and submitted inspection/audit reports by the Internal Audit Department or ICC, the AMLD shall prepare a checklist based evaluation report on the inspected branches in a considered half year time. In that report, beside other topics, the following topics must be included:

(a) Total number of branch and number of self-assessment report received from the branches;
(b) The number of branches inspected/audited by the Internal Audit Department at the time of reporting and the status of the branches (branch wise achieved number);
(c) Same kinds of irregularities that have been seen in maximum number of branches according to the received self-assessment report and measures taken by the AMLD 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 AMLD to prevent those irregularities; and
(e) Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as 'unsatisfactory' and 'marginal' in the received
### 10.5 OTHER RETURN SUBMISSION:

<table>
<thead>
<tr>
<th>Name of the Return</th>
<th>Description</th>
<th>Frequency</th>
<th>Due Date to Reach AMDL</th>
<th>Due Date to Reach BRAC Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTR</td>
<td>Daily cash transaction above $1 million</td>
<td>Monthly</td>
<td>12th of the following month</td>
<td>15th of the following month</td>
</tr>
<tr>
<td>Parichistogha</td>
<td>Statement of Suspicious Transaction</td>
<td>Quarterly</td>
<td>1st week of the following month</td>
<td>15th of the following month</td>
</tr>
<tr>
<td>Self Assessment &amp; Independent Testing</td>
<td></td>
<td>Half Yearly</td>
<td>15th of the following month</td>
<td>Following 60 days of half year end</td>
</tr>
</tbody>
</table>

### 10.5.1 Return Submission Process

1. All branches send report to AMLD, BRAC within due date.
2. AMLD, BRAC prepares report based on the branches' reports.
3. AMLD, BRAC sends report to BRAC Bank within due date.
RECRUITMENT, TRAINING AND AWARENESS

To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, bank should follow proper Screening Mechanism in case of recruitment and ensure proper training for their officials.

11.1 EMPLOYEE SCREENING
Bank is subject to ML & TF risk from its customers as well as from its employee in absence of proper risk mitigating measures. A fair recruitment process is already in place and followed by HR. 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. ICC shall examine the recruitment file during HR audit.

HR is advised to follow the following measures (at least one from below):
- Appoint a third Party to verify the information (Present Address, Permanent address, Certificate)
- reference check
- background check
- screening through or clearance from Law Enforcement Agency and sanction screening
- Personal guarantee.

Before assigning an employee in a particular job or desk, HR 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.

11.2 KNOW YOUR EMPLOYEE (KYE)

Know-your-customer, an essential precaution, must be coupled with know-your-employees. 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. KYE requirements should be included in the banks HR policy.

11.3 EDUCATION AND TRAINING PROGRAMS:

An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analyzing potential illicit transactions. Bank should, therefore, establish ongoing employee training programs. Training should be targeted at all employees but added emphasis should be placed on the training of compliance and audit staff because of their critical role in sensitizing the broader staff complement to AML/CFT issues and ensuring compliance with policy and procedures.

All relevant staff will be educated in the process of "Know Your Customer" requirements for money laundering prevention and combating terrorist financing purposes. The training in this respect would cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity.
11.3.1 CONTENT AND SCOPE OF THE TRAINING PROGRAM:
Every employee of a bank shall have at least basic AML & CFT training that should cover all the aspects of AML & CFT measures in Bangladesh. Basic AML & CFT training should be at least day long model having evaluation module of the trainees. Relevant provision of Acts, rules and circulars, guidelines, regulatory requirements, suspicious transaction or activity reporting should be covered in basic AML & CFT training course.
Training should be general as well as specific to the area in which the trainees operate. As staff members move between jobs, their training needs for AML/CFT may change. Training programs should, inter alia, incorporate:
a. Relevant money laundering and terrorism financing laws and regulations;
b. Definitions and examples of terrorist financing schemes;
c. How the institution can be used by launderers or terrorists;
d. The importance of adhering to customer due diligence policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;
e. The procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;
f. The completion of unusual and suspicious transaction reports;
g. Treatment of incomplete or declined transactions; and
h. The procedures to follow when working with law enforcement or the FIU on an investigation.

11.3.2 New Employees: A general appreciation of the background to money laundering & terrorism financing, and the subsequent need for reporting any suspicious transactions to the Anti-Money Laundering Compliance Officer (AMLCO) should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority.

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

11.3.4 Processing (Back Office) Staff: Officers who receive completed Account Opening, Payment Order/DD/TT/FDR application forms and cheques for deposit into customer’s account or other investments would receive the training given to cashiers and other front office staff. In addition, these officers should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Anti-Money Laundering Compliance Officer (or alternatively, a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.
11.4 SENIOR MANAGEMENT/OPERATIONS SUPERVISORS:
Without proper concern and awareness of senior management of a bank, it is difficult to have effective implementation of AML & CFT measures in the bank. AMLD under the supervision of MD is required to arrange, at least once in a year, an awareness program for all the members of its board of directors or in absence of board of directors, members of the highest policy making committee and people engaged with policy making of the bank.

A higher level of instruction covering all aspects of money laundering and terrorist financing procedures should be provided to those with the responsibility of supervising or managing staffs. The training will include internal reporting procedures and the requirements for verification of identity and the retention of records as well as the offences and penalties arising from the Act for non-reporting and assisting terrorist's activities.

11.5 CUSTOMER AWARENESS
The Bank has taken proper actions for broadcasting awareness building advertisement and documentaries regarding prevention of money laundering and terrorist financing through different mass media under Corporate Social Responsibility (CSR) fund.

11.6 AWARENESS OF MASS PEOPLE
Prevention of ML & TF largely depends on awareness at all level. For this, BFIU, BB, other regulators as well as the government sometimes arrange public awareness programs on AML & CFT issues. Banks are encouraged to participate in those initiatives. It is mandatory for the Branch to display AML/CFT related Poster in a visible place of their premises. Branch should also preserve brochure and distribute the same among the customer. Marketing department is advised to arrange public awareness programs like advertisements through billboard, poster, festoon and mass media, distribution of handbills, leaflet and so on.

11.7 REFRESHER TRAINING:
To keep the employees updated about AML & CFT measures, banks are required to impart refreshment training programs of its employees on a regular basis. It is also necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least once in a year to ensure that staff does not forget their responsibilities.

11.8 JOB SPECIFIC TRAINING:
Besides basic and refreshment AML & CFT training, bank shall arrange job specific training or focused training i.e., Trade based money laundering training for the trade professional employees who deal with foreign or domestic trade, UNSCR screening related training for all employees who deal with international transactions, customer relations and account opening; credit fraud and ML related training for all the employees who deal with advance and credit of the bank; customer due diligence and ongoing monitoring of transaction related training for the employees who conduct transaction of customers.
RECORD KEEPING

Record keeping is an essential component of the audit trail that the Laws and Regulations seek to establish in order to assist in any financial investigation and to ensure that criminal funds which are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

All concerns must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

12.2 LEGAL OBLIGATIONS

Obligations under MLPA, 2012 and MLP Rules 2013 and BFIU Circulars:

1. All necessary information/documents of customer’s domestic and foreign transactions has to be preserved for at least 5 (five) years after closing the account.
2. All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved for at least 5 (five) years after closing the account.
3. All necessary information/documents of a walk-in Customer’s transactions have to be preserved for at least 5 (five) years from the date of transaction.
4. Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence.
5. Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU.

12.3 RECORDS TO BE KEPT

The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that we can meet the obligations and that, in so far as is practicable, in any subsequent investigation we can provide the authorities with its section of the audit trail. The firm’s records should cover:

- Customer information transactions
- Internal and external suspicion report/reports from AMLD/CAMLCO
- Training and compliance monitoring information about the effectiveness of training

12.4 CUSTOMER INFORMATION

In relation to the evidence of a customer’s identity, banks must keep a copy of or the references to, the evidence of the customer’s identity obtained during the application of CDD measures. Where a bank has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. A bank may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring. Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. The date when the relationship with the customer ends is the date: an occasional transaction, or the last in a series of linked transactions, is carried out; or the business relationship ended, i.e. the closing of the account or accounts.
12.5 TRANSACTIONS
All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the bank's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips; cheques should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed.

12.6 INTERNAL AND EXTERNAL REPORTS
A bank should make and retain:
- Records of actions taken under the internal and external reporting requirements; and
- when the nominated officer has considered information or other material concerning possible money laundering but has not made a report to BFU, a record of the other material that was considered.

In addition, copies of any STRs made to the BFU should be retained for five years. Records of all internal and external reports should be retained for five years from the date the report was made.

12.7 OTHER MEASURES
HR records should include:
(a) In relation to training:
- Dates of AML training given;
- the nature of the training;
- The names of the staff who received training;
- Training material
- The results of the tests undertaken by staff, where appropriate.

(b) In relation to compliance monitoring:
- Reports by the CAMLCO to senior management; and
- Records of consideration of those reports and of any action taken as a consequence.

12.8 FORMATS AND RETRIEVAL OF RECORDS
To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of a bank, provided that they have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form and that can be reproduced and recollected without undue delay. It is not always necessary to retain documents in their original hard copy form, provided that the bank has reliable procedures for keeping records in electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, a bank may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on the bank itself and the responsibility is thus on the bank to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required.

However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.
13.1 INTRODUCTION
In line with rising awareness in the world economy, Bangladesh has also enacted a separate law, the Anti-Terrorism Act, 2009 (amended in 2013) for prevention of terrorism and effective punishment of certain terrorist acts and matters connected therewith. Accordingly financing of terrorism has been criminalized under this law. It is understood that Bangladesh had deliberately included provisions for countering terrorist financing into the Anti-Terrorism Act, 2009 instead of Anti Money Laundering Act 2009. This act sets out the expectations of the Bank and the Authority in relation to the minimum standards for combating the financing of terrorism (CFT) practices by all Financial Institutions.
Bangladesh has criminalized terrorist financing in line with the International Convention for the Suppression of the Financing of Terrorism (1999). Section 16 of Anti-Terrorism Rules, 2013 states the responsibilities of the reporting agencies regarding funds, financial assets or economic resources or related services held in or through them.

A bank like us that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activity, is committing a criminal offence under the laws of Bangladesh. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism. This risk is even more serious if the person or entity involved is later shown to have benefited from the lack of effective monitoring or willful blindness of a particular bank and thus was to carry out terrorist acts.

13.2 LEGAL OBLIGATIONS & BFU Circular
All relevant concerned shall take necessary measures, with appropriate caution and responsibility,

- To prevent and identify financial transactions through which it is connected to any offence
- If any suspicious transaction is identified, the bank shall spontaneously report it to Bangladesh Bank without any delay.
- The Board of Directors, shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, 2009; which are applicable to the bank, have been complied with or not.
- Before any international business transaction, every bank will review the transaction to identify whether the concerned parties of that transactions are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or proscribed by Bangladesh government. Immediately after the identification of any account of any listed individual or entity concerned bank will stop that transaction and inform BFU the detail information at the following working day.

13.3 NECESSITY OF FUNDS BY TERRORIST
Terrorist organizations need money to operate. Weapons and ammunition are expensive. Major international operations require substantial investments for personnel, training, travel and logistics. Organizations must have substantial fundraising operations, as well as mechanisms for moving funds to the organization and later to terrorist operators. These functions entail considerable risk of detection by authorities, but also pose major challenges to both the terrorists and intelligence agencies.
13.4 SOURCES OF TERRORIST FINANCING:
There are two primary sources of financing for terrorist activities. The first involves getting financial support from countries, organizations or individuals and the other one involves revenue-generating activities, which may be linked to legal or criminal fronts. These are explained below.

13.4.1 FINANCIAL SUPPORT:
Terrorism could be sponsored by a country or government, although this is believed to have declined in recent years. State support may be replaced by support from other sources, such as individuals with sufficient financial means.

13.4.2 REVENUE-GENERATING ACTIVITIES:
The revenue-generating activities of terrorist groups may include criminal acts, and therefore may appear similar to other criminal organizations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, terrorist groups may use smuggling, fraud, theft, robbery, and narcotics trafficking to generate funds.
Financing for terrorist groups may also include legitimately earned income, which might include collection of membership dues and subscriptions, sale of publications, speaking tours, cultural and social events, as well as solicitation and appeals within the community. This fund raising might be in the name of organizations with charitable or relief status, so that donors are led to believe they are giving to a legitimate good cause.
Only a few non-profit organizations or supposedly charitable organizations have been implicated in terrorist financing networks in the past worldwide. In these cases, the organizations may in fact have carried out some of the charitable or relief work. Members or donors may have had no idea that a portion of funds raised by the charity was being diverted to terrorist activities. This type of “legitimately earned” financing might also include donations by terrorist group members of a portion of their personal earnings.
In general, terrorist organizations may raise funds through: legitimate sources, including through abuse of charitable entities or legitimate businesses and self-financing, criminal activity, state sponsors and activities in failed states and other safe havens.

13.5 MOVEMENT OF TERRORIST FUND
There are three main methods to move money or transfer value. These are: the use of the financial system, the physical movement of money (for example, through the use of cash couriers) and the international trade system.

Often, terrorist organizations will abuse alternative remittance systems (ARS), charities, or other captive entities to disguise their use of these three methods to transfer value. Terrorist organizations use all three methods to maintain ongoing operation of the terrorist organization and undertake specific terrorist activities.
13.5.1 FORMAL FINANCIAL SECTOR
Financial institutions and other regulated financial service providers' services and products available through the formal financial sector serve as vehicles for moving funds that support terrorist organizations and fund acts of terrorism. The speed and ease with which funds can be moved within the international financial system allow terrorists to move funds efficiently and effectively and often without detection between and within jurisdictions. Combined with other mechanisms such as offshore corporate entities, formal financial institutions can provide terrorists with the cover they need to conduct transactions and launder proceeds of crime when such activity goes undetected.

13.5.2 TRADE SECTOR
The international trade system is subject to a wide range of risks and vulnerabilities which provide terrorist organizations the opportunity to transfer value and goods through seemingly legitimate trade flows. To exploit the trade system for terrorist financing purposes could assist in the development of measures to identify and combat such activity.

13.5.3 CASH COURIERS
The physical movement of cash is one way terrorists can move funds without encountering the AML/CFT safeguards established in financial institutions. It has been suggested that some groups have converted cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside of the financial system. The movement of cash across the borders is prevalent in the cash based economy and where the electronic banking system remains embryonic or is little used by the populace. Moving money using cash couriers may be expensive relative to wire transfers. As legitimate financial institutions tighten their due diligence practices, it has become an attractive method of transferring funds without leaving an audit trail. When cross border remittance of cash is interdicted, the origin and the end use of cash can be unclear. Cash raised and moved for terrorist purposes can be at very low levels – making detection and interdiction difficult.

13.5.4 USE OF ALTERNATIVE REMITTANCE SYSTEMS (ARS)
Alternative remittance systems (ARS) are used by terrorist organizations for convenience and access. ARS have the additional attraction of weaker and/or less opaque record-keeping and in many locations may be subject to generally less stringent regulatory oversight. Although FATF standards call for significantly strengthened controls over such service providers, the level of anonymity and the rapidity that such systems offer have served to make them a favored mechanism for terrorists.

13.5.5 USE OF CHARITIES AND NON-PROFIT ORGANISATIONS
Charities are attractive to terrorist networks as a means to move funds. Many thousands of legitimate charitable organizations exist all over the world that serve the interests of all societies, and often transmit funds to and from highly distressed parts of the globe. Terrorists who abuse the charitable sector have included using legitimate transactions to disguise terrorist cash travelling to the same destination; and broad exploitation of the charitable sector by charities affiliated with terrorist organizations. The sheer volume of funds and other assets held by the charitable sector means that the diversion of even a very small percentage of these funds to support terrorism constitutes a grave problem.

13.6 PROLIFERATION FINANCING:
Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials, in contravention of national laws or, where applicable, international obligations.
13.6.1. SIGNIFICANCE OF PREVENTION AND DETECTION OF PROLIFERATION AND ITS FINANCING

Proliferation financing facilitates the movement and development of proliferation-sensitive goods. The movement and development of such items can contribute to global instability and may ultimately result in a loss of life, if proliferation-sensitive items are deployed.

13.6.2 HOW CAN PROLIFERATION AND ITS FINANCING BE TARGETED?

There are two recognized mechanisms by which proliferation can be targeted; namely export controls and financial measures.

- **Export Controls:**
  Proliferators act globally, masking their acquisitions as legitimate trade. Proliferations are known to exploit global commerce, for example:
  
  - Operating in countries with weak export controls;
  - Utilizing free-trade zones where the obtaining and/or shipping of such goods are more likely to escape scrutiny; and
  - Operating in countries with high volumes of international trade.

- **Financial Measures**
  Financial measures act as a supplement to effective export controls, to address the financial activity associated with proliferation. Similar to international criminal networks, proliferation networks use the international financial system to carry out transactions and business deals. Bank shall be alert to the possibility that the customers may be engaged or facilitating proliferation activities.

There are three areas where bank has responsibilities in relation to proliferation financing, namely:

- The risk assessment of customers and products;
- Enhanced due diligence on high-risk transactions and entities; and
- Special attention to trade finance.

13.6.3 EDD ON HIGHER-RISK TRANSACTIONS AND ENTITIES

- Bank shall apply, on a risk-sensitive basis, enhanced customer due diligence measures in any situation which by nature can present a higher risk of money laundering.
• Enhanced due diligence measures shall be applied.
• Lists complied by national authorities can be a useful resource, as they provide information on individuals who may pose a proliferation concern. In individual cases where proliferation financing is a risk or concern, institution may wish to consider whether issuing banks, applicants or beneficiaries of letters of credit, or freight companies and shipping lines moving the goods, appear on such lists.
• Provide services to a trading company or any vehicle that itself has links to higher risk countries, from a proliferation perspective, development of a strategy will assist in responding to any proliferation risks. Such a strategy may call for systems to be put in place to monitor trading activities.

13.6.4 VERIFICATION OF GOODS

Identifying whether a particular good is a dual-use good or otherwise a proliferation concern, is acknowledged to be difficult. Thus, in higher risk scenario where the customer is importing or exporting goods, bank shall be alert to the need to mitigate against inadvertent proliferation financing. This can be achieved by asking the customer for the following:

• Valid export licenses; or
• License not required letters that are less than three months old.

If a customer is unable to provide the information referred to above, then an alternative is to ask that the customer provide evidence, by reference to export control requirements in the relevant jurisdiction, that the goods being exported do not require a license.

13.6.5 SPECIAL ATTENTION FOR TRADE FINANCE PRODUCTS

A fairly significant proportion of proliferation activities may use in trade finance as a vehicle. Special attention shall be given to certain trade finance, for example:

• Direct loans or general credit facility to facilitate exporttransactions;
• Purchase of promissory notes or bills of exchange issues by foreign buyers to exporters for the purchase of goods and services, freeing up cash for the exporter;
• Factoring- the purchase or discounting of a foreign account receivable for cash at a discount from face value;
• Provision of guarantees to or by financial institutions on behalf of exporters such as pre-shipment guarantees and performance guarantees; or
• Provision of insurance against certain risks in the trading process.

13.6.6 RED FLAG INDICATORS

To assist with the awareness of potential proliferation financing, a list of red flag indicators are provided below, which is not exhaustive because complexity of business, nature of risk may vary in case to case:
Customer

- The customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher risk jurisdictions.
- The customer or counter-party, or its address, is the same or similar to one of the parties found on publicly available lists.
- The customer is a military or research body connected with a higher risk jurisdiction of proliferation concern.
- Customer activity does not match the business profile.
- Customer is vague, particularly about end user and end use, provides incomplete information or is resistant to providing additional information when sought.
- A new customer requests a letter of credit from bank, whilst still awaiting approval of its account.
- Complicated structures to conceal involvement-use of layered letters of credit, front companies, intermediaries and brokers.

Transactions/Orders

- The transaction concerns dual-use, proliferation-sensitive or military goods, whether licensable or not.
- The transaction involves an individual or entity in a foreign country of proliferation concern.
- Transaction demonstrates a link between representatives of companies exchanging goods e.g. same owners or management, in order to evade scrutiny of the goods exchanged.
- Transaction involves the shipment of goods inconsistent with normal geographic trade patterns i.e. where the country involved does not normally export or import the types of goods concerned.
- Order for goods is placed by firms or individuals from foreign countries, other than the country of the stated end-user.

Jurisdiction

- Countries with weak financial safeguard and which are actively engaged with a sanctioned country.
- A presence of an industry that produces dual-use goods, proliferation-sensitive items or military goods.
- Deliberate insertion of extra links into the supply chain e.g. diverting shipments through a third country.

Other

- Final destination or end-use unclear.
- Project financing and complex loans, where there is a presence of other objective factors such as an identified end-user.
- Declared value of shipment under-valued in relation to shipping cost.
- Inconsistencies in information contained in trade documents and financial flow e.g. names, addresses, final destination.
- Use of fraudulent documents and identities e.g. false end-use certificates and forged export or re-export certificates.
- Use of facilitators to ensure the transfer of goods avoids inspection.
Innocuous commercial wording on customs declaration/export license e.g. pump (without further explanation of purpose/use).

- A freight forwarding firm being listed as the product's final destination.

- Wire instructions or payment from or due to entities not identified on the original letter of credit or other documentation.

- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

13.7 TARGETED FINANCIAL SANCTIONS

In recent years, the concept and strategy of targeted sanctions imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, have been receiving increased attention. Most of the countries agree that better targeting of such measures on the individuals responsible for the policies condemned by the international community, and the elites who benefit from and support them, would increase the effectiveness of sanctions, while minimizing the negative impact on the civilian population. The considerable interest in the development of targeted sanctions regimes has focused primarily on financial sanctions, travel and aviation bans, and embargoes on specific commodities such as arms or diamonds.

Targeted financial sanctions entail the use of financial instruments and institutions to apply coercive pressure on transgressing parties—senior officials, elites who support them, or members of non-governmental entities—in an effort to change or restrict their behavior. Sanctions are targeted in the sense that they apply only to a subset of the population—usually the leadership, responsible elites, or operationally responsible individuals; they are financial in that they involve the use of financial instruments, such as asset freezing, blocking of financial transactions, or financial services; and they are sanctions in that they are coercive measures applied to effect change or constrain action.

However, targeted financial sanctions represent a potential refinement of the sanctions tool that could be used in conjunction with other coercive efforts, such as travel bans, to minimize the unintended effects of comprehensive sanctions and achieve greater effectiveness.

To implement TFS in Bangladesh, the Government has issued Statutory Regulatory Order (SRO) under section 2 of the United Nations (Security Council) Act, 1948 (29 November, 2012) and amended the SRO to make it more comprehensive (June, 2013). To make the process enforceable, a separate section has been included in ATA, 2009 through amendment of ATA in 2013. Section 20(A) of ATA, 2009 covers all the requirements under UNSCR's tool were taken and will be taken under chapter VII of the charter of UN. Before that BFIU used to issue circular letters for reporting organisations to implement UNSCR resolutions.

For effective implementation of these provisions, detailed mechanism has been developed in Anti-terrorism Rules, 2013. Under rule 16 of AT rules, 2013, banks as a reporting agency have to maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. In case there is any fund or economic resources held by the listed individuals and entities, the banks should immediately stop payment or transaction of funds, financial assets or economic resources and report to the BFIU within the next working day with full particulars of the listed and/or the suspected individuals or entities or related or connected individual identities.

13.7.1 UNSC RESOLUTIONS

The following resolutions adopted by the UN Security Council under Chapter VII are relevant for the purposes of the guideline:

Operative elements of the TFS

1. Resolutions relating to the Al-Qaida sanctions under UNSCRs 1267/1999 and successors to 1267;
2. Resolutions relating to the Taliban sanctions under UNSCR 1988 and current and successor resolutions to resolution 1988 (2011);
3. Resolution 1373 (2001); and
4. Resolutions concerning weapons of mass destruction and sanctions imposed upon the Democratic People’s Republic of Korea (North Korea).

13.7.2 LOCAL SANCTIONS/BANNED LISTS

The political division of the Home Ministry of Bangladesh on April 2009 blacklisted 12 organizations. The organizations are Harkat-ul Jihad Islami (HuJI) Bangladesh, Jamaat-ul Mujahideen Bangladesh (JMB), Jagrata Muslim Janata Bangladesh (JMJB), Shahadat-e-al Haqima (SAH), Hizbut Tahrir, Islami Samaj, Ulama Anjuman al Balyinaat, Hizb-ut Tahrir, Islamic Democratic Party, Touhid Trust, Tamir ud-Deen, Alla’r Dal. Of these 12 groups, four including HuJI, SAH, JMB and JMB were previously banned.

13.7.3 WHAT, WHY, WHO AND WHEN SCREENING IS REQUIRED?

- Sanctions, PEPs and ‘Bad Guys’, Internal/local Banned Lists
- AML, Terrorist Financing, Proceeds of Crime
- Customers, Prospects, Vendors, Beneficiaries, Employees
- Customer On-boarding, Ongoing, Transaction (local/international) Screening

13.8 SANCTION SCREENING MECHANISM AT BRAC BANK

SANCTION list screening is not only a regulatory requirement but also required by SRO (Statutory Regulatory Order) and laws (Anti-Terrorism Act 2009, amended in 2013). Therefore, all concerned are advised to screen accounts against UN/OFAC/EU/French/Local List Sanction before account opening and for all cross border transactions including trade and remittance. Banks have already developed a SANCTION screening tool integrated with DEDUPE search engine as well as mRemit.

The Screening is integrated with our multiple in-house systems like DEDUPE, mRemit & Spotlight as well as in Finacle. Following are the key features of screening:

Ø Real Time Synchronization of Sanction List:

Office of Foreign Assets Control (OFAC), a wing of US Treasury Department is maintaining the updated list of United Nation Sanctions and one of the important features of this developed project
is to synchronize that list on daily basis automatically with OFAC site. So that we can check our accounts or transactions with any matched items from OFAC list.

Ø Implementation of Sound like and Score based Searching with Print option:

To make the searching easier, here two advance search algorithms have been used. Now, names that are similar to pronounce can be detected with any spelling and searching can be done based on the given matching percentage. Every search output can be printed from user end for subsequent attachment of that printed copy with the AOF.

Ø Periodic Searching of Entire Customer Base of the Bank with UN Sanctions:

This advance feature will periodically check Bank's existing Customer base with the updated Sanctions maintained by the Bank and report the suspicious individuals as well as organizations.

Ø Real Time Screening of Remittance Transactions:

1. Exchange house that used to share excel file to the Bank to remit the beneficiaries, those beneficiaries will be screened before paying the remittances through this project.

2. Exchange House that have direct credit arrangement with the bank, can directly credit to the beneficiaries and here, as the beneficiaries are our existing customers and we already performed the screening of those customers while opening the account and all of them are getting checked periodically, this project will generate report at day end if any beneficiary found matching very closely with any one of the sanctions.

3. A user interface has been developed to identify suspicious beneficiaries before performing remittance transactions anywhere through exchange house like Western Union.

Ø Real Time Screening of Trade Transactions:

Through this mechanism every trade transaction will be under screening before flowing into the SWIFT queue.

Ø Incorporation of Local, French & EU Sanctions:

Sanctions imposed by both Bangladesh and French Government on different individual organizations will be also under screening of this project. Besides, latest list of European Union (EU) has also been incorporated.

SANCTION Screening Manuals:

All manuals are attached with this guideline

13.9 ROLE OF BRAC BANK IN PREVENTING TF & PF

Ø BRAC Bank has issued Policy & procedure approved by the approval of Board of Directors for detection and prevention of financing of terrorism and financing in proliferation of weapons of mass destruction, issued various instructions about the duties of Bank officials.
All concerned of the Bank are advised to take necessary measures with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under ATA, 2009 and if any suspicious transaction is identified, the concerned shall spontaneously report it to AMLD without any delay.

If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, AMLD shall send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to BFU-I immediately.

BSL has developed a search engine to maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. Bank run regular checks on the given parameters, including transactional review, to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.

The bank has developed tools to check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009; individuals or entities owned or controlled directly or indirectly by such persons or entities, as well as persons and entities acting on behalf of, or at the direction of, individuals or entities listed or scheduled under the Act are holding any funds, financial assets or economic resources or related services or having any form of relationship with the bank.

CONCLUSION
BRAC Bank must comply with the requirement of this guideline for combating money laundering and terrorist financing. Where there is any confusion or any contradiction arises from this guideline, it should be referred to CAMLCO or DCAMLCO for further guidance. CAMLCO is the authority to explain sense and sentiment of the policy and can impose a tougher control mechanism or instructions not mentioned in this guideline on AML/CFT ground. In that case, he has to take advice from Managing Director and CEO of the Bank.
RISK MANAGEMENT GUIDELINES

Annexure-A

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Score</th>
<th>Treatment/Mitigation strategy</th>
</tr>
</thead>
</table>
| New customer | Likely | Moderate | Medium | a) Obtain full and accurate information.  
b) Verify the information.  
c) Screen the account against UNSCR sanctions and OFAC list before opening.  
d) Obtain required documents.  
e) Conduct KYC with appropriate risk grading.  
f) Perform Customer Due Diligence (CDD) |
| Walk-in customer | Unlikely | Minor | Low | a) Obtain purpose of transaction.  
b) Obtain relevant documents like NID and source of funds.  
c) Complete short KYC and perform CDD. |
| A new customer who wants to carry out a large transaction | Likely | Moderate | Medium | a) Analyze the circumstances under which customer wants to carry out the transaction.  
b) Collect documentary evidence in support of source of fund.  
c) Ensure that the transaction is commensurate with profession/source of income.  
d) Ensure that complete KYC is in place.  
e) Where required, attain information of beneficial owner.  
f) Perform Enhanced Due Diligence (EDD) |
| A customer or a group of customers making lots of transactions to the same individual or group | Very Likely | Moderate | High | a) Identify the list of accounts involved with the transactions.  
b) Analyze the transactions in terms of origination and destination of the transaction.  
c) Check declared TP with actual transactions.  
d) Monitoring the transactions exceeding the limits declared in their TPs, those taking place at different regions of the country.  
e) Obtain justification from the customer.  
f) Conduct Enhanced Due Diligence.  
g) In case of non-cooperation from customer end, close the accounts or raise STR. |
| A customer whose identification is difficult to check | Likely | Moderate | Medium | a) Apply Customer Due Diligence  
b) Conduct complete KYC  
c) Obtain information of beneficial owner |
|---|---|---|---|---|
| Customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates | Likely | Major | High | a) Ensure purpose of account opening  
b) Conduct Enhanced Due Diligence  
c) Obtain approval from senior management  
d) Get additional information as per approving authority.  
e) Grade the account in high risk category |
| 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. | Likely | Major | High | a) Identifying beneficial owners of the accounts and obtaining their complete information  
b) Monitoring the transactions exceeding the limits declared in their TPs  
c) Conduct Enhanced Due Diligence  
d) Where above are not possible, decline the transaction |

**Retail (Supreme and Priority)**

| A new customer who wants to carry out a large transaction. | Likely | Moderate | Medium | a) Obtain documents of Source of fund  
b) Crosscheck the income with occupation and nature of business  
c) Maintain proper TP  
d) Conduct complete KYC  
e) Apply Customer Due Diligence |
|---|---|---|---|---|
| Customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates | Likely | Moderate | Medium | a) Conduct complete KYC  
b) Perform EDD  
c) Obtain approval from senior management  
d) Obtain information of beneficial owner  
e) Search in media for any adverse news |
| Customer opens account in the name of his/her family member who intends to credit large amount of | Unlikely | High | Medium | a) Obtain documents of Source of fund  
b) Crosscheck the income with occupation and nature of business  
c) Conduct complete KYC  
d) Maintain proper TP  
e) Apply Customer Due Diligence |
<table>
<thead>
<tr>
<th>Deposits not consistent with the known sources of legitimate family income.</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Small Medium Enterprise</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customers with complex accounting and huge transaction</td>
<td>Very Likely</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>a) Monitoring of transaction and check whether it commensurate with source of fund</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Conduct Enhanced Due Diligence (EDD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receipt of donor fund, fund from foreign source</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
</tr>
<tr>
<td>a) Identify the source of fund with supporting document</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Conduct Enhanced Due Diligence (EDD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer which are reporting organization under MLP Act 2012 not complying with the reporting requirements</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
</tr>
<tr>
<td>a) Complete KYC of the customer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Obtain declaration whether the customer follows MLP Act 2012 as a reporting organization</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wholesale Banking Division</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A new customer who wants to carry out a large transaction.</td>
<td>Very Likely</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>a) Obtain documents regarding source of fund.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Check whether TP of the customer commensurate with the income and occupation; identify nature of business and transaction patterns.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) Complete bank’s prescribed KYC form</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d) Cash flow statement (audited/ unaudited)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e) Physical visit of client office premises.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f) Check sales register against deposit.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g) Previous bank statement.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h) Apply Enhanced Due Diligence.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A customer or a group of customers making lots of transactions to the same individual or group (wholesale).</td>
<td>Very Likely</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>a) Generate report from system and review transactions pattern.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Confirm the purpose of transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) In Cash Management business, transaction within the group is possible; however, it is governed by the cash management agreement and regular monitoring is conducted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d) Conduct Enhanced Due Diligence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A customer whose identification is difficult to check.</td>
<td>Unlikely</td>
<td>Minor</td>
<td>Low</td>
</tr>
<tr>
<td>a) RM does not open account without proper verification of identification.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Physically visit the client premises and develop call report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) Obtain information about the customer from market.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A non-resident customer</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
</tr>
<tr>
<td>a) Perform EDD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Obtain information about the customer from market.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ML & TF Risk Management Guidelines

<table>
<thead>
<tr>
<th>Credit Card</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Credit Card customer</strong></td>
<td>Very Likely</td>
<td>Minor</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Customer who changes static data frequently</strong></td>
<td>Likely</td>
<td>Moderate</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Customer doing frequent transaction &amp; payment through card (Prepaid &amp; Credit card)</strong></td>
<td>Very Likely</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td><strong>Customer doing high volume</strong></td>
<td>Very Likely</td>
<td>Major</td>
<td>Extreme</td>
</tr>
<tr>
<td><strong>Customers that are Politically Exposed Persons (PEPs) or Influential Persons (IPs) or head of International Organizations and their family members and close associates</strong></td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
</tr>
</tbody>
</table>

### C) Advance allowed considering the category.

- a) Obtain documents regarding source of fund.
- b) Check whether TP of customer commensurate with the income and occupation; identify nature of business and transaction patterns.
- c) Perform EDD
- d) Foreign Exchange Regulation Act 1947 and policy of BB in this regard are followed for PEPs.
- e) Obtain senior management approval before opening the account.

| 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. | Unlikely | Major | Medium |

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credit Card</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>New Credit Card customer</strong></td>
<td>Very Likely</td>
<td>Minor</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Customer who changes static data frequently</strong></td>
<td>Likely</td>
<td>Moderate</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Customer doing frequent transaction &amp; payment through card (Prepaid &amp; Credit card)</strong></td>
<td>Very Likely</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td><strong>Customer doing high volume</strong></td>
<td>Very Likely</td>
<td>Major</td>
<td>Extreme</td>
</tr>
</tbody>
</table>

### a) Identify beneficial owner of the account
- b) Perform CDD for beneficial owner.
- c) KYC of beneficial owner will be completed.

### b) Obtain documents requiring support of changed information
- a) Address & contact number verification through CPV.
- b) Obtain documents in support of changed information.
- c) Customer acknowledgement obtain by sending letter to old and new address.
- d) Conduct Enhanced Due Diligence.

### c) Apply enhanced due diligence.
- a) Match Transaction with customer’s income.
- b) Provide restriction on number and amount of transaction.
- c) Apply enhanced due diligence.

### d) SMS sent to customer mobile number
- a) Communicate with Customer to verify the transaction.
| transaction (merchant point) | Likely | Moderate | Medium | a) Screening against UNSCR/OFAC list  
b) EDD and obtain other BE prescribed ID  
c) confirm cell phone number |
|-------------------------------|--------|----------|--------|---------------------------------------------------------------------------------|
| Walk in customer without NID (WU & others) | Very Likely | Moderate | High | a) Screening against UNSCR/OFAC list  
b) Conduct EDD  
c) Old customer of other bank: obtain certificate from previous bank on "no overdue or outstanding bill of entry"  
d) New Customer: Confirm that all relevant documents including IRC/ERC are in place |
| A new customer (Import/Export) | Likely | Moderate | Medium | a) CDD of the customer  
b) Sanction screening  
c) Ensure the purpose of the remittance with supporting documents |
| A new customer (Outward remittance-through SWIFT) | Very Likely | Minor | Medium | a) CDD of the beneficiary  
b) Sanction screening  
c) Ensure the purpose of the remittance with supporting documents  
d) Obtain C form where applicable |
| A new customer who wants to carry out a large transaction (Import/Export) | Likely | Moderate | Medium | a) Screening against UNSCR/OFAC list  
b) Conduct CDD  
c) Old customer of other bank: obtain certificate from previous bank on "no overdue or outstanding bill of entry"  
d) New Customer: Confirm that all relevant documents |
| A new customer who wants to carry out a large transaction (Inward/outward remittance) | Unlikely | Major | Medium | a) In addition to above, perform EDD |
| A customer wants to conduct business beyond its line of business (Import/export/remittance) | Unlikely | Major | Medium | a) Check the business diversification  
b) Perform EDD |
| Customers that are politically exposed persons or influential persons or head of international | Likely | Major | High | a) Perform EDD |
### A new customer who wants to carry out a large transaction (Import Export)

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Score</th>
<th>Treatment/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASA (Savings Classic, Current Classic, Current Plus account, Easy, Future star etc.)</td>
<td>Likely</td>
<td>Moderate</td>
<td>Medium</td>
<td>a) Screening against UNSCR/OFAC list; b) Conduct CDD; c) Obtain certificate from previous bank on &quot;overdue or outstanding bill of entry&quot;; d) New Customer; e) Confirm that all relevant documents</td>
</tr>
<tr>
<td>High Value FDR</td>
<td>Likely</td>
<td>Moderate</td>
<td>Medium</td>
<td>a) Obtain documents of Source of fund; b) Obtain justification from the customer; c) Making sure that Transaction Profiles (TP) provided by the customers are proportionate with the sources of funds, and supported by necessary documents; d) Monitoring the transactions exceeding the limits declared in their TPs, those taking place at different regions of the country</td>
</tr>
<tr>
<td>Personal Loan, Salary Loan</td>
<td>Unlikely</td>
<td>Minor</td>
<td>Low</td>
<td>a) Obtain documents of Source of fund; b) Obtaining accurate and complete information from the customers and ensuring its verification and authenticity of documents; c) Collect complete details including guarantor information; d) Verifying information obtained from other financial institutions; e) Obtaining corroboration of information in employer letters, references, pay stubs or credit e) Strictly follow up of loan purpose</td>
</tr>
</tbody>
</table>

### Retail Privilege (Premium and Supreme)

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Score</th>
<th>Treatment/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triple benefit account with threshold 50 lac above</td>
<td>Likely</td>
<td>Moderate</td>
<td>Medium</td>
<td>a) Obtain documents of Source of fund; b) TIN required; c) Perform EDD; d) Ensure home/office address by physical visitation; e) Ensure business activity of the client</td>
</tr>
</tbody>
</table>
| Home and Car loan | Very Likely | Moderate | High | a) Obtain documents of Source of fund  
b) Obtain justification from the customer  
c) Making sure that Transaction Profiles (TF) provided by the customers are proportionate with the sources of funds, and supported by necessary documents  
d) Monitoring the transactions exceeding the limits declared in their TFs, those taking place at different regions of the country  
e) Conduct EDD |
| PO/DD | Very Likely | Moderate | High | a) Check background of the client  
b) Seek details on beneficiary  
c) Obtain purpose of PO  
d) Perform EDD |
| Small Medium Enterprise | Likely | Moderate | Medium | a) Check customer background  
b) Perform CDD  
c) Monitoring transaction and check whether it commensurate with source of fund  
d) Obtain document in support of source of fund  
e) Perform CDD of customer |
| FDR opened where source of fund is not clear | Likely | Moderate | Medium | a) Obtain declaration of specific reason of early encashment  
b) Perform CDD of customer  
c) Monitoring transaction and check whether it commensurate with source of fund  
d) Obtain document in support of source of fund  
e) Perform CDD of customer |
| Early encashment of FDR | Very Likely | Minor | Medium | a) Obtain declaration of specific reason of early encashment  
b) Perform CDD of customer  
c) Monitoring transaction and check whether it commensurate with source of fund  
d) Obtain document in support of source of fund  
e) Perform CDD of customer |
| Mixing of undisclosed money with regular sales proceeds. | Likely | Moderate | Medium | a) Perform CDD of customer  
b) Monitoring transaction and check whether it commensurate with source of fund  
c) Monitoring transaction and check whether it commensurate with source of fund  
d) Obtain document in support of source of fund  
e) Perform CDD of customer |
| Repayment of loan EMI from undisclosed source thus bringing undisclosed money as legal in the financial system. | Likely | Moderate | Medium | a) Monitoring transaction and check whether it commensurate with source of fund  
b) Arrange periodic visit at customer's business site  
c) Monitoring transaction and check whether it commensurate with source of fund  
d) Obtain document in support of source of fund  
e) Perform CDD of customer |
| Repayment of full loan amount before maturity | Likely | Moderate | Medium | a) Source of fund of repayment to be ensured before early adjustment of loan.  
b) Perform CDD of customer  
c) Monitoring transaction and check whether it commensurate with source of fund  
d) Obtain document in support of source of fund  
e) Perform CDD of customer |
| Loan amount utilized in undisclosed sector other than the sector specified during availing the loan. | Unlikely | Major | Medium | a) Utilization of loan to be monitored properly.  
b) Perform CDD of customer  
c) Monitoring transaction and check whether it commensurate with source of fund  
d) Obtain document in support of source of fund  
e) Perform CDD of customer |
## Repayment of EMI from undisclosed family income

<table>
<thead>
<tr>
<th>Likely</th>
<th>Moderate</th>
<th>Medium</th>
<th>a) Monitoring transaction and check whether it commensurate with source of fund</th>
</tr>
</thead>
</table>

## NGO taking loan from bank, but mixing this fund with fund from undisclosed source and providing loan to the NGO members

| Unlikely | Major | Medium | a) Perform EDD  
b) Monitor transaction vigorously |
|----------|-------|--------|--------------------------------------------------------------------------|

## Undisclosed source of fund used as security

<table>
<thead>
<tr>
<th>Unlikely</th>
<th>Minor</th>
<th>Low</th>
<th>a) Source of security fund (FDR) to be obtained</th>
</tr>
</thead>
</table>

### Wholesale Banking Division

#### Payment received from unrelated third parties

| Unlikely | Moderate | Low | a) Payment received only from the distributors, agents and suppliers of the customer.  
b) Obtain short KYC of depositor/withdrawer  
c) Monitor the transaction report on daily basis |
|----------|----------|-----|--------------------------------------------------------------------------|

#### Any new product & service developed

| Likely | Moderate | Medium | a) Identify ML & TF risk of the product  
b) Vetting obtain from AML department |
|--------|----------|--------|--------------------------------------------------------------------------|

#### High Value FDR

| Very Likely | Moderate | High | a) Cash Management book high value FDR of Large reputed corporate bodies and Govt. agencies.  
b) Source of fund is confirmed with supporting document  
c) Complete short KYC as per KYC profile format  
d) Conduct Enhanced Due Diligence |
|-------------|----------|------|--------------------------------------------------------------------------|

#### Term loan, SOD, LATR, Work Order Finance, Loan General, Lease finance, Bill Purchase

| Likely | Moderate | Medium | a) Comprehensive Credit memo is prepared to analysis client credit worthiness.  
b) Visit client office, factory and mortgaged properties |
|--------|----------|--------|--------------------------------------------------------------------------|

#### L/C Subsequent term loan, Letter of Guarantee

| Likely | Moderate | Medium | a) Proper verification of the value of the imported items  
b) Certificate from the respective country’s chamber of commerce  
c) Undertaking from the customer regarding the price |
|--------|----------|--------|--------------------------------------------------------------------------|

#### Custodial Service (Probashi Biyog)

| Likely | Moderate | Medium | a) Ensure that account opened with compliance of FER Guideline  
b) Close monitoring of transaction |
|--------|----------|--------|--------------------------------------------------------------------------|
| OBU                          | Likely | Moderate | Medium | a) Verifying other source of income.  
|------------------------------|--------|----------|--------|--------------------------------------  
|                              |        |          |        | a) Perform EDD                      2  
|                              |        |          |        | b) Obtain information about the customer from market 2  
|                              |        |          |        | c) Advance allowed considering the category. 2  
| Syndication Financing        |        |          |        | a) Proper verification of the value of planted machinery and imported items. 2  
|                              |        |          |        | b) Certificate from the respective country’s chamber of commerce. 2  
|                              |        |          |        | c) Undertaking from the customer regarding the price. 2  
| Payment received from unrelated third parties | Unlikely | Minor | Low | a) Payment received only from the distributors, agents and suppliers of the customer. 2  
|                              |        |          |        | b) Obtain short KYC of depositor/withdrawer 2  
|                              |        |          |        | c) Monitor the transaction report on daily basis. 2  
| DPS opened with big installment and small tenure | Very Likely | Moderate | High | a) Obtain document in support of source of fund 2  
|                              |        |          |        | b) Perform EDD of customer 2  
|                              |        |          |        | c) Checking other relationship of the customer with bank 2  
| Multiple deposit scheme opened by the same customer in a branch | Very Likely | Minor | Medium | a) Obtain document in support of source of fund 2  
|                              |        |          |        | b) Perform CDD of customer 2  
|                              |        |          |        | c) Checking other relationship of the customer with bank 2  
| Multiple deposit scheme opened by the same customer from different location | Likely | Moderate | Medium | a) Obtain document in support of source of fund 2  
|                              |        |          |        | b) Obtain written justification from the customer 2  
|                              |        |          |        | c) Perform CDD of customer 2  
|                              |        |          |        | d) Checking other relationship of the customer with bank 2  
| Opens DPS in the name of family member Or Installments paid from the account other than the customer’s account | Very Likely | Moderate | High | a) Identify beneficial owner and obtain complete information 2  
|                              |        |          |        | b) Obtain written justification from the customer 2  
|                              |        |          |        | c) Perform EDD of customer 2  
|                              |        |          |        | d) Checking other relationship of the customer with bank 2  
| Stand-alone DPS              | Likely | Moderate | Medium | a) Obtain document in support of source of fund 2  
|                              |        |          |        | b) Perform CDD of customer 2  
| Early encashment            | Very Likely | Minor | Medium | a) Obtain declaration of specific reason of early encashment 2  
| Credit Card                 |        |          |        | 2  
| BRAC Bank Ltd               |        |          |        | 2  
| Page 99 of 123              |        |          |        | 2  

ML & TF Risk Management Guidelines
### Supplementary Credit Card Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Likely</th>
<th>Moderate</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Collect all credit card docs as per PPG.</td>
<td>b) Mention relationship with supplementary cardholder</td>
<td>c) Complete KYC.</td>
<td>d) Collect &amp; Check CIB report.</td>
</tr>
<tr>
<td>e) Address &amp; contact number verification through CPV.</td>
<td>f) UNSCR sanction and OFAC list check</td>
<td>g) Duplicate card check.</td>
<td></td>
</tr>
<tr>
<td>Frequent use of Card Cheque and overpaid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Obtain the purpose of transaction</td>
<td>b) Review transactions</td>
<td>c) Relationship with the account holder, the account where the fund is transferred.</td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td>Minor</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>a) Allow the facility only to renowned and selected merchants</td>
<td>b) Conduct Enhanced Due Diligence (EDD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BFTN cheque or pay order as mode of payment instead of account opening at bank (Merchant)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Collect all credit card docs as per PPG.</td>
<td>b) Complete KYC.</td>
<td>c) Collect &amp; Check CIB report.</td>
<td></td>
</tr>
<tr>
<td>d) Address &amp; contact number verification through CPV.</td>
<td>e) Duplicate card check.</td>
<td>f) Transaction conducted as per Foreign Exchange policy guideline.</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card issuance against ERQ and RFC accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Check the business diversification</td>
<td>b) Arrange physical visitation at business place</td>
<td>c) Perform EDD</td>
<td></td>
</tr>
<tr>
<td>Under/Over invoicing (import/export/remittance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Crosscheck the unit price of the product intended for import and export with the present market price</td>
<td>b) Perform EDD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash retirement of import bills (import/export/remittance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Checking the size of the transaction with customer cash flow</td>
<td>b) Perform EDD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Confirm the purpose of remittance with supporting documents</td>
<td>b) Perform CDD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Trade and Remittance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line of business mismatch (import/export/remittance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Perform EDD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Under/Over invoicing (import/export/remittance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Crosscheck the unit price of the product intended for import and export with the present market price</td>
<td>b) Perform EDD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash retirement of import bills (import/export/remittance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Checking the size of the transaction with customer cash flow</td>
<td>b) Perform EDD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Confirm the purpose of remittance with supporting documents</td>
<td>b) Perform CDD.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 3. Business Practices/Delivery Methods or Channels

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Score</th>
<th>Treatment/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wholesale Banking Division</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Online (multiple small transaction through different branch) | Very Likely | Moderate | High | a) Generate report on on-line transaction and monitor  
| | | | | b) Obtain KYC of bearer  
| | | | | c) Conduct Enhanced Due Diligence |
| BFETN | Very Likely | Minor | Medium | a) Transaction executed as per agreement with the customer  
| | | | | b) Monitor transaction pattern, update TP and keep track of distributors |
| IDBP | Very Likely | Minor | Medium | a) Check the genuineness of the LC and acceptance from BB dashboard,  
| | | | | b) Perform CDD |
| **Retail (Credit Card)** | | | | |
| New Merchant sign up | Very Unlikely | Minor | Medium | a) Complete Merchant KYC  
| | | | | b) Visit Merchant physically and conduct feasibility analysis  
| | | | | c) Collect all documents as per PPG |
| High volume transaction through POS | Very Likely | Major | High | a) Check Merchant product & price and match with POS transaction  
| | | | | b) Check Transaction Profile of merchant  
| | | | | c) Conduct Enhanced Due Diligence |
| **ADC** | | | | |
| Large amount withdrawn from ATMs | Likely | Minor | Low | a) Generate report from the system and monitor the transactions.  
| | | | | b) Apply transaction restriction policy (transaction limit).  
| | | | | c) Inform issuer bank if possible.  
| | | | | d) Follow Central Bank, International Payment Association ML rules  
| | | | | e) Also inform the Cards payment Association (i.e. Visa, Master Card) |
| Larger amount transaction from different location and different time (midnight) through ATM | Likely | Moderate | Medium | a) Generate report from the system and monitor the transactions.  
| | | | | b) If any irregularities found, inform relevant branch and department |
| Large amount cash deposit in CDM | Likely | Minor | Low | a) Before giving input in CBS, branch people will ask the customer about the authenticity of the deposit.  
| | | | | b) If any irregularities found, inform relevant department. |
### Risk Management Guidelines

<table>
<thead>
<tr>
<th><strong>Huge fund transfer through Internet</strong></th>
<th><strong>Likely</strong></th>
<th><strong>Moderate</strong></th>
<th><strong>Medium</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Dual registration (both online and branch) at the time of taking internet banking facility.</td>
<td>b) Apply transaction restriction policy (transaction limit in terms of number and amount, session time limit).</td>
<td>c) Generate report from the system and monitor the transactions.</td>
<td>d) IR administrator communicates with customer if customer transaction reaches the highest level every time</td>
</tr>
<tr>
<td><strong>Customer to business transaction-Online Payment Gateway - Internet Banking</strong></td>
<td><strong>Very Likely</strong></td>
<td><strong>Moderate</strong></td>
<td><strong>High</strong></td>
</tr>
<tr>
<td>a) Only allow transaction with business houses that are listed under payment processors (e-commerce merchant) approved by Bangladesh Bank.</td>
<td>b) Arrange AML &amp; CFT training for payment processors and obtain KYC of business houses</td>
<td>c) Conduct Enhanced Due Diligence</td>
<td></td>
</tr>
</tbody>
</table>

#### Trade & Remittance

| **Customer sending remittance through SWIFT under single customer credit transfer.** | **Very Likely** | **Moderate** | **High** |
| a) Check whether the transaction meets the central Bank guide line/circular. | b) Obtain purpose of the remittance from the customer (documents if required). | c) Screen the customer details against UN/OFAC Sanction list. | d) Beneficiary’s proper identification should be taken (such as name, a/c number, full address, country name). |
| e) Applicant’s proper identification should be taken (such as name, a/c number, full address, country name). | f) Applicant, Beneficiary, Beneficiary’s Bank and Beneficiary’s correspondent should be checked whether they are under any sanction list or not. | g) Conduct Enhanced Due Diligence |

| **Existing customer/other bank customer receiving remittance through SWIFT.** | **Likely** | **Minor** | **Low** |
| a) C form should be taken (if necessary) before release of remittance. | b) Obtain any other document as and when required. | c) Conduct CDD |

#### 4 Country/Jurisdiction

<table>
<thead>
<tr>
<th><strong>Risk</strong></th>
<th><strong>Likelihood</strong></th>
<th><strong>Impact</strong></th>
<th><strong>Risk Score</strong></th>
<th><strong>Treatment/Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Import and export to sanction country</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
<td>a) Automated screening mechanism against Sanction list should be in place</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b) Procedure in place to treat such situation</td>
</tr>
</tbody>
</table>

---

BRAC Bank Ltd Page 102 of 123
### ML & TF Risk Management Guidelines

| Transshipments, container, flag vessel etc. under global sanction | Unlikely | Major | Medium | a) Automated screening mechanism against Sanction list should be in place  
b) Procedure in place to treat such situation |
| Establishing correspondent relationship with sanction bank and/or country | Unlikely | Major | Medium | a) Automated screening mechanism against Sanction list should be in place  
b) Procedure in place to treat such situation  
c) Perform KYC/CDD with the correspondence bank |
| Establishing correspondent relationship with poor AML practice country | Unlikely | Major | Medium | a) Obtain KYC from the correspondent bank  
b) ensure the specific purpose for establishing correspondent relationship  
c) Perform EDD |

#### b. Regulatory risk

Regulatory risk is associated with not meeting all obligations of banks under the Money Laundering Prevention Act, 2012, Anti-Terrorism Act, 2009 (including all amendments), the respective Rules issued under these two acts and instructions issued by BFIU. Following are some examples of ML&TF risk the bank faces in terms of non-compliance of regulations and the possible ways to reduce and manage those risks.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk score</th>
<th>Treatment/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not forming an AMLD</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Low</td>
<td>Formation of AMLD as per the requirement of BFIU on time</td>
</tr>
<tr>
<td>Not having an AML &amp; CFT Compliance Officer</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Low</td>
<td>Appointment of AML&amp;CFT Compliance Officer as per BB prescribed directive.</td>
</tr>
<tr>
<td>Not having Branch Anti-Money Laundering Compliance Officer</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Low</td>
<td>Appointment of Branch Anti Money Laundering Compliance Officer (BAMLCO) as per BFIU instruction</td>
</tr>
<tr>
<td>Not having an AML &amp; CFT program</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
<td>Developing AML &amp; CFT program and review from time to time</td>
</tr>
<tr>
<td>No senior management commitment to comply with MLP and AT Act</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Low</td>
<td>Senior management should be committed to comply with MLP and AT Act and share the commitment with bank officials at least annually</td>
</tr>
<tr>
<td>Not having an AML &amp; CFT policy guideline approved by the board</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Low</td>
<td>Develop policy guideline on MLP &amp; CTF and have it approved by the board</td>
</tr>
</tbody>
</table>
| Failure to follow the AMLD/BFIU circular, circular letter, instructions etc. | Unlikely | Major | High | a) Follow the AMLD/BFIU circular, circular letter, instructions  
b) Regular inspection |
<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Likelihood</th>
<th>Probability</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique account opening form not followed while opening account</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Develop account opening form for the bank in line with the unique account opening form prescribed by BFIU</td>
</tr>
<tr>
<td>Non screening of new and existing customers against UNSCR Sanction and OFAC lists</td>
<td>Likely</td>
<td>Moderate</td>
<td>Screen all new and existing customers against UNSCR Sanction and OFAC lists</td>
</tr>
<tr>
<td>Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts</td>
<td>Likely</td>
<td>Moderate</td>
<td>Follow the Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts</td>
</tr>
<tr>
<td>Accurate and complete information of customer not obtained</td>
<td>Likely</td>
<td>Moderate</td>
<td>Obtain accurate and complete information of customer, review and update from time to time</td>
</tr>
</tbody>
</table>
| Failure to verify the identity proof document and address of the customer   | Likely     | Major       | a) Verify the identity proof document with the support of database from concerned authority  
|                                                                          |            |             | b) Verify address by sending thanks letter or conduct CFV or physical verification by bank official and receive, record supporting document with AOF |
| Beneficial owner identification and verification not done properly          | Likely     | Major       | Identify beneficial owner of the account and obtain accurate and complete information |
| Customer Due Diligence (CDD) not practiced                                 | Likely     | Major       | Conduct Customer Due Diligence (CDD) as per BFIU instruction |
| Failure of doing 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,) | Likely     | Major       | a) Obtain Senior Management approval before opening such account  
|                                                                          |            |             | b) Conduct Enhanced Due Diligence (EDD) for high risk customers as per BFIU instruction |
| Failure to complete KYC of customer including walk in customer             | Likely     | Major       | Complete KYC profile form for all customer as per BFIU instruction |
| Failure to update TP and KYC of customer                                   | Likely     | Major       | Update TP & KYC as per the instruction of BFIU |
| Keep the legacy accounts operative without completing KYC                  | Unlikely   | Major       | Update KYC of legacy account else keep those as dormant |
| Failure to assess the ML & TF risk of a product or service before launching | Unlikely   | Major       | Assess the ML & TF risk of a product or service before launching and have the PPG approved by CAMLCO |
| Failure to complete the KYC of Correspondent Bank                         | Likely     | Major       | a) Complete the KYC of Correspondent Bank reciprocally  

BRAC Bank Ltd
<table>
<thead>
<tr>
<th>Event</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Management approval not obtained before entering into a</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
<td>Obtain Senior Management approval before entering into a</td>
</tr>
<tr>
<td>Correspondent Banking relationship</td>
<td></td>
<td></td>
<td></td>
<td>Correspondent Banking relationship</td>
</tr>
<tr>
<td>Enter into a relationship with shell bank</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
<td>Check whether the correspondent bank is a shell bank</td>
</tr>
<tr>
<td>Failure to comply with the instruction of BFIU by Foreign subsidiary</td>
<td>Likely</td>
<td>Major</td>
<td>Medium</td>
<td>a) Monitor the AML &amp; CFT activity of foreign subsidiary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b) Get confirmation from the subsidiary on compliance</td>
</tr>
<tr>
<td>Failure to keep record properly</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
<td>Keep records as per BFIU instruction</td>
</tr>
<tr>
<td>Failure to report complete and accurate CTR on time</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
<td>a) Rectify the lack in CBS reported in CTR on monthly basis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b) Ensure uniformity of CTR submitted through goAML web and FIU software</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>c) Submit complete and accurate CTR on time</td>
</tr>
<tr>
<td>Failure to monitor CTR</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
<td>Monitor the transactions reported in CTR on monthly basis</td>
</tr>
<tr>
<td>Failure to identify and monitor structuring</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
<td>Identify and monitor structuring on monthly basis</td>
</tr>
<tr>
<td>Failure to provide sufficient controls and monitoring systems for</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
<td>Generate high value transaction report, TP exceed report, structuring report from the system to analyze and detect STR</td>
</tr>
<tr>
<td>the timely detection and reporting of suspicious activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to report suspicious transaction report (STR)</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
<td>Monitor account transaction and customer activity and report when suspicious arise</td>
</tr>
<tr>
<td>Failure to conduct quarterly meeting properly.</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Low</td>
<td>Conduct quarterly meeting properly in line with the agenda and instruction of BFIU</td>
</tr>
<tr>
<td>Failure to conduct self-assessment properly</td>
<td>Likely</td>
<td>Moderate</td>
<td>Medium</td>
<td>a) Conduct self-assessment properly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b) Portray the actual strength, weakness and position of the branch in self-assessment</td>
</tr>
<tr>
<td>Failure to submit statement/report to BFIU on time</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
<td>Submission of statement/report to BFIU timely</td>
</tr>
<tr>
<td>Submit erroneous statement/report to BFIU</td>
<td>Likely</td>
<td>Major</td>
<td>High</td>
<td>Check minutely the statements before submitting the same to BFIU</td>
</tr>
<tr>
<td>Not complying with any order for freezing or suspension of</td>
<td>Unlikely</td>
<td>Major</td>
<td>Medium</td>
<td>Complying with order for freezing or suspension of</td>
</tr>
<tr>
<td>issued by BFIU or BB</td>
<td>transaction issued by BFIU or BB instantly</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not submitting accurate information or statement sought by</td>
<td>Provide accurate information to BFIU on time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely Moderate Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>senior management regularly</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to rectify the objections raised by BFIU or inspection teams on time</td>
<td>Regularize the objections raised by BFIU or inspection teams on time and submit compliance report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely Major High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to obtain information during wire transfer</td>
<td>Obtain information during wire transfer based on the threshold</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely Major High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank</td>
<td>Comply with the responsibilities of ordering, intermediary and beneficiary bank as per BFIU instruction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely Major High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to scrutinize staff properly</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely Major High</td>
<td>a) HR to screen the applicant’s details before recruitment b) Conduct reference check</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to circulate BFIU guidelines and circulars to branches</td>
<td>Update the branches on circulars/ circular letters/ instructions received from BFIU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely Major Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequate training/workshop arranged on AML &amp; CFT</td>
<td>Arrange workshop on MLP &amp; CFT for employees to build up awareness and conduct evaluation test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely Major Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No independent audit function to test the AML program</td>
<td>ICC to test the AML program and conduct independent testing procedure.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely Major Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### KYC Documentation Red Flags Pointing to ML/TF

<table>
<thead>
<tr>
<th>KYC Documentation Customer type</th>
<th>Standard Identification Document</th>
<th>Document for verification of source of funds</th>
<th>Document or strategy for verification of address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
<td>• Passport</td>
<td>• Salary Certificate (For salaried person)</td>
<td>• Acknowledgement receipt of thanks letter through postal department.</td>
</tr>
<tr>
<td></td>
<td>• National ID Card</td>
<td>• Employed ID (For ascertaining the level of employment).</td>
<td>• Proof of delivery of thanks letter through courier.</td>
</tr>
<tr>
<td></td>
<td>• Birth Registration Certificate (Printed copy, with seal &amp; signature from the Registrar)</td>
<td>• Self-declaration acceptable to the bank. (commensurate with declared occupation)</td>
<td>• Third party verification report.</td>
</tr>
<tr>
<td></td>
<td>• Valid driving license (if any) Credit Card (if any)</td>
<td>• Documents in support of beneficial owner's income (income of house wife, students etc.)</td>
<td>• Physical verification report of bank official.</td>
</tr>
<tr>
<td></td>
<td>• Any other documents that satisfy to the bank.</td>
<td>• Trade License if the customer declared to be a business person</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TIN (if any)</td>
<td>• Residential address appearing on an official document prepared by a Government Agency.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Documents of property sale. (if any)</td>
<td>• Third party verification report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other Bank statement (if any)</td>
<td>• Physical verification report of bank official.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Document of FDR encashment (if any)</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Document of foreign remittance (if any fund comes from outside the country)</td>
<td>• Residential address appearing on an official document prepared by a Government Agency.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Document of retirement benefit.</td>
<td>• Physical verification report of bank official.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bank loan.</td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**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 person 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.
<table>
<thead>
<tr>
<th>Joint Accounts</th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| • Passport  
• National ID Card  
• Birth Registration Certificate (Printed copy, with seal & signature from the Registrar)  
• Valid driving license (if any) Credit Card (if any)  
• Any other documents that satisfy to the bank | • Salary Certificate (For salaried person)  
• Employed ID (For ascertaining the level of employment)  
• Self-declaration acceptable to the bank. (commensurate with declared occupation)  
• Documents in support of beneficial owner’s income (income of housewife, students etc.)  
• Trade License if the customer declared to be a business person  
• TIN (if any)  
• Documents of property sale. (if any)  
• Other Bank statement (if any)  
• Document of FDR encashment (if any)  
• Document of foreign remittance (if any fund comes from outside the country)  
• Document of retirement benefit  
Bank loan. | • Acknowledgement receipt of thanks letter through postal department.  
• Proof of delivery of thanks letter through courier.  
• Third party verification report.  
• Physical verification report of bank official  
• 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.  
• Residential address appearing on an official document prepared by a Government Agency  
• Documents in support verification report  
• Any other documents that satisfy to the bank. income (income of housewife, students etc.)  
• 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.  
• Residential address appearing on an official document prepared by a Government Agency  
• Copy of the sale. (if any)  
• Other Bank statement (if any)  
• Document of FDR encashment (if any)  
• Document of foreign remittance (if any fund comes from outside the country)  
• Document of retirement benefit  
Bank loan. |
**Sole Proprietorships or Individuals doing business**

- Passport
- National ID Card
- Birth Registration Certificate (Printed copy, with seal & signature from the Registrar)
- Valid driving license (if any)
- Credit Card (if any)
- Rent receipt of the shop (if the shop is rental)
- Ownership documents of the shop (i.e., purchase documents of the shop or inheritance documents)
- Membership certificate of any association. (Chamber of commerce, market association, trade association i.e., Hardware association, cloth merchant association, hawker’s association etc.
- Any other documents that satisfy to the bank.
- Trade License TIN
- Self-declaration acceptable to the bank. (commensurate with nature and volume of business)
- Documents of property sale. (if injected any fund by selling personal property)
- Other Bank statement (if any)
- Document of FDR encashment (if any fund injected by encashing personal FDR)
- Acknowledgement receipt of thanks letter through postal department.
- Proof of delivery of thanks letter through courier.
- Third party verification report.
- Physical verification report of bank official
- 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.
- Residential address appearing on an official document prepared by Government Agency
- Documents of property through courier.

**Partnerships**

- Partnership deed/partnership letter
- Registered partnership deed (if registered)
- Resolution of the partners, specifying operational guidelines/instruction of the partnership account.
- Passport of partners
- National ID Card of partners
- Birth Registration Certificate of partners (Printed copy, with seal & signature from the Registrar)
- Trade License TIN
- Self-declaration acceptable to the bank. (commensurate with nature and volume of business)
- Documents of property sale. (if injected any fund by selling personal property)
- Other Bank statement (if any)
- Document of FDR encashment (if any fund injected by encashing personal FDR)
- Acknowledgement receipt of thanks letter through postal department.
- Proof of delivery of thanks letter through courier.
- Third party verification report.
- Physical verification report of bank official
**ML & TF Risk Management Guidelines**

<table>
<thead>
<tr>
<th>Private Limited Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Valid driving license of partners (if any)</td>
</tr>
<tr>
<td>• Credit Card of partners (if any)</td>
</tr>
<tr>
<td>• Rent receipt of the shop (if the shop is rental)</td>
</tr>
<tr>
<td>• Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents)</td>
</tr>
<tr>
<td>• Membership certificate of any association. (Chamber of commerce, market association, trade association i.e.; Hardware association, cloth merchant association, hawker's association etc.)</td>
</tr>
<tr>
<td>• Any other documents that satisfy to the bank.</td>
</tr>
</tbody>
</table>

| Document of foreign remittance (if any fund comes from outside the country) |
| Bank loan |
| Personal Borrowing (if any) |

| Copy of 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. |
| Residential address appearing on an official document prepared by a Government Agency |

| Passport of all the directors |
| National Id Card of all the directors |
| Certificate of incorporation |
| Memorandum and Articles of Association |
| List of directors |
| Resolution of the board of directors to open an account and identification of those who have authority to operate the account. |
| Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf. |
| Nature of the company's business Expected monthly turnover |
| 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 |

| A copy of last available financial statements duly authenticated by competent authority |
| Other Bank statement |
| Trade License TIN |
| VAT Registration |
| Bank Loan |

BRAC Bank Ltd

Page 110 of 123
<table>
<thead>
<tr>
<th>Public Limited Companies</th>
<th>Government-Owned Entities</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Passport of all the directors</td>
<td>• Statue of formation of the entity</td>
<td>• A copy of last available financial statements duly certified by a professional accountant</td>
<td>• N/A</td>
</tr>
<tr>
<td>• National Id Card of all the directors</td>
<td>• Resolution of the board to open an account and identification of those who have authority to operate the account</td>
<td>• Other Bank statement (if any)</td>
<td>• N/A</td>
</tr>
<tr>
<td>• Certificate of incorporation Memorandum and Articles of Association</td>
<td>• Passport and NID of the operator(s)</td>
<td>• Trade License TIN</td>
<td>• N/A</td>
</tr>
<tr>
<td>• Certificate of commencement of business</td>
<td></td>
<td>• Cash flow statement</td>
<td></td>
</tr>
<tr>
<td>• List of directors in form -XII Resolution of the board of directors to open an account and identification of those who have authority to operate the account</td>
<td></td>
<td>• VAT registration</td>
<td></td>
</tr>
<tr>
<td>• Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf.</td>
<td></td>
<td>• Bank Loan</td>
<td></td>
</tr>
<tr>
<td>• Nature of the company’s business Expected monthly turnover</td>
<td></td>
<td>• Any other genuine source</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGO</td>
<td>National Id Card of the operator(s)</td>
<td>Resolution of the board of directors to open an account and identification of those who have authority to operate the account.</td>
<td>A copy of last available financial statements duly certified by a professional accountant.</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Passport of the operator(s)</td>
<td>Documents of nature of the NGO</td>
<td>Other Bank statement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certificate of registration issued by competent authority</td>
<td>TIN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bye-laws (certified)</td>
<td>Certificate of Grand/Aid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>List of Management Committee/ Directors</td>
<td></td>
</tr>
</tbody>
</table>

BRAC Bank Ltd
<table>
<thead>
<tr>
<th>Charities or Religious Organizations</th>
<th>National Id Card of the operator(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Passport of the operator(s)</td>
</tr>
<tr>
<td></td>
<td>Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account.</td>
</tr>
<tr>
<td></td>
<td>Documents of nature of the organizations</td>
</tr>
<tr>
<td></td>
<td>Certificate of registration issued by competent authority (if any)</td>
</tr>
<tr>
<td></td>
<td>Bye-laws (certified)</td>
</tr>
<tr>
<td></td>
<td>List of Management Committee/Directors</td>
</tr>
<tr>
<td></td>
<td>A copy of last available financial statements duly certified by a professional accountant</td>
</tr>
<tr>
<td></td>
<td>Other Bank statement</td>
</tr>
<tr>
<td></td>
<td>Certificate of Grant/Aid</td>
</tr>
<tr>
<td></td>
<td>Donation</td>
</tr>
<tr>
<td></td>
<td>Any other legal source</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clubs or Societies</th>
<th>National Id Card of the operator(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Passport of the operator(s)</td>
</tr>
<tr>
<td></td>
<td>Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account.</td>
</tr>
<tr>
<td></td>
<td>Documents of nature of the organizations</td>
</tr>
<tr>
<td></td>
<td>Certificate of registration issued by competent authority (if any)</td>
</tr>
<tr>
<td></td>
<td>Bye-laws (certified)</td>
</tr>
<tr>
<td></td>
<td>List of Management Committee/Directors</td>
</tr>
<tr>
<td></td>
<td>A copy of last available financial statements duly certified by a professional (if registered)</td>
</tr>
<tr>
<td></td>
<td>Other Bank statement</td>
</tr>
<tr>
<td></td>
<td>Certificate of Grant/Aid</td>
</tr>
<tr>
<td></td>
<td>Subscription if unregistered declaration of authorized person/body.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trusts, Foundations or similar entities</th>
<th>National Id Card of the trustee(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Passport of the trustee(s)</td>
</tr>
<tr>
<td></td>
<td>Resolution of the Managing body of the Foundation/Association to open an account and identification of those who have authority to operate the account.</td>
</tr>
<tr>
<td></td>
<td>Certified true copy of the Trust Deed</td>
</tr>
<tr>
<td></td>
<td>Bye-laws (certified)</td>
</tr>
<tr>
<td></td>
<td>Power of attorney allowing transaction in the account.</td>
</tr>
<tr>
<td></td>
<td>A copy of last available financial statements duly certified by a professional (if registered)</td>
</tr>
<tr>
<td></td>
<td>Other Bank statement</td>
</tr>
<tr>
<td></td>
<td>Donation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial Institutions (NBFI)</th>
<th>Passport of all the directors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>National Id Card of all the directors</td>
</tr>
<tr>
<td></td>
<td>Certificate of incorporation Memorandum and Articles of Association</td>
</tr>
<tr>
<td></td>
<td>Certificate of commencement of business</td>
</tr>
<tr>
<td></td>
<td>List of directors in form -XII</td>
</tr>
<tr>
<td></td>
<td>Resolution of the board of directors to open an account and identification</td>
</tr>
<tr>
<td></td>
<td>A copy of last available financial statements duly certified by a professional accountant.</td>
</tr>
<tr>
<td></td>
<td>Other Bank statement</td>
</tr>
<tr>
<td></td>
<td>Trade License TIN</td>
</tr>
<tr>
<td></td>
<td>VAT registration</td>
</tr>
<tr>
<td></td>
<td>Cash flow statement</td>
</tr>
<tr>
<td>of those who have authority to operate the account.</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>• Power of attorney granted to its Managers, Officials or Employees to transact business on its behalf.</td>
<td></td>
</tr>
<tr>
<td>• Nature of the company's business</td>
<td></td>
</tr>
<tr>
<td>• Expected monthly turnover</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Embassies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Valid Passport with visa of the authorized official</td>
</tr>
<tr>
<td>• Clearance of the foreign ministry</td>
</tr>
<tr>
<td>• Other relevant documents in support of opening account</td>
</tr>
</tbody>
</table>

Important: This is an indicative list of documents. However, any contradiction with existing policy should be referred to CAMLCO/CCC for better guidance.
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 wishes 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 includes 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 transshipped 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

Behavioral 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.
August 26, 2015

EXTRACT FROM THE RESOLUTION OF THE 188TH BOARD MEETING OF BRAC BANK LIMITED HELD ON MONDAY, AUGUST 24, 2015 AT THE BOARD ROOM OF BRAC BANK LIMITED 1, GULSHAN AVENUE, GULSHAN-1, DHAKA -1212, BANGLADESH.

AGENDA: 18

Approval memo on Bkash oversight policy

Approval Memo BBL/HO/CS/188/2015 dated August 16, 2015 on Bkash oversight policy was tabled and noted.

Resolved that the guideline on Bkash oversight policy is hereby approved.

Extract attested by,

Rais Uddin Ahmad
Company Secretary,
Head of Legal and Regulatory Affairs
and CAMLCO
Memorandum: to the Board of Directors

August 16, 2015

Board Memo # BBL/HO/CS/188/2015

Agenda # 1.8

Approval memo on Bkash oversight policy

Bangladesh Bank issued mobile banking-license to BRAC Bank Limited (BBL) as a part of financial inclusion. On the other hand, BRAC Bank has formed bKash as their subsidiary to handle Mobile Financial Services (MFS). BRAC Bank must ensure that bKash is performing its activity following the MFS guideline and directive issued by Central Bank of Bangladesh. Therefore, it becomes necessary for BRAC Bank to have an oversight Policy in place on bKash to ensure smooth operation of business, services and compliance issue of bKash Ltd. Accordingly, we have developed a BRAC Bank oversight document of bKash in light of AML, KYC and CFT as regulatory requirement, as well as MasterCard for their incoming remittance initiative.

We place this guideline for the approval of Board of Directors.

Rais Ud Din Ahmad
Company Secretary,
Head of Legal & Regulatory Affairs
and CAMLCO

Syed Mahbubur Rahman
Managing Director & CEO

BRAC Bank Ltd
INTRODUCTION
Bangladesh Bank acting as Central Bank has always had a close interest in the safety and efficiency of payment and settlement systems. Payment and settlement systems are a crucial part of the financial infrastructure of a country and it is essential that they function safely and efficiently. The Government of Bangladesh has promulgated Anti Money Laundering Act, 2012 ("AML") and Anti-Terrorism (Amendment) Act, 2009 ("CFT"). To implement these laws among Banks and Financial Institutions, Bangladesh Bank has issued various Policy/Guideline on Money Laundering and Terrorist Financing through BFIU Circulars and directives. Bangladesh Bank also issued Mobile Financial Services (MFS) guidelines for the Banks and its subsidiaries for smooth operation of MFS.

Bangladesh Bank issued mobile banking license to bKash Limited as a subsidiary of BRAC Bank Limited to handle MFS within the broader concept of 'Financial Inclusion'. BRAC Bank Limited must ensure that bKash Limited is performing its activity following the MFS guidelines and directives issued by Bangladesh Bank (Central Bank of Bangladesh). Therefore, it becomes necessary for BRAC Bank Limited to have an oversight Policy in place on bKash Limited to ensure smooth operation of business, services and compliance issue of bKash Limited.

PURPOSE
The purpose of this guideline is to:
1. Ensure regulatory framework of bKash Limited for the MFS operation;
2. Ensure compliance with Anti-Money Laundering and Combating Financing of Terrorism (AML & CFT) standards set by AML & CFT rules, regulations, guidelines and instructions issued by Bangladesh Bank.

PROCESS
In accordance with Bangladesh Financial Intelligence Unit (BFIU) of Bangladesh Bank Master Circular 10 dated 28 December, 2014 Article 1.5, the core responsibility for AML & CFT for bKash Limited as a subsidiary of BRAC Bank Limited lies with bKash Limited. In terms of AML & CFT, bKash Limited will function as an Independent Reporting Organization, established its own Independent Compliance Organization to monitor and deal with AML & CFT issues. BRAC Bank will be responsible for ensuring that bKash Limited has taken necessary measures for AML & CFT compliances as per rules, regulations, guidelines and instructions issued by Bangladesh Bank. Therefore, BRAC Bank Limited Compliance Team will take necessary steps to ensure to oversee that bKash Limited is conforming to the guidelines. The following steps will be initiated by BRAC Bank Limited Compliance Team:

1. **Training & Awareness:** BRAC Bank Limited Compliance Team will monitor Training and Awareness Program arranged and conducted by the Chief Anti-Money Laundering Compliance Officer (CAMLCO) of bKash Limited. bKash Limited will be responsible to conduct its own AML & CFT Training and Awareness activities for its employees and stakeholders. In addition, Training of Trainers for bKash Limited employees associated with compliance responsibility may be arranged by BRAC Bank Limited Compliance Team. Assistance regarding AML & CFT training may also be sought from Bangladesh Bank. In addition to the training organized by bKash Limited, BRAC Bank Limited Compliance Team may conduct AML & CFT training for bKash Distributors and Agents. AML & CFT training conducted by BRAC Bank Limited may be arranged in various locations.

2. **Distributor Due Diligence:** BRAC Bank Limited will ensure through the Compliance Organization (CAMLCO) of bKash Limited that bKash Limited follows set of Due Diligence processes for their prospective Distributors. The criteria are:
- Trade License of existing business; Certificate of Incorporation with Joint Stock Registrar.
- Photo ID photocopy (copy of National ID/Passport/Driving License).
- 2 copies of passport size photographs.
- Tax Identification Certificate (TIN).
- Agreement between bKash Limited and Distributor.
- Applicant’s existing Business Profile.
- Customer Due Diligence (CDD) of KYC of the Distributor.

bKash Limited will conduct AML & CFT Compliance Field Assessments of Distributors/Agents through its own Compliance Field Assessment Team (CFAT) functioning under the CAMLCO of bKash Limited and monitored by the Central Compliance Committee (CCC) of bKash Limited. bKash Limited will cover the prescribed numbers of Compliance Field Assessment Inspections as per Bangladesh Bank requirements. In addition, BRAC Bank Limited may conduct inspection at Distributor/Agent location at any point in time with prior notification. bKash Limited will provide necessary support to BRAC Bank Limited in doing the same.

3. **Customer KYC**: The potential Customers of bKash Limited will have to fill out the complete standard KYC Form incorporating the guidelines of Bangladesh Bank. bKash Limited will use its best endeavor to verify the identity of any person seeking to open an Account to the extent reasonable and practicable. bKash Limited will also maintain records of the information used to verify a person’s identity, including name, address and other identifying information. bKash Limited shall provide the updated information/documents as requested by BRAC Bank Limited.

4. **Identity Verification**: bKash Limited will undertake reasonable steps to ensure that true and accurate information from the prospective Customer has been taken. bKash Limited will take reasonable steps to ensure that the person opening the bKash Account is the genuine owner of the SIM provided for Account opening as per the available verification system/process implemented by Bangladesh Bank. A Customer will be allowed to open Accounts as per regulatory guidelines of Bangladesh Bank.

5. **Agent Information/Selection of Agents**: The prospective Agents of bKash Limited shall provide required documents/information at the time of opening of Agent Account, as and/or where applicable, such as photo, proof of identity (copy of National ID/Passport/Driving License), Trade License / Bank Account details, properly filled out Agent KYC, etc.

The following issues should be taken into account for selection of Partners/Agents:
1. Competence to implement and support the proposed activity.
2. Financial soundness.
3. Ability to meet commitments under adverse conditions.
5. Security and internal control, compliance coverage, reporting and monitoring environment.

6. **COMPLIANCE PROGRAM**: bKash Limited will establish arrangement for internal compliance monitoring and control through formation of a Central Compliance Committee (CCC) under the leadership of a high official at the Head Office. This CCC will function independently as per the guidelines of Bangladesh Bank laid vide BFIU Master Circular 10. However, the CCC of bKash Limited will liaison with the Compliance Team of BRAC Bank Limited as and when required. bKash Limited will designate a CAMLCO at its Head Office who is to be sufficiently authorized to implement and
enforce corporate-wide AML & CFT policies, procedures, Compliance Field Assessments, dispute resolution and other associated measures. The CAMLCO will directly report to the Chief Executive Officer (CEO) of bKash Limited. The CAMLCO will also be responsible to coordinate and monitor day to day compliance with applicable AML & CFT related laws, rules and regulations as well as with its internal policies, practices, procedures, monitoring, controls and self-assessment.

7. TRANSACTION MONITORING:
bKash Limited will establish reasonable measures to monitor the Customer transactions as per the regulatory rules, guidelines and instructions of Bangladesh Bank. bKash Limited should have sufficient systematic tools in place to monitor the transactions. bKash Limited will generate a monthly report where the maximum allowable amount of a Account is fully used by the account holder.

8. SUSPICIOUS ACTIVITY REPORT (SAR)/SUSPICIOUS TRANSACTION REPORT (STR):
BRAC Bank Limited will monitor that bKash Limited generates SAR/STR in accordance with the guidelines of Bangladesh Bank. bKash Limited will implement a SAR/STR Process copy of which is to be forwarded to the Compliance Team of BARC Bank Limited. It would be prudent for CAMLCO of bKash Limited to record his/her determination in writing and where there is a doubt, it would also be prudent for the CAMLCO to make a report to the Bangladesh Bank. Therefore the CAMLCO of bKash Limited will keep a written record of every matter reported to him, of whether or not the suggestion was negated or reported, and of his reasons for his decision. SAR/STR will be submitted in the prescribed format directly to the General Manager, BFIU, Bangladesh Bank, Head Office, Dhaka under sealed cover note mentioned on the cover “Highly Confidential-SAR/STR”. bKash Limited will also provide a copy of SAR/STR to CAMLCO/DCAMLCO of BRAC Bank Limited.

9. REPORTS:
The CAMLCO of bKash Limited will submit AML & CFT Compliance reports to Bangladesh Bank as per BFIU guideline laid down in Master Circular 10. In case of future Guidelines of Bangladesh Bank, the up-to-date requirements of reporting to Bangladesh Bank are to be complied with bKash Limited. Copy of such reports is to be send to the Compliance Team of BRAC Bank Limited. BRAC Bank Limited may request for any other reports on requirement.

10. FIELD COMPLIANCE ASSESSMENT REPORT / INDEPENDENT AUDIT REPORTS:
bKash Limited will generate quarterly report on the Field Compliance Assessment Inspections conducted under the guidance by the CAMLCO and monitored through the CCC of bKash Limited. bKash Limited will share half yearly Field Compliance Assessment Inspection Report with BRAC Bank Limited. BRAC Bank Limited may also request compliance report as and when required. bKash Limited may also appoint external audit firms to carry out audit as per the requirement of bKash Limited. Besides, internal audit of bKash Limited will carry out audit as per the 'Annual Audit Plan'. Additionally, BRAC Bank Limited Audit Team will also conduct audit at bKash Limited.

11. SECURITY ISSUES:
bKash Limited shall address the following properties to offer a secure infrastructure for financial transactions using mobile technology:
   a. Confidentiality: Property that ensures transaction information cannot be viewed by unauthorized persons.
   b. Integrity: Property that the transaction information remains intact during transmission and cannot be altered.
c. Authorization: Property that the authentic user has proper permission to perform the particular transaction. It ensures how the system decides what the user can do.

d. Nonrepudiation: Property that the particular transaction initiated by a user cannot be denied by him/her later.

All the transactions must be authenticated by the Account holders using their respective Personal Identification Number (PIN) or similar other secured mechanism. To facilitate the MFS, the said PIN may be issued and authenticated by maintaining proper protection and security features.

12. RECORD KEEPING:
BRAC Bank Limited to monitor that the Compliance Organization of bKash Limited ensures that there is adequate system in place to preserve all necessary records on transactions as per Bangladesh Bank guidelines. BRAC Bank Limited will also monitor that bKash Limited Compliance Organization ensures preservation of records on customer identification (e.g. copies or records of official identification documents like National ID Cards, Passports, Driving Licenses, or any other ID Cards and documents acceptable by Bangladesh Bank), account files and business correspondence for minimum 6 (six) years even after the account is closed. These documents will be available to domestic competent authorities in the context of relevant criminal prosecutions and/or investigations.

13. CONCLUSION:
bKash Limited shall have to follow rules, regulations, guidelines and instructions issued by Bangladesh Bank from time to time and preserve records for BRAC Bank Limited oversight.
Fahad

From: Rais Uddin Ahmad
Sent: Wednesday, October 9, 2019 1:54 PM
To: All
Subject: Very important, must be read: AML/CFT Risk Management Guideline:

Dear Colleagues,

As you may know, Bangladesh Financial Intelligence Unit has issue Master Circular 19 and BBL has also updated its AML&CFT policy. The amended policy has been uploaded in the bank’s intranet at the link provided below. Summary of the changes is appended below.

<table>
<thead>
<tr>
<th>Money Laundering &amp; Terrorist Financing Risk Management Guidelines 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision incorporated more insights on CDD, EDD, KYC, reporting requirements and specific roles by stakeholders.</td>
</tr>
<tr>
<td>This policy has been incorporated with modified requirements stated through BFIU Circular No.1p dated September 17, 2017 which replaced Circular 10.</td>
</tr>
<tr>
<td>The more specific responsibilities of Central Compliance Committee (CCC) and its secretariat, Anti-Money Laundering Division in order to ensure proper implementation of strategic initiatives to combat ML, TF and PF.</td>
</tr>
<tr>
<td>Directives to perform appropriate diligence in wire transfer transactions as per BFIU Circular No. 21: Amendment of Section 9 of BFIU Circular- 19 and enhanced due diligence (EDD) in correspondent banking relationships have been emphasized as per the BFIU Circular No.19 dated September 17, 2017. Considerations pertaining to risk assessment for customers, transaction, delivery channels, and locations have been modified as per requirement.</td>
</tr>
<tr>
<td>A clause on verification of ultimate beneficial ownership (UBO) of the accounts has been incorporated in compliance to the international best practices focused by Fourth EU Money Laundering Directive, Section 325 and 326 of USA Patriot ACT, UK Money Laundering Regulations 2007 and FATF Recommendations 24 and 25.</td>
</tr>
</tbody>
</table>

Soft copy of this guideline is available in BBL TOUCH.
(BBL TOUCH>>Operations Manual>>Guideline>> BBL Guideline)


Amendment to the Bank’s HR Policy has been amended to include AML&CFT issues for proper implementation of AML & CFT measures:
In addition to the above, to accommodate the requirement of Money Laundering & Terrorist Financing Risk Management Guidelines by Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank; “Bank’s HR Policy has been amended to include the following issues for proper implementation of AML & CFT measures:

- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- Proper weight should be given in the annual performance evaluation of employees for extra ordinary preventive action vis a vis for non-compliance;
- Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;
- Other measures that shall be taken in case of non-compliance by the bank.”

In line with the above guideline, the Management proposed to insert the following measures or procedure for Compliance / noncompliance of AML & CFT measures in BRAC Bank’s Employees Terms of Service. This was subsequently approved by the Board of Directors.

1. Compliance / noncompliance of AML & CFT measures

- HRD, in coordination with the Anti-Money Laundering Division, will review the compliance / noncompliance of AML & CFT measures at branches & HO departments. AMLD will provide a rating for individual branches & departments as per pre-agreed criteria by January of the following calendar year for consolidation purposes at HR.

- In case of any non-compliance/failure identified, the liable employee’s shall be penalized as follows in the immediate Performance Assessment –
  - Performance Rating will be downgraded by 1 or 2 notch depending on the severity of the case
  - Values rating will also be rated as “C or D” depending on the severity of the case
  - HR will take Management approval separately, for each individual case
  - Performance Bonus amount will be reduced accordingly

- Performance Bonus amount will be increased by 20% for taking extra ordinary preventive action by the employees.

2. In case of Fine Imposed by BFIU

- If any fine imposed on Bank; it will be paid by the Bank immediately. Simultaneously,
  - A proper/formal investigation will be initiated jointly by AMLD & ICC Division
  - After the completion of the investigation, the final report will be submitted to the Board Audit Committee for review and onward submission to the Board of Directors. If any employee/s found liable, Board at its discretion fix the fined amount or ratio of the fined amount to be recovered from the employee/s concerned.
  - As per previously practice, 20% of the fined amount will be recovered from the liable employees proportionally based on seniority; for branches it will be 50% BM/BAMLCO and 50% from other liable employees.
  - For any exception, it will be placed before the Board for its review and final decision

- If any fine imposed on individual employee; it has to be paid by the employee concerned. Whereas, considering the scenario, Bank may provide personal loan/Staff loan to assist him/her to pay the fined amount subject to meeting all eligibility criteria to avail the loan.

If you need any clarification, please do not hesitate to talk to your line-manager, HR or AMLD.

Thanks & Regards
Rais

(Rais Uddin Ahmad)
Company Secretary
Head of Regulatory Affairs and CAMLCO
BRAC Bank Ltd
Anik Tower, 220/B Gulshan Tejgaon Link Road
Dhaka, Bangladesh
Tel # +88029884292(Ext-2028), +88028801266
Swift : BRAKBDDH
Web: www.bracbank.com
Time zone: UTC +6