RULES GOVERNING
ANTI-MONEY LAUNDERING &
COMBATING TERRORIST FINANCING

For all banks and money exchangers and foreign banks' branches operating in the Kingdom of Saudi Arabia

Third Update
February 2012
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Content Description</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>1.1</td>
<td>Saudi Arabia Initiatives</td>
<td>5</td>
</tr>
<tr>
<td>1.1.1</td>
<td>International Level</td>
<td>5</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Regional &amp; Group Level</td>
<td>5</td>
</tr>
<tr>
<td>1.1.3</td>
<td>National Level</td>
<td>6</td>
</tr>
<tr>
<td>1.2</td>
<td>SAMA Initiatives</td>
<td>6</td>
</tr>
<tr>
<td>1.2.1</td>
<td>AML / CTF Regulations</td>
<td>6</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Account Opening Regulations for Banks</td>
<td>7</td>
</tr>
<tr>
<td>1.2.3</td>
<td>Other Relevant Regulations</td>
<td>7</td>
</tr>
<tr>
<td>1.3</td>
<td>Objectives</td>
<td>8</td>
</tr>
<tr>
<td>1.4</td>
<td>General Developments &amp; Trends</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Legal Framework &amp; Regulatory Requirements</td>
<td>8</td>
</tr>
<tr>
<td>2.1</td>
<td>The Saudi AML Law &amp; Bylaws</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>SAMA - Regulatory &amp; Supervisory Body</td>
<td>9</td>
</tr>
<tr>
<td>2.3</td>
<td>Domestic Banks &amp; Money Exchangers &amp; Foreign Banks' Branches Operating in the Kingdom</td>
<td>10</td>
</tr>
<tr>
<td>2.4</td>
<td>Overseas Branches &amp; Subsidiaries of Saudi Bank &amp; MEs</td>
<td>10</td>
</tr>
<tr>
<td>2.5</td>
<td>Legal Responsibilities Of Banks/ MEs &amp; Employees</td>
<td>10</td>
</tr>
<tr>
<td>2.6</td>
<td>Financial Intelligence Unit (FIU)</td>
<td>10</td>
</tr>
<tr>
<td>2.7</td>
<td>Cooperation Among Authorities &amp; Banks/ MEs</td>
<td>11</td>
</tr>
<tr>
<td>2.7.1</td>
<td>Cooperation With Local Authorities</td>
<td>10</td>
</tr>
<tr>
<td>2.7.2</td>
<td>Cooperation Among Banks/ MEs Operating in the Kingdom</td>
<td>11</td>
</tr>
<tr>
<td>2.7.3</td>
<td>International Cooperation</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>Money Laundering &amp; Terrorist Financing</td>
<td>12</td>
</tr>
<tr>
<td>3.1</td>
<td>Money Laundering</td>
<td>12</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Definition of Money Laundering</td>
<td>12</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Processes of Money Laundering</td>
<td>13</td>
</tr>
<tr>
<td>3.2</td>
<td>Terrorist Financing</td>
<td>13</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Definition of Terrorist Financing</td>
<td>13</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Processes of Terrorist Financing</td>
<td>14</td>
</tr>
<tr>
<td>3.3</td>
<td>Typologies</td>
<td>14</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Definition of Money Laundering</td>
<td>12</td>
</tr>
<tr>
<td>3.3.2</td>
<td>Processes of Money Laundering</td>
<td>13</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Typologies</td>
<td>14</td>
</tr>
</tbody>
</table>

Page 2 of 70
<table>
<thead>
<tr>
<th>4</th>
<th>Policies &amp; Standards</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Risk-Based Approach</td>
<td>16</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Business Risk Assessment</td>
<td>17</td>
</tr>
<tr>
<td>4.2</td>
<td>AML/CTF Compliance Programs</td>
<td>18</td>
</tr>
<tr>
<td>4.3</td>
<td>Know Your Customer Standards</td>
<td>19</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Customer Identification Process</td>
<td>20</td>
</tr>
<tr>
<td>4.4</td>
<td>Customer Due Diligence (CDD)</td>
<td>21</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Beneficial Owners (Natural &amp; Legal)</td>
<td>22</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Customer &amp; Transaction Profiling</td>
<td>23</td>
</tr>
<tr>
<td>4.4.3</td>
<td>Name Checking of Designated Persons</td>
<td>24</td>
</tr>
<tr>
<td>4.5</td>
<td>Customer Risk Assessment</td>
<td>25</td>
</tr>
<tr>
<td>4.6</td>
<td>Customer Risks</td>
<td>25</td>
</tr>
<tr>
<td>4.6.1</td>
<td>Individual Personal Accounts</td>
<td>26</td>
</tr>
<tr>
<td>4.6.2</td>
<td>Private Banking Customers</td>
<td>27</td>
</tr>
<tr>
<td>4.6.3</td>
<td>Commercial Entities Accounts</td>
<td>28</td>
</tr>
<tr>
<td>4.6.4</td>
<td>Politically Exposed Persons</td>
<td>30</td>
</tr>
<tr>
<td>4.6.5</td>
<td>Walk-In Customers</td>
<td>30</td>
</tr>
<tr>
<td>4.6.6</td>
<td>Charity &amp; Non-Profit Organizations</td>
<td>31</td>
</tr>
<tr>
<td>4.6.7</td>
<td>Trustees, Nominees &amp; Intermediaries Accounts</td>
<td>32</td>
</tr>
<tr>
<td>4.6.8</td>
<td>Insurance Companies Accounts</td>
<td>33</td>
</tr>
<tr>
<td>4.6.9</td>
<td>Introduced &amp; Referred Businesses</td>
<td>34</td>
</tr>
<tr>
<td>4.6.10</td>
<td>Correspondent Banking Relationships</td>
<td>35</td>
</tr>
<tr>
<td>4.7</td>
<td>Operations Monitoring</td>
<td>36</td>
</tr>
<tr>
<td>4.7.1</td>
<td>Monitoring Process</td>
<td>36</td>
</tr>
<tr>
<td>4.7.2</td>
<td>Financial Investigation Process</td>
<td>38</td>
</tr>
<tr>
<td>4.7.3</td>
<td>Transaction Monitoring &amp; Reinforcement</td>
<td>39</td>
</tr>
<tr>
<td>4.8</td>
<td>Suspicious Transaction</td>
<td>39</td>
</tr>
<tr>
<td>4.8.1</td>
<td>Reporting Suspicious Transactions</td>
<td>39</td>
</tr>
<tr>
<td>4.8.2</td>
<td>Reporting Requirements</td>
<td>40</td>
</tr>
<tr>
<td>4.8.3</td>
<td>Tipping Off</td>
<td>40</td>
</tr>
<tr>
<td>4.8.4</td>
<td>Money Laundering Control Unit (MLCU)</td>
<td>41</td>
</tr>
<tr>
<td>4.9</td>
<td>Internal Controls</td>
<td>42</td>
</tr>
<tr>
<td>4.9.1</td>
<td>Internal Control Procedures</td>
<td>42</td>
</tr>
<tr>
<td>4.9.2</td>
<td>Assessment of Internal Controls</td>
<td>43</td>
</tr>
<tr>
<td>4.10</td>
<td>Staff Training &amp; Hiring</td>
<td>43</td>
</tr>
<tr>
<td>4.10.1</td>
<td>Staff Training &amp; Awareness</td>
<td>43</td>
</tr>
<tr>
<td>4.10.2</td>
<td>Staff Hiring &amp; Appointment of Senior Positions</td>
<td>44</td>
</tr>
<tr>
<td>4.11</td>
<td>Record Keeping &amp; Retention</td>
<td>44</td>
</tr>
<tr>
<td>5</td>
<td>AML/CTF Other Risks</td>
<td>46</td>
</tr>
<tr>
<td>5.1</td>
<td>Product/ Service Risks</td>
<td>46</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Cash</td>
<td>46</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Wire Transfers</td>
<td>47</td>
</tr>
<tr>
<td>5.1.3</td>
<td>Alternative Remittances</td>
<td>50</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Money Exchangers</td>
<td>51</td>
</tr>
<tr>
<td>5.1.5</td>
<td>Electronic Banking</td>
<td>51</td>
</tr>
</tbody>
</table>

**SAMA RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST FINANCING**
5.1.6 International Trade 52
5.2 Country Geographic Risks 52
5.3 Risk Variables 54
6 Glossary 55
7 Appendices 58
7- A Saudi AML Law & Bylaws 58
7- B FATF 40 Recommendations on Anti-Money Laundering 58
7- C FATF Member Countries 58
7- D Basel Committee Standards 58
7- E UN Security Council Resolutions 58
7- F Other Useful Resources & Links 58
8 Suspicious Transaction Report (STR) 59
9 Cash Declaration Form 61
10 Red Flag Indicators 63
1. Introduction

1.1 Saudi Arabia Initiatives

The past few years have seen rapid and far-reaching developments in the international financial sector involving a comprehensive and coordinated fight against money laundering and terrorist financing. Consequently, the Kingdom of Saudi Arabia has adopted a variety of initiatives involving legislative and other measures that are responsive to international developments. Some of these initiatives adopted by Saudi Arabia are listed below:

1.1.1 International Level

- The Kingdom of Saudi Arabia signed the UN Convention Against Corruption in January 2004.
- Saudi Arabia has implemented all relevant United Nations Security Council (UNSC) Resolutions, such as Resolutions # 1267 (1999), 1333 (2000), 1373 (2001).
- Saudi Arabia is a member country of the Gulf Cooperation Council (GCC), which is a full member of the Financial Action Task Force (FATF).
- In September 2003, Saudi Arabia completed the Mutual Evaluation by a team of FATF assessors, based on the 40+8 FATF Recommendations and was one of the first countries evaluated under this new methodology. The result of this evaluation was discussed in February 2004 Plenary Meeting in Paris and was highly positive.
- The Kingdom of Saudi Arabia underwent a joint Assessment conducted by the Middle East and North Africa Financial Action Task Force (MENAFATF) in participation with FATF, based on the 40+8 FATF Recommendations. The result of this assessment was discussed in May 2010 in the MENAFATF meeting in Tunisia and was also discussed in the plenary meeting of FATF held in June 2010 in Amsterdam where the Kingdom achieved a very positive result. The assessment report of the Kingdom can be found on the websites of (MENAFATF and FATF).

1.1.2 Regional & Group Level

- At a meeting held in April 1998, Saudi Arabia signed and ratified the Arab Anti-Terrorism Agreement under the auspices of the Arab League.
- In July 1999, Saudi Arabia signed and ratified the Organization of Islamic Conference (OIC) Agreement for the suppression of international terrorism.
- In May 2004, Saudi Arabia signed and ratified the GCC Anti-Terrorism Agreement.
- Saudi Arabia is a founding member of the Middle East-North Africa FATF (MENA-FATF), which was created in November 2004 with the purpose of promoting and implementing international AML/CTF standards in the region, and adopting the FATF 40+9 Recommendations on Anti-Money Laundering and Combating Terrorist Financing.

1.2 The Kingdom of Saudi Arabia

- The past few years have seen rapid and far-reaching developments in the international financial sector involving a comprehensive and coordinated fight against money laundering and terrorist financing. Consequently, the Kingdom of Saudi Arabia has adopted a variety of initiatives involving legislative and other measures that are responsive to international developments. Some of these initiatives adopted by Saudi Arabia are listed below:

1.2.1 International Level

- Saudi Arabia went under a joint assessment conducted by the Middle East and North Africa Financial Action Task Force (MENAFATF) in participation with FATF, based on the 40+8 FATF Recommendations. The result of this assessment was discussed in May 2010 in the MENAFATF meeting in Tunisia and was also discussed in the plenary meeting of FATF held in June 2010 in Amsterdam where the Kingdom achieved a very positive result. The assessment report of the Kingdom can be found on the websites of (MENAFATF and FATF).

1.2.2 Regional & Group Level

- At a meeting held in April 1998, Saudi Arabia signed and ratified the Arab Anti-Terrorism Agreement under the auspices of the Arab League.
- In July 1999, Saudi Arabia signed and ratified the Organization of Islamic Conference (OIC) Agreement for the suppression of international terrorism.
- In May 2004, Saudi Arabia signed and ratified the GCC Anti-Terrorism Agreement.
1.3 National Level

• Saudi Arabia passed the Anti-Money Laundering Law and Bylaws, under Royal Decree # M/39 dated 25/6/1424H, ratifying the Council of Ministers Decision # 167 dated 20/6/1424H, providing a statutory basis for criminalizing money laundering and terrorist financing activities.

• In accordance with the Saudi AML Law Article 11, the Saudi Financial Intelligence Unit (SAFIU) was established under the control of the Ministry of Interior, as the central authority for receiving and analyzing suspicious transaction reports relating to money laundering and terrorist financing activities.

• Saudi Arabia has set up two National Permanent Committees from different Ministries and Government Agencies, including SAMA, to respectively deal with money laundering and terrorist financing issues in the Kingdom.

1.2 SAMA Initiatives

Since its inception in 1952, the Saudi Arabian Monetary Agency (SAMA) has been issuing various directives to banks and money exchangers relating to establishing customers' identity and other information, observing necessary due diligence when dealing with customers, record keeping of relevant documents and files as well as reporting of suspicious transactions to the competent authorities. These directives have since been put together into a number of major regulatory manuals, including:

1.2.1 AML/CTF Regulations

In November 1995, SAMA issued its first set of guidelines relating to AML activities to all banks operating in Saudi Arabia. Consequently, in recognition of the international and legal supervisory efforts to combat the spread of money laundering, And terrorist financing SAMA further updated the initial 1995 AML Guidelines and in May 2003, issued a more extensive set of "Rules Governing Anti-Money Laundering & Combating Terrorist Financing".

The First Update issued in May 2003 provided a substantial improvement to the initial regulations and also included regulations relating to combating terrorist financing. It provided basic measures and actions to be taken to prevent, detect, control and report money laundering and terrorist financing activities. Since then, in SAMA's continued efforts to further improve and refine the regulations, the second Update was issued in December 2008. And to cope with the local, regional and global developments, SAMA has issued this Third Update.

Banks and money exchangers are required to make these regulations and provisions an integral part of their systems and procedures aimed at controlling, detecting, preventing,
and reporting suspicious activities. In this regard, SAMA intends to verify the implementation of these rules by banks and money exchangers operating in Saudi Arabia through SAMA's on-site inspections, receipt of regular compliance reports and certificates prepared by external auditors.

1.2.2 Account Opening Regulations for Banks

In May 2002, SAMA issued its first set of “Rules Governing Opening of Bank Accounts & General Operation Guidelines”. The new rules, in addition to consolidating all the previous SAMA circulars on the subject, were significantly improved with new requirements to facilitate implementation and conform to the best international banking practices in line with the Basel Committee principles. The rules outlined the standard requirements applicable to all banks to serve as a regulatory instrument to strengthen internal controls with a view of protecting the banking industry against illegal financial activities.

In order to cope with ongoing developments and to provide more explanation and clarification to the issues raised by local banks, the initial rules were further enhanced in the First Update released in April 2003. The Second Update of the rules was issued by SAMA in February 2007, the Third Update in December 2008, and the Fourth Update in February 2012 in keeping with the domestic, regional and international developments in this field. SAMA is continuously reviewing and updating the Account Opening regulations and will be issuing new updates to banks and money exchangers in future.

1.2.3 Other Relevant Regulations

SAMA has also issued a number of other regulations in support of its efforts to combat money laundering, terrorist financing and other financial crime activities. Therefore, these AML/CTF Rules should be read in conjunction with the following documents issued by SAMA, in addition to the AML Law and Bylaws issued by the Saudi Government:

- Designation Requirements for the Leading Professions in the Work in KSA, issued in April 2005
- Internal Control Manual for Banks Operating in the Kingdom, issued in December 1989
- Risk Based on- sit Inspection “Policy Framework & Procedures” issued by SAMA in April 2011.
- Risk Based Approach for AML/CFT Supervision issued by SAMA in February 2012.
- Other relevant SAMA Regulatory Circulars.

The new rules, in addition to consolidating all the previous SAMA circulars on the subject, were significantly improved with new requirements to facilitate implementation and conform to the best international banking practices in line with the Basel Committee principles. The rules outlined the standard requirements applicable to all banks to serve as a regulatory instrument to strengthen internal controls with a view of protecting the banking industry against illegal financial activities.
1.3 Objectives

The core objectives of SAMA in issuing these regulations are as follows:

1. To ensure compliance of banks and money exchangers in Saudi Arabia with regulations and instructions related to combating money laundering and terrorist financing in general and the Saudi AML Law & Bylaws in particular.

2. To help banks and money exchangers operating in Saudi Arabia to comply with the Banking Control Law, AML Law, SAMA Regulations, and all relevant United Nations Security Council Resolutions.

3. To implement policies, standards, procedures and systems for the prevention, detection, control and reporting of money laundering and terrorist financing activities in accordance with the Basel Committee Principles and the FATF Recommendations on AML/CTF.

4. To protect banks and money exchangers operating in Saudi Arabia from being exploited as channels for passing illegal transactions arising from money laundering, terrorist financing and any other criminal activities.

5. To maintain, enhance and protect the credibility, integrity and reputation of the Saudi Arabian banking and financial systems.

6. To provide the highest degree of protection for customers.

1.4 General Developments & Trends

At the global level, money laundering activities, particularly those related to drugs now constitute a multi-million dollar business annually. It is inconceivable and unlikely that such large amounts of money can be saved or moved without the cooperation or voluntary participation of many international financial institutions and banking systems. In many quarters, money laundering is considered a serious threat to the integrity of many international banks and even banking systems.

Money laundering has become a widespread phenomenon involving highly sophisticated techniques to penetrate different banking systems. This has led lawmakers, law enforcement agencies and supervisory authorities in many countries to cooperate, locally and internationally, to combat this phenomenon. In this respect, the FATF was created and it has carried out extensive work and issued Recommendations to counter the spread of money laundering and terrorist financing.

The techniques used by money launderers constantly evolve to match the sources and volume of funds to be laundered, and the legal, regulatory, law enforcement environment of the market place in which the money launderers operate.

2. Legal Framework & Regulatory Requirements

2.1 The Saudi AML Law & Bylaws

The Kingdom of Saudi Arabia, in its contributions towards the international initiatives to combat money laundering and terrorist financing crimes, has enacted the Anti-Money Laundering Law in August 2003. The Law criminalizes money laundering and terrorist financing acts and has created offenses, responsibilities and penalties for violation, aimed at preventing these crimes.


2.2 **SAMA – Regulatory & Supervisory Authority**

The Saudi Arabian Monetary Agency (SAMA), in accordance with the authority and powers vested on it under relevant Saudi laws, is the legislative body responsible for exercising regulatory and supervisory control over banks and money exchangers, issuing general rules and overseeing that all banks and money exchangers comply with and effectively implement the following relevant laws and regulations:

1. The Charter of Saudi Arabian Monetary Agency.
2. The Banking Control Law.

SAMA regards the adoption and implementation by all banks and money exchangers of effective policies, procedures and controls for the deterrence and prevention of money laundering, terrorist financing and other financial crimes as very vital. SAMA expects all banks and money exchangers and their employees to conduct business in accordance with these rules and all applicable laws by applying the highest ethical standards. SAMA will use these rules and other standards to measure the adequacy of each bank's or money exchanger's implementation strategies. SAMA will take appropriate disciplinary measures and actions against banks and money exchangers for any violations, in accordance with the Banking Control Law Article 25 (Rules for Enforcing Provision of the Banking Control Law).

As the regulatory and supervisory authority for banks and money exchangers, SAMA has a duty not only to ensure banks and money exchangers maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking sector. Therefore, SAMA will exercise the following responsibilities:

1. Monitoring that banks and money exchangers are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis.
2. Ensuring that appropriate internal controls are in place and banks and money exchangers are in compliance with supervisory and regulatory requirements.
3. SAMA examination will include review of bank’s and money exchanger’s policies and procedures, customer files including sampling of some accounts, documentation related to accounts maintained and the analysis made to detect unusual or suspicious transactions.
4. Taking appropriate action against banks or money exchangers and their officers and employees who demonstrably fail to follow the required procedures and regulatory requirements.

**2.3 Domestic Banks & Money Exchangers & Foreign**

The AML Law, through its Articles and the Bylaws, is applicable to all banks and money exchangers and requires all financial institutions to have in place adequate policies, systems, measures and controls in place, relating to customer identification, know your customer/ due diligence, risk assessment, monitoring and reporting suspicious, training and record keeping to deter and prevent money laundering and terrorist financing acts.
Banks’ Branches Operating in the Kingdom

The provisions of these rules shall apply to domestic banks, money exchangers, and foreign banks’ branches operating in the Kingdom. All banks and money exchangers and foreign banks’ branches shall have in place effective policies, procedures and controls to combat and prevent money laundering and terrorist financing and other financial crimes. Foreign banks’ branches operating in the Kingdom must apply the requirements compatible with regulations and rules applicable in the Kingdom as a minimum and the requirements of the country of origin if such requirements are stronger. They must also inform SAMA in case of being unable to comply with the requirements, or for reasons imposed by the laws of the country of origin.

2.4 Overseas Branches & Subsidiaries of Saudi Banks & Money Exchangers

As per the Saudi AML Law, these regulations are also applicable to overseas branches and subsidiaries of all Saudi banks and domestic money exchangers, banks and money exchangers should ensure all their foreign branches and subsidiaries apply the requirements of both the Saudi AML Law and these Rules. In addition, banks and money exchangers should ensure the following:

1. Paying particular attention to their foreign branches and subsidiaries located in countries that do not or insufficiently apply FATF Recommendations.
2. Ensuring their foreign branches and subsidiaries apply higher requirements of either the host country or the home country in case the requirements of the host and home countries differ.
3. Informing SAMA when a foreign branch or subsidiary is unable to observe appropriate AML/CTF requirements because it is prohibited by its local laws, regulations or other measures.

2.5 Legal Responsibilities of Banks/ Money Exchangers & Employees

The Saudi AML Law and Bylaws stipulate responsibilities, offenses, violations and penalties that have direct or indirect implications on financial institutions including banks and money exchangers- and on their staff personally. This is in addition to the responsibilities stipulated in the Banking Control Law and the Decision Regulating Money Changing Business applicable to practitioners of banking activities such as banks, money exchangers and their employees.

(For full details of the AML Law and Bylaws, refer to Appendix7- A):

2.6 Financial Intelligence Unit (FIU)

The FIU shall receive reports of suspected transactions related to money laundering and terrorist financing for their verification and analysis and direct them to authorities concerned to effectively carry out their role in combating and preventing money laundering, terrorist financing and other financial crimes. To this end, countries around the world have created specialized governmental agencies, known as Financial Intelligence Units, to be the central entities for receiving such suspicion reports.

Similarly, Saudi Arabia, According to the Saudi AML Law, has formed a Financial Intelligence Unit (SAFIU) to be responsible for receiving, analyzing and reporting to competent authorities on suspicious activities.

المملكة

تشريح أحكام هذه القواعد على البنوك المحلية ومحلات الصراfacraa وفروع البنك الأجنبي المئذنة، في المملكة وتطبيق أحكام هذه القواعد يجب أن تضم جميع البنوك ومحلات الصراfacraa وفروع البنك الأجنبي المئذنة وإجراءات وضوابط تطبيق الأحكام، ومع مثل هذه بعض الأحوال ومعالجة الإلغاء المالي الأخرى، كما يجب على فروع البنك الأجنبي المئذنة في المملكة تطبيق م책ات إذا وضعت الجمعية العامة، بالإضافة إلى ذلك يجب على البنك ومحلات الصراfacraa ما يلي:

1. وجود اهتمام خاص بفروعهم في الخارج وشركائهم التابعة الموجودة في الدول التي لا تتوفر أو لا تطبق بشكل كافي قواعد العمل المحلي ذات الأمر.
2. ضمان أن فروعهم في الخارج وشركائهم التابعة تطبق م책ات القصوى للبنك المضيف.
3. تفعيل مساعدة البنك السعودي عندما يكون على موجب أو شركة خاصة غير قادرة على التأكد من مغيّرات الصراfacea لفروعهم في الخارج أو شركاتهم التابعة.
4. نشر القواعد المحلية للكيانات المذكورة أعلاه، أو أنظمتها أو تدابير أخرى.

المسؤولية القانونية على البنوك ومحلات الصراfaceا معمول بها

حدد نظام مكافحة غسل الأموال وآلة التحريات في المملكة العربية السعودية المسؤوليات والإجراءات والعقوبات التي لها أثر مباشر أو غير مباشر على المؤسسات المالية بما فيها البنوك ومحلات الصراfaceا أو مؤسسة للبنك المضيف عن مغيّرات البنوك المضيفة. تضم منظمات البنوك وفروع البنك خارج المملكة لتمكينها من متابعة عمليات الصراfaceا من مستويات تبرد على مدار الأنشطة المصرفيّة من بنوك ومحلات الصراfaceا معمول بها.

(نظام مكافحة غسل الأموال ولائحته التنفيذية موجودة في الملحق 5).

وحدة الاتصال المالية

تقوم وحدة الاتصال المالية بمهمة تفعيل علاقات البنوك والمؤسسات المالية المتصلة بقضايا غسل الأموال وتمويل الإرهاب وتعطيل النشاطات المالية الأخرى، واستغلالها لذلك تختص الدول وكالات حكومية مختلفة تعرف ب지요ات وحدات الاتصال المالية. كنائب للهيئة المركزيّة، تتلقى المؤسسات المالية، بنوك وفروع البنوك الأخرى على الشريعة المذكورة أعلاه.

وعلية نحو الشروط أعلنت مهنة العلاقة المالية السعودية وفقًا نظام مكافحة غسل الأموال الإلكتروني. وحدة الاتصال المالية تؤدي مسؤولية على مقام الأطراف المعنية بها في الجهات المالية الأخرى، وغيرها المالية وتحليها وتحليها مستندات من المعنيّة.
### 2.7 Cooperation Among Authorities & Banks/ Money Exchangers

Cooperation among banks/ money exchangers and various competent authorities, in the exchange and sharing of relevant information, is very vital in the AML/CTF initiatives. However, such information exchange and sharing should be coordinated and achieved only through SAMA because of the importance and sensitivity of maintaining confidentiality of banking and financial operations and strengthening customer confidence in the Saudi banking system.

#### 2.7.1 Cooperation With Local Authorities

Under the Saudi AML Law, financial institutions are authorized and required to cooperate and share relevant information with local competent authorities, such as FIU and law enforcement authorities, for matters relating to money laundering, terrorist financing and other financial crimes. Banks and money exchangers should, therefore, have in place appropriate policies and procedures, as follows:

1. Establishment of a Money Laundering Control Unit (MLCU) or appointing a designated Compliance Officer within the bank or money exchanger, responsible - among other things - for receiving internal reports (from branches or other department within the bank or money exchanger) and informing FIU of suspected money laundering or terrorist financing activities. (Refer to Rule 4.8.4 of these Rules for details about the tasks and responsibilities of MLCU).

2. The manner and method in which the MLCU/ designated Compliance Officer should contact the authorities and pass relevant transactional information to them.

3. Where records are to be provided to the authorities, establishing the form of such records (original or copies) and the receipt and forms to be used for providing and receiving information by the MLCU/ designated Compliance Officer.

4. When information is to be provided verbally to authorities, the manner and form of such information shall be defined.

5. In some cases, depending upon the case, a new or a different procedure may need to be followed. For example, in the event of a large cash transfer, telephone notification may be quicker than filing a report especially if immediate decision to prevent the transfer is required.

### 2.7.2 Cooperation Among Banks & Money Exchangers Operating in the Kingdom

Banks and money exchangers should cooperate locally and abroad through their representatives in the Financial Crimes & Money Laundering Committee (FCML) for AML/CTF matters. This should be done through the exchange of information with banks' and money exchangers' supervisory bodies, and SAMA, about cases and transactions that they may discover, or suspect to be of money laundering or terrorist financing nature as required by the Saudi AML Law and Bylaws. However, at the same time they must strictly follow the legal and regulatory procedures that aim to protect customer confidentiality and banking secrecy. Banks and money exchangers must coordinate in advance with SAMA in case they agree to mutually assist or exchange information.
2.7.3 International Cooperation
In recognition for the need to cooperate with the international community in combating and preventing money laundering, terrorist financing and other financial crimes, Saudi Arabia has included provisions for this matter in its AML Law, taking into consideration the agreed conventions and reciprocity agreements. In accordance with the Saudi AML Law allowing, after prior coordination with SAMA, cooperation with international governmental authorities for cases involving money laundering and terrorist financing, any exchange of information with a foreign party whether another bank (affiliation, branch, correspondent) or a foreign governmental authority, for strictly follow the legal and regulatory procedures that aim to protect customer confidentiality and banking secrecy.

3. Money Laundering and Terrorist Financing

3.1 Money Laundering

3.1.1 Definition of Money Laundering
The Saudi AML Law defines money laundering as: any actual or attempted act aims at concealing or camouflaging the nature or illegally or illegitimately earned property to make it look as proceeds from legal sources. The AML Law’s Implementing Regulations states the underlying crimes relating to money laundering.

FATF defines money laundering as: the process by which proceeds from criminal activities are disguised to conceal their illicit origin, and exposing them to money laundering.

Criminal activities, such as drug trade, illegal arms sales, smuggling, human trafficking, prostitution, corruption, embezzlement, and other activities of organized crimes, tend to generate large profits for the individuals or groups carrying out such acts. By using funds from such illicit sources, criminals risk drawing the authorities’ attention to the underlying criminal activity and exposing themselves to criminal prosecution. In order to benefit freely from the proceeds of their crime, they must therefore conceal the illicit origin of these funds.

The United Nations Vienna Convention (1988) and the United Nations Palermo Convention (2000) provisions describe money laundering as the process by which proceeds from a criminal activity are disguised to conceal their illicit origin, and they encompass three distinct, alternative acts:

1. The exchange or transfer of proceeds, knowing that they are a result of a crime;
2. The concealment or disguise of the real nature, source, location, placement, movement or ownership of or rights with respect to proceeds, knowing that they are a result of a crime;
3. The acquisition, possession or use of proceeds, knowing, at the time of the receipt, that they are a result of a crime.

3.1.2 Processes of Money Laundering
There are three stages of money laundering, explained as

3.2.2 Utilisé pour l’élaboration des crimes

3.2.2 Utilisé pour l’élaboration des crimes
SAMA RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST FINANCING

1. Placement
Placement involves the introduction of illegally obtained funds into the financial system, usually through banks. This is achieved through cash deposits, purchase of financial instruments for cash, currency exchange, purchase of shares or insurance contracts, check cashing services, retail (through cash purchases), and smuggling of cash between countries.

2. Layering
The stage II of money laundering is the layering, which usually consists of a series of transactions, through transferring and movement of funds, designed to conceal their origin. This may involve sending wire transfers to other banks, purchase and sale of investments, financial instruments, and insurance contracts, fraudulent investments or trade schemes, and the like.

3. Integration
The last stage is integration, which involves the re-entering of the funds into the legitimate economy. This is accomplished through the purchase of assets, shares/financial assets, or luxury goods, and investment in real estate or projects.

3.2 Terrorist Financing
3.2.1 Definition of Terrorist Financing
The Article 1 of the Saudi AML Law defines criminal activity as: any activity sanctioned by Shariah or law including the financing of terrorism, terrorist acts and terrorist organizations. The Article 2 of the AML Law's Implementing Regulations 2.1 describes "financing terrorism, terrorist acts and terrorist organizations includes even funds obtained from legitimate sources".

The International Convention for the Suppression of the Financing of Terrorism adopted by the UN in 1999 describes terrorist financing as follows:

"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully or willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex.

b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by nature or context, is to intimidate a population, or compel a government or an international organization to do or to abstain from doing any act."

Saud Arabia is committed to all relevant UN Security Council's resolutions directed towards combating terrorist financing and criminalizes financing of terrorism, terrorist acts and terrorist organizations.

SAMA requires to all banks, money exchangers, and foreign banks' branches operating in the Kingdom strict compliance with the recommendations of the UN and recommendations of the FATF. If a bank or money exchanger has any reason to believe that an individual, commercial institution or organization is, by any means, directly or indirectly, providing or collecting funds in the knowledge that such funds will be used for illegal purposes, it must refrain from entering into


2. The evasion of the provisions of the United Nations resolution on the consolidated list of terrorist funds and property (1267) of 1999, and the resolutions of the FATF and the UN Security Council regarding the freezing of the assets and funds of terrorist organizations and the freezing of the personal assets of persons designated as terrorists by the UN Security Council.

3. The evasion of the provisions of the United Nations resolution on the establishment of a list of persons and entities associated with terrorist organizations and the freezing of their assets and funds, or the freezing of the personal assets of persons designated as associates of terrorist organizations by the UN Security Council.

4. The evasion of the provisions of the United Nations resolution on the establishment of a list of persons and entities associated with terrorist organizations and the freezing of their assets and funds, or the freezing of the personal assets of persons designated as associates of terrorist organizations by the UN Security Council.

5. The evasion of the provisions of the United Nations resolution on the establishment of a list of persons and entities associated with terrorist organizations and the freezing of their assets and funds, or the freezing of the personal assets of persons designated as associates of terrorist organizations by the UN Security Council.
3.2.2 Processes of Terrorist Financing
The techniques and methods used to finance terrorism are essentially similar to those used to conceal the sources of money laundering and its uses; however, the main differences between the two are that (a) small amounts are often required to commit individual terrorist acts, making it difficult to track terrorist funds; and (b) terrorists can be financed by legitimately obtained funds, making it difficult to identify the stage at which legitimate funds become terrorist funds. Terrorists may derive their finance from a variety of sources, often combining both lawful and unlawful funding. The forms of financing can be categorized into the following types:

1. **Financial Support**
This finance could be in the form of charitable donations, community solicitation and other fund raising initiatives, which may come from entities or individuals.

2. **Illegitimate Sources**
This finance is often derived from criminal activities such as money laundering, fraud and other financial crimes.

3. **Legitimate Source**
This form of finance may fully or partially originate from legitimate business activity.

3.3 Typologies
The various techniques or methods used to launder money or finance terrorism are generally referred to as *typologies*. A typological study is a useful tool to examine in depth a particular issue of concern to provide a view and knowledge on emerging interconnected risks and how they should be addressed.

FATF and MENA-FATF regularly issue studies relating to typologies of money laundering and terrorist financing. They can be found on [www.fatf.org/pages](http://www.fatf.org/pages) and [http://www.menafatf.org/images/UploadFiles/ML_TF_Trends_and_Indicators_in_the_MENA_Region_Arabic.pdf](http://www.menafatf.org/images/UploadFiles/ML_TF_Trends_and_Indicators_in_the_MENA_Region_Arabic.pdf)

SAMA also issued circulation No. 5403/MAT/12263 dated 6/3/1432H. to all financial institutions, regarding typologies of money laundering and terrorist financing. Banks and money exchangers should update their systems with the new typologies applicable to their businesses. The following are examples of the typologies relating to money laundering and terrorist financing:
Alternative remittance services (hawala, hundi, etc.): Informal mechanisms rely on trust-based networks for remitting funds. They often work in parallel with the traditional banking sector but they are illegal. They are exploited by money launderers and terrorist financiers to move funds without detection and to obscure the identity of those controlling them.

Structuring (smurfing): A method involving multiple transactions (deposits, withdrawals, transfers), executed often by various people and high volumes of small transactions and sometimes various accounts to avoid financial institutions’ obligations of threshold reporting.

Currency exchanges: Used to assist with smuggling funds to another jurisdiction, exploit low reporting obligations on currency exchange houses, and minimize risk of detection, e.g., purchasing of travelers checks to transport funds to another country.

Cash couriers/ currency smuggling: Concealed movement of currency across borders to avoid transaction/ cash reporting measures.

Use of credit cards, checks, etc.: Used as instruments to access funds held in bank accounts, often in another jurisdiction.

Purchase of valuable assets (e.g., real estate, vehicles, shares, etc.): Criminal proceeds are invested in high-value negotiable goods, taking advantage of reduced reporting requirements to obscure the source of such proceeds.

Use of wire transfers: To electronically transfer funds between banks and often to another jurisdiction to avoid detection and confiscation.

Trade-based money laundering: Usually involves invoice manipulation and uses trade finance methods and commodities to avoid financial transparency laws and regulations.

Abuse of non-profitorganizations: Non-profit organizations may be misused to raise funds for terrorist purposes, obscure the source and nature of funds and to distribute funds to finance terrorism.

Investment in capital markets: Obscuring the source of criminal activities proceeds by purchasing negotiable instruments, often exploiting relatively low reporting requirements.

Mingling (business investment): A key step in money laundering involves combining proceeds of crime with legitimate business funds to obscure their source.

Use of shell companies/ corporations: A technique used to obscure the identity of persons controlling funds and to exploit relatively low reporting requirements.

Use of offshore businesses, including trust company service providers: To obscure the identity of people controlling funds and to move monies away from monitoring measures of domestic authorities.

Use of legal arrangements, brokers, trustees, or third parties, etc.: To obscure the identity of persons controlling illicit funds.

Use of foreign bank accounts: To move funds away from measures of domestic authorities and obscure the identity of persons controlling illicit funds.

Identity fraud/ false identity: Used to obscure identity of those involved in money laundering and terrorist financing.

Use professional services (lawyers, accountants, brokers, etc.): To obscure identity of beneficiaries and the source of illicit funds. This may also include corrupt professionals who offer ‘specialist’ money laundering services to criminals.

Khums observing the money laundering (الحالة، المصرف الإسلامي، إلخ)؛ وسائل تحويل غير رسمية تركز على شبكات عميقة تستخدم على الأفكار لتحويل الأموال، عادة ما تعمل بشكل متوازٍ مع التنافس بحيث تكون بشكل ثابت بين النسب المكثفة وتقدير عدد الأموال والمتوسط الإحذاء لقليل الأموال دون أن يتم تبليغها لإخفاء هوية المستثمرين على ذلك الأموال.

النظام (الإيرادات المحتملة)؛ تطبيق رسوم عديدة (الladığı، التمويل،...) وغالباً ما تضم مجموعة من الأشخاص، وأعداد هائلة من العمليات الصغيرة الموثقة وأحيانًا حسابات تم تجميلها تم تعديل الزامات المؤسسات المالية بالتمويه عن العمليات المالية التي تتجاوز حدود معينة. تبديل النطاق: تستخدم هذه الطريقة للمساسة في عمليات هيبير بين دول أو لاستغلال ضعف النطاق لمتى قرينة المدفوعات والتدقيق من مخاطر التنظيم (الإيرادات المحتملة): تحوّل الأموال إلكترونية بين البلدان وغالباً ما يكون ذلك دون تبليغ أو تدقيق أو تحمل:

ضاحي القلق / تهريب المبلغ: قلق المال بالطرق الخفية غير الحدود تقدّم إجرادات

الأعمال التجارية من العملاء الماليين.

استخدام مراكز التنسيق والمنظمة، إلخ: تستخدم كأدوات للوصول إلى الأموال المدوّنة في حسابات البنوك التي تكون غالباً في دولة أخرى. شراء أصول قيمة (مثل العقارات، والسياحات، وأعمال، إلخ): تستعرض عادات شخصية في الشكل المالي للأنشطة الإجرامية في شراء السلع المالية التي يمكن تداولها باستفادة من فرقة تجارة الشائعات المتفاصلة. استخدام الأوامر الرقمية (القانون): تحويل الأموال الإلكترونية بين البنك وغالباً ما يكون ذلك دون تبليغ أو تدقيق أو تحمل:

نظام المثليات في عهد القلق/ تهريب المبلغ: يمثل نظام خدمة العملاء لتجنب تبليغ عمليات تمويل بالتجارة:

استخدام المؤسسات والوسيطاء أو الأشخاص الفعليين، إلخ: استخدام الترتيبات القانونية والأعمال التجارية方も استغلال متطلبات التبليغ الأقل نسبياً.

الخلاصة (الاستفادة): عملة رئيسية في عملية غسل الأموال تشمل الجمع بين عادات الأنشطة الإجرامية في فصل الأموال وكشف الأموال غير المشروعة من خلال شراء بعض الأشخاص الذين يتحكمون بالأموال، ولاستغلال متطلبات التبليغ الأقل نسبياً.

استخدام المؤسسات والوسيطاء أو الأشخاص الفعليين، إلخ: استخدام الترتيبات القانونية والأعمال التجارية非凡ية: إخفاء هوية الأشخاص الذين يتحكمون بالأموال وغالباً ما يكون ذلك دون تبليغ أو تدقيق أو تحمل:

العمولات المحتملة أو الأشخاص الذين يتحكمون بالأموال من المؤسسات المالية.

استخدام مراكز التنسيق وال Mansion، إلخ: للاستفادة من الأشخاص الذين يتحكمون بالأموال من المؤسسات المالية. الكشف عن الفحوصات/ المال النقدي.

تهريب الأموال والتحويلات، وغالباً ما تضم مجموعة من الأشخاص، وأعداد هائلة من العمليات الصغيرة الموثقة وأحيانًا حسابات تم تجميلها تم تعديل الزامات المؤسسات المالية بالتمويه عن العمليات المالية التي تتجاوز حدود معينة. تبديل النطاق: تستخدم هذه الطريقة للمساسة في عمليات هيبير بين دول أو لاستغلال ضعف النطاق لمتى قرينة المدفوعات والتدقيق من مخاطر التنظيم (الإيرادات المحتملة): تحوّل الأموال إلكترونية بين البلدان وغالباً ما يكون ذلك دون تبليغ أو تدقيق أو تحمل:

ضاحي القلق / تهريب المبلغ: قلق المال بالطرق الخفية غير الحدود تقدّم إجرادات

الأعمال التجارية من العملاء الماليين.

استخدام مراكز التنسيق والمنظمة، إلخ: تستخدم كأدوات للوصول إلى الأموال المدوّنة في حسابات البنوك التي تكون غالباً في دولة أخرى. شراء أصول قيمة (مثل العقارات، والسياحات، وأعمال، إلخ): تستعرض عادات شخصية في الشكل المالي للأنشطة الإجرامية في شراء السلع المالية التي يمكن تداولها باستفادة من فرقة تجارة الشائعات المتفاصلة. استخدام الأوامر الرقمية (القانون): تحويل الأموال الإلكترونية بين البنك وغالباً ما يكون ذلك دون تبليغ أو تدقيق أو تحمل:

نظام المثليات في عهد القلق/ تهريب المبلغ: يمثل نظام خدمة العملاء لتجنب تبليغ عمليات تمويل بالتجارة:

استخدام المؤسسات والوسيطاء أو الأشخاص الفعليين، إلخ: استخدام الترتيبات القانونية والأعمال التجارية非凡ية: إخفاء هوية الأشخاص الذين يتحكمون بالأموال، ولاستغلال متطلبات التبليغ الأقل نسبياً.

الخلاصة (الاستفادة): عملة رئيسية في عملية غسل الأموال تشمل الجمع بين عادات الأنشطة الإجرامية في فصل الأموال وكشف الأموال غير المشروعة من خلال شراء بعض الأشخاص الذين يتحكمون بالأموال، ولاستغلال متطلبات التبليغ الأقل نسبياً.

استخدام المؤسسات والوسيطاء أو الأشخاص الفعليين، إلخ: استخدام الترتيبات القانونية والأعمال التجارية非凡ية: إخفاء هوية الأشخاص الذين يتحكمون بالأموال، ولاستغلال متطلبات التبليغ الأقل نسبياً.

الخلاصة (الاستفادة): عملة رئيسية في عملية غسل الأموال تشمل الجمع بين عادات الأنشطة الإجرامية في فصل الأموال وكشف الأموال غير المشروعة من خلال شراء بعض الأشخاص الذين يتحكمون بالأموال، ولاستغلال متطلبات التبليغ الأقل نسبياً.

استخدام المؤسسات والوسيطاء أو الأشخاص الفعليين، إلخ: استخدام الترتيبات القانونية والأعمال التجارية非凡ية: إخفاء هوية الأشخاص الذين يتحكمون بالأموال، ولاستغلال متطلبات التبليغ الأقل نسبياً.
4. Policies and Standards

4.1 Risk-Based Approach

Banks and money exchangers shall adopt a risk-based approach in designing their Anti-Money Laundering (AML) and Combating Terrorist Financing (CTF) programs to ensure that measures used to mitigate money laundering and terrorist financing are commensurate to the risks identified in their organizations. This will also allow resources to be allocated in the most efficient ways. Some of the benefits of utilizing the risk-based approach is verification of levels of due diligence measures by banks or money exchangers as follows:

1. Allowing banks and money exchangers to differentiate between risks of customers in a particular business by focusing on the highest risks of them, thus improving the overall outcome of the process;
2. While establishing minimum standards, allowing a bank or money exchanger to apply its own approach to systems, controls and arrangements in particular circumstances, thus allowing more flexibility as risks evolve; and
3. Helping to create the best management of risks and cost effective system.

It should be born in mind that application of a risk-based approach does not mean to any type of business or customers from verification of (KYC) basic requirements or from meeting customers due diligence (CDD) requirements used to restrain transactions of money laundering and terrorist financing.

A risk-based approach will serve to balance the burden placed on banks and money exchangers and on their customers, along with a realistic assessment of risks of business being used in money laundering or terrorist financing by focusing efforts on areas where they are needed and have the most impact.

Banks and money exchangers may face some challenges that must be considered while implementing the risk-based approach. These challenges should be regarded as offering opportunities to implement a more effective system in combating activities of money laundering and terrorist financing. Some of these challenges can be summarized as follows:

1. Risk Assessment Methodology: Identifying appropriate information to conduct a precise risk analysis and overall assessment.
2. Judgmental Decisions: Greater needs for more specialist staff capable of making sound decisions regarding identification and evaluation of risks.
3. Transitional Costs: Costs relating to transition from prescription method to risk based method.

The risk-based approach requires certain actions to be taken in assessing the best cost effective methods and their appropriateness to the management and in mitigation the risks of money laundering and terrorist financing faced by a bank. These actions are:

1. Identifying risks of money laundering and terrorist financing that are relevant to the bank or money exchanger to ensure a well-built foundation for the approach used and well-understood risks.
2. Assessing the risks identified by bank’s or money exchanger from all the following aspects:
   a. Customers;
   b. Products and services;
   c. Service delivery channels;
   d. Geographical area of operation.

   The weight given to the above risk aspects in assessing the overall risk of money laundering and terrorist financing may vary from one bank or money exchanger to another, depending on their respective circumstances. Consequently, each bank or money exchanger will have to make its own standard of assessing the varying risks.

3. Establishing and implementing monitoring controls to mitigate these assessed risks.

4. Monitoring and improving the effective operation of such controls.

5. Recording appropriately what has been done and explaining the reasons and rationale.

The Risk-based approach may contribute to identifying suspicious activities as follows:

1. Directing additional resources towards areas identified by a bank or money exchanger as high-risk areas.

2. Expansion in investigation process is dependent on the risks identified.

3. A bank or money exchanger shall use information provided by authorities to identify and report suspicious activities.

4. A bank or money exchanger must periodically assess the adequacy of its identification system of suspicious transactions and reporting thereof.

FATF regularly issues studies on risk-based approach. Such studies can be viewed at:

4.1.1 Business Risk Assessment

Banks and money exchangers shall conduct and document the above business risk assessment and update this assessment on an annual basis to identify changes in their business areas (e.g., organizational structure), their customers and the jurisdictions with which customers are connected, and their products and services and how they should be delivered. Banks and money exchangers shall build their AML/CTF compliance programs based on the conclusions of the business risk assessment. To achieve an adequate assessment, banks or money exchangers shall consider the possibility of exposure to money laundering and terrorist financing risks by:

1. Covering all risks posed by money laundering and terrorist financing relating to different businesses within the bank or money exchanger.

2. Considering organizational factors that may increase the level of exposure to the risk of money laundering and terrorist financing, e.g., business volumes, capacity issues, and authorization of others for account management.

3. Considering the nature, scale and complexity of business, the diversity of their operations (including geographical diversity), the volume and size of their transactions, and the level of risk associated with all areas of their business.

4. Considering the type and nature of customers and their businesses, focusing on the ones defined as high risk (political persons, charity associations, jewelry shops, etc.).

5. Considering any additional risks posed by the jurisdictions with which customers (including brokers and financial institutions)

---

4.1.2 Tackling Money Laundering

Money laundering is a criminal activity that involves the use of a bank or money exchanger to conceal the origin and ownership of illegal funds or profits that result from criminal activity. Money laundering is a serious crime that can undermine the integrity of the financial system and lead to the diversion of wealth from legitimate economic activities.

The Financial Action Task Force (FATF) is an intergovernmental organization that promotes international cooperation in the field of combating money laundering and terrorist financing. The FATF has developed a set of recommendations that countries must implement to prevent and disrupt money laundering and terrorist financing.

The FATF recommendations are based on the principle that all countries should have in place measures to prevent and detect money laundering, terrorist financing, and other related offenses, and to ensure that criminal proceeds are not used to pay for the financing of terrorist activities.

The FATF recommendations cover a wide range of topics, including the establishment of a national strategy for preventing money laundering and terrorist financing, the development of effective legal and regulatory frameworks, the implementation of effective risk-based due diligence measures, and the establishment of effective cooperation and information exchange mechanisms.

The FATF recommendations are regularly reviewed and updated to reflect new challenges and emerging threats.

---

SAMA RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST Financing
service providers) are connected. Risks exposed to by banks in their relationships with other jurisdictions are sensitive to a number of factors such as high levels of organized crime, increased vulnerabilities to bribery and corruption, and inadequate scopes of work for preventing and detecting money laundering and financing of terrorism.

6. Considering the characteristics of the products and services provided by banks or money exchangers and assessing the associated vulnerabilities posed by each product and service, including service delivery methods. For example:

a. Current accounts and money transfers, which are more vulnerable because they allow funds to be transferred to and from third parties, including cash transactions.

b. The use of third parties such as a group entities, service providers and brokers to obtain information about the customer.

c. Brokers’ combined accounts are more vulnerable because of the anonymity of the source of funds due to the mingling of assets or funds belonging to several customers by the broker.

d. Conversely, products that do not permit third party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable.

7. Considering how they establish and deliver products and services to their customers as risks are likely to be greater when relationships are established remotely (non-face-to-face), or when transactions are controlled remotely by the customer (straight-through processing of transactions).

8. Recording, updating and retaining their business risk assessment.

4.2 AML / CTF Compliance Programs

The Saudi AML Law requires financial institutions to develop appropriate AML/CTF programs which should include, as a minimum, the following:

1. Internal AML/CTF policies, measures and controls and informing the staff thereof including ID verification and due diligence measures, maintaining records, monitoring of transaction and compliance with the requirement of reporting suspicious transactions.

2. Appropriate programs for compliance management and appointing a compliance officer to ensure compliance with AML/CTF requirements. He should work independently, have the power to communicate with a superior management level, and have the right to view customers’ identity data, due diligence information and other related transaction records.

3. Establishing an independent accounting and auditing unit provided with adequate resources for testing compliance with such measures; policies and controls in accordance with the risk-based approach.

4. Developing ongoing training programs for all employees and the specialized to keep them informed of new laws, instructions and any updates in the area of combating money laundering to upgrade their skills in identifying such operations, their patterns and the method of combating them.

5. Application of test measures to ensure availability of highly efficient standards for appointment of employees.

Therefore, banks and money exchangers should prepare adequate AML/CTF compliance programs, basically covering the following elements:

---

6. 6. 6. 6. 6.

---
1. Setting out, as mentioned above, detailed elements for the compliance program and plans and strategies by banks or money exchangers for ensuring compliance with their written policies and measures to effectively cover AML and CTF requirements.

2. Including review plan and self-assessment to monitor effectiveness of AML and CTF controls.

3. Detailing assigned responsibilities and identifying actions to be taken during the year in addition to any pending correction actions stemming from accounting and auditing operations.

4. Including appropriate staff awareness programs and training plans over the year.

5. Preparing and revising the compliance program on an annual basis to ensure its effectiveness and inclusion of the changing typologies of money laundering and terrorist financing risks.

The program should also include what has been achieved in the risk-based approach and the rationale of such achievement. Therefore, each bank or money exchanger should appropriately tailor policies and measures of AML/CTF program to identify:

1. How a bank or money exchanger assesses threats and risks it exposed to in money laundering or terrorist financing.

2. How a bank or money exchanger applies appropriate law or takes appropriate actions based on risk assessment, including due diligence requirements.

3. How a bank or money exchanger monitors enhancement of the effectiveness of its system and procedures.

4. Reporting process to senior management on performance of control measures.

4.3 Know Your Customer Principle (KYC)

The KYC principle is intended to enable a bank or money exchanger to have an appropriate perspective that it knows the true identity of each customer with an appropriate degree of confidence and knows the types of business and the true identity of each customer with an appropriate degree.

The program should include what has been achieved in the risk-based approach and the rationale of such achievement. Therefore, each bank or money exchanger should appropriately tailor policies and measures of AML/CTF program to identify:

1. Identification and verification of all permanent and casual customers and beneficiaries owner on a continuous basis and in accordance with the Rules Governing the Opening of Bank Accounts and the General Operational Guidelines.

2. Identification and verification of beneficiaries owner of all transactions executed by customers to an extent to which ensures their perfect understanding.

3. Assessing risks connected with different types of customers and taking proper measures for enhancing requirements of identification and verification of customers or beneficiaries owner.

4. Adopting proper measures that ensure updating requirements of identification and verification of customers and beneficiaries owner on a continuous basis.

5. Following up changes in the identity of customers and beneficiaries owner and taking the necessary decision on their impact on control and supervision requirements.

6. Making records of identification of customers and beneficiaries owner available to the compliance officer.

2. An تشتمل على خطة مراجعة وتنفيذ منهجي للرقابة المصرفية في ضوابط مكافحة غسل الأموال وتمويل الإرهاب.

3. تقييم المسؤوليات وتحديد الإجراءات التي يجب اتخاذها خلال السنة بالإضافة إلى أية إجراءات تعديلية متعلقة بتعزيزها المصرفية والرقابة.

4. يشمل الإجراءات التنفيذية طويلة الأمد خلال السنة.

5. يجب إعداد وتحديث برنامج الالتزام على أساس سنوي، وذلك لضمان فعاليته وeliness.

6. من ضمنه للأعمال المتغيرة مكافحة غسل الأموال وتمويل الإرهاب.

كما يجب أن يتضمن البرنامج ما يتم إنجازه مع المرتبط ويفضل يبقى بالأسلوب المركزي على المدى الطويل. وبالتالي يجب أن يكون كل بنك أو محل صراف بإمكانه أن يمارس ما هو مناسب من سياسات إجراءات برنامج مكافحة غسل الأموال وتمويل الإرهاب لتحقيق ما يلي:

1. كيفية تقييم المخاطر والمخاطر التي يتعرض لها البنك أو محل الصراف فيما يتعلق بعملات الأموال أو مكافحة الإرهاب.

2. كيفية قيام البنك أو محل الصراف بتطبيق أو تنفيذ النظام والإجراءات المناسبة بما في ذلك تطبيقات المراجعة الواجبة بناء على تقييم المخاطر.

3. كيفية قيام البنك أو محل الصراف بالعملية الرسمية لتحسين نظام وإجراءاته.

4. عملية قيام التقارير للإدارة العليا فيما يتعلق بعمل إجراءات المراجعة الخاصة به.

3.4 مبدأ إذاع عملك

إن الغرض من تطبيق هذا المبدأ هو تحديد البنك أو محل الصراف من تكوين صورة مناسبة بأنه يوفر الهيئة الحقيقية لكل عمل به من العملاء، وأنه يعرف أنواع الأعمال والأعمال والعمليات التي يتمثل أن يقوم بها العمل مع البنك أو محل الصراف، ويجب أن تشمل إجراءات البنك وسجل الصرافات من خلال تحديد النشاطات المتعلقة.

1. التعرف وتعقب المنتجات من معاملات العملاء الذين يتعرضون للأنشطة المصرفية وشروط تأنيث.

2. التعرف وتعقب من هوية المستفيدين الحقيقيين للكافة الاتصالات التي بحوزتها العملاء والمستفيدين الحقيقيين من تنظيمات.

3. تقييم المخاطر المتعلقة بسجلات المعاملات واتخاذ الإجراءات المناسبة بشأن تطهير.

4. تقييم التعرف والتعقب من هوية عملاء والمستفيدين الحقيقيين من تنظيمات حسب ما يتم من منظمات.

5. متابعة الفواتير في إجراءات العملاء والمستفيدين الحقيقيين واتخاذ اللازم بشأن تأنيثه على منظمات البارك واتخاذ.

6. ينبغي أن تكون سجلات تحديد هوية العملاء والمستفيدين الحقيقيين متصلة للمسؤول عن الإجراءات بائه مكافحة غسل الأموال وتمويل الإرهاب والمسؤولين المعنيين ذوي الصلاة.

7. أن يتم التحقق من هوية العملاء والمستفيدين الحقيقيين من مصادرة موثوقة ومسلطة.
4.3.1 Customer Identification Process

The Saudi AML Law and its Implementing Regulations require financial institutions not to carry out any financial, commercial or similar operations under anonymous or fictitious names. Banks are also prohibited from opening or dealing with numbered accounts. Banks and money exchangers must verify the identity of the customer and beneficiaries owner depending on official documents provided at the start of dealing with such customer or upon concluding commercial transactions therewith in person or in proxy. Banks and money exchangers must further verify legal person’s official documents that indicate the name of the entity, its address, names and addresses of its owners, managing directors, and any other relevant data.

Banks and money exchangers should, as a minimum, apply the following rules for appropriate identification of customers and beneficiaries owner:


2. At the outset of the relationship or account, obtaining a copy of the customer identification documents and verifying them against their original.

3. Obtaining SAMA approval for opening accounts or establishing relationships with non-residents, except with GCC citizens.

4. Not to open accounts for or establish relationships with any non-face-to-face customers (refer to SAMA’s Rules Governing the Opening of Bank Accounts), and subject all accounts to interview and identity verification.

5. Identification is limited to customers having accounts at the bank; it should also include those who benefit from other banking or financial services, such as credit cards, express remittances, large transfers/transactions, foreign exchange transactions and safe deposit boxes. It should also cover owners, authorized signers, holders of powers of attorney, directors, trustees and partners.

6. Setting a systematic measure for identifying customers and not to establish any relationship or process any transaction until the personal or commercial valid identity of the individual or legal entity has been verified satisfactorily.

7. Obtaining customer personal information, such as name, address, signature, contact telephone numbers, occupation, source of funds/ income or wealth, and other information depending on the type of customer, as stated in the SAMA’s Rules Governing the Opening of Bank Accounts.

8. Requesting from the customer to provide information about any existing bank accounts or relationships with other local banks, which should be followed up if suspicions arise.

9. Conducting further due diligence and efforts if there are doubts about the integrity or accuracy of previously obtained customer identification data and, in such case, re-verifying the identity of the customer and re-assessing the relationship.

10. Not to accept any transactions from walk-in customers, with the exception of transactions stated in the SAMA’s Rules Governing the Opening of Bank Accounts.

11. No new accounts, business relationships or transactions are opened unless there is a written request from the customer and the identification process is completed.

Rules Governing the Opening of Bank Accounts in the SAMA

1. Rules Governing the Opening of Bank Accounts in the SAMA

2. Setting a systematic measure for identifying customers and not to establish any relationship or process any transaction until the personal or commercial valid identity of the individual or legal entity has been verified satisfactorily.

3. Obtaining customer personal information, such as name, address, signature, contact telephone numbers, occupation, source of funds/ income or wealth, and other information depending on the type of customer, as stated in the SAMA’s Rules Governing the Opening of Bank Accounts.

4. Requesting from the customer to provide information about any existing bank accounts or relationships with other local banks, which should be followed up if suspicions arise.

5. Conducting further due diligence and efforts if there are doubts about the integrity or accuracy of previously obtained customer identification data and, in such case, re-verifying the identity of the customer and re-assessing the relationship.

6. Not to accept any transactions from walk-in customers, with the exception of transactions stated in the SAMA’s Rules Governing the Opening of Bank Accounts.

7. No new accounts, business relationships or transactions are opened unless there is a written request from the customer and the identification process is completed.
should be accepted, and any freezing or any existing account, business relationship or transaction when:

a. Identity of the customer cannot be verified;

b. Identity of the beneficial owner is not known; and/or

c. Failure to obtain information on the purpose and nature of the relevant business.

4.4 Customer Due Diligence (CDD)

Application of due diligence means the effort made by banks and money exchangers to monitor financial transactions of customers and beneficiaries owner, ensure they understand them, and verify all business of customers, data required for opening bank accounts or establishing a banking relationship, and ensure their authenticity and clarity.

Instructions require banks and money exchangers operating in the Kingdom to apply basic due diligence measures on all permanent and casual customers and beneficiaries owner. Such measures shall be continuous and consistent with the risk level of business and transactions of customers as follows:

1. Following up activities of financial transactions and their consistency with the purpose provided upon opening of the account.

2. Due diligence required upon establishing a business relationship, execution of casual transactions over the single or aggregated disclosed limits or being suspected of their connection with money laundering or terrorist financing, regardless of exemptions or limits specified for amounts of transactions, or if there are doubts about the accuracy or adequacy of previously obtained customer identification data.

3. Verifying any person (natural or legal) acting on behalf of the customer and ensuring validity of such action.

4. Identifying persons (natural or legal) who have control on the customer.

5. Increasing level of due diligence with respect of those customers business relationships that are determined to be of higher risk. This may be the result of the customer’s business activity, ownership structure, volume or types of potential or actual transactions, including those transactions involving higher risk countries or defined by the applicable law or instructions as posing higher risk, such as correspondent banking relationships and PEPs.

6. Simple CDD measures and arrangements are not acceptable whenever there are suspicious transactions of money laundering or terrorist financing.

7. The CDD requirements may be reduced with respect to low risk relationships, such as:

a. Companies listed in the Capital Market which are subject to regulatory disclosure requirements.

b. Other banks or financial institutions (domestic or foreign) working within the AML/CTF system in consistency with the FATF Recommendations.

c. Individuals whose main source of funds is a salary, pension or social assistance from identified and appropriate sources where transactions are commensurate with the source of funds.

d. Transactions involving small amounts or particular types of transactions.

Thus, when designing and implementing controls related to due diligence to manage and mitigate the identified risks, according to the risk-based approach, banks and money exchangers should follow the following steps:

- Monitor: Identify those customers who are subject to certain due diligence requirements.

- Assess: Evaluate the risk associated with each customer relationship.

- Mitigate: Implement appropriate controls to manage the identified risks.

- Review: Regularly review and update due diligence policies and procedures.

4.4 Customer Due Diligence (CDD)

Application of due diligence means the effort made by banks and money exchangers to monitor financial transactions of customers and beneficiaries owner, ensure they understand them, and verify all business of customers, data required for opening bank accounts or establishing a banking relationship, and ensure their authenticity and clarity.

Instructions require banks and money exchangers operating in the Kingdom to apply basic due diligence measures on all permanent and casual customers and beneficiaries owner. Such measures shall be continuous and consistent with the risk level of business and transactions of customers as follows:

1. Following up activities of financial transactions and their consistency with the purpose provided upon opening of the account.

2. Due diligence required upon establishing a business relationship, execution of casual transactions over the single or aggregated disclosed limits or being suspected of their connection with money laundering or terrorist financing, regardless of exemptions or limits specified for amounts of transactions, or if there are doubts about the accuracy or adequacy of previously obtained customer identification data.

3. Verifying any person (natural or legal) acting on behalf of the customer and ensuring validity of such action.

4. Identifying persons (natural or legal) who have control on the customer.

5. Increasing level of due diligence with respect of those customers business relationships that are determined to be of higher risk. This may be the result of the customer’s business activity, ownership structure, volume or types of potential or actual transactions, including those transactions involving higher risk countries or defined by the applicable law or instructions as posing higher risk, such as correspondent banking relationships and PEPs.

6. Simple CDD measures and arrangements are not acceptable whenever there are suspicious transactions of money laundering or terrorist financing.

7. The CDD requirements may be reduced with respect to low risk relationships, such as:

a. Companies listed in the Capital Market which are subject to regulatory disclosure requirements.

b. Other banks or financial institutions (domestic or foreign) working within the AML/CTF system in consistency with the FATF Recommendations.

c. Individuals whose main source of funds is a salary, pension or social assistance from identified and appropriate sources where transactions are commensurate with the source of funds.

d. Transactions involving small amounts or particular types of transactions.

Thus, when designing and implementing controls related to due diligence to manage and mitigate the identified risks, according to the risk-based approach, banks and money exchangers should follow the following steps:

- Monitor: Identify those customers who are subject to certain due diligence requirements.

- Assess: Evaluate the risk associated with each customer relationship.

- Mitigate: Implement appropriate controls to manage the identified risks.

- Review: Regularly review and update due diligence policies and procedures.
1. Managing and mitigating the identified risks by developing measures to verify the customer's identity; collect additional information about the customer and monitor the customer's transactions.

2. Establishing control measures for:
   a. Introducing a customer identification program, actions of which vary appropriately with the customer’s risks in the area of money laundering and terrorist financing.
   b. Requiring the quality of evidence, documents, technologies, and third-party guarantees to be of a specific standard.
   c. Obtaining additional information on the customer. Such information should be appropriate to the customer’s assessed money laundering and terrorist financing risks.
   d. Monitoring customer’s transactions and activities.

3. Establishing a customer identification program that is graduated to reflect risks, involving:
   a. A basic database, held in which all data on customers.
   b. Basic verification requirements for all customers.
   c. More extensive due diligence on acceptance of high-risk customers.
   d. Specific basic measures for identity verification of low risk customers and products.
   e. Monitoring the customer’s activities and transactions based on the risk assessed.

4. Investigation into the customer’s source of funds and wealth for high-risk customers.

5. Developing monitoring guidelines for high risk customers versus low risk customers.

---

4.4.1 Beneficiaries owner (Natural & Legal)
Banks and money exchangers should verify the beneficiaries owner of all accounts and relationships and should conduct due diligence on all final beneficiaries owner in accordance with the following:

1. Natural Persons
When the account or relationship is in the name of an individual, the bank or money exchanger should determine whether the account is used in the interest of the client in whose name it was recorded and for the purpose for which it was opened. If doubt exists, the bank should establish the capacity in which and on whose behalf the customer is acting. Identity of the beneficiaries owner should be established to the bank’s or money exchanger’s satisfaction by reference to official identity documents. Banks and money exchangers should also ensure that any person claims to act on behalf of the customer, is so identified, and identify and verify the identity of that person.

2. Legal Persons / Companies
Where the customer is a legal person/ company or establishment, the bank or money exchanger should understand the ownership structure of the establishment or the company sufficiently to determine the provider of funds, principal owners of the shares and those who ultimately own or have control over the assets such as the directors, based on the memorandum of association of the establishment/company and those with the power to give direction to the directors of the company in accordance with the company's articles of association.

With regards to a joint stock company, the bank or money exchanger should establish the identity of all shareholders or
4.4.2 Customer & Transaction Profiling

Banks and money exchangers should have a process in place to capture sufficient information about customers, and their anticipated use of their products and services, that will allow to develop a customer profile of expected activity to provide a basis for recognizing unusual and higher risk activities and transactions, which may indicate money laundering or terrorist financing. The information should be obtained at the establishment of a relationship or opening of an account and prepared for all types of relationships, including accounts and credit cards.

The extent and nature of the information details depend on the different levels of risk resulting from the customer’s relationship with the bank or money exchanger. Higher risk relationships, accounts and transactions will require greater scrutiny than lower risk ones.

The information should be kept up-to-date and monitoring of activity and transactions should be undertaken throughout the course of the relationship to ensure that the activity or transaction being conducted is consistent with the bank’s or money exchanger’s knowledge of the customer. Customer Profiles and Transaction Profiles should be reviewed and updated continuously whenever there is a suspicion of illegal transactions or activities.

1. Customer Profile

A customer profile is a means of collecting detailed information on a customer or an account/relationship. Depending on the type of the customer, profiling will include basic information such as owners’ names (including beneficial owners), partners, shareholders (except for minor shareholders of a joint stock company, holding less than 5%), authorized signers, power of attorney holders, etc.; customers’ addresses including phone numbers, postal and street/location address, e-mail, fax, etc.; purpose and the intended nature of business relationship, information of the business activities, financial information, capital amount, source of funds, source of wealth, branches, countries and products dealing in, etc. At the discretion of the bank or money exchanger, this could be an automated process. Customer identification information and documents should be remain continuously at customer profile.

2. Transaction Profiles

Transaction profiles are means of collecting detailed information about transactions or accounts being conducted and relating to a customer. They are reviewed and updated periodically. The information is collected before any transaction or account is established. The information includes: transaction type, amount, value, time and location of the transaction, source of funds, nature of the business, etc.

3. Customer & Transaction Profile

A customer & transaction profile is a means of collecting detailed information about a customer and their transactions. It is a combination of the customer profile and the transaction profile. The information is collected before any transaction or account is established and is updated periodically. The information includes: customer’s name, address, occupation, source of funds, nature of the business, etc.

4. Money Laundering

Money laundering is the act of illegally acquiring money and then disguising it as legitimate income. It is a criminal offense and can lead to serious penalties. Financial institutions are required to monitor and report any suspicious activity that may indicate money laundering.

5. Terrorist Financing

Terrorist financing is the act of illegally acquiring money and then using it to fund terrorist activities. It is a criminal offense and can lead to serious penalties. Financial institutions are required to monitor and report any suspicious activity that may indicate terrorist financing.

6. Customer Identification

Customer identification is the process of verifying a customer’s identity and ensuring that the customer is not involved in money laundering or terrorist financing. Financial institutions are required to carry out customer identification procedures before establishing a relationship with a customer.

7. Customer Due Diligence

Customer due diligence is the process of verifying a customer’s identity and ensuring that the customer is not involved in money laundering or terrorist financing. Financial institutions are required to carry out customer due diligence procedures before establishing a relationship with a customer.

8. Risk Assessment

Risk assessment is the process of determining the level of risk associated with a customer or transaction. Financial institutions are required to carry out risk assessment procedures before establishing a relationship with a customer or conducting a transaction.

9. Reporting

Reporting is the process of reporting suspicious activity to regulatory authorities. Financial institutions are required to report any suspicious activity that may indicate money laundering or terrorist financing.

10. Sanctions

Sanctions are the use of legal and economic tools to prevent or deter terrorist financing. Financial institutions are required to comply with sanctions regulations.

11. Compliance

Compliance is the process of ensuring that financial institutions are following all applicable laws and regulations related to anti-money laundering and combating terrorist financing. Financial institutions are required to comply with all applicable laws and regulations.

12. Customer Risk Profile

Customer risk profile is a means of evaluating a customer’s risk level and determining the appropriate level of due diligence. Financial institutions are required to create a customer risk profile before establishing a relationship with a customer.
2. Transaction Profile

A transaction profile should be prepared to capture the number of transactions expected to be used by a customer, and the value of transactions for an average month, for each product and service. Banks and money exchangers should develop a system using specialized software to provide automatic preparation of transaction profiles and detect unusual patterns of transactions and trends that may indicate suspicious activities that are not consistent with initial assessments or expectations. All efforts should be made to establish the source of funds to the bank's or money exchanger's satisfaction and the customer and transaction profiling methodology should assist in establishing source of funds.

Transaction profile is not required for employed/payroll, pension and fixed-income individual accounts or relationships, whose source of funds and usage of account can be determined, provided the account or relationship is used for the intended purpose. However, for accounts and relationships used for business purpose and for high-risk accounts, an appropriate transaction profile based on risk assessment, should be prepared to include all types of products and services expected to be used by the customer in the account, during the period of a month, the number of expected transactions, and their estimated monetary value, especially for high-risk products/services such as cash, transfers, etc. The transaction profile should be reviewed and updated continuously to establish continued consistency between the profile and the actual transactions. Major inconsistencies should be investigated.

Banks and money exchangers may prepare a transaction profile on the basis of generic expected activity and transactions for certain types of products and services, however, for more complex products or services a tailored transaction profile will be necessary.

4.4.3 Name Checking of Designated Persons

Saudi Arabia is committed to all relevant United Nations Security Council Resolutions directed towards combating terrorist financing. The UN, through its Security Council Resolutions (UNSCR 1267 of 1999 and successor resolutions), lists a series of “designated persons”, those that are subject to certain sanction measures. Based on Saudi competent authorities’ instructions, SAMA also notifies banks and money exchangers the names of “designated persons” and requires banks and money exchangers to implement the Saudi laws and the UN resolutions in this regard, including freezing of assets of individuals and entities who have been categorized as designated persons by UN or SAMA.

The following measures should be required for all banks and money exchangers:

1. Put in place an effective process to check all their customers' names (individuals, entities, beneficial owners, etc.) against the names that have been categorized as “designated persons” by SAMA and the UN, prior to opening account, establishing a relationship or conducting a transaction, especially for transfers in which case both the remitter’s and the beneficiary’s names should be checked.

2. In case a customer has been identified as being a “designated person”, immediately freeze the account, reporting the transaction and notify SAMA, giving full details of the account or transaction. The account or transaction should continue to be frozen.

The following measures should be applied:

1. In case a customer has been identified as being a “designated person”, immediately freeze the account, reporting the transaction and notify SAMA, giving full details of the account or transaction. The account or transaction should continue to be frozen.

2. In case a customer has been identified as being a “designated person”, immediately freeze the account, reporting the transaction and notify SAMA, giving full details of the account or transaction. The account or transaction should continue to be frozen.
3. The AML/CFT code obliges financial institutions to ensure that their customers' identity is not masked or falsified. This is crucial to comply with AML/CFT laws and regulations.

4. The AML/CFT code requires financial institutions to monitor and report suspicious activities or transactions that may indicate money laundering or terrorist financing. This includes maintaining detailed records of all transactions and reporting any suspicious activity to the relevant authorities.

5. The AML/CFT code mandates financial institutions to conduct due diligence on all new customers and to review the risk profile of existing customers regularly. This includes verifying the identity of customers and their source of funds.

6. The AML/CFT code requires financial institutions to implement internal controls and policies to prevent money laundering and terrorist financing. This includes implementing a risk assessment framework and establishing a compliance program.

7. The AML/CFT code imposes fines and penalties on financial institutions that fail to comply with its provisions. This includes fines for failing to report suspicious activities or for failing to maintain accurate records of transactions.

4.5 Customer Risk Assessment

Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF's Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

4.6 Customer Risks

Customer risks are those that a particular customer or a category of customers may create due to their activities or behavior. Determining the potential money laundering or terrorist financing risks, to the extent that such risk can be identified, posed by a customer, or category of customers, is critical to the development of an overall risk-based framework. Based on its own criteria, a bank or money exchanger should determine whether a particular customer

5.1 The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

5.2 Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

5.3 Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

5.4 Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

5.5 Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

5.6 Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

6.4 Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such classifications as high risk should be subject to enhanced due diligence, closer monitoring, and their risk statuses reviewed and updated continuously.

6.5 Every relationship, account, or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF’s Recommendations, as explained in Rule 5.2;
2. High-risk businesses or customers, as explained in Rule 4.6;
3. High-risk products and services the customer may be dealing in, as explained in Rule 5.1;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in Rule 5.3.
poses a higher risk and the potential impact of any mitigating factors on that assessment. Banks and Money Exchangers shall classify all their customers based on risk. Application of risk variables may mitigate or aggravate the risk assessment.

The types of customers or relationships, and the potential risks they may pose, are described below:

### 4.6.1 Individual Personal Accounts

These are accounts of individuals who open personal accounts for non-commercial and personal use. This category includes mainly employed/ payroll, fixed-income, pensioners, and self-employed individuals. Such personal accounts normally constitute a mass consumer business for many banks and generally do not involve close relationship management by a specific relationship manager. The sheer number of these accounts and the scale of transactions, usually small ticket, make the processes of monitoring demanding for banks.

While the AML risks for employed/ payroll individuals, pensioners and fixed income may be regarded as low, due to the fact that their sources of income can reasonably be established and are generally of smaller value, banks should be alert and exercise more due diligence for individuals who are self-employed. For these customers, it is difficult to reasonably determine their sources of income due to lack of any formal/ official supporting documents. In addition, self-employed individuals are relatively of higher risk due to their free-lancing activities. They may act as agents, on behalf of others, in real estate or other activities and receive a commission in return for their services.

### The following rules should apply as minimum standards for accounts of individual customers:

**1. Employed/ Payroll, Pensioners & Fixed Income Individuals**

These are individuals who are employed/ on payroll, on pension or with a regular fixed income and whose transactions commensurate with the funds. Such personal accounts normally constitute a mass consumer business for many banks and generally do not involve close relationship management by a specific relationship manager. The sheer number of these accounts and the scale of transactions, usually small ticket, make the processes of monitoring demanding for banks.

While the AML risks for employed/ payroll individuals, pensioners and fixed income may be regarded as low, due to the fact that their sources of income can reasonably be established and are generally of smaller value, banks should be alert and exercise more due diligence for individuals who are self-employed. For these customers, it is difficult to reasonably determine their sources of income due to lack of any formal/ official supporting documents. In addition, self-employed individuals are relatively of higher risk due to their free-lancing activities. They may act as agents, on behalf of others, in real estate or other activities and receive a commission in return for their services. These customers are considered as low-risk and the following basic information is sufficient to constitute customer profile:

1. Obtaining proper and valid identification of the customer as stated in SAMA Account Opening Rules.
2. Ensuring customer's identification shows ID number, name, nationality and date/ place of birth.
3. Ensuring customer is not a PEP; otherwise extra due diligence is required as per Rule 4.5.4.
4. Obtaining address and telephone/ mobile number. Also fax number and/ or e-mail address, if available.
5. Account is used for the purpose intended and not for commercial purpose; otherwise it should be treated as commercial account and additional information on the business activity obtained.
6. Taking reasonable measures to determine source of funds/ income; for example, using any one of the following means:
   a. Employment identification card for government, public and private sectors employees;
   b. Payroll slip, pension slip (for pensioners), electronic or paper salary certificate, or letter from employer;
   c. Copy of statement of another bank if salary is

### 6.1.1 The following means:

1. Obtaining proper and valid identification of the customer as stated in SAMA Account Opening Rules.
2. Ensuring customer's identification shows ID number, name, nationality and date/ place of birth.
3. Ensuring customer is not a PEP; otherwise extra due diligence is required as per Rule 4.5.4.
4. Obtaining address and telephone/ mobile number. Also fax number and/ or e-mail address, if available.
5. Account is used for the purpose intended and not for commercial purpose; otherwise it should be treated as commercial account and additional information on the business activity obtained.
6. Taking reasonable measures to determine source of funds/ income; for example, using any one of the following means:
   a. Employment identification card for government, public and private sectors employees;
   b. Payroll slip, pension slip (for pensioners), electronic or paper salary certificate, or letter from employer;
   c. Copy of statement of another bank if salary is
transferred to that bank;

d. If salary is directly transferred to the same bank (individually or through payroll system) no need of further evidence;

e. Salary transferred through SARIE, indicating thereon as payroll/salary;

f. Customer’s self-declaration indicating his/her employer’s name, salary/income and position; or

g. Any other reasonable means satisfactory to the bank and money exchanger;

h. However, in case of doubt, an official documentary confirmation of the customer’s salary/ income should be obtained.

7. Conducting extra due diligence if a bank or money exchangers becomes aware that another bank or money exchanger has refused to deal with a particular customer on AML/ CFT grounds.

2. Self-Employed Individuals (Free Dealers, Agents, etc.)

For self-employed, in addition to above requirements, a self-declaration signed by the customer confirming his/her income, source of funds and business activity should be obtained. In case of doubt, enhanced due diligence procedure should be made to determine the source of funds, and the type of activity the customer is engaged in, as these individuals are relatively high risk due to their free-lancing activities.

3. High Net Worth Individuals

For High Net Worth Individuals, who are considered as high-risk due to the size and nature of their activities and transactions, in addition to above, an enhanced due diligence procedure is required and a detailed customer and transaction profiles should be prepared to also include the customer’s source of funds and source of wealth, and anticipated activity.

In all the above cases, where any doubt or suspicion arises as to the identity, address or source of income/ funds or any other information of a customer during the course of the relationship, the bank or money exchanger should re-verify all the information by reasonable means and reassess the relationship.

4.6.2 Private Banking Customers

Private Banking is the term used for preferential banking services provided to high net-worth customers by a bank. Private Banking normally caters for very wealthy, powerful and influential individuals, including PEPs. These customers are assigned a private banker or relationship manager to act as a liaison between the customer and the bank, and to facilitate the customer’s use of a wide range of financial services and products that usually involve complex transactions and large sums of money, including investment services, trust vehicles and wealth management. These clients demand a high level of confidentiality. As a result, Private Banking is exposed to greater externally laundering vulnerability and terrorist financing and banks should apply enhanced due diligence to such operations.

Banks should have clear customer acceptance policies for handling Private Banking customers, recognizing the money laundering and terrorist financing risks inherent in this category of accounts. They shall categorize of private account customers under high risk customers and conduct continuous due diligence procedures. Banks should endeavor to accept only those clients whose source of wealth and funds can reasonably be established to be legitimate. The following rules should apply as a minimum:

1. Establish the identity of the clients and all the beneficial owners (formally or informally).

2. In case of dealing with non-professional persons, the bank or money exchanger should assess whether the customer has a background in a profession related to financial transactions.

3. In case of doubt, an official documentary confirmation of the customer’s salary/ income should be obtained.

4. Conducting extra due diligence if a bank or money exchangers becomes aware that another bank or money exchanger has refused to deal with a particular customer on AML/ CFT grounds.

2. If salary is directly transferred to the same bank (individually or through payroll system) no need of further evidence;

3. Salary transferred through SARIE, indicating thereon as payroll/salary;

4. Customer’s self-declaration indicating his/her employer’s name, salary/income and position; or

5. Any other reasonable means satisfactory to the bank and money exchanger;

6. However, in case of doubt, an official documentary confirmation of the customer’s salary/ income should be obtained.

7. Conducting extra due diligence if a bank or money exchangers becomes aware that another bank or money exchanger has refused to deal with a particular customer on AML/ CFT grounds.

2. Self-Employed Individuals (Free Dealers, Agents, etc.)

For self-employed, in addition to above requirements, a self-declaration signed by the customer confirming his/her income, source of funds and business activity should be obtained. In case of doubt, enhanced due diligence procedure should be made to determine the source of funds, and the type of activity the customer is engaged in, as these individuals are relatively high risk due to their free-lancing activities.

3. High Net Worth Individuals

For High Net Worth Individuals, who are considered as high-risk due to the size and nature of their activities and transactions, in addition to above, an enhanced due diligence procedure is required and a detailed customer and transaction profiles should be prepared to also include the customer’s source of funds and source of wealth, and anticipated activity.

In all the above cases, where any doubt or suspicion arises as to the identity, address or source of income/ funds or any other information of a customer during the course of the relationship, the bank or money exchanger should re-verify all the information by reasonable means and reassess the relationship.

4.6.2 Private Banking Customers

Private Banking is the term used for preferential banking services provided to high net-worth customers by a bank. Private Banking normally caters for very wealthy, powerful and influential individuals, including PEPs. These customers are assigned a private banker or relationship manager to act as a liaison between the customer and the bank, and to facilitate the customer’s use of a wide range of financial services and products that usually involve complex transactions and large sums of money, including investment services, trust vehicles and wealth management. These clients demand a high level of confidentiality. As a result, Private Banking is exposed to greater externally laundering vulnerability and terrorist financing and banks should apply enhanced due diligence to such operations.

Banks should have clear customer acceptance policies for handling Private Banking customers, recognizing the money laundering and terrorist financing risks inherent in this category of accounts. They shall categorize of private account customers under high risk customers and conduct continuous due diligence procedures. Banks should endeavor to accept only those clients whose source of wealth and funds can reasonably be established to be legitimate. The following rules should apply as a minimum:

1. Establish the identity of the clients and all the beneficial owners (formally or informally).

2. In case of dealing with non-professional persons, the bank or money exchanger should assess whether the customer has a background in a profession related to financial transactions.

3. In case of doubt, an official documentary confirmation of the customer’s salary/ income should be obtained.

4. Conducting extra due diligence if a bank or money exchangers becomes aware that another bank or money exchanger has refused to deal with a particular customer on AML/ CFT grounds.
owners.
2. Obtain proper and valid identification documents as per SAMA Account Opening Rules.
3. If there are any intermediaries involved, extra due diligence should be required to cover the intermediary as well.
4. The profiling process for a Private Banking account should include obtaining and recording the following minimum information:
   a. Purpose and reasons for opening the account.
   b. Anticipated account activity.
   c. Documentation of Source of wealth (description of customer’s commercial/ economic activities which have generated the net worth) and estimated net worth of the customer.
   d. Source of funds (description of the origin and the means of transfer for monies that are expected for the account opening and subsequent large transfers).
   e. References or other sources to corroborate reputation, where available.
5. Bank officers handling the account should personally meet the prospect.
6. Anonymous, fictitious name, coded or numbered accounts should not be allowed.
7. All account opening should be subject to senior management approvals in addition to the relationship manager.
8. If the Private Banking customer is also a PEP, then the requirements for PEP should apply, as per Rule 4.6.4 above.
9. All Private Banking accounts should be subject to close monitoring by a senior officer, covering unusual or suspicious activities.
10. Large cash transactions should be scrutinized more closely, in particular those of complicated nature or lacking a clear economic purpose undertaken during the period of the relationship. Enhanced due diligence procedures should be compiled with. In case there are doubts of money laundering and terrorist financing, FIU shall be reported thereof.

4.6.3 Commercial Entities’ Accounts
These are accounts opened by legal entities for the purpose of conducting commercial activities. Commercial entities include small enterprises such as sole proprietorships and establishments to large companies and corporations. Banks should maintain a customer profile for each commercial relationship, which should cover business and financial related information, source of funds, purpose of account, deposits and banking needs. The extent of details and nature of the information to be requested will vary in relation to the size, structure, risk and type of commercial activities of the business entities, as described below.

1. Small Business Entities
Small businesses are those commercial entities with lower turnover of transactions (e.g., less than SAR one million per annum). These entities range from sole traders/ proprietorships, small establishments and small family concerns to partnerships, professional firms and small private companies.

2. Corporations & Large Business Entities
These are incorporated legal bodies such as corporations, public companies, private companies, partnerships, etc. large businesses are defined as those with significant turnover (e.g., SAR one million per annum and above), whether they are sole traders/ proprietorships, small establishments, small family businesses, partnerships, professional firms or small

3. In case of a merger of two or more the institution it is not necessary to notify the FIU about the merger.
4. If the Private Banking customer is also a PEP, then the requirements for PEP should apply, as per Rule 4.6.4 above.
5. All Private Banking accounts should be subject to close monitoring by a senior officer, covering unusual or suspicious activities.
6. Large cash transactions should be scrutinized more closely, in particular those of complicated nature or lacking a clear economic purpose undertaken during the period of the relationship. Enhanced due diligence procedures should be compiled with. In case there are doubts of money laundering and terrorist financing, FIU

4.6.3 Commercial Entities’ Accounts
These are accounts opened by legal entities for the purpose of conducting commercial activities. Commercial entities include small enterprises such as sole proprietorships and establishments to large companies and corporations. Banks should maintain a customer profile for each commercial relationship, which should cover business and financial related information, source of funds, purpose of account, deposits and banking needs. The extent of details and nature of the information to be requested will vary in relation to the size, structure, risk and type of commercial activities of the business entities, as described below.

1. Small Business Entities
Small businesses are those commercial entities with lower turnover of transactions (e.g., less than SAR one million per annum). These entities range from sole traders/ proprietorships, small establishments and small family concerns to partnerships, professional firms and small private companies.

2. Corporations & Large Business Entities
These are incorporated legal bodies such as corporations, public companies, private companies, partnerships, etc. large businesses are defined as those with significant turnover (e.g., SAR one million per annum and above), whether they are sole traders/ proprietorships, small establishments, small family businesses, partnerships, professional firms or small
Banks should obtain the following information for all commercial entities at the time of opening account/relationship for applying the customer due diligence in accordance with the risk assessment of the customer:

1. Valid and original identification documents as required in the SAMA Account Opening Rules.
2. Large business entities and corporations: The financial structure and nature of the business entity and its annual financial statements.
4. Names of beneficial owners, partners, managers, powers-of-attorney, authorized signatories, shareholders (except for minor shareholders of joint stock companies, owning less than 5%), etc., as applicable.
5. Description of customer's line of business and business activities.
6. Types and nature of products and services the entity may be dealing in.
7. List of significant suppliers, customers and their geographical locations, as applicable.
8. Description of geographical coverage where the business entity carries out its activities, as applicable.
9. List and locations of branches and outlets, if any.
10. Purpose and intended nature of the business relationship/account. The account should be used for the purpose it is opened.
11. For large business entities and corporations, bank employees should pay site visits to acquaint themselves with the nature of business activities. All customer visits should be properly documented and the records maintained.
12. For small business entities, where feasible/practical, bank employees may pay site visits to acquaint themselves with the nature of business activities, and the customer visits documented and records maintained.
13. Individual accounts used for commercial purposes should be treated as small business entities in terms of profiling.
14. Banks should seek information on the customer's relationship with other banks and seek information from these banks if suspicions arise about their dealings with the customer. Extra due diligence is needed, if the bank has reason to believe that other bank(s) rejected this relationship.
15. Banks should collect direct or indirect information about the business entity from any known or available sources.
16. Banks should ascertain the accuracy of the information provided by the business entity when opening an account, e.g., ascertaining the business address, etc.
17. Banks should use their best efforts, through customer profiling and transaction profiling, to ascertain the sources of all deposits, paying additional attention to large cash deposits.
18. These entities' accounts shall be operated by Saudi citizens. Entities may not grant a power of attorney to Non-Saudis.
4.6.4 Politically Recognized Persons

Individuals who are or have been occupying or are expected to occupy in the future leadership positions, for example heads of state or of government, senior public sectors, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, or employees of regional and international organizations. In addition, business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or less important individuals in the foregoing categories.

The political influence and power of PEPs could give rise to abuse of the positions to illegally amass wealth, the proceeds of which are often transferred and concealed under the names of relatives or close associates. Banks and money exchangers should apply the following standards, as a minimum:

1. Comply with all the SAMA Account Opening Rules relating to opening accounts for individuals.

2. Have policies in place to identify and categorize PEPs and related individuals for closer scrutiny. Identification of PEPs should include the existing & new customers as well as the beneficial owners.

3. To put in place appropriate risk management systems to determine whether a potential customer, existing customer or the beneficial owner is a politically exposed person.

4. Determine the source of funds, source of wealth and beneficial owners for all PEPs.

5. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, Banks and money exchangers should be required to obtain senior management approval to continue the business relationship.

6. Categorize all such accounts and relationships as High Risk for enhanced due diligence, and should require approval of a General Manager, Managing Director, or CEO

7. Where Banks and money exchangers are in a business relationship with PEP, they should be required to conduct enhanced ongoing monitoring on that relationship.

8. Accounts of PEPs and related individuals should be reviewed continuously and must be approved by General Manager, Managing Director, or CEO for retaining the relationship/ account.

4.6.5 Walk-In Customers

A walk-in or occasional customer is one who conducts a transaction with a bank or money exchanger but does not maintain an account or any type of relationship with the bank or exchanger. These include citizens, residents and visitors on a temporary visa/ residence. As banks and money exchangers do not have adequate background information about these individuals, banks or money exchangers may be at risk if they conduct financial transactions for them. Therefore, banks and money exchangers should not accept any transactions from walk-in customers unless they fall under the following categories:

1. Citizen or Resident Not Holding accounts; Banks and money exchangers are allowed to accept settlement of bills of services and public utilities (electricity, water, telecommunication) and payments to state authorities and government dues (traffic, passports, etc.). They may

SAMA RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST FINANCING

4.6.4.4 The Polsitical recognition of the person (SA)

The individuals who are or have been occupying or are expected to occupy in the future leadership positions, for example heads of state or of government, senior public sectors, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, or employees of regional and international organizations. In addition, business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or less important individuals in the foregoing categories.

The political influence and power of PEPs could give rise to abuse of the positions to illegally amass wealth, the proceeds of which are often transferred and concealed under the names of relatives or close associates. Banks and money exchangers should apply the following standards, as a minimum:

1. Comply with all the SAMA Account Opening Rules relating to opening accounts for individuals.

2. Have policies in place to identify and categorize PEPs and related individuals for closer scrutiny. Identification of PEPs should include the existing & new customers as well as the beneficial owners.

3. To put in place appropriate risk management systems to determine whether a potential customer, existing customer or the beneficial owner is a politically exposed person.

4. Determine the source of funds, source of wealth and beneficial owners for all PEPs.

5. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, Banks and money exchangers should be required to obtain senior management approval to continue the business relationship.

6. Categorize all such accounts and relationships as High Risk for enhanced due diligence, and should require approval of a General Manager, Managing Director, or CEO

7. Where Banks and money exchangers are in a business relationship with PEP, they should be required to conduct enhanced ongoing monitoring on that relationship.

8. Accounts of PEPs and related individuals should be reviewed continuously and must be approved by General Manager, Managing Director, or CEO for retaining the relationship/ account.
exchange currencies no exceeding (SAR 5000) per transaction of its equivalent, with a total of no more than (SAR 50,000) during one year, provided the identification of information for citizen and passport information of expatriate should be obtained and a currency exchange form should be filled out thereof. Banks and money dealers shall establish an electronic reference using the customer's identification number.

2. Visitors on a temporary visa/residence (Foreign Pilgrims, Tourists, Businessmen & Diplomats): Banks and money exchangers are allowed to accept settlement of bills of any services and public utilities, payments to state authorities and government dues, and encashment of travelers checks. Currency exchange and receiving remittances up to (SAR 5000) per transaction and not exceeding the equivalent of (SAR 50,000) in total within the validity of the visa. A copy of the passport should be obtained including the pages showing the entry and visa stamps. Genuinity of the copy should be verified by the customer and the bank. Banks and money exchangers shall establish an electronic reference using the customer's passport number during this time.

3. For the allowed receiving remittances, a copy of the passport should be obtained including the page evidencing the visa. Full compliance with all the instructions issued concerning money transfers regulation, other details such as home country address, contact in Saudi Arabia and signature should be obtained.

4. In case of suspicion, the bank or money exchanger should report the transaction to FIU enclosing copies of the identification or passport and the transaction, and customer details.

4.6.6 Charity Organizations & Non-Profit Entities

A charity organization or non-profit entity refers to a legal organization that primarily engages in raising/collecting donations and/or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of benevolent deeds.

Banks and money exchangers should have in place policies, procedures and controls to comply with SAMA Account Opening Rules requirements regarding the handling of accounts and transactions for charity organizations and non-profit entities. When dealing with accounts, relationship or transactions of any charity organizations or non-profit entities, banks and money exchangers should observe the following:

1. Not to open an account or set up a relationship for any charity organization or non-profit entity (local or international) unless it meets statutory requirements related to this type of accounts that provided in the Rules Governing the Opening of Bank Accounts & General Operational Guidelines and obtains the official registration by the relevant government ministry or authority, specifying the purpose and activity.

2. To strictly comply with the SAMA Account Opening Rules relating to specific requirements and restrictions when dealing with charity organization accounts.

3. Not to open accounts in the names of chairmen or managers of charities for managing charity funds.

4. To classify charity organization accounts as High Risk and exercise extra and continuous due diligence.

5. Not to accept any transfers or payments (incoming or outgoing) of any donations or contributions into or out of Saudi Arabia except permitted entities in accordance with the rules for opening bank accounts and the general operational rules. This is regardless of whether the funds

in نموذج استخدام العملة. والتحقق بتمل.getenv أو رقم الحوالات كمرجع للعمليات المذكورة.

2. الزائر (الحجّاج الأجنبية، الوافدين، والزائرون)

: يسمح للبنوك ومحلات الصرافة بقبول أموال غير المفتوحة المالية (الكثير من وسائل التحقق من المستحقات المالية، وتتسليط الرؤية، واتخاذ التدابير المناسبة، والدعم النفيسي). وفرص البنوك المالية السهولة (لا تتجاوز مبلغ (SAR 50,000) (05,000) إن لم يكن متعمداً أو مساعد على تحديماً لا يتجاوز مبلغ (SAR 2,111) رديسكي لمبادلة عميل أو القائمة الإختيارية أن يتم استلام معلومات جواز السفر بواسطة صورة منه معدلة على دورة منزل الدولة والناشرة ورقمها ويصادق عليه من المصدر الأصلي من قبل كلاً من الخدمة وموظف البنك، وعلى البنك والعملة المرتبطة لصالح من قبل كل من العملة والموضوع البنك، وفقاً

3. عند فتح الحوامل المالية يجب الحصول على نسخة عن جواز السفر بما في ذلك الصفحة التي تظهر تأشيرة الدخول وذلك عند القيام بالعمليات المسموح بها، وبناء نزاع مقاطعات التاسيسات المالية الأخرى بما في ذلك تلك القابضة الأخرى من العمال في البنك، رقم شخص أو جهية الأعمال في المملكة العربية السعودية والعقارية أو التنمية.

4. في حال وجود شبهة يجب أن يبلغ البنك أو مصرف الصرافة عن العملية لوحدة التحريات المالية ويرفض بها نسخة عن الهوية أو جواز السفر العملية وتفاهم عن العمله.

الجمعيات والمنظمات الخيرية والجهات غير الهدف من تبليغ ما يلي:

1. عدم تحويل أي حساب أو إقامة لأي جمعية منظمة خيرية أو جهية غير هادفة للربح (إصرار محدودة) إلا إذا تم إبلاغ الجهات المالية популية للملفات، وفقاً للقواعد المحددة عند التفاعل مع الجمعيات والمنظمات الخيرية أو جهات غير الهدف من الترحيل.

2. التحقق من الحوامل المالية الخاصة بالعملات والسندات ومؤسسات النقد العربي السعودي وخاصة بالأحكام والقيود المحددة عند التعامل مع حسابات الجمعيات والمنظمات الخيرية أو جهات غير الهدف من الترحيل.

3. عدم تحويل أي مساهمات برامج خاصة أم مديري الجمعيات والمنظمات الخيرية لإدارة الأمور الخيرية.

4. تصفح حالات الجمعيات والمنظمات الخيرية في خدمة المحافظة العامة لمتابعة إجراءات الأعمال المالية الخاصة عند التحقيق من مبادلة العملة.

5. عدم تحويل أي أموالات أو مساهمات (الودائع أو المصطلح) لأي من التبرعات أو المساهمات التي تدخل إلى الملكة أو تخرج منها على أساس الجمعيات والمنظمات الخيريةئة بها ذلك وفقاً
to the funds transfer system (for incoming and outgoing transfers) to be capable of detecting customer names against designated persons of UN or SAMA, prior to processing the transaction for the purpose taking appropriate action.

9. Not to allow to transferring funds in favor of any charity organizations outside the Kingdom of Saudi Arabia other than permitted entities, in accordance with the rules for opening bank accounts and the general operational rules.

10. Full compliance with all the instructions issued concerning money transfers regulation, ensuring the application of the rules of cable transfers (see paragraph 5.1.2).

4.6.7 Truste{s, Nominees & Intermediaries Accounts

1. **Trustee & Nominee Accounts**

These accounts are normally used to provide an extra layer of security to protect the confidentiality of legitimate customers. However, these structures can also be misused to circumvent customer identification procedures for the purpose of money laundering. Therefore, it is essential that the true relationship is understood. Banks should have in place procedures to ensure the following:

1. Establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee or nominee.

2. If the customer is acting on behalf of another person, ensure that he/she has the authorization to do so, and identify and verify the identity of the beneficiaries' owner.

3. Where the customer is a trustee, understand the structure of the trust sufficiently to determine the provider of funds, those who have control over the funds (trustees) and any persons or entities who have the power to remove the trustees.

4. Make a reasonable judgment as to the need for further due diligence and obtain appropriate evidence of formation and existence along with identification of the settler/grantor, trustees or persons exercising effective control over the trust and the principal beneficiaries.

5. Exercise special care in initiating business transactions with companies that have ordinary shareholders; obtain satisfactory evidence of the identity of beneficiaries owner of all such companies; and monitor the identity of actual beneficiaries owner.

2. **Intermediaries ’clients Accounts**

These accounts are opened by professional intermediaries (such as lawyers, independent financial advisors, etc.) who act as professional asset managers on behalf of other clients.
These accounts could be pooled accounts managed by professional intermediaries on behalf of entities such as, pension funds, or managed by lawyers or that represent funds held on deposit or in escrow for a range of clients.

These types of accounts are potentially vulnerable to the money laundering subsequent to the placement phase. Specific vulnerable activities include:

1. Intentional or unwitting facilitation of a customer's money laundering scheme and the activities of rogue employees who undertake illegal activities.
2. Sale washes or other fictitious trading schemes to transfer money.
3. Transfer of value between parties through the sale of shares in small, illiquid issues at artificially arranged prices, without regard to fair market value.

Due to risks accompanying these accounts, banks should have procedures in place and ensure the following:

1. The broker is registered and legal.
2. Perform reinforced due diligence on the intermediary itself and the account should be classified as High Risk.
3. Verify and be satisfied with the broker's reputation and integrity.
4. Establish that the broker has in place a sound documented due diligence process, including KYC and identification requirements, and activity monitoring of its customers and beneficiaries owner, which is satisfactory to the bank.
5. Establish that the broker has in place written policies, procedures and internal controls to address and the risks of its business being used as a vehicle for illegal activities, including the establishment of management controls to prevent the involvement of the broker in money laundering and terrorist financing schemes.
6. When a bank has knowledge or reason to believe that a client account opened by a professional broker is on behalf of a single client, that client must be identified.
7. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficiaries owner, all beneficiaries owner of the account held by the intermediary must be identified.
8. Where the funds are co-mingled, the bank should look through to the beneficial owners, unless the bank can establish that the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as that of the bank.
9. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries.
10. In the absence of the above requirements, then the bank should not permit the intermediary to open an account.

4.6.8 Insurance Companies Accounts

These are accounts opened by insurance companies who offer insurance products directly to their customers or through agents. The insurance sector is potentially at risk and can provide the opportunity for misuse, knowingly or unknowingly, for money laundering and financing of terrorism.

As insurance companies deal with their own customers, banks should exercise due diligence on these accounts, and, in addition to SAMA's Insurance Companies Accounts Opening Rules requirements, banks should have procedures

4.6.8 Insurance Companies Accounts

These are accounts opened by insurance companies who offer insurance products directly to their customers or through agents. The insurance sector is potentially at risk and can provide the opportunity for misuse, knowingly or unknowingly, for money laundering and financing of terrorism.

As insurance companies deal with their own customers, banks should exercise due diligence on these accounts, and, in addition to SAMA's Insurance Companies Accounts Opening Rules requirements, banks should have procedures.
4.6.9 Introduced & Referred Businesses

It is customary for banks to rely on the procedures undertaken by other banks or introducers (person, entity or a professional intermediary) when business is being referred. In doing so, banks risk placing reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks’ own KYC procedures, or that are unwilling to share copies of due diligence documentation.

1. Introduced Business

Banks that use introducers should carefully assess whether the introducers are reputable and are exercising the necessary due diligence in accordance with the acceptable KYC standards. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:

- The bank must satisfy itself as to the reliability of the system put in place by the introducer to verify the identity of the customer.
- The bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage.
- nKBas should reach agreement with the introducer that it will be permitted, upon its request, to obtain and carefully review all relevant identification data and other documentation pertaining to the customer and the introducer.
- The decision to open the account should not be solely based on the introducer’s reputation; rather all KYC process should take place for the introducer as well as the account owner.
- This type of accounts should be classified as High Risk, and reinforced due diligence should be performed on accounts related to those entities.

2. Performance extra due diligence on the insurance companies and classifying the accounts as High Risk.

3. Verifying and being satisfied with the insurance company’s reputation and integrity.

4. Establishing that the insurance company has in place a sound documented due diligence process, including KYC and identification requirements, and activity monitoring for its customers, that is satisfactory to the bank.

5. Establishing that the insurance company has in place written policies, procedures and internal controls to address the risks of its business being used as a vehicle for illegal activities, including the establishment of management controls to prevent the involvement of the insurance company in money laundering and terrorist financing schemes.

6. In the absence of the above requirements, then the bank should not permit the insurance company to open an account.

The customer due diligence procedures of the introducer should be stronger than those which the bank would have conducted itself for the customer. The banks should also ensure that the required due diligence includes that of the introducer.

1. The bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer.
2. The bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage.
3. nKBas should reach agreement with the introducer that it will be permitted, upon its request, to obtain and carefully review all relevant identification data and other documentation pertaining to the customer and the introducer.
4. The decision to open the account should not be solely based on the introducer’s reputation; rather all KYC process should take place for the introducer as well as the account owner.
5. This type of accounts should be classified as High Risk, and reinforced due diligence should be performed on accounts related to those entities.

The ultimate responsibility of the recipient bank to know its customers always lies with the bank. Banks should use the KYC standards. The ultimate responsibility of the introducer is to ensure that the required due diligence includes that of the customer. It is customary for banks to rely on the procedures of the introducer (either personal, or an intermediary) when business is being referred. In doing so, banks risk placing reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks’ own KYC procedures, or that are unwilling to share copies of due diligence documentation.

1. The bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer.
2. The bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage.
3. nKBas should reach agreement with the introducer that it will be permitted, upon its request, to obtain and carefully review all relevant identification data and other documentation pertaining to the customer and the introducer.
4. The decision to open the account should not be solely based on the introducer’s reputation; rather all KYC process should take place for the introducer as well as the account owner.
5. This type of accounts should be classified as High Risk, and reinforced due diligence should be performed on accounts related to those entities.
6. Referred banking relationships developments must be followed up on a continuous basis.

2. Referred Business

This means a relationship referred by one branch to another, within one bank or externally from other banks inside or outside the country. In such cases, the branch/bank accepting the relationship should conduct normal KYC process. Due diligence should include full verification of the customer's identification and information, including beneficiaries owner, comprising the following steps:

1. Banks must take all reasonable steps to identify suspicious transactions. This should require banks to have a reasonable understanding of the normal nature of the customer's business, and having a reasonable understanding of the commercial basis of the transaction to be undertaken or service to be provided.
2. Where a foreign branch, subsidiary or associate refers business to a bank in Saudi Arabia, in addition to the above procedures, the bank should seek the full business rationale for the referral, and determine whether it complies with Saudi Arabian laws and regulations.
3. If the referred branch determines that it has insufficient information to enable it to accept the referral, the business must be declined and the referring branch, subsidiary or associate notified.

4.6.10 Correspondent Banking Relationships

Correspondent banking is the provision of banking services by one bank (correspondent bank) to another bank (respondent bank) by means of a correspondent account. Through the correspondent account, respondent banks can conduct transactions for themselves and for their customers in jurisdiction where they have no physical presence. These services include cash management, international wire transfers of funds, check collection, and foreign exchange services, which usually involve large amounts and numerous transactions.

Correspondent banking, by its nature, creates an indirect relationship whereby the correspondent bank carries out financial transactions for the respondent bank on behalf of its customers (individuals or entities) without having enough information about the customers or by relying on the information and KYC due diligence provided by the respondent bank. This anomaly, coupled with the fact that the correspondent bank may have inadequate AML/CTF standards, poses additional risks in this relationship.

Therefore, banks and money exchangers who maintain correspondent banking relationships should take strict measures to prevent the use of their correspondent accounts for money laundering, terrorist financing and other illegal purposes. Prior to opening any account, banks should fully understand and appropriately document full details of the correspondent bank's management and nature of the business. In addition to requirements relating to correspondent banks relationship as stipulated in SAMA Account Opening Rules, the following requirements should apply as minimum standards for opening and maintaining correspondent bank accounts:

1. Banks should not open a correspondent account for or deal with a Shell Bank.
2. Correspondent bank accounts shall not be opened before the approval of the compliance officer in addition to that of the chief executive officer/director.
3. Banks should immediately inform SAMA of opening correspondent bank account in Saudi Riyal.

<table>
<thead>
<tr>
<th>4.6.10 Correspondent Banking Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correspondent banking is the provision of banking services by one bank (correspondent bank) to another bank (respondent bank) by means of a correspondent account. Through the correspondent account, respondent banks can conduct transactions for themselves and for their customers in jurisdiction where they have no physical presence. These services include cash management, international wire transfers of funds, check collection, and foreign exchange services, which usually involve large amounts and numerous transactions.</td>
</tr>
</tbody>
</table>

Correspondent banking, by its nature, creates an indirect relationship whereby the correspondent bank carries out financial transactions for the respondent bank on behalf of its customers (individuals or entities) without having enough information about the customers or by relying on the information and KYC due diligence provided by the respondent bank. This anomaly, coupled with the fact that the correspondent bank may have inadequate AML/CTF standards, poses additional risks in this relationship.

Therefore, banks and money exchangers who maintain correspondent banking relationships should take strict measures to prevent the use of their correspondent accounts for money laundering, terrorist financing and other illegal purposes. Prior to opening any account, banks should fully understand and appropriately document full details of the correspondent bank's management and nature of the business. In addition to requirements relating to correspondent banks relationship as stipulated in SAMA Account Opening Rules, the following requirements should apply as minimum standards for opening and maintaining correspondent bank accounts:

1. Banks should not open a correspondent account for or deal with a Shell Bank.
2. Correspondent bank accounts shall not be opened before the approval of the compliance officer in addition to that of the chief executive officer/director.
3. Banks should immediately inform SAMA of opening correspondent bank account in Saudi Riyal.
4. Third parties are prohibited from operating correspondent bank accounts.
5. local cash deposits should not be allowed. This arrangement, known as "Payable-Through Accounts" should not be accepted.
6. The correspondent bank should not be under sanctions by the UN or Saudi Arabia.
7. Banks should also determine from any available information (e.g., internet) whether the correspondent bank has been subject to any money laundering or terrorist financing investigations or regulatory action.
8. Banks should obtain certification of AML/CTF compliance for all correspondent relationships, which should include the following information:
   a. The location, major business activities, and management.
   b. That they are under jurisdiction of their central bank or a similar monetary authority and are committed to the FATF recommendations.
   c. That they are governed by and committed to AML/CTF and KYC policies and procedures.
   d. That they have procedures in place for reporting suspicious transactions.
   e. That they are not dealing with any Shell Bank.
   f. Any other pertinent information that can reassure the bank that sufficient focus is being directed to combating money laundering and terrorist financing.
   g. The certification should be either renewed or confirmed by the correspondent bank every three years.
9. Banks and money exchangers should apply satisfactory due diligence on a continuous basis regarding the banking correspondence relationships, document the responsibilities of AML/CTF, which are the correspondent and receiving banks responsibilities and apply due diligence regarding all banking correspondence relationships, including correspondence relationships that already exist.

4.7 Operations Monitoring

4.7.1 Monitoring Process

Monitoring process of operations means pursuance actions of all operations conducted by all permanent or casual customers to deduce any unusual operations. Banking Control Law, money exchanging regulating decision and article 6 of the Saudi AML Law require all financial institutions to take actions to monitor operations and have in place internal precautionary and supervisory measures to detect and foil any of the offensives stated herein, and comply with all instructions issued by the concerned supervisory authorities in this area.

The size of the bank or money exchanger, the AML/CTF risks it faces, number and volume of transactions and the type of activity under scrutiny will impact the degree and nature of monitoring. In applying a risk-based approach to monitoring, banks and money exchangers must recognize that not all transactions, accounts or customers will be monitored in the same way. The degree of monitoring will be based on the perceived risks associated with the customer, the products or services being used by the customer and the location of the customer and the transactions. The principal aim of monitoring in a risk-based system is to respond to institution-wide issues based on each bank’s or money exchanger’s analysis of its major risks. As a general rule, banks and money exchangers should however ensure that all customer transactions are being monitored.

4.8

It is also important for banks and money exchangers to have in place a system to monitor operations and have in place a continuous approach to money laundering and terrorist financing investigations or regulatory action. This approach should include the following:

a. The location, major business activities, and management.

b. That they are under jurisdiction of their central bank or a similar monetary authority and are committed to the FATF recommendations.

c. That they are governed by and committed to AML/CTF and KYC policies and procedures.

d. That they have procedures in place for reporting suspicious transactions.

e. That they are not dealing with any Shell Bank.

f. Any other pertinent information that can reassure the bank that sufficient focus is being directed to combating money laundering and terrorist financing.

g. The certification should be either renewed or confirmed by the correspondent bank every three years.

9. Banks and money exchangers should apply satisfactory due diligence on a continuous basis regarding the banking correspondence relationships, document the responsibilities of AML/CTF, which are the correspondent and receiving banks responsibilities and apply due diligence regarding all banking correspondence relationships, including correspondence relationships that already exist.
Risk-based approach monitoring allows banks and money exchangers to create financial thresholds below which an activity review procedures will be mitigated, and clarify justifications on which these thresholds are based. Thresholds used for this purpose should be reviewed on a continuous basis to assess capability of the risk levels established. Banks and money exchangers should also assess the adequacy of any systems and processes.

 Certain types of transactions or group of events should alert banks and money exchangers to the possibility that the customer is conducting suspicious activities. For example:

1. Unusual patterns of transactions that do not have apparent or visible economic, lawful or commercial purpose;
2. Events that involve complex transactions;
3. Unusual large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer;
4. Very high account turnover, inconsistent with the size of the balance;
5. Transactions connected with entities or individuals, who are the subject of the local or UN sanctions;
6. Business relationship or transactions with entities or individuals from or in countries which do not sufficiently comply with the FATF Recommendations or have weak AML/CTF systems.
7. A customer who provides false or misleading information, refuses to provide relevant information, or refuses to provide his/her identity or whose identity cannot be verified.
8. Requests for information received from domestic and international correspondent banks in regard to inquiries about the operations and activities of some customers.
9. Requests for disclosure of customer balances and accounts and inquiries received from the local supervisory and regulatory authorities.
10. Requests for seizure and operation prohibition received from local authorities, international organizations and lists of other countries.

All the above may indicate the existence of money laundering or terrorist financing transactions through the account. The background and purpose of such transactions should be examined as far as possible and documented in writing. Those results should be provided upon request by the supervisory authority and be retained at least for 10 years, and suspicious transactions should be reported in writing to FIU.

When applying risk-based monitoring approach for money laundering and terrorist financing, the following points should be taken into consideration:

1. No transaction shall be excluded from monitoring.
2. Transaction amount shall not be a factor of risk determination.
3. Focus is given on particular high-risk businesses and accounts.
4. Focus is given for particular individuals, organizations and countries.
5. Before applying risk-based approach, banks and money exchangers should identify a more comprehensive set of indicators of the method and techniques used for money laundering and terrorist financing, which can then be turned into strategies to assess money laundering and terrorist financing risk and devise controls to mitigate such risk.

4.7.2 Financial Investigation Process

Banks and money exchangers should have a process in place for the financial investigation and analysis of unusual customer activity or transactions, which should include the expected frequency, size, volume and origin/destination of customer funds whether specific to an individual customer, or for a generic customer, type or product type; and the presence of risk factors specific to the bank’s or money exchanger’s nature of the activity and customer base.

The investigation and analysis of the unusual and higher risk activity and transactions should be conducted by an independent reviewer, and should include the following:

1. Reviewing the identified activity/transaction in light of the customer risk assessment and the customer due diligence information that it holds;
2. Making further enquiries to obtain additional information required to enable a determination as to whether the activity/transaction has a rational explanation;
3. Considering the activity/transaction in the context of any other relationships connected with the customer by referring to the relevant customer due diligence information and making enquiries to reach for appropriate conclusions;
4. Updating customer due diligence information to record the results of the enquiries made;
5. Not to alert the customer that his transactions are under review, monitoring etc.
6. Reviewing the appropriateness of the customer risk assessment in light of the unusual activity and additional customer due diligence information obtained;
7. Considering whether further improvements of the monitoring process is required (staff training, enhancing the monitoring system parameters, strengthening controls for more vulnerable products/services);
8. Applying increased levels of monitoring to particular relationships;
9. Where the activity or transaction does not have a rational explanation, considering whether the circumstances require a suspicious activity report to be submitted to the bank’s or money exchanger’s Money Laundering Control Unit (MLCU) or designated Compliance Officer.
10. In case a bank or money exchanger, through its monitoring and investigation process, finds that an activity or transaction of a customer is suspicious, further due diligence should be conducted including re-verifying the customer’s information, obtaining additional information, and re-assessing the relationship.

4.7.3 Transaction Monitoring Reinforcement

Monitoring high-risk transactions conducted throughout the relationship period should be strengthened and enhanced, taking in consideration the importance of compliance with requirements of identity verification procedures, due diligence procedures and transactions monitor despite their nature & amount.

2074

عمالة التتبع العامل (التحقيق)

يرجى على البنوك ومحلات الصرافة وضع آلة التتبع (التحقيق) والتحليل المالي للأنشطة أو العمليات غير العادية التي يقوم بها العملاء، بحيث تتضمن عدد مرات تكرار وحجم ومصدر أو وجهة أموال العملاء المتوقعة، سواء كانت متعلقة عملياً واحداً أو مجموعة من العملاة أو نوع من المنتجات، فضلاً عن وجود عوامل المخاطر الخاصة بطيعية نشاط البنك أو محل الصرافة وقاعدة عملائه.

كما يُجب أن يتم إجراءات التتبع والتحليل في الشاشة والمحلات غير المعاملة ذات المخاطر العالية من قبل مراجع مستقل حيث تتضمن ما يلي:

1. مراقبة النشاط/العملية في ضوء تقييم مخاطر العملاء ومعلومات العناية الواجبة الخاصة به.
2. طلب الحصول على معلومات إضافية والتي تسمح بإيجاد تفسير منطقي للنشاط/العملية المتوقع.
3. الأخذ في الاعتبار وضع النشاط/العملية في سياق أي مخالفة أخرى مرتبطة بالعملاء من خلال الرجوع إلى معلومات العناية الواجبة الخاصة بالعملاء وعمل الإستفسارات الفورية للوصول إلى نتائج ممسحة.
4. تحديد معلومات العناية الواجبة لتسجيل نتائج الإستفسارات التي تمت في هذا الخصوص.
5. عدم تنبيه العملاء عن مراجعته أو المراقبة وحده ذلك.
6. مراجعة مدى صحة تقييم مخاطر العملاء في ضوء الظروف الخاصة بالعملاء غير الاعتيادي الذي تم توثيقه بالعملاء والمعلومات الإضافية التي تم الوصول إليها من خلال مراجعة العناية الواجبة لهذا العملاء.
7. التحسين المستمر لعملية المراقبة (كدرب الموظفين، وتحسين معايير نظام المراقبة، وتعزيز الضوابط المتعلقة بالأنشطة الأكثر عرضة للمخاطر).
8. زيادة مستويات الرقابة على بعض العلاقات المحددة.
9. في حال عدم وجود تفسير منطقي للنشاط أو العملية، يجب دراسة الظروف المحيطة مع مراجعة مدى الحاجة إلى إعادة تقييم العملاء المشتبه بها لتقديمه إلى وحدة مراقبة العملاء أو إلى مسؤول الامتياز لدى البنك أو محل الصرافة.
10. في حال إكتشاف البنك أو محل الصرافة عبر عمليات الصرافة والتحويل، خلال نشاط المليت، أو عملية التي تجربة/الشأن، يجب تدشين إجراءات العناية الواجبة، بما في ذلك إعداد التحقق من المعلومات التي قام بها العملاء، والحصول على معلومات إضافية لتفاوضك المعاة معه.

2074

تعزيز مراقبة العمليات
4.8 Suspicious Transaction

4.8.1 Reporting Suspicious Transactions

The reporting of suspicious transaction or activity is critical to the competent authorities’ ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. The Saudi AML Law and its implementation regulation require banks and money exchangers to file Suspicious Transaction Report (STR) once a suspicion has been formed.

The AML Law and its implementation regulation shall be applicable to banks, money exchangers and their employees. Employees whose suspicions are aroused, but who then deliberately fail to make further inquiries, wishing to remain ignorant or demonstrate “willful blindness”, may be deliberately fail to make further inquiries, wishing to remain ignorant or demonstrate “willful blindness”, may be considered under the Saudi AML Law to have the requisite knowledge. However, the Saudi AML Law relieve the bank or money exchanger, management and employees from any liability that may be caused by performing the duties provided for or by violating the provisions of confidentiality, unless it is established that they have acted in bad faith to hurt the involved person.

Thus, banks and money exchangers reporting policy should mandate employees to do the following:

1. If an employee suspects that a money laundering transaction is taking place, he/she should immediately report it to the bank’s or money exchanger’s internal MLCU or designated Compliance Officer. (Refer to Rule 4.7.4 for details).
2. Attempts of suspicious transactions, which have been identified as suspicious but were foiled before occurrence, must be reported.
3. Banks and money exchangers should make available, to the appropriate authorities all documents, statements and related transactions.
4. All documents, reports and information relating to internally investigated cases not reported to the authorities for lack of suspicion, should be maintained by the bank and money exchanger for record purposes in accordance with records documentation referred to in Article 4.11.
5. It is a criminal offence for bank or money exchanger employees to tip off or assist any customer or individual that they know or suspect of having been involved in any money laundering or terrorist financing activities. If an employee thinks that a transaction may be related to a criminal activity, this must be immediately reported to the bank’s or money exchanger’s MLCU/ Compliance Officer.
6. The notifying bank or money exchanger and its employees are free of any blame or charge in respect of any AML/CTF notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.

The notifying bank or money exchanger and its employees are free of any blame or charge in respect of any AML/CTF notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.
4.8.2 Reporting Requirements

According to the AML Law, financial institutions including banks and money exchangers are required to report all transactions suspected to relate to money laundering or terrorist financing, including any attempts to conduct such transactions to FIU. The Law also requires banks and money exchangers to submit a detailed report including all available information and supporting documentation on the parties involved, and provide it to the FIU. In order to achieve the requirements above, the following should be fulfilled:

i. Reporting should be in accordance with the form approved by the FIU and the form of the provided by SAMA, and should contain the following:
   1. Names of suspected individuals/ entities, their identities, addresses and phone numbers.
   2. Statement with respect to the suspected transaction/s, the involved parties, how it was discovered and present condition/status.
   3. The exact amount of the suspected transaction/s and related banking accounts.
   4. Reasons of suspicion upon which the bank or money exchanger staff had depended/based on.

ii. Banks and money exchangers should provide the technical report on reported cases to the FIU within 10 days from the reporting date, including the following:
   1. Ensure completion of all the data and filling in of all fields in the reporting form regarding suspected transactions, including any attempted transactions, related to money laundering, indicating the name of the branch and the region, where the suspected account is domiciled.
   2. Submit the original suspicion report, statement of account of 6 months, attachments of account (opening account documents) and technical report on studying the reported account to the FIU.
   3. Take the following actions after reporting:
      1. keep records, copies of the report and notification, the technical record and its attachment to be used as a reference in future.
      2. Follow-up the reported customer activity. In case the suspected activities persist and no feedback is received from the FIU within two months of the date of notification, the notification should be reconfirmed by reporting the same to the FIU.
      3. Follow-up the report to the FIU concerning a feedback on all reports after six months from the date of reporting.

4.8.3 Tipping Off

Banks and money exchangers and their directors, officers and employees should not disclose the fact that a customer is being or has been investigated or reported for a suspicious transaction. Banks and money exchangers should exercise extreme caution when performing additional customer due diligence (CDD) because of suspicious transaction, so as not to unintentionally tip off the customer. In case the bank or money exchanger feels the performance of CDD may tip off the customer, it could then decide to discontinue the CDD but to file a suspicious activity report to FIU.

The Saudi AML Law and Bylaws prohibit financial institutions and their employees from alerting customers or other related parties about suspicions of their activities or about their notification to the authorities. The Saudi AML Law, notification of suspected money laundering and terrorist financing cases to the authorities does not conflict with the provision of banking secrecy or customer confidentiality under the Saudi

4.8.4 Tipping of the BLAgs

Tipping of the BLAgs is prohibited by the Saudi AML Law. The banks and money exchangers must not communicate any suspicions or suspicions of their clients to the authorities or disclose any information about their notification to the authorities. The Saudi AML Law, notification of suspected money laundering and terrorist financing cases to the authorities does not conflict with the provision of banking secrecy or customer confidentiality under the Saudi
banksing laws and regulations.

4.8.4 Money Laundering Control Unit (MLCU)

Banks and money exchangers must establish an independent and dedicated function to handle money laundering and terrorist financing and reporting activities. For banks and money exchangers, with five branches and less this function can be handled by the designated Compliance Officer for the bank or money exchanger. For banks and money exchangers with more than five branches, an independent and dedicated Money Laundering Control Unit should be established with adequate staff. In both the above situations, the designation of the MLCU staff or Compliance Officer to handle the money laundering and terrorist financing control function, should be a Saudi, of senior management level, and with more than five years’ experience in the field of anti-money laundering and terrorist financing.

The officer-in-charge of the money laundering control function, as an individual or a unit, should have sufficient authority, independence, accountability and resources, and he/she should be granted timely access to customer information (such as identification data, due diligence information, transaction records and other relevant data) to enable him/her to discharge his/her functions effectively.

MLCU, or designated Compliance Officer, will have the following functions and responsibilities:

1. Monitoring of all transactions for the purpose of detecting activities that may involve money laundering and terrorist financing activities.
2. Receiving suspicious transactions relating to money laundering and terrorist finance from branches, transfer centers and various internal departments of the bank or money exchanger, and taking necessary actions for the collection of information about it, analysis of the data collected, and making necessary decision for taking action, which should be documented in writing.
3. Reporting suspicious transactions to the Saudi Financial Intelligence Unit (SAFIU), when suspicions have been determined, in accordance with established requirements, supported by a detailed technical report on the suspicious case.
4. Developing electronic programs for controlling and detecting unusual operations as well as large cash transactions and complex operations which have no legal or economic purpose and other operations that may have a connection with activities of money laundering and terrorism financing, and updating the indicators that reflect existence of suspicious money laundering and terrorism financing acts in a manner consistent with the development and diversity of the techniques adopted in committing financial crimes.
5. Submission of proposals targeting development of internal policies, plans, procedures and controls along with methods for facilitating application of the same. Approval of a state-of-the-art automated system in the area of anti-money laundering.
6. Ensuring that staff, in branches and other departments, comply with the instructions and procedures pertaining to accounts monitoring; and ensuring that employees understand the importance of such procedures and instructions as well as the importance of the adopted procedures for suspicious activities and reporting requirements.
7. Supporting of Compliance Department in its task of verifying that the established rules, regulations and procedures for controlling illegal transactions are properly implemented and that the MLCU reports all suspicious transactions to the supervisory authorities.

4.8.4.1 Money Laundering Control Unit (MLCU)

Money Laundering and Terrorist Financing Unit (MLCU) shall have the following functions and responsibilities:

The MLU, or designated Compliance Officer, will have the following functions and responsibilities:

1. Monitoring all transactions for the purpose of detecting activities that may involve money laundering and terrorist financing activities.
2. Receiving suspicious transactions relating to money laundering and terrorist financing from branches, transfer centers and various internal departments of the bank or money exchanger, and taking necessary actions for the collection of information about it, analysis of the data collected, and making necessary decision for taking action, which should be documented in writing.
3. Reporting suspicious transactions to the Saudi Financial Intelligence Unit (SAFIU), when suspicions have been determined, in accordance with established requirements, supported by a detailed technical report on the suspicious case.
4. Developing electronic programs for controlling and detecting unusual operations as well as large cash transactions and complex operations which have no legal or economic purpose and other operations that may have a connection with activities of money laundering and terrorism financing, and updating the indicators that reflect existence of suspicious money laundering and terrorism financing acts in a manner consistent with the development and diversity of the techniques adopted in committing financial crimes.
5. Submission of proposals targeting development of internal policies, plans, procedures and controls along with methods for facilitating application of the same. Approval of a state-of-the-art automated system in the area of anti-money laundering.
6. Ensuring that staff, in branches and other departments, comply with the instructions and procedures pertaining to accounts monitoring; and ensuring that employees understand the importance of such procedures and instructions as well as the importance of the adopted procedures for suspicious activities and reporting requirements.
7. Supporting of Compliance Department in its task of verifying that the established rules, regulations and procedures for controlling illegal transactions are properly implemented and that the MLCU reports all suspicious transactions to the supervisory authorities.

4.8.4.2 Money Laundering Control Unit (MLCU)

Money Laundering and Terrorist Financing Unit (MLCU) shall have the following functions and responsibilities:

The MLU, or designated Compliance Officer, will have the following functions and responsibilities:

1. Monitoring all transactions for the purpose of detecting activities that may involve money laundering and terrorist financing activities.
2. Receiving suspicious transactions relating to money laundering and terrorist financing from branches, transfer centers and various internal departments of the bank or money exchanger, and taking necessary actions for the collection of information about it, analysis of the data collected, and making necessary decision for taking action, which should be documented in writing.
3. Reporting suspicious transactions to the Saudi Financial Intelligence Unit (SAFIU), when suspicions have been determined, in accordance with established requirements, supported by a detailed technical report on the suspicious case.
4. Developing electronic programs for controlling and detecting unusual operations as well as large cash transactions and complex operations which have no legal or economic purpose and other operations that may have a connection with activities of money laundering and terrorism financing, and updating the indicators that reflect existence of suspicious money laundering and terrorism financing acts in a manner consistent with the development and diversity of the techniques adopted in committing financial crimes.
5. Submission of proposals targeting development of internal policies, plans, procedures and controls along with methods for facilitating application of the same. Approval of a state-of-the-art automated system in the area of anti-money laundering.
6. Ensuring that staff, in branches and other departments, comply with the instructions and procedures pertaining to accounts monitoring; and ensuring that employees understand the importance of such procedures and instructions as well as the importance of the adopted procedures for suspicious activities and reporting requirements.
7. Supporting of Compliance Department in its task of verifying that the established rules, regulations and procedures for controlling illegal transactions are properly implemented and that the MLCU reports all suspicious transactions to the supervisory authorities.
4.9 Internal Control

4.9.1 Internal Control Procedures

Under the Saudi AML Law, The Banking Control Law. Decision of the Minister of Finance & National Economy on Regulating Money Changing Business, financial institutions are required to establish internal control procedures and prevent themselves from being used for purposes of money laundering and terrorist financing.

To apply an effective approach, the internal control procedures of the banks or money exchangers must be imbedded within their systems, programs and procedures to cover the issue of money laundering and terrorist financing. Senior management is ultimately responsible for ensuring that a bank or money exchanger maintains an effective internal control structure, including suspicious activity monitoring and reporting. The strength of senior management leadership and compliance with AML/CTF are an important aspect of the application of the procedure. Senior management must create a culture of compliance, ensuring that all employees adhere to the bank's or money exchanger's policies, procedures and processes designed to limit and control risks.

In addition to other compliance internal controls, the nature and extent of AML/CTF controls will depend upon a number of factors, including:

1. Nature, scale and complexity of a bank's or money exchanger's business.
2. Diversity of a bank's or money exchanger's operations, including geographical diversity.
3. Bank's or money exchanger's customer, product and

requirements are effectively applied in compliance with AML/CTF requirements.
8. Selection of qualified staff to fill the positions in the unit and the development of ongoing training materials to provide them with latest information on money laundering and terrorist financing activities, with the aim of enhancing their knowledge to identify such activities, trends and nature of activities, and how these can avoided and dealt with.
9. Preparation and submission of periodic reports regarding the activities conducted by MLCU/ designated Compliance Officer for money laundering and terrorist financing activities as well as the general status of the bank or money exchanger and its various departments and branches vis-à-vis this matter which need to be supported by statistical data for those activities, and recommendations made for their development/improvements.
10. Responding to all SAMA's circulars and requests relating to customer accounts statements and blocking, and preparation of the required information in the proper form and timeframe.
11. Maintaining a database comprising all data relating to money laundering and terrorist financing matters in the bank or money exchanger, such as the suspicious cases reported, blocked accounts, etc. and updating of all the old cases in the database.
12. Making appropriate continuous supervisory visits to the banks' various sectors and departments, including branches and money transfer centers.
14. Participation in the process of educating and training all the bank staff categories and all customers segments.

9.4.1 إجراءات الرقابة الداخلية

9.4.1.1 إجراءات الرقابة الداخلية

نظام مكافحة غسل الأموال والحفاظ على مالية المصرفية المحتفظة عن أمراض وقائية على البنك أو محل الصرافة، وذلك من خلال تطبيق إجراءات الرقابة المالية ومركز التحويل.

من أجل تطبيق أسلوب عمل، يجب أن يُدرج إجراءات الرقابة الداخلية الخاصة بمحال مكافحة غسل الأموال ومركزية بالتبادل أو محال البنوك، وتحقيق الأهداف الخاصة بالᅮالة. بالإضافة إلى ذلك، يجب أن يكون من الواجب على الإدارة العليا أن يكون لها المسؤولية الإدارية والمهنية للأعمال التي قد يتم استخدامها لأغراض غسل الأموال، ومعالجة الشكاوى المتعلقة بها.

يجب على الإدارة العليا أن تضمن جمع المعلومات المتعلقة بالإجراءات والإجراءات المالية التي توضحها البنك أو محل الصرافة، وذلك من خلال تطبيق إجراءات الرقابة الداخلية الخاصة بمحال مكافحة غسل الأموال ومركزية بالتبادل أو محال البنوك، وتحقيق الأهداف الخاصة بالعتمد.

وإلى جانب الضوابط الداخلية الأخرى للاكتشاف، ترتبط طبيعة مندوب الضوابط الخاصة بمكافحة غسل الأموال ومركزية بالتبادل بعد من العملاء ومنها:

1. طبيعة ودرجة ودبياخن أعمال البنك أو محل الصرافة.
2. توزيع المهام الخاصة بال🚫 في تلك النقطة الجغرافية.
3. عمل البنك أو محل الصرافة والمعلومات عن منتجاته ونشاطها وقواعدهم المدنية المستخدمة.
activity profile and distribution channels used.
4. Volume and size of the transactions.
5. Degree of risk associated with each area of the bank’s or money exchanger’s operation.
6. Extent to which the bank or money exchanger is dealing directly with the customer or through third parties.

Therefore the framework of internal control procedures of banks or money exchangers should:

1. Provide increased focus on a bank’s or money exchanger’s operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
2. Provide for regular review of the risk assessment and management processes, taking into account the environment within which the bank or money exchanger operates and the activity in the market place.
3. Provide for an AML/CTF compliance function and designate an individual at management level responsible for managing the compliance function.
4. Ensure that adequate controls are in place before new products are offered.
5. Inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.
6. Focus on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CTF compliance and provide for timely updates in response to changes in regulations.
7. Implement risk-based customer due diligence policies, procedures and processes.
8. Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
9. Enable timely identification of reportable transactions and ensure accurate filing of required reports.
10. Include AML/CTF compliance in job descriptions and performance evaluations of appropriate personnel.
11. Provide for appropriate continuous training to be given to all relevant staff.

4.9.2 Assessment of Internal Controls

Banks and money exchangers should establish means of independently and periodically assessing the effectiveness of the internal controls and the adequacy of the overall AML/CTF programs. The assessment should include:

1. Determining the risk profile of the bank or money exchanger, taking preventive measures to reduce the occurrence and severity of money laundering and terrorist financing.
2. Identifying and understanding the overall business and geographic locations that are more vulnerable to money laundering and terrorist financing.
3. Developing training programs to educate their employees on money laundering and terrorist financing.
4. Ensure that adequate controls are in place before new products are offered.
5. Informing senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.
6. Focusing on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CTF compliance and provide for timely updates in response to changes in regulations.
7. Implementing risk-based customer due diligence policies, procedures and processes.
8. Providing for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
9. Enabling timely identification of reportable transactions and ensuring accurate filing of required reports.
10. Including AML/CTF compliance in job descriptions and performance evaluations of appropriate personnel.
11. Providing for appropriate continuous training to be given to all relevant staff.

4.10 Staff Training & Hiring

4.10.1 Staff Training & Awareness

The AML Law and bylaws mandate all financial institutions to develop training programs to educate their employees and enhance their understanding of Due Diligence, KYC principles, money laundering and terrorist financing risks, trends and preventive methods. As employees become familiar with such activity, they can play an effective role by taking preventive measures to reduce the occurrence and severity of money laundering and terrorist financing.
control of money laundering and terrorist financing.

Banks and money exchangers should provide their employees with appropriate and adequate training, and ongoing awareness, with regard to money laundering and terrorist financing. A bank or money exchanger must have successful controls based on at least general information on AML/CTF laws, regulations and internal policies on compliance.

Applying a risk-based approach to the various methods available for training, however, gives each bank or money exchanger, additional flexibility regarding the frequency, delivery mechanisms and focus of such training. A bank or money exchanger should review its own workforce and available resources and implement training programs that provide appropriate AML/CTF information, as follows:

1. Tailored to the appropriate staff responsibility (e.g., front-line staff, compliance staff, or customer relations staff, account opening and operations).
2. At the appropriate level of detail (e.g., complex products, new products and services, trends).
3. At a frequency related to the risk level of the business line involved.
4. All new staff, before starting their work, should be educated in the importance of AML/CTF policies while regular and continuous refresher training should be provided to staff to ensure that they are reminded of their responsibilities and kept informed of new developments.
5. Testing to assess staff knowledge commensurate with the detail of information provided.
6. Training programs shall include various levels of staff in the bank or money exchanger including members of the Board, Directors in charge and Executive Directors.

Additionally, banks and money exchangers should make all their staff aware of their responsibilities, personal obligations, liability and penalties under the legislation, should they fail to comply with the relevant requirements, as stated in Saudi AML Law.

4.10.2 Staff Hiring & Appointment of Senior Positions

Banks and money exchangers should put in place adequate background screening procedures to ensure high standards when hiring employees. Banks and money exchangers can develop a risk-based approach on the level of screening based on the function and responsibilities associated with a particular position.

In addition, banks and money exchangers should comply with the provisions stipulated in the SAMA Directive issued in April 2005, relating to Qualifications Requirement for Appointment to Senior Positions in Banks, including notifying SAMA for each senior appointment and the annual submission of a list of all senior positions.

4.11 Record Keeping & Retention

Banks and money exchangers must keep all records (documents, instructions, transactions, files and reports) relating to their operations in accordance with normal business practices, for ease of access and their own use, and for supervisory/ regulatory and other authorities, and for internal and external auditors. The records should be adequate enough to be able to reconstruct a transaction and offer a complete audit trail of all financial transactions, in particular cash transactions and funds transfer.
The Saudi AML Law requires financial institutions to maintain, for a minimum of ten years following the conclusion of an operation/transaction or termination of an account/relationship, all records and documents that explain the financial, commercial and monetary transactions, whether local or foreign, the files of account documentation, related correspondence and copies of the identification documents. Taking into consideration the local law, customer transaction records, such as agreements, checks, etc., should be retained indefinitely.

In specific cases, banks and money exchangers may be instructed by SAMA or other Saudi competent authorities, to maintain any transactions or account records beyond the minimum period time period stated below. Banks and money exchangers should keep and retain these records in the form and for the period as indicated below:

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Form</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Customer account opening agreements and related account documents</td>
<td>Original form</td>
<td>Permanently</td>
</tr>
<tr>
<td>b. Certified/attested copies of customer identification documents</td>
<td>Originals of the certified/attested copies</td>
<td>Permanently</td>
</tr>
<tr>
<td>c. All customer transaction records and instructions: i. Manual instructions (e.g., checks, transfer applications, etc.) ii. Automated instructions (e.g., internet, phone banking, ATM, incoming wire transfers, etc.)</td>
<td>One of the following: i. Original form ii. Electronic form</td>
<td>Permanently</td>
</tr>
<tr>
<td>d. Statements and details of customer accounts and balances.</td>
<td>Electronic form</td>
<td>Permanently</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Form</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Customer profiles, risk assessments and all other KYC related documents</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>b. Investigations, suspicious activity reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>c. Automated and manual reports</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>d. Reviews, self-assessments, audit reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
</tbody>
</table>

The above requirements apply to all financial institutions, whether local or foreign, and all records and documents related to financial, commercial and monetary transactions, whether local or foreign, including the files of account documentation, related correspondence and copies of identification documents. Taking into consideration the local law, customer transaction records, such as agreements, checks, etc., should be retained indefinitely.

In specific cases, banks and money exchangers may be instructed by SAMA or other Saudi competent authorities, to maintain any transactions or account records beyond the minimum period time period stated below. Banks and money exchangers should keep and retain these records in the form and for the period as indicated below:

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Form</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Customer account opening agreements and related account documents</td>
<td>Original form</td>
<td>Permanently</td>
</tr>
<tr>
<td>b. Certified/attested copies of customer identification documents</td>
<td>Originals of the certified/attested copies</td>
<td>Permanently</td>
</tr>
<tr>
<td>c. All customer transaction records and instructions: i. Manual instructions (e.g., checks, transfer applications, etc.) ii. Automated instructions (e.g., internet, phone banking, ATM, incoming wire transfers, etc.)</td>
<td>One of the following: i. Original form ii. Electronic form</td>
<td>Permanently</td>
</tr>
<tr>
<td>d. Statements and details of customer accounts and balances.</td>
<td>Electronic form</td>
<td>Permanently</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Form</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Customer profiles, risk assessments and all other KYC related documents</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>b. Investigations, suspicious activity reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>c. Automated and manual reports</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>d. Reviews, self-assessments, audit reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
</tbody>
</table>

**5. AML / CTF Other Risks**

5.1 **Product/Service Risks**

Product or service risks are the potential risks inherent in the

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Form</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Customer account opening agreements and related account documents</td>
<td>Original form</td>
<td>Permanently</td>
</tr>
<tr>
<td>b. Certified/attested copies of customer identification documents</td>
<td>Originals of the certified/attested copies</td>
<td>Permanently</td>
</tr>
<tr>
<td>c. All customer transaction records and instructions: i. Manual instructions (e.g., checks, transfer applications, etc.) ii. Automated instructions (e.g., internet, phone banking, ATM, incoming wire transfers, etc.)</td>
<td>One of the following: i. Original form ii. Electronic form</td>
<td>Permanently</td>
</tr>
<tr>
<td>d. Statements and details of customer accounts and balances.</td>
<td>Electronic form</td>
<td>Permanently</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Form</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Customer profiles, risk assessments and all other KYC related documents</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>b. Investigations, suspicious activity reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>c. Automated and manual reports</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>d. Reviews, self-assessments, audit reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
</tbody>
</table>

**5.2 Secondary/Non-Financial Records**

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Retention Form</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Customer profiles, risk assessments and all other KYC related documents</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>b. Investigations, suspicious activity reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>c. Automated and manual reports</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
<tr>
<td>d. Reviews, self-assessments, audit reports, etc.</td>
<td>Original and/or electronic form</td>
<td>Minimum 10 years</td>
</tr>
</tbody>
</table>
5.1.1 Cash

Physical cash is often the ideal and most commonly used method for transfer of funds and undertaking criminal activities, including money laundering and terrorist financing, simply because the perpetrator is anonymous, untraceable, requires no intermediary, is widely accepted and provides for immediate settlement. While the provision of services to cash-generating business is a particular area of concern, however, some businesses are legitimately cash-based, especially in the retail sector, and so there will often be a high level of cash deposits associated with some of these accounts.

1. Cash Transactions

SAMA has participated for many years in the efforts to transform the Saudi economy to a bank-based payment society and has taken significant steps to discourage large cash transactions and encourage the use of banking payment systems, including SARIE, SWIFT, ATM/SPAN, POS, SADAD, Internet banking, credit cards, etc. SAMA Account Opening Rules require banks and money exchangers to accept cash from customers only through an account or relationship, where a full due diligence and KYC process has been established.

Banks and money changers should urge and encourage customers to reduce the use of cash and provide alternative banking services such as the use of electronic financial payment systems.

Banks and money exchangers should have a process in place to detect cash transactions that could be deemed as suspicious, such as:

1. Large cash deposits, not in line with the customer’s type of business or occupation.
2. Numerous cash deposits of small amounts, known as structuring or smurfing, to avoid detection.
3. Cash deposits followed by a transfer (wire transfer, bank check, etc.).
4. Structured cash payments for outstanding credit card balances, with relatively large sums as payments.

2. Cross-Border Transportation of Cash

In accordance with Saudi AML Law and its implementation regulation, banks and money exchangers should comply with the requirements relating to cross-border transportation of cash coming into or going out of Saudi Arabia for their own use. The cash may be carried directly or through cash transportation firms by way of cargo, postal parcels, etc. Banks and money exchangers or their cash transportation firms should adhere to the requirements by completing a special declaration form for any cash shipment about the money to be disclosed, in compliance with a special security safety and SAMA Rules for Cash Transportation issued on 29 April 2007 to Banks and Money Exchangers.
The term wire transfer or funds transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a bank or money exchanger for the purpose of making a amount available to a beneficiary at another bank or money exchanger. The originator and the beneficiary may be the same person/ entity. The transfer could be a cross-border transfer (to/ from a different country) or a domestic transfer (within the same country).

SAMA Account Opening Rules require banks and money exchangers to obtain full information about the originator/ remitter. To enhance the transparency of wire transfers for effective AML/CTF programs, banks and money exchangers should adopt the following measures when executing transfers for their customers:

1. Exercise Enhanced due diligence when processing transfers relating to accounts of Politicians Exposed Persons (PEPs).
2. Not to accept any incoming or outgoing transfers outside Saudi Arabia, for any charity or non-profit organizations, other than permitted entities, in accordance with the rules for opening bank accounts and the general operational rules.
3. When implementing any new electronic fund transfer and payment systems, ensure they are designed with capabilities for preventing and detecting money laundering and terrorist financing transactions. Examples of the new electronic payment methods include prepaid cards, electronic pure/store value cards, mobile payments, internet payment services, etc. Ensure these services are offered only to customers who already have an account or other bank relationship agreement with the bank or money exchanger.
4. Comply with standards of transparency and ensure that the letters of remittances (enclosed with the transfer), sent and received by remitting, receiving and correspondent banks and transfer services companies, include full information about the remitter and the beneficiary, as determined below.
5. Obtain full information about the remitter of outgoing remittances and keep the information in the transfer letter, which should include the following:
   - Remitter’s name.
   - Remitter’s account / membership No.
   - Remitter’s address, if not available, it may be replaced by government ID No. (National ID of citizens, Iqama No. of expatriate and commercial registration No. of companies) or both date and place of birth.
   - The purpose of transfer should be determined in details.
   - Identity information of the transfer beneficiary and as a minimum the ID government identification number issued by the beneficiary’s country.
6. In case of incoming transfers, taking into consideration the applicable procedures of the countries and their financial institutions operating therein, full information must be obtained about the remitter to be attached fully to the transfer letter. Identity information of the beneficiary of the remittance shall be obtained from the remitter. The identity of beneficiary means the government identity card issued by the beneficiary’s country.
7. Taking continuous due diligence in respect of customers.
exporting and import remittances and checking transactions implemented during that relationship to ensure they are complete and compatible with the size of customers activity, including the source of income. Conducting KYC/ due diligence on the remitter/ originator is the responsibility of the remitting bank or money exchanger, whether foreign or local.

8. In case of wire transfers which are not accompanied with full information of remitter, banks and money exchanger operating in the Kingdom shall adopt effective measures, and act against such transfers as follows:

5/1- obtain missing information from the correspondent bank or the company providing transfer services and this applies to all local and international banks.

5/2- reject the transaction and return the remittance in the case the correspondent bank does not respond.

5/3- In case of suspicion in such a transaction and if the correspondent bank does not respond, the case should be reported to the Financial Investigation Unit.

5/4- Document decisions made in writing, including reasons and keep hand and soft copies of records for 10 years in compliance with the rules on anti-money laundering and terrorism financing issued by SAMA.

5/5- Incoming remittance shall include name of the bank, originating country, correspondent bank and the country. Correspondent banks shall comply therewith, and in case of a change in the remitter’s information, the beneficiary bank should be notified thereof.

9. In case of sending cross-border wire transfers by one remitter as part of combined transfer to beneficiaries in another country, all information related to the remitter and accompanied with wire transfer should be inserted with the transfer for each cross-border wire transfer provided that the combined transfer file (in which individual wire transfers are grouped) should have full information about the remitter that can be tracked easily.

10. In situations where technical restrictions prevent sending full information of the remitter that is accompanied with a cross-border wire transfer with local wire transfer linked to it (during the period necessary to adapt payment systems), intermediary financial institutions receiving a transfer shall keep a record containing all information received from the financial institution exporting the transfer for a period of 10 years in compliance with the rules on combating money laundering and terrorist financing issued by SAMA, taking into consideration the commitment for a period no longer than (72 working hours) to respond to any inquiries received from the correspondent bank or the relevant authorities.

11. In case of repetition of lack of information situations, and non-cooperation by transfer originator banks, a correspondent bank or transfer service company, banks and money exchanger operating in the Kingdom should evaluate the relationship with the bank or the company and consider restricting or even ending the relationship therewith.

12. In case of suspecting transactions or relationship with a correspondent bank or transfer services company from the perspective of money laundering or terrorist financing, this must be reported immediately to the FIU, and these cases shall be documented.

13. Prior approval of SAMA shall be taken in the case of
contracting with agents or companies that offer financial transfers services.

14. There should be a possibility for banks and money exchangers operating in the Kingdom and contracting with financial transfer service companies to obtain full information about the parties of financial transfers carried out by such companies on their behalf.

15. The business of the contracted companies providing a remittance service regarding transactions carried out through banks and money exchangers operating in the Kingdom shall be subject to supervision and control by the bank or money exchanger through which those companies operate.

16. During the study of the relationship with a correspondent bank or a financial transfer service company and in case of going to the end of the relationship with them, finding alternative correspondent banks or financial transfer service companies shall be taken into account in order to avoid stopping of the transfer service with the country in question.

17. Monitor relationships with correspondent banks and financial transfer service companies, make sure they are lawful and evaluate the relationship whether the activity of the bank / company and their controls to combat money laundering and terrorist financing and transparency standards are consistent with what have been emphasized at the beginning of the relationship. Correspondent banks and financial transfer service companies shall obtain a certificate to confirm compliance with combating money laundering and terrorist financing on a continuing basis according to the rules of opening bank accounts and the general operational rules issued by SAMA.

18. Compliance with confidentiality of information exchanged between correspondent banks, receiving banks and financial transfer service companies, and is used only for authorized purposes in order to maintain the terms and conditions of banking secrecy and prevent its use for any other purpose.

19. Check names of wire transfer originators and beneficiaries against lists of individuals and entities that their assets should be stopped, refused or frozen based on international lists (e.g. resolutions of the United Nations 1373 and 1267), and take actions thereon.

20. Check names of individuals, entities, banks/financial transfer service companies and originator, intermediary or beneficiary countries against international lists (e.g. UN, OFAC, INTERPOL, FATF, etc...), and take actions thereon.

21. Banks and money exchanger operating in the Kingdom shall apply effective measures in all its business based on the effective measures to ensure fulfillment of KYC and due diligence requirements and relative importance. Extra due diligence for funds transferred from or to countries that do not apply or do not fully apply FATF’s require.

22. Monitor all transactions (incoming and outgoing transfers) to detect the types of unusual activities that do not have a clear legal or economic purpose, check the background of these transactions and their purpose to the maximum extent, and document findings reached in writing.

23. Whenever there are logical reasons to suspect that customers’ money, operations and transactions represent proceeds of criminal activity or have connection or relationship with money laundering or terrorist financing, the FIU shall be informed.

خدمات التحويلات المالية من الحصول على المعلومات الكاملة عن أطراف عمليات
التمويل المالي التي تجري بتلك الشركات مباشرةً نية عمليات.

15. يجب أن تتضمن أعمال الشركات المقدمة خدمات التحويلات المالية المعتمدة معها والمتعلقة بالمعلومات المقدمة من خلال الودائع وحالات الصرف الافتراضي في المملكة
للإشراف ورقابة البنك أو محال الصرف الذي تعمل من خلال تلك الشركات.

16. أثناء دراسة العلاقة بالبنك الممارس أو شركة تقدم خدمات التحويل وفي حال التوجه إلى قطع العلاقة سواء، يجب مراجعة الجهة عنيف بمسؤولية أو شروط تقديم خدمات تحويل بديلة تتطلب تقديم خدمات التحويل والتأكد من نظاميات وثائق العلاقة بالشركة المقابلة أو مالية أو منظمة أخرى تركز على فحص الردود المالية أو مهنة الشركات وتقييم العلاقة وكيفية تقديم خدمات التحويل أو التحويلات إلى الأفراد المحتملين في العلاقة.

17. في حالة عدم قدرة البنك أو شركة تحويلات على اتخاذ الإجراءات اللازمة غر مكافحة غسل الأموال، فإن البنك أو شركة تحويلات ينبغي توقيع الإشارة على القانون لوقف الصرف.

18. قد يتعين على البنك أو الشركة المقابلة أن تأخذ الإجراءات اللازمة حيال ذلك.

19. قد يتضمن الشروط القياسية لرسوم وكليات التحويلات الموالية بقانون البنك أو الشركة المقابلة.

20. على سبيل المثال، فإنا قد نشترط أن يتم تقديم خدمات التحويلات الموالية من خلال شركات الصرافة أو البنوك أو الشركات المدفوعة على الأقران.

21. كما يمكن أن تشمل الشروط الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

22. يمكن أن تتضمن الشروط الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

23. يجب أن تتوفر شروط مالية معينة لإعداد الأعمال أو الخدمات المقدمة بواسطة الشركات المذكورة.

24. في حالة عدم الالتزام بالوائح المصرفية، فإن البنك أو الشركة المقابلة ينبغي أن تتوفر الإجراءات اللازمة.

25. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

26. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

27. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

28. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

29. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

30. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

31. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

32. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

33. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

34. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

35. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

36. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

37. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

38. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

39. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

40. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

41. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

42. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

43. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

44. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

45. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

46. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

47. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

48. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

49. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

50. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

51. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

52. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

53. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

54. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

55. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

56. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

57. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

58. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

59. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

60. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

61. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

62. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

63. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

64. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

65. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

66. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

67. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

68. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

69. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.

70. يمكن أن تشمل الفوائد الأخرى في حالة عدم قدرة البنك أو الشركة المقابلة على اتخاذ الإجراءات اللازمة.
24. In case of receipt of a remittance from outside the Kingdom on behalf of a beneficiary, it shall be paid only by an account or by creating a relationship to ensure obtaining complete information about the beneficiary. A customer can open the account or establish the relationship when he receives the remittance, taking into account the rules for opening and operating accounts issued by SAMA.

25. For domestic transfers (within Saudi Arabia), ensure the remitter's name and account number is included, which should be recorded and retained in the system of remitting bank or money exchanger for prompt retrieval if requested by authorized authorities. Also should be Verify the identity of the beneficiary of a local remittance (incoming) in accordance with the rules for opening bank accounts and the general operational rules.

26. It is not allowed to receive any transfer from a particular country to be passed through one of the banks operating in the Kingdom for a beneficiary in a bank located abroad in any currency other than the Saudi riyal.

27. When receiving a transfer in Saudi riyal from a particular country to be passed through one of the banks operating in the Kingdom for a beneficiary in a bank located outside the Kingdom, the purpose of remittance shall be determined in details.

28. Retain all physical and system records of all funds transfers in accordance with the prevailing record retention periods.

5.1.3 Alternative Remittances

Alternative remittance system refers to a type of financial service involving the transfer of funds or value from one geographic location to another through informal and unlicensed networks or mechanisms, which usually operate outside the regulated conventional financial sector. The very features (efficiency, anonymity and lack of paper trail, low cost, no need to prove identity, and the exchange rate) which make alternative remittance system attractive to customers with legitimate income (mainly expatriates remitting money to relatives in home countries), also make the system convenient for the transfer of illicit funds.

Therefore, due to this inherent risk, these systems have proven themselves vulnerable to misuse for money laundering and especially for terrorist financing purposes. Quite often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms, most common being "Door-to-Door", "Hawala", or "Hundi". In addition to the vulnerability for misuse, unauthorized or unlicensed alternative remittance services are illegal in Saudi Arabia and in violation of the Banking Control Law. Those who practice such activities are subject to legal penalties. Therefore, banks and licensed money exchangers should endeavor to assist authorities in fighting such unlawful activities.

Persons who offer these illegal services, at a certain point, channel their funds in "blocks" through the banking system by cash deposits and then remit the funds to the beneficiary by a transfer, or communication/ message. Therefore, banks and money exchangers should apply prudent measures to identify and prevent the use of customer accounts for this illegal business. While such suspicious transactions may be difficult to monitor, the application of due diligence process and relevant red flags indicators can help in identifying such transactions. As a minimum, banks and money exchangers should implement the following steps:

1. Have a mechanism in place to monitor customer...
The number of banks providing banking services through electronic means is growing considerably, with increasing range of services becoming available, including account services, credit cards, transfers, bill paying services, shares trading, etc. Therefore, electronic banking is vulnerable to money laundering and terrorist financing because of its user.

5.1.5 Electronic Banking

Electronic banking is a broad term encompassing delivery of information, products and services by electronic means (such as telephones/mobiles, internet, automated teller machines, points of sales and automated clearing houses). Electronic banking provides opportunities for banks to offer a variety of their banking products and services in a faster, more convenient and cheaper way.

5.1.4 Money Exchangers

Money Exchange is a regulated business in Saudi Arabia and all money exchangers are subject to the Ministerial Order # 31920 dated 16/2/1402H, which requires all money exchangers to obtain specific license from SAMA. The Ministerial Order prohibits money exchangers from accepting deposits and restricts their activities to purchase and sale of foreign currencies, travelers checks, bank drafts and making remittances inside and outside Saudi Arabia as per the license granted to them by SAMA. The Banking Control Law also prohibits non-banking entities from conducting banking business and, as per authority given, SAMA can impose penalties including revoking of license.

SAMA Account Opening Rules permit banks to open accounts for licensed money exchangers, provided that they have been registered by Ministry of Commerce and licensed by SAMA with a valid licence, specifically indicating that they are allowed to conduct this activity taking into consideration that the license allows cross-border transfers. Therefore, these entities should be categorized as High Risk for an extra customer due diligence and closer scrutiny.

5.1.5 Electronic Banking

Electronic banking is a broad term encompassing delivery of information, products and services by electronic means (such as telephones/mobiles, internet, automated teller machines, points of sales and automated clearing houses). Electronic banking provides opportunities for banks to offer a variety of their banking products and services in a faster, more convenient and cheaper way.

The number of banks providing banking services through electronic means is growing considerably, with increasing range of services becoming available, including account services, credit cards, transfers, bill paying services, shares trading, etc. Therefore, electronic banking is vulnerable to money laundering and terrorist financing because of its user.
5.1.6 International Trade

International trade, which deals in the movement of goods and services, can be used either as a cover for the movement of illicit funds or as the money laundering mechanism itself. Criminals will utilize normal trade-related products and services offered by banks relating to import and export operations, such as letters of credit, guarantees, documentary bills for collection, trade financing services, etc., to legitimize the proceeds of their money laundering activities or to provide funding for terrorist organizations, with a relatively low risk of detection. The techniques used basically are: misrepresentation of the price (over-, under- and multi-invoicing of goods/services), quantity (over- and under-shipments of goods/services), or quality of imports or exports (falsely described goods/services).

Banks should watch out for the following examples of red flag indicators that are commonly used to identify trade-based money laundering activities:

1. Discrepancies between the description of the goods on the invoice and bill of lading.
2. The size of the shipment or the type of goods appears inconsistent with the customer’s regular business activities.
3. The letter of credit amount is unusually large or sudden surge in number of letters of credit issuance that appears to deviate from the customer’s normal business activity.
4. The type of goods being shipped is designated as high risk or involves a high-risk jurisdiction.
5. The transaction involves receipt of payment (especially cash) from third parties with no apparent connection with the transaction.
6. The transaction involves the use of repeatedly amended or frequently extended letter of credit.
7. The transaction involves the use of front (or shell) companies.

5.2 Country/Geographic Risks

Country or geographic risks can be defined as risks posed by countries that are subject to sanctions by United Nations (UN), or warnings have been issued against them by other recognized sources, or if SAMA issues certain instructions about some countries and how to deal with the associated transactions due to one factor or a combination of factors, as determined by UN, FATF or SAMA, such as weak AML/CTF laws, regulations and other measures, and noncompliance with instructions and recommendations issued by said entities, providing funding or support for terrorist activities; or having significant levels of financial criminal activities.

Banks and money exchangers should exercise additional due diligence and pay special attention to business relations and
transactions with persons, including companies and banks working or doing such activities within these countries or regions. In addition to their duties relating to verification of names of persons and entities listed on the various types of lists and alarming data issued by the above mentioned, Banks and money exchangers should take appropriate countermeasures to reduce the risk of dealing with entities existing in the countries and regions that have weaknesses in their procedures regarding combating money laundering and terrorist financing or do not adequately apply the recommendations of the Financial Action Task Force (FATF).

1. Paying particular attention to business and transactions relations with persons (including legal persons and other financial institutions) from or in countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF).

2. Classification of the risk level of all countries indicated by international organizations, for example, without limitation, Financial Action Task Force (FATF), the Security Council or the Committee on Chapter VII of the UN Charter and others, that warning bulletins have been issued thereon in accordance with a specified risk rate of these entities as a minimum for the classification of the organizations. The actions to be taken to monitor transactions or limit the formation of business relationships with financial organizations or persons in these countries.

3. Compliance with the application of information of those organizations, whether the warning issued by the Financial Action Task Force (FATF) or decisions of the Security Council and the Chapter VII Commission of the UN Charter, list of any transactions related thereto, preparation of detailed reports thereon, and follow up what relevant authorities issue and take necessary actions thereon.

4. intensification the customer identification requirements in order to know the identity of the beneficiaries owner before establishing work relationships with individuals or companies from these countries.

5. Immediate suspension of dealing with parties, persons or financial institutions of the countries against which financial prohibition decisions have been issued by Security Council and the Chapter VII Commission of the UN Charter. The suspension shall include all banking operations.

6. Exerting enhanced due diligence when making new dealing agreement or opening accounts for correspondent banks with countries of which warning bulletins were issued, whether by FATF, Security Council or Chapter VII Committee of the UN Charter, and making sure not to include the correspondent bank in domestic lists of penalties and prohibition or those issued by the UN.

7. Making immediate updates for AML/CTF requirements and exerting enhanced due diligence procedures on all banking transactions of related parties in those countries.

8. Classifying all banking businesses and relationships the bank makes with entities relating to countries of which warning bulletins were issued (government relationships, correspondent banks relationships, companies or individuals commercial relationships, resident customers relationships, etc) at risks level consistent with the nature of those businesses, relationships and the risks level of these countries.

9. Verifying that all banking businesses and relationships, which the bank makes with individuals or entities relating to countries of which warning bulletins were

10. To explain the importance of business and transactions relations with persons (including legal persons and other financial institutions) from or in countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF), the Security Council or the Committee on Chapter VII of the UN Charter and others, warning bulletins have been issued thereon in accordance with a specified risk rate of these entities as a minimum for the classification of the organizations.

11. The actions to be taken to monitor transactions or limit the formation of business relationships with financial organizations or persons in these countries.

12. Compliance with the application of information of those organizations, whether the warning issued by the Financial Action Task Force (FATF) or decisions of the Security Council and the Chapter VII Commission of the UN Charter, list of any transactions related thereto, preparation of detailed reports thereon, and follow up what relevant authorities issue and take necessary actions thereon.

13. intensification the customer identification requirements in order to know the identity of the beneficiaries owner before establishing work relationships with individuals or companies from these countries.

14. Immediate suspension of dealing with parties, persons or financial institutions of the countries against which financial prohibition decisions have been issued by Security Council and the Chapter VII Commission of the UN Charter. The suspension shall include all banking operations.

15. Exerting enhanced due diligence when making new dealing agreement or opening accounts for correspondent banks with countries of which warning bulletins were issued, whether by FATF, Security Council or Chapter VII Committee of the UN Charter, and making sure not to include the correspondent bank in domestic lists of penalties and prohibition or those issued by the UN.

16. Making immediate updates for AML/CTF requirements and exerting enhanced due diligence procedures on all banking transactions of related parties in those countries.

17. Classifying all banking businesses and relationships the bank makes with entities relating to countries of which warning bulletins were issued (government relationships, correspondent banks relationships, companies or individuals commercial relationships, resident customers relationships, etc) at risks level consistent with the nature of those businesses, relationships and the risks level of these countries.

18. Verifying that all banking businesses and relationships, which the bank makes with individuals or entities relating to countries of which warning bulletins were
5.3 Risk Variables

A bank’s or money exchanger’s risk-based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include:

1. The purpose of an account or relationship.
2. The level of assets to be deposited in relation to the customer’s profile.
3. The level of regulatory oversight to which a customer is subject.
4. The regularity or duration of the relationship.
5. The familiarity with a country and regulatory structure.

1. The purpose of an account or relationship.
2. The level of assets to be deposited in relation to the customer’s profile.
3. The level of regulatory oversight to which a customer is subject.
4. The regularity or duration of the relationship.
5. The familiarity with a country and regulatory structure.
Account

"Account" should be taken to include, in addition to a bank account, any other similar banking relationships (such as credit card, remittance service relationships, etc.) between the bank or money exchanger and its customer.

Anonymous, Fictitious Name or Numbered Account

Anonymous, Fictitious Name or Numbered Account is generally a bank account for which the customer's name does not appear on the bank's records/systems, documents and statements. Instead, a unique number or code-name is recorded. The customer's identity is known only to a small number of the bank's officials. While such accounts are offered by some banks in the world for a legitimate purpose, such as providing confidentiality and additional protection for private matters, they can also be misused to hide the proceeds of financial crimes.

Beneficial Owner

The natural person who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also includes a person who exercises ultimate effective control over a legal person or arrangement.

Competent Authority

All administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including SAMA and SAFIU.

Enhanced Due Diligence (EDD)

This is an additional due diligence process needed for all High Risk accounts/relationships and where the bank/ME deems it necessary. EDD is needed for PEPS, private banking customers, correspondent banks, non-profit charity organizations, and for other types of customers categorized as high risk by the bank/ME.

Financial Action Task Force (FATF)

It is an international body entitled to oversee AML-CTF efforts. Saudi Arabia is a member of this organization through its membership of the GOC.

Financial Intelligence Unit (FIU)

The UN Convention adopted this definition, stating, "Each state shall consider the establishment of a financial intelligence unit to serve as a national center for the collection, analysis and dissemination of information regarding potential money laundering." Based on the Saudi AML Law of 2003, the Saudi Financial Intelligence Unit was established under the authority of the Ministry of Interior. This is the authority that receives and analyzes suspicious activity reports from all financial & non-financial institutions.

Intermediary

A professional intermediary is a firm or person (such as an accountant, banker, broker, lawyer or similar professional) who manages an account or transacts on behalf of a client.

The customer's identity is known only to a few people (such as an accountant, banker, financial advisor, etc.).

A professional intermediary is a firm or person (such as an accountant, banker, lawyer or similar professional) who manages an account or transacts on behalf of a client.

A professional intermediary is a firm or person (such as an accountant, banker, lawyer or similar professional) who manages an account or transacts on behalf of a client.
Money Exchanger (ME)

A natural or legal person who provides a money/ currency changing service and/ or providing a money/ value transfer/ remittance service. The person must be registered by Ministry of Commerce and licensed by SAMA. These entities are subject to SAMA regulations as per authority given through the Banking Control Law, the AMIL Law (Bylaw 1.1) and the Ministerial Order # 31920.

Nominee

A person or firm (registered owner) into whose name securities or other assets are transferred and held under a custodial agreement in order to facilitate transactions, while leaving the customer as the actual owner (beneficial owner). A "nominee account" is a type of account in which a stockbroker holds shares belonging to clients, making buying and selling those shares easier.

Countries that do not apply or do not fully apply FATF’s requirements

FATF publishes reports and data on countries which do not comply adequately with requirements in the light against money laundering. The list is maintained and updated by FATF and may be consulted on the FATF website. Banks/MEs should give special attention to business relations and transactions with customers from countries included in these reports, and exercise extra due diligence.

Payable-Through Account

This is a demand deposit account maintained at a local bank by a foreign bank or corporation, whereby the foreign bank channels deposits and checks of its customers (usually individuals or businesses located outside the country) into the account. The foreign customers have signing authority over the account and can thereby conduct normal international banking activities. This makes it impossible to implement KYC policy and monitoring of suspicious activity process for the customers using the account.

Shell Bank

Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

Source of Funds

Source of funds is the activity which generates the funds for a relationship, e.g., a customer's occupation or business activities.

Source of Wealth

Source of wealth is different from source of funds, and describes the activities which have generated the total net worth of a person both within and outside of a relationship, that is those activities which have generated a customer's funds and property.

Subsidiaries

This refers to majority owned subsidiaries of a bank or money exchanger, inside or outside the country.

---

Money Laundering

.You provide a service or products that could be used for money laundering.

Client identification

You identify your customers adequately and maintain records of your customers and their transactions.

Customer due diligence

You apply enhanced due diligence measures to high risk customers.

Transaction monitoring

You monitor your financial transactions and maintain records of suspicious activity.

Internal controls

You have effective internal controls to prevent money laundering.

Risk assessment

You assess and manage your money laundering risks.

Customer尽

You identify your customers adequately and maintain records of your customers and their transactions.

Customer due diligence

You apply enhanced due diligence measures to high risk customers.

Transaction monitoring

You monitor your financial transactions and maintain records of suspicious activity.

Internal controls

You have effective internal controls to prevent money laundering.

Risk assessment

You assess and manage your money laundering risks.

Customer 尽
### Suspicious Transaction

A suspicious transaction is one in respect of which a banks/ME has reason to believe that some type of wrongdoing or illegal activity may be involved. Suspicious transactions must be reported to the appropriate authorities through Suspicious Transaction Report (STR). The notifying bank/ME and its employees are free of any blame or charge in respect of any notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.

### Trustee

A person (an individual or entity) who holds and administers the assets in a trust fund separate from the trustee's own assets, for the benefit of another person/s (the beneficiary/ies). The trustee invests and disposes of the assets in accordance with the settlor’s trust agreement, taking into account of any letter of wishes. There may also be a protector, who may have power to veto the trustees’ proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

### Unusual Transaction

An activity or transaction that is inconsistent with or deviates from the expected pattern of activity within a particular customer, or with the normal business activities for the type of product or service offered. Unusual activity or transaction should alert banks to the possibility of suspicious transactions.
### 7. Appendices

<table>
<thead>
<tr>
<th>SN</th>
<th>Topic</th>
<th>Related Website Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Saudi AML Law &amp; Bylaws</td>
<td><a href="http://www.sama.gov.sa">www.sama.gov.sa</a></td>
</tr>
<tr>
<td>B</td>
<td>FATF Recommendations</td>
<td><a href="http://www.fatf-gafi.org/document">www.fatf-gafi.org/document</a></td>
</tr>
<tr>
<td>C</td>
<td>FATF Member Countries</td>
<td><a href="http://www.fatf-gafi.org/pages">www.fatf-gafi.org/pages</a></td>
</tr>
<tr>
<td>D</td>
<td>Basel Committee Standards</td>
<td><a href="http://www.bis.org/publ">www.bis.org/publ</a></td>
</tr>
<tr>
<td>E</td>
<td>UN Security Council Resolutions</td>
<td><a href="http://www.un.org/sc/committees">www.un.org/sc/committees</a></td>
</tr>
<tr>
<td>F</td>
<td>Other Useful Resources &amp; Links</td>
<td><a href="http://www.menafatf.org">www.menafatf.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.customs.gov.sa/Customs">www.customs.gov.sa/Customs</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>لمحة عن الروابط ذات الصلة</th>
<th>المواقع ذات الصلة</th>
</tr>
</thead>
<tbody>
<tr>
<td>النظم العربي لمكافحة غسل الأموال ويلائحته التنفيذية.</td>
<td><a href="http://www.fatf-gafi.org/document">www.fatf-gafi.org/document</a></td>
</tr>
<tr>
<td>التوصيات الصادرة عن مجموعة العمل المالي (فاتف)</td>
<td><a href="http://www.fatf-gafi.org/pages">www.fatf-gafi.org/pages</a></td>
</tr>
<tr>
<td>الدول الأعضاء في مجموعة العمل المالي (فاتف)</td>
<td><a href="http://www.un.org/sc/committees">www.un.org/sc/committees</a></td>
</tr>
<tr>
<td>معايير لجنة بازل</td>
<td><a href="http://www.bis.org/publ">www.bis.org/publ</a></td>
</tr>
<tr>
<td>قرارات مجلس الأمن - الأمم المتحدة</td>
<td><a href="http://www.un.org/sc/committees">www.un.org/sc/committees</a></td>
</tr>
<tr>
<td>مصادر وروابط أخرى مفيدة</td>
<td><a href="http://www.menafatf.org">www.menafatf.org</a> <a href="http://www.customs.gov.sa/Customs">www.customs.gov.sa/Customs</a></td>
</tr>
</tbody>
</table>
نموذج تقرير المعاملات المشتبه بها

<table>
<thead>
<tr>
<th>رقم المرجع</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>التاريخ</td>
<td></td>
</tr>
<tr>
<td>الموافق لـ:</td>
<td></td>
</tr>
</tbody>
</table>

الملاحظات

<table>
<thead>
<tr>
<th>اسم المؤسسة</th>
<th>مؤسسة غير مالية</th>
</tr>
</thead>
<tbody>
<tr>
<td>إسم البنك أو محل الصرافة (المصرف)</td>
<td>مؤسسة مالية (بنك أو محل الصرافة)</td>
</tr>
<tr>
<td>رقم الهاتف</td>
<td>رقم الهاتف</td>
</tr>
<tr>
<td>المدينة</td>
<td>الفرع</td>
</tr>
<tr>
<td>الفرع</td>
<td>المدينة</td>
</tr>
</tbody>
</table>

معلومات عن الجهة المبلغة

<table>
<thead>
<tr>
<th>مؤسسة غير مالية</th>
<th>مؤسسة مالية (بنك أو محل الصرافة)</th>
</tr>
</thead>
<tbody>
<tr>
<td>إسم المؤسسة</td>
<td>إسم البنك أو محل الصرافة (المصرف)</td>
</tr>
<tr>
<td>المدينة</td>
<td>الفرع</td>
</tr>
<tr>
<td>الفرع</td>
<td>المدينة</td>
</tr>
</tbody>
</table>

محتويات التقرير

<table>
<thead>
<tr>
<th>نوع النشاط/المعاملة</th>
<th>إيداع</th>
<th>التحويل</th>
<th>الشيك</th>
<th>الصراف الآلي</th>
</tr>
</thead>
<tbody>
<tr>
<td>التاريخ</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>الوقت</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>الجهة المبلغة</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>المبلغ الإجمالي</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>بالأحرف</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>بالأرقام</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>اسم الفرع</th>
<th>رقم الحساب</th>
</tr>
</thead>
<tbody>
<tr>
<td>إسم المستفيد</td>
<td>رقم الحساب</td>
</tr>
<tr>
<td>البنك</td>
<td></td>
</tr>
</tbody>
</table>

أسباب الإشتباه

<table>
<thead>
<tr>
<th>مطلب تكرير حجم المنطقة</th>
<th>المستفيد</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>اسم المستفيد</th>
<th>الجنس</th>
<th>رقم بطاقة الهوية</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>اسم</th>
<th>البلد</th>
<th>الجنسية</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>اسم المستفيد</th>
<th>رقم الفرع</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

تجدون أعلاه تقرير المعاملات المشتبه بها الذي تعرضه عليكم للمراجعة واتخاذ القرار المناسب بشأنه.

التوقيع:                                                                                                           

الختم الرسمي:
APPENDIX (8)

Suspicious Transaction Report

Confidential

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Date</th>
<th>Corresponding</th>
<th>Annexes</th>
</tr>
</thead>
</table>

**Reporting Party Information**

<table>
<thead>
<tr>
<th>Financial Institution (Bank or Money Exchanger)</th>
<th>Bank or ME Name</th>
<th>City</th>
<th>Branch</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Financial Institution</td>
<td>Institution Name</td>
<td>City</td>
<td>Branch</td>
<td>Phone Number</td>
</tr>
</tbody>
</table>

**Report Contents**

<table>
<thead>
<tr>
<th>Activity/Transaction Type</th>
<th>Deposit</th>
<th>Withdrawal</th>
<th>Transfer</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check</td>
<td>Branch</td>
<td>ATM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Execution Date</td>
<td>Time</td>
<td>Day</td>
<td>Date</td>
<td>Month / Year</td>
</tr>
<tr>
<td>Total Amount</td>
<td>In Figures</td>
<td>In Words</td>
<td>Currency Type</td>
<td></td>
</tr>
<tr>
<td>Transaction Executor</td>
<td>Account Number</td>
<td>Branch Name/ No.</td>
<td>Bank</td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Beneficiary**

<table>
<thead>
<tr>
<th>Name</th>
<th>ID Number</th>
<th>Nationality</th>
<th>Country</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Number</td>
<td>Branch Name/ No.</td>
<td>Beneficiary Bank</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please find above our Suspicious Transaction Report for your review and taking the appropriate decision.

Official Seal: ____________________________
Signature: ____________________________
نموذج الإقرار النقدي

المملكة العربية السعودية
وزارة المالية
الجمارك السعودية

الساعة:
التاريخ:

يعتبر هذا النموذج لكل شخص يملك بحوزته مبلغ 300,000 ريال سعودي أو أكثر أو ما يعادله.

<table>
<thead>
<tr>
<th>الاسم الكامل:</th>
<th>الجنسية:</th>
</tr>
</thead>
<tbody>
<tr>
<td>تاريخ الولادة:</td>
<td></td>
</tr>
<tr>
<td>رقم جواز السفر:</td>
<td></td>
</tr>
<tr>
<td>تاريخ ومكان الإصدار:</td>
<td></td>
</tr>
</tbody>
</table>

العنوان في المملكة العربية السعودية ورقم الهاتف:
البلد القادمة منه:
البلد المتوّجه إليه:
اسم المطار/ المرفأ/ الحدود:
رقم الرحلة:

العملة / المعادن الثمينة

<table>
<thead>
<tr>
<th>عملة:</th>
</tr>
</thead>
</table>
| قيمتها بالريل:

الذهب: 
المجوهرات الأخرى: 
معادل القيمة بالريل: 
 المصدر/الغرام من المعادن الثمينة/المعادن الثمينة:

إعداد المسافر:

التاريخ: 
لاستخدام الرسمي

الإسم الموظف: 
الرقم: 
التاريخ: 

ان عدم الإقرار يعرضك للإستحوبي القانوني.
# APPENDIX 9

## Cash Declaration Form

**Kingdom of Saudi Arabia**  
**Ministry of Finance**  
**Saudi Customs**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>This form is required to be filled out by whoever having in his possession SR60,000 or more or its equivalent.</strong></th>
</tr>
</thead>
</table>

**Full Name:**  
______________________________________________

**Nationality:** ..................  
**Date of Birth:** ..................  

**Passport No.:**  
______________________________________________

**Place & Date of Issue:**  
______________________________________________

**KSA Address & Tel. No.:**  
______________________________________________

**Purpose of Travel:**  
______________________________________________

**Arriving from:** ..................  
**Departing to:** ..................  

**Name of the Airport/Seaport/Crossing Border:**  
______________________________________________

**Flight No.:**  
______________________________________________

### Currency / Precious Metals

**Currency Type:**  
______________________________________________

**Amount in Riyals:**  
______________________________________________

**Metals:**  
\[ \square \text{Gold} \quad \square \text{Diamond} \quad \square \text{Other Jewelries} \]  

**The Equivalent in Riyals:**  
______________________________________________

**Source/Purpose of cash amounts/precious metals:**  
______________________________________________

---

I hereby acknowledge that the information declared above is correct and I shall be criminally responsible for any mis-declaration.

**Traveler Signature:** ..................  
**Date:** ..................  

---

### Official Use

<table>
<thead>
<tr>
<th><strong>Employee Name:</strong></th>
<th><strong>No.:</strong></th>
<th><strong>Signature:</strong></th>
<th><strong>Date:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Not declaring will expose you to legal questioning.**
10. Red Flag Indicators

A. Key Indicators of Regulatory & Legal Weakness (High Risk Geographies)

Money launderers can exploit any country or a geographical region that has weaknesses in its legal and regulatory framework and those involved in financing terrorism and can become a center for money laundering and terrorist financing. As money-laundering and terrorist financing transactions normally require a significant period to complete their stages, money launderers and terrorism financiers often focus on countries with serious shortcomings in their laws and procedures to base their operations.

The existence of the following weaknesses in the legislation of a country can generally create an environment that is conducive for money laundering and terrorist financing transactions to penetrate its banking system:

- Adopting and applying strict banking secrecy laws, thus hindering the flow of information from money-laundering transactions.
- Countries that have lax requirements for the formation and registration of companies and permit the use of bearer shares.
- Absence of any foreign exchange controls on incoming and outgoing funds.
- Countries that do not require or apply strict "Know Your Customer" principles, thus facilitating the opening of untraceable numbered accounts or accounts with fictitious names.
- Facilitating the issuance of financial instruments payable to bearers by banks.
- Countries in which money laundering and terrorist financing is not considered a crime.
- Countries that do not require banks/MEs to notify the concerned authorities of large or unusual fund transfers.
- Countries that do not necessitate notification of suspicious transactions to the concerned authorities.
- Absence of confiscation regulations, or lax enforcement or even non-enforcement of such regulations if they exist.
- Countries that have significant dealings in outgoing foreign draft transfers of cash instruments.
- Countries that have international markets in precious metals and where it is easy to transact such trades.
- Countries that permit the free trading of the U.S. Dollar and particularly where banks are allowed to accept dollar deposits.
- Countries that have banking control laws that facilitate the establishment of banks/MEs particularly in free trade zones where supervisory controls or banking regulations are lax or non-existent.

The classification of an account as high-risk based on the geography of where the customer conducts its business activities depends on whether or not the country is on the FATF list. Since the list keeps on changing, reference should be made to FATF website.

The following are the key indicators of regulatory and legal weaknesses in countries:

- Adopting and applying strict banking secrecy laws, thus hindering the flow of information from money-laundering transactions.
- Countries that have lax requirements for the formation and registration of companies and permit the use of bearer shares.
- Absence of any foreign exchange controls on incoming and outgoing funds.
- Countries that do not require or apply strict "Know Your Customer" principles, thus facilitating the opening of untraceable numbered accounts or accounts with fictitious names.
- Facilitating the issuance of financial instruments payable to bearers by banks.
- Countries in which money laundering and terrorist financing is not considered a crime.
- Countries that do not require banks/MEs to notify the concerned authorities of large or unusual fund transfers.
- Countries that do not necessitate notification of suspicious transactions to the concerned authorities.
- Absence of confiscation regulations, or lax enforcement or even non-enforcement of such regulations if they exist.
- Countries that have significant dealings in outgoing foreign draft transfers of cash instruments.
- Countries that have international markets in precious metals and where it is easy to transact such trades.
- Countries that permit the free trading of the U.S. Dollar and particularly where banks are allowed to accept dollar deposits.
- Countries that have banking control laws that facilitate the establishment of banks/MEs particularly in free trade zones where supervisory controls or banking regulations are lax or non-existent.

The following are the key indicators of regulatory and legal weaknesses in countries:

- Adopting and applying strict banking secrecy laws, thus hindering the flow of information from money-laundering transactions.
- Countries that have lax requirements for the formation and registration of companies and permit the use of bearer shares.
- Absence of any foreign exchange controls on incoming and outgoing funds.
- Countries that do not require or apply strict "Know Your Customer" principles, thus facilitating the opening of untraceable numbered accounts or accounts with fictitious names.
- Facilitating the issuance of financial instruments payable to bearers by banks.
- Countries in which money laundering and terrorist financing is not considered a crime.
- Countries that do not require banks/MEs to notify the concerned authorities of large or unusual fund transfers.
- Countries that do not necessitate notification of suspicious transactions to the concerned authorities.
- Absence of confiscation regulations, or lax enforcement or even non-enforcement of such regulations if they exist.
- Countries that have significant dealings in outgoing foreign draft transfers of cash instruments.
- Countries that have international markets in precious metals and where it is easy to transact such trades.
- Countries that permit the free trading of the U.S. Dollar and particularly where banks are allowed to accept dollar deposits.
- Countries that have banking control laws that facilitate the establishment of banks/MEs particularly in free trade zones where supervisory controls or banking regulations are lax or non-existent.

The following are the key indicators of regulatory and legal weaknesses in countries:

- Adopting and applying strict banking secrecy laws, thus hindering the flow of information from money-laundering transactions.
- Countries that have lax requirements for the formation and registration of companies and permit the use of bearer shares.
- Absence of any foreign exchange controls on incoming and outgoing funds.
- Countries that do not require or apply strict "Know Your Customer" principles, thus facilitating the opening of untraceable numbered accounts or accounts with fictitious names.
- Facilitating the issuance of financial instruments payable to bearers by banks.
- Countries in which money laundering and terrorist financing is not considered a crime.
- Countries that do not require banks/MEs to notify the concerned authorities of large or unusual fund transfers.
- Countries that do not necessitate notification of suspicious transactions to the concerned authorities.
- Absence of confiscation regulations, or lax enforcement or even non-enforcement of such regulations if they exist.
- Countries that have significant dealings in outgoing foreign draft transfers of cash instruments.
- Countries that have international markets in precious metals and where it is easy to transact such trades.
- Countries that permit the free trading of the U.S. Dollar and particularly where banks are allowed to accept dollar deposits.
- Countries that have banking control laws that facilitate the establishment of banks/MEs particularly in free trade zones where supervisory controls or banking regulations are lax or non-existent.
B. Businesses Prone to Money Laundering Activities

Money laundering and terrorist financing can adopt a variety of disguises, but there are certain types of businesses, which are more attractive to criminals. There is also a tendency to use countries that have adopted strict secrecy laws for banks and for companies, which make it difficult to obtain sufficient information to understand the nature and type of business activities being undertaken by these organizations.

The following guidance provides an insight into what those businesses might be.

<table>
<thead>
<tr>
<th>Type of Business</th>
<th>What to Look For</th>
<th>Types of Businesses Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import/Export Businesses</strong></td>
<td>If there are unusual transactions out of line with the usual pattern of import/export, and where the transactions are conducted through a variety of countries (not necessarily a regular customer base).</td>
<td>Potentially any business.</td>
</tr>
<tr>
<td><strong>Travel Agencies</strong></td>
<td>Payments to countries with a weak link in their financial system with a pattern of international payments.</td>
<td>Potentially any business.</td>
</tr>
<tr>
<td><strong>Financial Institutions (Non-Bank)</strong></td>
<td>If there is an unusual pattern of transactions, such as large payments or deposits, or if there is a pattern of international transactions.</td>
<td>Potentially any business.</td>
</tr>
<tr>
<td><strong>Shell Corporations</strong></td>
<td>If there is a pattern of international transactions, or if there is a pattern of international transactions with a limited number of countries.</td>
<td>Potentially any business.</td>
</tr>
<tr>
<td><strong>Businesses Prone to Money Laundering Activities</strong></td>
<td>Payments to countries with a weak link in their financial system with a pattern of international payments.</td>
<td>Potentially any business.</td>
</tr>
</tbody>
</table>

Note: These are general guidelines and may vary depending on the specific circumstances and location.
Precious Commodities

The placement of cash, but more usually layering can be facilitated within businesses where large value transactions are common, and the commodities traded are difficult to value objectively, thereby allowing inflated values to be used to support requests for payments.

Types of business covered: Precious Metals, Jewel Store; Antique Shops and Fine Art Galleries.

What to look for: Trading patterns with countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF).” not normally associated with the commodity in question; unusual fluctuations in turnover or types of financial instruments used.

Cash Driven Businesses

The types of business that normally accept cash are useful to the launderer at the placement stage, and could be used for layering purposes.

Types of businesses covered: Used Car Dealers; Garages; Corner Shops (especially those in some countries who offer check encashment facilities); Electrical Good Stores; Leather Goods Shops; Building & Garden Supplies; Builders or Decorators.

What to look for: Increases in cash deposits which do not seem to be matched by an increase in business; the maintenance of cash flow levels when business is falling off, unusual payment patterns from cash deposits seemingly unrelated to the business activities.

Offshore Financial Services

Many of the laundering or terrorist financing operations, which have been uncovered, have involved the transfer of funds through offshore financial service companies to layer transactions and provide anonymity. As there is no underlying business against which to test the commercial basis for a transaction it is extremely difficult to detect “unusual” or “suspicious” transaction patterns.

Type of businesses covered: Trust Companies; Commodity Traders, Financial Advisers.

What to look for: Small operations that appear to have only one or two clients; unusually complex ownership structures; lack of interest in costs incurred when processing transactions; links with countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF) investing in instruments that carry anonymity (e.g. bearer bonds) when uneconomic to do so.

Charitable or Non-Profit Organizations

When opening an account for a Charitable or Non-profit Organization, valid authorization from the appropriate government agencies and SAMA must be obtained.

C. Key Indicators of MLTF Transactions & Activities (High Risk Products/Services)

The purpose of this section is to increase the understanding of Bank/ME employees in order to help them in identifying money laundering and terrorist financing transactions. The existence of one or more of these indicators does not necessarily mean that a money laundering or terrorist financing transaction is taking place but it should raise some concerns and lead to further investigation.

These indicators are not exhaustive and should be taken by Bank/ME employees for guidance purposes only. Bank/ME employees should depend on their experience, skills and expertise to make a sound judgment on suspected money laundering or terrorist financing transactions, when in doubt, contact the MLCU.
### General Indicators
- A transaction whose general form is indicative of illegitimate or unknown purposes.
- Existence of movements in the customer's account not related to his activities such as:
  - Continuous cash deposits in other companies and establishment accounts.
  - Unusual purchase of cashier checks and payment orders against cash.
  - Withdrawal of cash amounts after a short-term deposit.
  - Large deposits of checks, incoming drafts and payment orders that are inappropriate to the nature of customer's activity.
  - Large withdrawals or deposits inconsistent with customer's activities.
  - Transfers for unknown objectives, which do not adhere to the activity of the company its subsidiaries or branches.
- Existence of a large number of deposits of small amounts, whether in cash, by check or by incoming draft whose total or approximate total amount deposited, is then transferred to another city or country in one transaction.

### Bank Accounts
- Opening of more than one account by a customer in his name in the same bank without any clear reason, and existence of inter-account transfer among these accounts.
- Accounts opened in names of Tellers in the bank who receive regular deposits or periodic incoming drafts.
- Payments or transfers by many persons to a single account whether in cash or through internal drafts.
- Opening by a customer of more than one account in the name(s) of his family members and being authorized to manage these accounts on their behalf.
- Opening an account by a customer without him physically appearing in the bank or even being known to bank employees or ever visiting the branch for long periods of time.
- The existence of bank accounts with address outside the geographical region of the bank.
- Existence of large number of movements of big amounts in the account while the balance is kept low or fixed.
- Opening of many accounts by the customer with normal balances while the total represents a big amount.
- Current or savings account used only to receive incoming drafts from outside in a continuous manner without any justifiable reasons.

### Credit Activities
- Unexpected settlement by the customer, of a loan due without disclosing the source of the funds.
- Obtaining a loan or credit facilities against guarantees issued by a bank operating outside the Kingdom without a clear commercial reason.
- Submittal by the customer, of company's shares of which the bank is unable to confirm its business activities, or as a guarantee for obtaining the loan or credit facilities.

### Teller Transactions
- Frequent cash deposits by the customer of dirty or excessively used notes.
- Cash deposits of large amounts whose source is apparently one of the banks in the same region.
- Exchange of a large cash amount consisting of small-denominated notes to the same amount and currency, in bigger denominated notes.
- Purchase of cashiers check or precious metals in large amounts.
- Transfer of an amount outside of the country without any clear reason.
- Deposit of a large number of check or cash amounts by the customer or by other customers without any withdrawals.

### Takaful and Insurance
- Existence of a large number of deposits of small amounts, whether in cash, by check or by incoming draft whose total or approximate total amount deposited, is then transferred to another city or country in one transaction.

### Credit Activities
- Large deposits of checks, incoming drafts and payment orders that are inappropriate to the nature of customer's activity.
- Large withdrawals or deposits inconsistent with customer's activities.
- Transfers for unknown objectives, which do not adhere to the activity of the company its subsidiaries or branches.
- Existence of a large number of deposits of small amounts, whether in cash, by check or by incoming draft whose total or approximate total amount deposited, is then transferred to another city or country in one transaction.

### Teller Transactions
- Frequent cash deposits by the customer of dirty or excessively used notes.
- Cash deposits of large amounts whose source is apparently one of the banks in the same region.
- Exchange of a large cash amount consisting of small-denominated notes to the same amount and currency, in bigger denominated notes.
- Purchase of cashiers check or precious metals in large amounts.
- Transfer of an amount outside of the country without any clear reason.
- Deposit of a large number of check or cash amounts by the customer or by other customers without any withdrawals.

### Bank Accounts
- Opening of more than one account by a customer in his name in the same bank without any clear reason, and existence of inter-account transfer among these accounts.
- Accounts opened in names of Tellers in the bank who receive regular deposits or periodic incoming drafts.
- Payments or transfers by many persons to a single account whether in cash or through internal drafts.
- Opening by a customer of more than one account in the name(s) of his family members and being authorized to manage these accounts on their behalf.
- Opening an account by a customer without him physically appearing in the bank or even being known to bank employees or ever visiting the branch for long periods of time.
- The existence of bank accounts with address outside the geographical region of the bank.
- Existence of large number of movements of big amounts in the account while the balance is kept low or fixed.
- Opening of many accounts by the customer with normal balances while the total represents a big amount.
- Current or savings account used only to receive incoming drafts from outside in a continuous manner without any justifiable reasons.

### Credit Activities
- Unexpected settlement by the customer, of a loan due without disclosing the source of the funds.
- Obtaining a loan or credit facilities against guarantees issued by a bank operating outside the Kingdom without a clear commercial reason.
- Submittal by the customer, of company's shares of which the bank is unable to confirm its business activities, or as a guarantee for obtaining the loan or credit facilities.

### Teller Transactions
- Frequent cash deposits by the customer of dirty or excessively used notes.
- Cash deposits of large amounts whose source is apparently one of the banks in the same region.
- Exchange of a large cash amount consisting of small-denominated notes to the same amount and currency, in bigger denominated notes.
- Purchase of cashiers check or precious metals in large amounts.
- Transfer of an amount outside of the country without any clear reason.
- Deposit of a large number of check or cash amounts by the customer or by other customers without any withdrawals.

### Bank Accounts
- Opening of more than one account by a customer in his name in the same bank without any clear reason, and existence of inter-account transfer among these accounts.
- Accounts opened in names of Tellers in the bank who receive regular deposits or periodic incoming drafts.
- Payments or transfers by many persons to a single account whether in cash or through internal drafts.
- Opening by a customer of more than one account in the name(s) of his family members and being authorized to manage these accounts on their behalf.
- Opening an account by a customer without him physically appearing in the bank or even being known to bank employees or ever visiting the branch for long periods of time.
- The existence of bank accounts with address outside the geographical region of the bank.
- Existence of large number of movements of big amounts in the account while the balance is kept low or fixed.
- Opening of many accounts by the customer with normal balances while the total represents a big amount.
- Current or savings account used only to receive incoming drafts from outside in a continuous manner without any justifiable reasons.

### Credit Activities
- Unexpected settlement by the customer, of a loan due without disclosing the source of the funds.
- Obtaining a loan or credit facilities against guarantees issued by a bank operating outside the Kingdom without a clear commercial reason.
- Submittal by the customer, of company's shares of which the bank is unable to confirm its business activities, or as a guarantee for obtaining the loan or credit facilities.

### Teller Transactions
- Frequent cash deposits by the customer of dirty or excessively used notes.
- Cash deposits of large amounts whose source is apparently one of the banks in the same region.
- Exchange of a large cash amount consisting of small-denominated notes to the same amount and currency, in bigger denominated notes.
- Purchase of cashiers check or precious metals in large amounts.
- Transfer of an amount outside of the country without any clear reason.
- Deposit of a large number of check or cash amounts by the customer or by other customers without any withdrawals.

### Bank Accounts
- Opening of more than one account by a customer in his name in the same bank without any clear reason, and existence of inter-account transfer among these accounts.
- Accounts opened in names of Tellers in the bank who receive regular deposits or periodic incoming drafts.
- Payments or transfers by many persons to a single account whether in cash or through internal drafts.
- Opening by a customer of more than one account in the name(s) of his family members and being authorized to manage these accounts on their behalf.
- Opening an account by a customer without him physically appearing in the bank or even being known to bank employees or ever visiting the branch for long periods of time.
- The existence of bank accounts with address outside the geographical region of the bank.
- Existence of large number of movements of big amounts in the account while the balance is kept low or fixed.
- Opening of many accounts by the customer with normal balances while the total represents a big amount.
- Current or savings account used only to receive incoming drafts from outside in a continuous manner without any justifiable reasons.

### Credit Activities
- Unexpected settlement by the customer, of a loan due without disclosing the source of the funds.
- Obtaining a loan or credit facilities against guarantees issued by a bank operating outside the Kingdom without a clear commercial reason.
- Submittal by the customer, of company's shares of which the bank is unable to confirm its business activities, or as a guarantee for obtaining the loan or credit facilities.

### Teller Transactions
- Frequent cash deposits by the customer of dirty or excessively used notes.
- Cash deposits of large amounts whose source is apparently one of the banks in the same region.
- Exchange of a large cash amount consisting of small-denominated notes to the same amount and currency, in bigger denominated notes.
- Purchase of cashiers check or precious metals in large amounts.
- Transfer of an amount outside of the country without any clear reason.
- Deposit of a large number of check or cash amounts by the customer or by other customers without any withdrawals.

### Bank Accounts
- Opening of more than one account by a customer in his name in the same bank without any clear reason, and existence of inter-account transfer among these accounts.
- Accounts opened in names of Tellers in the bank who receive regular deposits or periodic incoming drafts.
- Payments or transfers by many persons to a single account whether in cash or through internal drafts.
- Opening by a customer of more than one account in the name(s) of his family members and being authorized to manage these accounts on their behalf.
- Opening an account by a customer without him physically appearing in the bank or even being known to bank employees or ever visiting the branch for long periods of time.
- The existence of bank accounts with address outside the geographical region of the bank.
- Existence of large number of movements of big amounts in the account while the balance is kept low or fixed.
- Opening of many accounts by the customer with normal balances while the total represents a big amount.
- Current or savings account used only to receive incoming drafts from outside in a continuous manner without any justifiable reasons.
a loan or credit facilities.

- Submittal, by unknown parties to the bank, of additional guarantees in favor of the customer such as the mortgage of assets or warranties while the bank is unable to define the relationships with the customer or existence of justified reason for such guarantees.
- The bank grants loans to customers having deposit accounts in foreign banks in a country having strict banking secrecy laws.
- A bank granting loans to foreign companies without a justifiable business reason.
- A customer receives a loan and immediately requests the loan amount to be transferred to other bank(s).
- Use of credit facilities given to the customer for purposes other than that mentioned in the loan application.

Drafts

- The amount of draft does not fit with the physical appearance of the sender or the nature of his commercial activity.
- The customer's intentional misrepresentation of information given to the bank.
- Frequent transfers of large amounts against check under clearing or not cleared.
- Incoming drafts used immediately to purchase financial instruments such as (certificates of deposit, cashier check, etc.) in favor of other parties.
- Continuous purchase of bank drafts by customers.
- Frequent deposits by a customer of cashier's check issued by foreign banks into his account.

Customer

- Customers who avoid identifying themselves while attempting to process account transactions or even providing incorrect or incomplete information.
- The customer attempts to transfer a large amount and then withdraws this application because of the fear of the bank/ME notifying law enforcement authorities.
- The customer tries to influence the bank/ME employee not to inform the authorities about a transaction being processed.
- The customer refrains from providing information about his previous and current commercial activities and banking relationships and transactions.
- The bank/ME employee is suspicious of the customer's identification documentation.
- A customer who opens an account without having a local address or a person to verify his or her identity.
- The customer gives special instructions to process his transactions by fax or telex without a justified reason to use this communications method.
### Accounts

- An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organization and that shows movements of funds above the expected level of income.

### D. Terrorist Financing Indicators

<table>
<thead>
<tr>
<th>Banks &amp; ME's Personnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>An employee whose standard of living is not commensurate with his salary.</td>
</tr>
<tr>
<td>An employee who works for very long periods without requesting vacations or having any sick days.</td>
</tr>
<tr>
<td>The connection of an employee with many suspicious transactions while performing his or her duties.</td>
</tr>
<tr>
<td>The employee attempts to facilitate rendering a banking service to customer (individual or company) without applying normal internal banking procedures.</td>
</tr>
<tr>
<td>Changes in Branch Transactions</td>
</tr>
<tr>
<td>Overriding or not implementing the bank’s/ME’s internal control directives or intentional non-compliance with the bank’s policies and procedures by an employee.</td>
</tr>
<tr>
<td>Increase of money in circulation in large cash denominations that do not match with the nature of work, transactions or location of the branch.</td>
</tr>
<tr>
<td>Material change in the volume of branch transactions with one or more correspondent banks.</td>
</tr>
<tr>
<td>Unusual increase of the volume of drafts issued by a branch or a significant increase in its cash holdings.</td>
</tr>
<tr>
<td>An increase of cashier’s check or payment orders sold to Walk-in customers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Moaylight of the banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>An account opened in the name of a legal entity, a foundation or an association, whose activities are related to the aim of the association or foundation.</td>
</tr>
</tbody>
</table>

### Accounts

- Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate financial background through which additional fraudulent activities may be carried out.
- A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.
- When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.
- An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).
- An account opened by a legal entity or an organization that has the same address as other legal entities or organizations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.)
- An account opened in the name of a recently formed legal entity and in which the opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.
- An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organization.
- An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organization and that shows movements of funds above the expected level of income.
• Deposits for a business entity in combinations of monetary instruments that are a typical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security check).

• Large cash withdrawals made from a business account not normally associated with cash transactions.

• Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in check or other payment instruments.

• Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

• Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

• The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

• The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

• The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

• The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

---

**Wire Transfers**

• Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

• Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

• Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

• Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

• Characteristics of the customer or his/her business activities.

• Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals from the same origin from countries of specific concern acting on behalf of similar business types.

• Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation for example, student, unemployed, self-employed, etc.

• Stated occupation of the transaction is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

• Regarding non-profit or charitable organizations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

• A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

• Frequent transfers of amounts to other banks without mentioning the name of the beneficiary.

• The amount of draft does not fit with the physical appearance of the sender or the nature of his commercial activity.

• Frequent transfers of large amounts to and from countries known to be financial centers.
SAMA RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST FINANCING

a source for drugs

- Fragmenting a large amount into smaller amounts upon transfer.
- Frequent transfers to banks in countries known with strict banking secrecy laws.
- Cash transfers in large amounts.
- Deposits in different accounts and then consolidating these amounts in one account and then transferring the total amount outside of the Kingdom.
- Requests by the customer to the bank to transfer amounts to foreign banks against incoming drafts to the same account with equivalent amounts.

Transaction Linked to Locations of Concern

- Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF).
- Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF).
- A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is through or from locations of specific concern.
- The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.
- A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.
- The opening of accounts of financial institutions from locations of specific concern.

- حصول تحاويل متهاكمة لمبالغ ضخمة إلى ومن البلدان المعروفة بكونها مصدرًا للمخدرات.
- تجزئة كميات كبيرة من الأموال إلى مبالغ صغيرة عند إجراء التحويل.
- حصول تحاويل متكررة إلى البنوك الجارة في البلدان التي تطبق قوانين صارمة في مجال السياسة المصرفية.
- حصول تحاويل متكررة لمبالغ ضخمة.
- وضع ودفع بมากๆات مختلفة، ثم ضمه إلى حساب واحد قبل تحويل المبلغ الإجمالي إلى الخارج.
- طلب العمل من البنك تحويل مبالغ إلى بنوك أجنبية مقابل حوالة واردات إلى الحساب نفسه بقيمة معادلة.

العمليات المرتبطة بمواقع تبثت على القلق:

- العمليات التي تعتمد على مبادلات العملات الأجنبية تتبعها بعد فترة قصيرة حوالات برقية لمواقع تبثت على القلق بشكل خاص (كانت من المستهدفة المحددة من قبل السلطات القانونية أو الكيانات المدرجة في البيانات الحذيرية لمجموعة العمل المالية).
- عمليات إيداع تتم بعد فترة وجيزة مبالغ مالية خصوصًا تلك التي تتم إلى أو من داخل موقع يبعث على القلق بشكل خاص (كانت من المستهدفة المحددة من قبل السلطات القانونية أو الكيانات المدرجة في البيانات الحذيرية لمجموعة العمل المالية).
- حساب تجاري ينفع عليه عدد كبير من الحوالة اليدوية الواردة أو الصادرة ولا يبدو أن هناك غرض تجاري أو اقتصادي طبيعي لها خصوصًا عندما تتم هذه العمليات إلى أو من خلال موقع تبثت على القلق بشكل خاص.
- استخدام عدد من الحوامل لتجميع الأموال ومن ثم تحويل المبالغ لعدد صغير من الأجانب سواء كانوا أفراد أو مؤسسات تجارية خصوصًا إذا كانوا في مناطق تبثت على القلق.
- حصول التهم على أداء التماسك أو إجراء عمليات مالية تجارية تضمن تحريك الأموال من أو إلى مواقع تبثت على القلق بشكل خاص في غياب أي أسباب تجارية منطقة للاستعمال مع تلك المواقع.
- فتح حسابات لمؤسسات مالية من مناطق تبثت على القلق بشكل خاص.