A brief on Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 and Guidelines
A brief on Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 and Guidelines


These regulations would repeal Circular No. 28 of 2017 dated 16 November 2017, Circular No 12 dated 28 April 2009, Circular No 29 of 2009 dated 9 September 2009 respectively; and (3) SRO 20(1)/2012 dated 11 January 2012.

The OBJECTIVE

The Objective of these Regulations is to identify, prevent, report and investigate money laundering (ML) and Terrorism Financing (TF) activities and take precautions to alleviate the risk of ML and TF. This brief explains the scope and requirements of Anti Money Laundering and Countering Financing of Terrorism Regulations [“AML/CFT”] laws and Financial Action Task Force [“FATF”] recommendations and providing a high-level approach to fulfill these AML and CFT requirements effectively.

APPLICABILITY

These Regulations shall apply to all Securities brokers, Futures brokers, Insurers, Takaful Operators, NBFCs and Modarabas (hereinafter referred to as [“Regulated Persons”] or [“RPs”]).

These Regulations shall come into force at once that is to say from the date of its promulgation viz. 13 June 2018.

THE IMPLICATIONS

The implications of money laundering are significant as the AML regulations and guidelines criminalize the offence of money laundering and terrorism financing. Over the last decade it has been apparent that developing countries have been vulnerable target of money laundering activities which destabilizes the economic and political stability of the country as a whole.

Additionally, in September 2018, the SECP issued Guidelines on Implementation of AML/CFT Framework under the Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018 [“Guidelines”] designed to assist RPs in complying with the Regulations. It clarifies and explains the general requirements of the legislation to help RPs in applying AML/CFT measures, developing an effective AML/CFT risk assessment and compliance framework suitable to their business, and in detecting and reporting suspicious activities.

This publication contains a synopsis of these regulations and the related guidelines.

KPMG Taseer Hadi & Co. Chartered Accountants
Executive Summary

The Securities and Exchange Commission of Pakistan ("SECP") has notified "Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018" vide S.R.O. 770 (1)/2018 dated 13 June 2018. These Regulations are fully compliant with the recommendations of Financial Action Task Force ("FATF").

The purpose of these Regulations and issuance of the Guidelines is to carry out self-risk assessment relating to money laundering and terrorist financing risks and provide greater self-awareness in financial institutions and accordingly, enabling them to implement internal control measures that commensurate with their risk profile, which would ensure that criminals are not able to hide their identity through use of complex ownership structure of companies, partnerships, trusts or other similar forms, the financial institutions are required to identify the ultimate beneficial owner, who is a natural person, of all legal persons and legal arrangements before offering their services to them.

These provide a single set of regulations for all the aforementioned financial institutions with the aim to harmonize the AML/CFT regime. The main emphasis of these Regulations is to:

- assess risk through documenting, determining, identifying, categorizing level of risk and reporting the risk assessment to the Commission.
- manage and mitigate risk of money laundering and terrorism financing through developing, implementing policies, procedures and control and to monitor implementation of policies, procedures and controls and enhance them if necessary
- assess and identify risk of money laundering and terror financing that may arise in respect of new products, practices and technologies;
- understand beneficial ownership of legal persons and legal arrangements and customers’ business; and identify natural persons beneficially owning the business
- identify and carry-out due diligence in respect of natural person, named as the Beneficiary In case of Life Insurance or Takaful Policies Identification to;
- implement appropriate internal risk management systems, policies, procedures and controls to determine if any customer or a beneficial owner is a Politically Exposed Persons.

The onus and responsibility under these Regulations is that regulated persons, who are required to take appropriate steps identify, assess and understand, its money laundering and terrorism financing risks and to implement mechanism to deter such risks.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process for Risk Assessment and Customer Due Diligence</td>
<td>5</td>
</tr>
<tr>
<td>The Three Lines of Defense</td>
<td>5</td>
</tr>
<tr>
<td>Risk Assessment, Mitigation and Applying Risk Based Approach</td>
<td>5</td>
</tr>
<tr>
<td>New Products, Practices and Technologies</td>
<td>7</td>
</tr>
<tr>
<td>Customer Due Diligence</td>
<td>7</td>
</tr>
<tr>
<td>Beneficial Ownership of Legal Persons and Legal Arrangements</td>
<td>8</td>
</tr>
<tr>
<td>Identification of Beneficiary for Life Insurance or Takaful Policies</td>
<td>9</td>
</tr>
<tr>
<td>Enhanced Due Diligence</td>
<td>9</td>
</tr>
<tr>
<td>Politically Exposed Persons</td>
<td>10</td>
</tr>
<tr>
<td>Simplified Due Diligence</td>
<td>10</td>
</tr>
<tr>
<td>Reliance on Third Parties</td>
<td>11</td>
</tr>
<tr>
<td>Ongoing Monitoring of Business Relationship</td>
<td>11</td>
</tr>
<tr>
<td>Reporting of Transactions</td>
<td>12</td>
</tr>
<tr>
<td>Monitoring AML/CFT Systems and Controls</td>
<td>13</td>
</tr>
<tr>
<td>Counter Measures against high risk countries</td>
<td>13</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>13</td>
</tr>
<tr>
<td>Record Keeping</td>
<td>13</td>
</tr>
<tr>
<td>Foreign Branches and Subsidiaries</td>
<td>14</td>
</tr>
<tr>
<td>Correspondent Relationship</td>
<td>14</td>
</tr>
<tr>
<td>Appointment of Compliance Officer</td>
<td>15</td>
</tr>
<tr>
<td>Financial Groups</td>
<td>16</td>
</tr>
<tr>
<td>Screening and Training</td>
<td>16</td>
</tr>
<tr>
<td>Documentation and Reporting</td>
<td>17</td>
</tr>
<tr>
<td>Audit Function</td>
<td>17</td>
</tr>
<tr>
<td>Penalty</td>
<td>17</td>
</tr>
<tr>
<td>Sanctions Compliance</td>
<td>17</td>
</tr>
<tr>
<td>Annexure - A</td>
<td>19</td>
</tr>
<tr>
<td>Annexure - B</td>
<td>22</td>
</tr>
<tr>
<td>Glossary</td>
<td>25</td>
</tr>
<tr>
<td>Definition</td>
<td>26</td>
</tr>
</tbody>
</table>
Process for Risk Assessment and Customer Due Diligence

The Three Lines of Defense

Guidelines
- RPs should establish the following three lines of defense to combat ML/TF:
  - the business units (e.g. front office, customer-facing activity);
  - the CO, the compliance function and human resources or technology; and
  - the internal audit function.
- The first line of defense is to carry out the AML/CFT due diligence which includes specifying written policies and procedures and communicating it to all employees including description of obligations, instructions and guidance on compliance with Regulations. There should be internal procedures for detecting, monitoring and reporting suspicious transactions.
- As part of second line of defense, the CO must have the authority and ability to oversee the effectiveness of RPs’ AML/CFT systems, compliance with legislation and provide guidance in day-to-day operations.
- The third line of defense, internal audit, should periodically conduct AML/CFT audits on an Institution-wide basis and be proactive in following up their findings and recommendations.

Risk Assessment, Mitigation and Applying Risk Based Approach

Regulation 3
- RP shall take appropriate steps to identify, assess and understand risks with respect to ML/TF.
- The steps include documentation, consideration of relevant risk factors to determine mitigation measures and updating risk assessment; determination level of overall risk and categorization of risk as high, medium or low; and reporting risk assessment to the SECP.

Regulation 4
RP shall implement counter ML and TF measures which have regard to the ML and TF risks and the size of the business, and
- develop, implement and monitor policies, procedures and controls as approved by the BOD and, if required, improve the same.
- manage and mitigate higher risks by undertaking enhanced measures.
- establish an independent audit function to test the system.

Guidelines
- The process of ML/TF risk assessment has four stages:
  - identifying the area of the business operations susceptible to ML/TF;
  - conducting an analysis in order to assess the likelihood and impact of ML/TF;
  - managing the risks; and
  - regular monitoring and review of those risks.
- For the analysis, the RP should identify the likelihood and the probability that these categories of risk will be misused for ML/TF purposes.
- Example of risk classification factors:
### Classification | Factors
--- | ---
**High Risk** | **Customer risk factors:**
- business relationship is conducted in unusual circumstances;
- non-resident customers;
- Legal persons or arrangements
- companies that have nominee shareholders;
- business that is cash-intensive;
- complex ownership structure;
- PEPS;
- shell companies;
- trusts; and
- requested/applied quantum of business does not match with the profile/particulars of client.

**Country or geographic risk factors:**
- countries identified as not having adequate AML/CFT systems;
- countries subject to sanctions, embargos or similar measures issued by the United Nations;
- countries identified as having significant levels of corruption or other criminal activity; and
- countries identified as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

**Product, service, transaction or delivery channel risk factors:**
- anonymous transactions (which may include cash);
- non-face-to-face business relationships or transactions;
- payments received from unknown or un-associated third parties;
- the surrender of single premium life products and other insurance products with a surrender value;
- international transactions, or involve high volumes of currency (or currency equivalent) transactions;
- new or innovative products or services that are not provided directly by the RP;*
- products that involve large payment or receipt in cash; and
- one-off transactions.

**Low risk** | **Customer risk factors:**
- RP and banks provided they are subject to requirements to combat ML/TF consistent with the FATF recommendations and are supervised for compliance with those requirements; and
- public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership.

**Country risk factors:**
- countries identified as having effective AML/CFT systems; and
- countries identified as having a low level of corruption or other criminal activity.

**Product, service, transaction or delivery channel risk factors:**
- insurance policies for pension schemes with no early surrender option and the policy cannot be used as collateral;
- life insurance policies where the premium is low;
- group insurance policies; and
- pension or superannuation or similar scheme.
• RP should also have appropriate mechanisms to provide risk assessment information to SECP. (Repetition of regulation 3 (2)(e)).

• RPs may use a risk matrix, given in Annexure 1 of the Guidelines, as a method of assessing risk in order to identify the categories of customers.

• The nature and extent of AML/CFT controls will depend on a number of aspects including nature, scale and complexity of the RP’s business, geographical diversity of operations, customer / product profile, volume and size of transactions and the extent of dealing through third parties.

• RPs should evaluate their residual risk after implementing mitigation measures. Residual risks should be in line with the RP’s overall risk tolerance. In case residual risk exceeds its risk tolerance, the RP should enhance the risk mitigation measures that are in place.

• Risk mitigation measures include:
  - determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;
  - setting transaction limits for higher-risk customers or products;
  - determining transactions requiring senior management approval, including higher risk transactions and those involving PEPs;
  - determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services.

New Products, Practices and Technologies

Regulation 5

• RPs shall:
  assessing and identify risk of ML/TF for new products, business practices, delivery mechanism, developing and existing technologies.

manage, mitigate, undertake risk assessments and appropriate measures prior to launch or use of such products, practices and technologies.

Guidelines

• Identification and assessment of risk includes the use of electronic verification of documentation and data and transaction screening systems.

• It is not appropriate that RP should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures. However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied.

Customer Due Diligence

Regulation 6

• RPs are prohibited to open or maintain anonymous account or account in fictitious name.

• RP shall ensure applying CDD measures while establishing business relationship with a customer; CDD in broader terms include:
  - identify customer or beneficial owner; obtain information on the purpose and intended nature of the business; monitor accounts/transactions on ongoing basis; obtain such documents from different types of customers as provided in Annexure - A; verify identity of customer and beneficial owner;
  - adopt risk management procedures under which a customer may utilize business relationship prior to verification;
  - categorize each customer as high, medium or low risk, depending on the outcome of the CDD process;
  - maintain a list of all customers/accounts where the business relationship was refused or closed due to negative verification;
  - application of CDD on existing customers, considering materiality and risk; should also conduct due diligence on existing relations at appropriate times; and
• unable to satisfactorily complete required CDD measures, account shall not be opened or existing business relationship shall be terminated and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR in relation to the customer.

• A regulated person shall not form business relationship with entities and/or individuals that are:
  - designated under the United Nations Security Council Resolutions and adopted by the Government of Pakistan;
  - proscribed under the Anti Terrorism Act, 1997(XXVII of 1997); and
  - associates/facilitators of persons mentioned herein preceding two paras.

• In case of suspicion of ML/TF, and it is reasonably believed that performing the CDD process will tip-off the customer, it may not pursue the CDD process, and instead should file an STR in accordance with the terms of AML Act.

• Government entities accounts shall not be opened in the personal names and account which is to be operated by an officer of Federal/ Provincial/ Local Government has to be duly authorized by concerned Government. RPs need to take into account the governing laws of such Government entities relating to bank accounts.

Guidelines

• The RP shall conduct ongoing due diligence in accordance with the business and risk profile of the customer. Annexure 3 to the Guidelines contains a template to be adopted by RPs for risk assessment.

• Annexure -B gives some examples of potentially suspicious activities or “red flags” for ML/TF.

• RPs shall monitor transactions to determine whether they are linked. Transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold.

• RPs shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys.

• The RP should also verify whether that authorized person is properly authorized to act on behalf of the customer. RPs shall conduct CDD on the authorized person using the same standards that are applicable to a customer. Additionally, RPs shall ascertain the reason for such authorization and obtain a copy of the authorization document.

• In case the applicant (customer) has been refused facilities by another RP - classify that applicant as higher-risk and apply EDD procedures to the customer, file an STR and consider not accepting the customer.

• Verification is to be undertaken prior to entry to the business, however, there are circumstances where verification is permissible after establishment of business relationship. These include:
  - non face-to-face business;
  - securities transactions; and
  - telephone or electronic business, where payment is or is expected to be made from a bank or other account.

• Where CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/TF, RP should not voluntarily agree to open accounts with such customers. RP should file an STR with the FMU and ensure that the customer is not informed.

• RPs should not adopt SDD measures where the ML/TF risks are high.

Beneficial Ownership of Legal Persons and Legal Arrangements

Regulation 7

• For legal person, RPs, in addition to other measures, are required to acquire and use requisite information and data obtained from a reliable source, are also required to:
  - understand the nature of business, ownership and control structure;
  - identify and verify the identity of natural
A brief on Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 and Guidelines

Identification of Beneficiary for Life Insurance or Takaful Policies

**Regulation 8**

- In addition to the requirements of these regulations, an insurer/ takaful operator is required to conduct following CDD measures when a beneficiary of such policy is identified or designated:
  - identified - obtain full name and identity;
  - designated - obtain sufficient information of the beneficiary to establish the identity at the time of payout;
  - for both the above cases, the verification of identity should occur at the time of payout.

- An insurer/ takaful operator shall:
  - take measures at the time of payout, to determine whether the beneficial owner(s) are PEPs and where higher risks are identified, inform senior management before the payout, to conduct enhanced scrutiny of the business relationship and to consider making a STR.
  - include the beneficiary of a life insurance policy as a relevant risk factor in determining whether EDD are required and where an insurer/ takaful operator determines that a beneficiary presents a higher risk, it shall take enhanced measures to identify and verify beneficial owner, at the time of payout.

Enhanced Due Diligence

**Regulation 9**

- RP shall implement internal risk management systems to determine high risk customer of ML/TF. This includes:
  - customers/ policy holders belonging to countries which are non-compliant with AML regulations according to FATF;
  - such body corporate, partnerships, associations and legal arrangements including non-governmental organizations or not-for-profit organizations which receive donations; and
  - legal persons or arrangements with complex ownership structures.

- RPs shall perform EDD proportionate to risk posed to the business relationship by the customers, that are identified as high risk, or are notified as such by the Commission., these measures includes:
  - obtain approval from RP’s senior management to establish or continue business relations with such customers;
  - establish, by appropriate means, the sources of wealth and/or funds or beneficial ownership of funds; and
  - conduct enhanced monitoring of business relations with the customer.
Guidelines

- “Hold Mail” accounts should be regularly monitored and reviewed and necessary steps taken to obtain the identity of the account holder where such evidence is not already in the RP file.

- While assessing risk of a country, RPs are encouraged to consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index.

- Useful websites for information on countries vulnerable to corruption include:
  - FATF website: [www.fatf-gafi.org](http://www.fatf-gafi.org); and
  - Transparency International: [www.transparency.org](http://www.transparency.org)

Politically Exposed Persons

Regulation 10

- RPs are need to implement appropriate internal risk management systems to determine if any customer or a beneficial owner is a PEP. In case of foreign PEPs and higher risk domestic PEPs, RPs shall perform EDD.

- These requirements are also applicable on family members and close associates of foreign and domestic PEPs.

Guidelines

- Family members of a PEP are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

- Close associates to PEPs are individuals who are closely connected to PEP, either socially or professionally.

- RP shall consider factors such as whether the customer who is a PEP:
  - is from a high risk country;
  - has prominent public functions in sectors known to be exposed to corruption; and
  - has business interests that can cause conflict of interests (with the position held);
  - information provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
  - funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
  - uses multiple bank accounts for no apparent commercial or other reason; and
  - from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

- PEP who is no longer a PEP - Factors to be considered include:
  - the level of (informal) influence that the individual could still exercise; and
  - whether the individual’s previous and current function are linked in any way.

Simplified Due Diligence

Regulation 11

- In case low risk is identified, RPs may apply SDD measures – which needs to be documented.

- SDD measures are limited to the following:
  - reducing the frequency of customer identification updates;
  - reducing the degree of on-going monitoring and scrutinizing transactions; and
  - not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship. In case of suspicion of ML/TF or where specific higher-risk scenarios apply, Simplified CDD measures are not acceptable.

Guidelines

- In case of low risk, the RPs are allowed to rely on third parties for verifying the identity of the applicants and beneficial owners.
Relevance on Third Parties

**Regulation 12**

- RPs may rely on a third party to conduct CDD on its behalf provided that RPs shall-
  - obtain immediately, necessary information relating to identification of the customer, beneficial owner and/or the nature of his business;
  - take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
  - satisfy itself that the third party is regulated, and supervised or monitored for and has measures in place for compliance with CDD and record-keeping requirements in line with these regulations; and
  - maintain data/information confidentiality and non-disclosure agreement with the third party.

- RPs may rely on a third party pertaining to same financial group if the group applies CDD and record-keeping requirements and programmes against ML/TF, in accordance with these regulations; any higher country risk should be adequately mitigated by the group’s AML/CFT policies, and implementation of those CDD and record-keeping requirements and AML/CFT programmes shall be supervised at a group level by a competent authority.

- Notwithstanding the reliance upon a third party, RPs are responsible for ongoing monitoring of its customers and, RPs shall ultimately remain responsible for its AML/CFT obligations including generating STRs and shall carry out ongoing monitoring of such customers itself.

**Guidelines**

- The RP shall conduct the due diligence on the proposed service provider to whom it intends to outsource and also ensure that the service provider is fit and proper to perform the activity.

- RP shall ensure that the outsourcing agreement clearly sets out the obligations of both parties.

- RPs must not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

- RPs shall ensure that the outsourcing agreement requires OSPs to file a STR with the FMU in case of suspicions arising in the course of performing the outsourced activity.

Ongoing Monitoring of Business Relationship

**Regulation 13**

- All business relations with customers need to be monitored on an ongoing basis to ensure that the transactions are consistent with RPs’ knowledge of the customer, its business and risk profile and the sources of funds.

- For all complex and unusual transactions, RPs need to obtain information and examine the background and purpose of such transactions and findings need to be documented so that the information can be made available to the relevant authorities when required.

- Periodically review the adequacy of customer and beneficial owner’s information and ensure that the information obtained and ensure that the information is kept up to date and relevant by undertaking reviews of the existing records, particularly for higher risk categories of customers and the review period and procedures thereof should be defined by regulated person in their AML/CFT policies, as per risk based approach.

- Customers’ profiles should be revised keeping in view the spirit of KYC/CDD and basis of revision shall be documented and customers may be consulted, if necessary.

- In the event if RPs consider to retain customer after filing of STR on suspicion that existing business relations with a customer are connected with ML/TF, in such case, RPs shall substantiate and documents the reasons for retaining customer and relations shall be subject to proportionate risk mitigation measure.

- RPs should monitor relationships with the entities or individual on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, RPs shall take immediate action as per law, including freezing the funds and assets of
such proscribed entity/individual and reporting to the Commission.

Guidelines

- Examples of triggering events to consider updating customer CDD include:
  - material changes to the customer risk profile or changes to the way that the account usually operates;
  - RP lacks sufficient or significant information on that particular customer;
  - where a significant transaction takes place;
  - where there is a significant change in customer documentation standards; and
  - significant changes in the business relationship like:
    - new products or services;
    - a significant increase in a customer’s salary being deposited;
    - the stated turnover or activity of a corporate customer increases;
    - a person has just been designated as a PEP; or
    - the nature, volume or size of transactions changes.

- Possible areas to monitor for inconsistency / significant changes in pattern of transactions are:
  - transaction type;
  - frequency;
  - amount;
  - geographical origin/destination; and
  - account signatories.

Reporting of Transactions

Regulation 14

- RPs shall comply with the provisions of the AML Act and rules, regulations and directives issued there under for reporting suspicious transactions/ currency transactions in the context of ML/TF.

- RPs shall implement appropriate internal policies, procedures and controls for meeting their obligations under the AML Act.

- (Repeat of Regulation 13)

- The transactions, which are out of character, are inconsistent with the history, pattern, or normal operation of the account or are not commensurate with the level of income of a customer shall be viewed with suspicion, be properly investigated and referred to CO for possible reporting to FMU.

- RPs should note that STRs, including attempted transactions, should be reported regardless of the amount of the transactions; and, the CTRs should be reported for the transactions of rupees two million and above.

- The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion.

- The employees of RPs are strictly prohibited to disclose the fact to the customer or any other quarter that a STR or related information is being or has been reported to any authority, except if required by law.

- RPs without disclosing the contents of STRs, shall intimate to the SECP on bi-annual basis the number of STRs reported to FMU and RPs shall ensure that status report (indicating No. of STRs only) shall reach the AML Department within seven days of close of each half year.

Guidelines

- Activities which should require further enquiry may be recognizable as:
  - any unusual financial activity of the customer in the context of the customer’s own usual activities;
  - any unusual transaction in the course of some usual financial activity;
  - any unusually-linked transactions;
  - any unusual method of settlement;
  - any unusual or disadvantageous early
redemption of an investment product; and
- any unwillingness to provide the information requested.

- The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.

- Vigilance systems should require the maintenance of a register of all reports made to the FMU. Such registers should contain details of:
  - the date of the report;
  - the person who made the report;
  - the person(s) to whom the report was forwarded; and
  - reference by which supporting evidence is identifiable.

Monitoring AML/CFT Systems and Controls

Guidelines

- RPs shall assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement. RP will need to consider monitoring certain aspects which include:
  - the ability to identify changes in a customer profile or transaction activity / behavior, which come to light in the normal course of business;
  - the potential for abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;
  - the adequacy of employee training and awareness;
  - the adequacy of internal coordination mechanisms;
  - the compliance arrangements;
  - the performance of third parties who were relied on for CDD purposes;
  - changes in relevant laws or regulatory requirements; and
  - changes in the risk profile of countries to which the RPs or its customers are exposed to.

Counter Measures against high risk countries

Regulations 14A

- RPs are required to adopt counter measures, including but not limited to, enhance due diligence proportionate to the risk, to the business relationship and transactions with their customer belonging to such countries for which this is called upon by FATF and/or as notified by the Federal Government.

- The Commission, on the advice of the Federal Government regarding weakness in the AML/CFT systems of other counties, shall direct the Regulated Person to adopt counter measures in accordance with these regulations with the customers belonging to such countries.

Miscellaneous

Record Keeping

Regulation 15

- RPs are required to maintain all necessary records on transactions, both domestic and international, including the results of any analysis undertaken for a minimum period of five years from completion of transaction but in case of customers or accounts involve litigation or if required by court or other competent authority, the record shall be retained for a longer period.

- The records need to be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions – enabling to provide evidence for prosecution of criminal activity and the transactions records may be maintained in paper or electronic form, provided it is admissible as evidence in a court of law.

- The records of identification data obtained through CDD process like copies of identification documents, account opening forms, KYC forms and verification documents, other documents and result of any analysis undertaken along with records of account files and business
correspondence shall be maintained for a minimum period of five years after termination of the business relationship.

- Upon directions of SECP, FMU and law enforcement agencies, RPs should make available all CDD and transaction records.

Guidelines

- RPs should ensure that all information obtained in the context of CDD is recorded. This includes both;
  - recording the documents RP is provided with; and
  - transcription into the RP’s own IT systems of the relevant CDD information contained in such documents or obtained by other means.

- Beneficial ownership information must be maintained for at least 5 years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer of the RP.

- Records relating to verification of identity comprise:
  - a description of the nature of all the evidence received relating to the identity of the verification subject; and
  - the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

- Records relating to transactions comprise:
  - details of personal identity, including the names and addresses of customers, beneficial owner and any counter party.
  - details of securities and investments transacted including:
    - the nature of such securities/investments;
    - valuations and prices;
    - memoranda of purchase and sale;
    - sources and volume of funds and securities;
    - destination(s) of funds and securities;
    - memoranda of instructions and authorities;
    - book entries;
    - custody of title documentation;
    - the nature of the transaction;
    - the date of the transaction; and
    - the form (e.g. cash, cheque) in which funds are offered and paid out.

Foreign Branches and Subsidiaries

Regulation 16

- RPs should ensure that their foreign subsidiaries and branches comply with FATF Recommendations and their AML/ CFT policies are observed by them.

- RPs need to apply their AML/ CFT policies to all of their foreign branches and subsidiaries to the extent that laws and regulations of the host country permits.

- Where the AML/ CFT requirements in the host country or jurisdiction differ from those in Pakistan, RPs shall require their overseas branches or subsidiaries to apply the higher of the two standards.

- Where the law of the host country conflicts with the AML/ CFT requirements of Pakistan so that the overseas branch or subsidiary is unable to fully observe the higher standards, RPs shall report this to the SECP and comply with such further directions as may be issued.

Correspondent Relationship

Regulation 17

- A RPs shall perform the following measures when forming a correspondent relationship:
  - assess the suitability of the respondent financial institution through following steps-
    - gathering adequate information about the respondent FI;
    - determine from any available sources the reputation of the respondent FI and the quality of supervision over the respondent FI whether it is subjected to any ML/TF investigation or regulatory
action; and
- assess the respondent FI’s AML/ CFT controls and ascertain that they are adequate and effective;
- clearly understand and document the respective AML/ CFT responsibilities of the FI and the respondent FI;
- assess the respondent FI in the context of sanctions/embargoes and Advisories about risks; and
- obtain approval from the FIs’ senior management before providing correspondent services to a new FI.

• RPs shall document basis for its satisfaction that requirements of this regulations are met.

• RPs shall pay special attention when establishing or continuing correspondent relationship with FIs which are located in jurisdictions that have been identified or called for by FATF for inadequate and poor AML/ CFT standards in the fight against ML/TF.

• No RPs shall enter into or continue correspondent relationship with another FI that does not have adequate controls against money laundering or terrorism financing activities, is not effectively supervised by the relevant authorities or is a shell FI.

• To take appropriate measures and satisfy itself that it’s respondent FIs do not permit their accounts to be used by shell FIs.

Appointment of Compliance Officer

Regulation 18

• RPs shall-
  - appoint a management level officer as CO, who shall report directly to the board of directors or to another equivalent executive position or committee;
  - ensure that the CO has timely access to all customer records and other relevant information which they may require;
  - the CO shall primarily be responsible for the areas including, but not limited to:
    - effective compliance with relevant laws, regulations, rules, other directions and guidelines as may be amended from time to time;
    - ensuring internal policies, procedures and controls against ML/TF are approved by the BOD and are effectively implemented;
    - monitoring, reviewing and updating AML/ CFT policies and procedures;
    - providing assistance in compliance to other departments and branches;
    - timely submission of accurate data/ returns as required under the applicable laws;
    - monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
    - such other responsibilities as RPs may deem necessary in order to ensure compliance with these regulations.

Guidelines

• CO must be a person who is fit and proper to assume the role and who:
  - has sufficient skills and experience to develop and maintain systems and controls;
  - reports directly and periodically to the BOD;
  - has sufficient resources, including time and support staff;
  - has access to all information necessary to perform the AML/CFT compliance function;
  - ensures regular audits of the AML/CFT program;
  - maintains various logs, as necessary, which should include logs with respect to declined business, PEPs, and requests from Commission, FMU and Law Enforcement Agencies particularly in relation to investigations; and
  - responds promptly to requests for information from authorities.
Financial Groups

Regulation 19

- Financial groups should implement group-wide programmes against ML/TF, which should be applicable to all branches and majority-owned subsidiaries of the financial group and these should include the measures set out in these regulations and also-

  - policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;
  - the provision, at group-level compliance, audit, and/or AML/ CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/ CFT purposes; and
  - adequate safeguards on the confidentiality and use of information exchanged.

Guidelines

- RPs should have robust information-sharing among the head office and all of its branches and subsidiaries. RP’s' compliance and internal audit staff should evaluate compliance with all aspects of their group’s policies and procedures, including the effectiveness of centralized CDD policies and the requirements for sharing information and responding to queries from head office.

Screening and Training

Regulation 20

- RP shall:

  - develop and implement a comprehensive employee due diligence policy and procedure to be carried out at the time of hiring all employees, conduct verification of antecedents and screening procedures to verify that person being inducted/ hired has a clean history;
  - have screening procedures to ensure high standards when hiring employees; and
  - chalk out and implement suitable training program for relevant employees on annual basis, in order to effectively implement the regulatory requirements and RPs own policies and procedures relating to AML/ CFT.

Guidelines

- RPs shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, the RP may verify:

  - the references provided by the prospective employee at the time of recruitment;
  - the employee’s employment history, professional membership and qualifications;
  - details of any regulatory actions or actions taken by a professional body;
  - details of any criminal convictions; and
  - whether the employee has any connections with the sanctioned countries or parties.

- RPs shall consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read the RP’s AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.

- Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer’s identity, for new and existing customers. Training should be given on the factors which may give rise to suspicions about a customer’s activities, and actions to be taken when a transaction is considered to be suspicious.

- Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances.

- Supervisors, managers and senior management (including BoD) should receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity
and retention of records.

- The CO should receive in-depth training on all aspects of the primary legislation, the Regulations, regulatory guidance and relevant internal policies. They should also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

Documentation and Reporting Guidelines

- RPs must document their RBA and be able to demonstrate to SECP in there on-site inspection the following:
  - adequacy of risk assessment systems;
  - details of the implementation of systems and procedures;
  - how it monitors and improves the effectiveness of its systems and procedures; and
  - the arrangements for reporting to senior management the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

- RPs shall ensure that their ML/TF risk management processes are kept under regular review which is at least annually.

- RPs shall maintain Control Assessment Template (prescribed in Annexure 2 of the Guidelines) within the period as required by the SECP from time to time.

Audit Function Guidelines

- A RP should conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The assessment includes:
  - test the overall integrity and effectiveness of the AML/CFT systems and controls;
  - assess the adequacy of internal policies and procedures in addressing identified risks, including CDD measures, record keeping and retention, third party reliance, and transaction monitoring;
  - assess compliance with the relevant laws and regulations;
  - test transactions in all areas of the RP;
  - assess employees’ knowledge;
  - assess the adequacy, accuracy and completeness of training programs;
  - assess the effectiveness of compliance oversight and quality control; and
  - assess the adequacy of the RP’s process of identifying suspicious activity including screening sanctions lists.

Penalty

Regulation 21

- Any person who contravenes or fails to comply with any provision of these regulations made shall be liable to pay such sum as provided in section 40 of the Securities and Exchange Commission of Pakistan Act, 1997 (XIII of 1997), in addition to any penalty provided under AML Act.

Sanctions Compliance Guidelines

- The Regulations require RPs not to form business relationship with the individuals/entities and their associates that are either sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

- The UNSC Sanctions Committee, maintains the consolidated list of individuals and entities subject to the sanctions which is available at the UN sanctions committee’s website, at following link:
The Ministry of Interior issues Notifications of proscribed individuals/entities to implement sanction measures under UNSCR 1373 (2001), and the regularly updated consolidated list is available at the National Counter Terrorism Authority’s website, at following link: http://nacta.gov.pk/proscribed-organizations/

- RPs shall make their sanctions compliance program an integral part of their overall AML/CFT compliance program and accordingly should have policies, procedures, systems and controls in relation to sanctions compliance. RPs shall provide adequate sanctions related training to their staff.

- When conducting risk assessments, RPs shall, take into account any sanctions that may apply (to customers or countries).

- RPs shall document and record all the actions that have been taken to comply with the sanctions regime, and the rationale for each such action.

- RPs are expected to keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed.

- In case there is not 100% match but sufficient grounds of suspicion that customer/funds belong to sanctioned entity/individual, the RPs may consider raising an STR to FMU.
<table>
<thead>
<tr>
<th>S No.</th>
<th>Type of Customer</th>
<th>Information/ Documents to be Obtained</th>
</tr>
</thead>
</table>
| 1.    | Individuals    | A photocopy of any one of the following valid identity documents;  
        |                | (i) Computerized National Identity Card (CNIC) issued by NADRA.  
        |                | (ii) National Identity Card for Overseas Pakistani (NICOP) issued by  
        |                | NADRA.  
        |                | (iii) Pakistan Origin Card (POC) issued by NADRA.  
        |                | (iv) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only).  
        |                | (v) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only). |
| 2.    | Sole proprietorship | (i) Photocopy of identity document as per Sr. No. 1 above of the proprietor.  
        |                | (ii) Copy of registration certificate for registered concerns.  
        |                | (iii) Copy of certificate or proof of membership of trade bodies, etc, wherever applicable.  
        |                | (iv) Declaration of sole proprietorship on business letter head.  
        |                | (v) Account opening requisition on business letter head.  
        |                | (vi) Registered/ Business address. |
| 3.    | Partnership    | (i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories;  
        |                | (ii) Attested copy of ‘Partnership Deed’;  
        |                | (iii) Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form;  
        |                | (iv) Authority letter from all partners, in original, authorizing the person(s) to operate firm’s account; and  
        |                | (v) Registered/ Business address. |
| 4.    | Limited Companies/ Corporations | (i) Certified copies of:  
        |                | (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account;  
        |                | (b) Memorandum and Articles of Association;  
        |                | (c) Certificate of Incorporation;  
        |                | (d) Certificate of Commencement of Business, wherever applicable;  
        |                | (e) List of Directors on ‘Form-A/Form-B’ issued under Companies Act, 2017, as applicable; and  
<pre><code>    |                | (f) Form-29, wherever applicable. |
</code></pre>
<table>
<thead>
<tr>
<th>S No.</th>
<th>Type of Customer</th>
<th>Information/ Documents to be Obtained</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Branch Office or Liaison Office of Foreign Companies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(i) Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) A copy of permission letter from relevant authority i.e. Board of Investment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iii) Photocopies of valid passports of all the signatories of account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iv) List of directors on company letter head or prescribed format under relevant laws/regulations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(v) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(vi) Branch/Liaison office address.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Trust, Clubs, Societies and Associations etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(i) Certified copies of:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) Certificate of Registration/ Instrument of Trust</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) By-laws/Rules &amp; Regulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iv) Registered address/ Business address where applicable.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>NGOs/NPOs/Charities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(i) Certified copies of:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) Registration documents/certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) By-laws/Rules &amp; Regulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iv) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(v) Registered address/ Business address.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Agents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(i) Certified copy of ‘Power of Attorney’ or ‘Agency Agreement’.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) Photocopy of identity document as per Sr. No. 1 above of the agent and principal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(iv) Registered/ Business address.</td>
<td></td>
</tr>
<tr>
<td>S No.</td>
<td>Type of Customer</td>
<td>Information/ Documents to be Obtained</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9.</td>
<td>Executors and Administrators</td>
<td>(i) Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(ii) A certified copy of Letter of Administration or Probate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(iii) Registered address/ Business address.</td>
</tr>
<tr>
<td>10.</td>
<td>Minor Accounts</td>
<td>(i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(ii) Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.</td>
</tr>
</tbody>
</table>
## Annexure - B

A brief on Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 and Guidelines

<table>
<thead>
<tr>
<th>S No.</th>
<th>Type of RP</th>
<th>ML/TF Warning Signs/ Red Flags</th>
</tr>
</thead>
</table>
| 1.    | Insurance entities | - Requests for a return of premium to be remitted to persons other than the policy holder;  
       |                     | - Claims payments paid to persons other than policyholders and beneficiaries;  
       |                     | - Unusually complex holding company or trust ownership structure;  
       |                     | - Making a false claim;  
       |                     | - A change in beneficiaries (for instance, to include non-family members);  
       |                     | - A change/increase of the premium payment (for instance which appear unusual in the light of the policyholder’s income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party);  
       |                     | - Use of cash and/or payment of large single premiums;  
       |                     | - Payment/surrender by a wire transfer from/to foreign parties;  
       |                     | - Payment by banking instruments that allow anonymity of the transaction;  
       |                     | - Payment from third parties;  
       |                     | - Change of address and/or place of residence of the policyholder;  
       |                     | - Lump sum top-ups to an existing life insurance contract;  
       |                     | - Lump sum contributions to personal pension contracts;  
       |                     | - Requests for prepayment of benefits;  
       |                     | - Use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution);  
       |                     | - Change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment);  
       |                     | - Early surrender of the policy or change of the duration (particularly where this results in penalties); and  
       |                     | - Requests for multiple policies to be taken out for premiums slightly below any publicized limits for performing checks, such as checks on the source of wealth or cash payments. |
| 2.    | Lending NBFCs       | - Loans secured by pledged assets held by third parties unrelated to the borrower;  
       |                     | - Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties;  
       |                     | - Borrower defaults on cash-secured loan or any loan that is secured by assets that are readily convertible into currency;  
<pre><code>   |                     | - Loans are made for, or are paid on behalf of, a third party with no reasonable explanation; |
</code></pre>
<table>
<thead>
<tr>
<th>S No.</th>
<th>Type of RP</th>
<th>ML/TF Warning Signs/ Red Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via a currency or multiple monetary instruments; and</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Loans that lack a legitimate business purpose, provide the bank with significant fees or assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower or back to back loans without any identifiable and legally admissible purpose);</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Sudden and unexplained subscriptions and redemptions;</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Quick purchase and redemption of units despite penalties;</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Requests to pay redemptions proceeds to a third (unrelated) party; and</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Customer that exhibits unusual concern with compliance with AML/CFT reporting requirements or other (AML/CFT) policies and procedures.</td>
</tr>
</tbody>
</table>

3. Brokerage Houses

- Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
- Customers who wish to deal on a large scale but are completely unknown to the broker;
- Customers who wish to invest or settle using cash;
- Customers who use cheque drawn on an account other than their own;
- Customers who change the settlement details at the last moment;
- Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
- Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
- Customers who have no obvious reason for using the services of the broker;
- Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
- Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
- Customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
- Customer trades frequently, selling at a loss
- Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
- Customers who wish to maintain a number of trustee or customers’ accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
- Any transaction involving an undisclosed party;
<table>
<thead>
<tr>
<th>S No.</th>
<th>Type of RP</th>
<th>ML/TF Warning Signs/ Red Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Significant variation in the pattern of investment without reasonable or acceptable explanation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/reporting thresholds;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Transactions involve penny/microcap stocks;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customer invests in securities suddenly in large volumes, deviating from previous transactional activity;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customer conducts mirror trades; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>AML Act</td>
<td>Anti-Money Laundering Act 2010</td>
<td></td>
</tr>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering and Countering Financing of Terrorism</td>
<td></td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
<td></td>
</tr>
<tr>
<td>BOD</td>
<td>Board of Directors</td>
<td></td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
<td></td>
</tr>
<tr>
<td>CO</td>
<td>Compliance Officer</td>
<td></td>
</tr>
<tr>
<td>CTR</td>
<td>Currency Transaction Report</td>
<td></td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Due Diligence</td>
<td></td>
</tr>
<tr>
<td>FI</td>
<td>Financial Institutions</td>
<td></td>
</tr>
<tr>
<td>FMU</td>
<td>Financial Monitoring Unit</td>
<td></td>
</tr>
<tr>
<td>GoP</td>
<td>Government of Pakistan</td>
<td></td>
</tr>
<tr>
<td>ML/TF</td>
<td>Money laundering and terrorism financing</td>
<td></td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
<td></td>
</tr>
<tr>
<td>RBA</td>
<td>Risk Based Approach</td>
<td></td>
</tr>
<tr>
<td>Regulations</td>
<td>Securities and Exchange Commission of Pakistan (Anti-Money Laundering and Countering Financing of Terrorism) Regulations, 2018</td>
<td></td>
</tr>
<tr>
<td>RPs</td>
<td>Regulated Persons</td>
<td></td>
</tr>
<tr>
<td>SDD</td>
<td>Simple Due Diligence</td>
<td></td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
<td></td>
</tr>
<tr>
<td>SECP</td>
<td>Securities and Exchange Commission of Pakistan</td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Beneficial owner</strong></td>
<td>The natural person who ultimately owns or control a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Explanation:- For the purposes of this definition the expression “ultimately own or control” or “ultimate effective control” refers to situation in which the ownership or control is exercise through a chain of ownership having substantial shareholding, directly or indirectly, or by means of control other than direct control and includes beneficial owners of a beneficiary under a life or other investment linked insurance policy or scheme or any other instrument availed by the customer in financial services market.</td>
<td></td>
</tr>
<tr>
<td><strong>Beneficiary</strong></td>
<td>(i) in case of trust, is the person or persons who are entitled to the benefit of any trust arrangement;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii) in the context of life insurance/takaful, life-contingent annuity contracts or another investment linked insurance/takaful policy, is a natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when or if an event occurs, which is covered by the policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Business relations</strong></td>
<td>Means provision of any financial services by the regulated person under the administered legislation.</td>
<td></td>
</tr>
<tr>
<td><strong>Correspondent relationship</strong></td>
<td>A relationship between the regulated person (Correspondent), or any party acting on its behalf and processing orders on behalf of the regulated person, and an intermediary (Respondent) which is regulated and supervised by a supervisory authority, transmitting orders on behalf of its underlying customers.</td>
<td></td>
</tr>
<tr>
<td><strong>Customer</strong></td>
<td>Any natural person, legal person or legal arrangement to whom financial services has been extended by a regulated person,</td>
<td></td>
</tr>
<tr>
<td><strong>Financial group</strong></td>
<td>A group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision, together with branches and/or subsidiaries that are subject to anti-money laundering and counter financing of terrorism policies and procedures at the group level.</td>
<td></td>
</tr>
<tr>
<td><strong>Legal arrangements</strong></td>
<td>Includes express trusts or any other similar legal arrangements</td>
<td></td>
</tr>
<tr>
<td><strong>Legal persons</strong></td>
<td>Entities other than natural persons whether incorporated or not or a legal arrangement that can establish a permanent customer relationship with a regulated person or otherwise own property and include companies, bodies corporate, foundations, Limited Liability partnership (LLP), partnerships, or associations and other relevantly similar entities</td>
<td></td>
</tr>
</tbody>
</table>
**Politically exposed persons**

PEPs include-

(i) foreign PEPs, individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;

(ii) domestic PEPs, individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;

(iii) persons who are or have been entrusted with a prominent function by an international organization, means members of senior management and members of the board or equivalent functions:

Provided that middle ranking or more junior individuals in the above referred categories are not included in the definition of PEPs.

**Regulated Person**

Securities brokers, futures brokers, Insurers, Takaful Operators, NBFCs and Modarabas.

**Senior management**

Includes, chief executive officer/ managing director, deputy managing director, chief operating officer, company secretary, chief financial officer, chief compliance officer and chief regulatory officer or holder of such positions by whatever name called.

**Shell Financial Institution**

FI incorporated, formed or established in a country or jurisdiction where the FI has no physical presence and which is unaffiliated with a financial group that is subject to effective consolidated supervision.
Offices in Pakistan

**Karachi Office**
Sheikh Sultan Trust Building No. 2
Beaumont Road
Karachi 75300
Phone +92 (21) 3568 5847
Fax +92 (21) 3568 5095
email karachi@kpmg.com

**Lahore Office**
351-Shadman-1, Main Jail Road,
Lahore Pakistan
Phone +92 (42) 111-KPMGTH (576484)
Fax +92 (42) 3742 9907
email lahore@kpmg.com

**Islamabad Office**
Sixth Floor, State Life Building
Blue Area
Islamabad
Phone +92 (51) 282 3558
Fax +92 (51) 282 2671
email islamabad@kpmg.com

www.kpmg.com.pk