# SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

# GUIDELINES

# ON

# ANTI-MONEY LAUNDERING,

# COUNTERING FINANCING OF TERRORISM, AND

# PROLIFERATION FINANCING

**Issued by**

**Securities and Exchange Commission of Pakistan**

**September 2018**

# Table of Contents

**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**

## 1. Introduction, Purpose and Scope

i. Money Laundering ("ML") and Terrorist Financing ("TF") are economic crimes that threaten a country's overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF. An effective Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime requires financial institutions to adopt and effectively implement appropriate ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF.

ii. Securities and Exchange Commission of Pakistan ("SECP"), in order to maintain the integrity of its regulated financial sector *inter-alia*; the brokers, insurers, NBFCs and modarabas, in respect of preventing and combating ML and TF, notified the Securities and Exchange Commission of Pakistan' Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 ("the SECP AML/CFT Regulations" or "the Regulations") . The SECP AML/CFT Regulations require relevant Regulated Persons (RPs) to establish systems to detect ML and TF, and therefore assist in the prevention of abuse of their financial products and services.

iii. These Guidelines are applicable to all Regulated Persons ("RPs") as defined under the SECP AML/CFT Regulations conducting relevant financial business and designed to assist RPs in complying with the Regulations. It supplements the Regulations and the AML/CFT regime by clarifying and explaining the general requirements of the legislation to help RPs in applying national AML/CFT measures, developing an effective AML/CFT risk assessment and compliance framework suitable to their business, and in particular, in detecting and reporting suspicious activities.

iv. These Guidelines are based on Pakistan' AML/CFT legislation and reflect, so far as applicable, the 40 Recommendations and guidance papers issued by the Financial Action Task Force ("FATF").

## 2. Obligation of RP in Establishing an Effective AML /CFT Governance and Compliance Regime

i. RPs should understand their obligation of establishing an effective AML/CFT regime to deter criminals from using financial system for ML or TF purposes, and to develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations.

ii. RPs' Board of Directors and senior management must be engaged in the decision making on AML/CFT policies, procedures and control and take ownership of the risk based approach. They must be aware of the level of ML/TF risk the RP is exposed to and take a view on whether it is equipped to mitigate that risk effectively.

iii. RP must give due priority to establishing and maintaining an effective AML/CFT compliance culture and must adequately train its staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with the Regulations.

iv. RPs must establish written internal procedures so that, in the event of a suspicious activity being discovered, employees are aware of the reporting chain and the procedures to be followed. Such procedures should be periodically updated to reflect any legislative changes.

v. To oversee the compliance function, the Regulations require RP to appoint a Compliance Officer ("CO") at the management level, who shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit (FMU).

vi. Each RP should ensure that any suspicious transaction report must be made by employees to the CO, who are well versed in the different types of transactions which the RP handles and which may give rise to opportunities for ML/TF.

vii. The RP is responsible for ensuring that employees should be aware of their reporting obligations and the procedure to follow when making a suspicious transaction report.

## 3. Program and Systems to prevent ML and TF

i. RPs should establish and maintain programs and systems to prevent, detect and report ML/TF. The systems should be appropriate to the size of the RP and the ML/TF risks to which it is exposed and should include:

   a) Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;
   b) Policies and procedures to undertake a Risk Based Approach ("RBA");
   c) Internal policies, procedures and controls to combat ML/TF, including appropriate risk management arrangements;
   d) Customer due diligence measures;
   e) Record keeping procedures;
   f) Group-wide AML/CFT programs
   g) An audit function to test the AML/CFT system;
   h) Screening procedures to ensure high standards when hiring employees; and
   i) An appropriate employee-training program.

ii. It is the responsibility of the senior management to ensure that appropriate systems are in place to prevent and report ML/TF and the RP is in compliance with the applicable legislative and regulatory obligations.

## 4. The Three Lines of Defense

i. RPs should establish the following three lines of defense to combat ML/TF;

   - First the business units (e.g. front office, customer-facing activity): They should know and carry out the AML/CFT due diligence related policies and procedures and be allotted sufficient resources to do this effectively.
   - Second the Compliance Officer, the compliance function and human resources or technology.
   - Third the internal audit function

ii. As part of first line of defense, policies and procedures should be clearly specified in writing, and communicated to all employees. They should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the reporting entity in compliance with the Regulations. There should be internal procedures for detecting, monitoring and reporting suspicious transactions.

iii. 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 applicable AML/CFT legislation and provide guidance in day-to-day operations of the AML/CFT policies and procedures.

iv. CO must be a person who is fit and proper to assume the role and who:

   (1) has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
   (2) reports directly and periodically to the Board of Directors ("Board") or equivalent on AML/CFT systems and controls;

(3) has sufficient resources, including time and support staff;
(4) has access to all information necessary to perform the AML/CFT compliance function;
(5) ensures regular audits of the AML/CFT program;
(6) maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and requests from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigations; and
(7) responds promptly to requests for information by the SECP/Law enforcement agency.

v. Internal audit, the third line of defense, should periodically conduct AML/CFT audits on an Institution-wide basis and be proactive in following up their findings and recommendations. As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate, subject to any prescribed auditing requirements applicable to AML/CFT measures.

# Monitoring AML/CFTT Systems and Controls

## 5. Monitoring AML/CFT Systems and Controls

i. RPs will need to have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. RPs shall update their systems as appropriate to suit the change in risks.

ii. Additionally, RPs shall assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed. For that purpose, the RP will need to consider monitoring certain aspects which include:

1) the ability to identify changes in a customer profile or transaction activity/behaviour, which come to light in the normal course of business;
2) 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.;
3) the adequacy of employee training and awareness;
4) the adequacy of internal coordination mechanisms i.e., between AML/CFT compliance and other functions/areas;
5) the compliance arrangements (such as internal audit);
6) the performance of third parties who were relied on for CDD purposes;
7) changes in relevant laws or regulatory requirements; and
8) changes in the risk profile of countries to which the RPs or its customers are exposed to.

## 6. Documentation and Reporting

i. RPs must document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the RP to demonstrate to the Commission:

1) risk assessment systems including how the RP assesses ML/TF risks;
2) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;
3) how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
4) the arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

ii. RPs shall note that the ML/TF risk assessment is not a one-time exercise and therefore, they must ensure that their ML/TF risk management processes are kept under regular review which is at least annually. Further, the RP management should review the program's adequacy when the reporting entity adds new products or services, opens or closes accounts with high-risk customers, or expands through mergers or acquisitions.

iii. RP should be able to demonstrate to the Commission, the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance policy; its procedures and policies concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT, during the SECP's on-site inspection. RPs shall maintain Risk Assessment Tables (Annex 1) and AML/CFT Compliance Assessment Template (Annex 2) within the period as required by the Commission from time to time.

## 7. New Products and Technologies

i. RPs should have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:

    1) electronic verification of documentation;
    2) data and transaction screening systems; or
    3) the use of virtual or digital currencies.

ii. RPs should undertake a risk assessment prior to the launch or use of such products, practices and technologies; and take appropriate measures to manage and mitigate the risks.

iii. RPs should have policies and procedures to prevent the misuse of technological development in ML/TF schemes, particularly those technologies that favour anonymity. For example, securities trading and investment business on the Internet, add a new dimension to RPs' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF, and fraud.
    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.

iv. To maintain adequate systems, RPs should ensure that its systems and procedures are kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by the RPs. Risks identified must be fed into the RPs' business risk assessment.

## 8. Cross-border Correspondent Relationship

i. Cross-border correspondent relationships is the provision of services by one institution to another institution (the respondent institution). Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's) customers may present high ML/TF risk and as such may require EDD.

ii. In order for RPs to manage their risks effectively, they shall consider entering into a written agreement with the respondent institution before entering into the correspondent relationship.

iii. In addition to setting out the responsibilities of each institution, the agreement could include details on how the RP will monitor the relationship to ascertain how effectively the respondent institution is applying CDD measures to its customers, and implementing AML/CFT controls.

iv. Correspondent Institutions are encouraged to maintain an ongoing and open dialogue with the respondent institutions to discuss the emerging risks, strengthening AML/CFT controls, and help the respondent institutions in understanding the correspondent institutions' AML/CFT policies and expectations of the correspondent relationship.

## 9. Customer Due Diligence

i. RPs shall take steps to know who their customers are. RPs shall not keep anonymous accounts or accounts in fictitious names. RPs shall take steps to ensure that their customers are who they purport themselves to be. RPs shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who is the beneficial owner), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer.

ii. RP shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the RP's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds. RPs shall conduct CDD when establishing a business relationship if:

   (1) There is a suspicion of ML/TF, Annex 3 gives some examples of potentially suspicious activities or "red flags" for ML/TF. Although these may not be exhaustive in nature, it may help RPs recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose.; or

   (2) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.

iii. In case of suspicion of ML/TF, an RP should:

   (1) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and
   (2) File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law.

iv. 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.

v. RPs shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys. Similarly, RPs shall identify and verify the customer's beneficial owner(s) to ensure that the RP understands who the ultimate beneficial owner is.

vi. RPs shall ensure that they understand the purpose and intended nature of the proposed business relationship or transaction. RPs shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

vii. The Regulations require RPs to identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person"). 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(s) 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.

viii. RPs may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could

apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

ix. When performing CDD measures in relation to customers that are legal persons or legal arrangements, RPs should identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure.

x. The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and second, to take appropriate steps to mitigate the risks. In this context, RPs should identify the customer and verify its identity. The type of information that would normally be needed to perform this function should be as specified in Annexure 1 of the Regulations.

xi. If RP has any reason to believe that an applicant has been refused facilities by another RP due to concerns over illicit activities of the customer, it should consider classifying that applicant as higher-risk and apply enhanced due diligence procedures to the customer and the relationship, filing an STR and/or not accepting the customer in accordance with its own risk assessments and procedures.

**a) Timing of Verification**

i. The best time to undertake verification is prior to entry into the business relationship or conducting a transaction. However, as provided in the Regulations RPs may complete verification after the establishment of the business relationship.

ii. Examples of the types of circumstances (in addition to those referred for beneficiaries of life insurance or Takaful policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

(1) Non face-to-face business.
(2) Securities transactions. In the securities industry intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
(3) In cases of telephone or electronic business where payment is or is expected to be made from a bank or other account, the person verifying identity should:
    (a) satisfy himself/herself that such account is held in the name of the customer at or before the time of payment; and
    (b) not remit the proceeds of any transaction to the customer or his/her order until verification of identity has been completed.

iii. The above are only examples and RPs should adopt risk management procedures with respect to the conditions under which an applicant may utilize the business relationship prior to verification. Such conditions may include restricting the funds received from being passed to third parties, imposing a limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. For the avoidance of doubt, RPs should not postpone the verification where the ML/TF risks are high and enhanced due diligence measures are required to be performed. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If an

applicant does not pursue an application, the RP's staff could consider that this in itself is suspicious, and they should evaluate whether a STR to FMU is required.

iv. 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. In such situations, RP should file an STR with the FMU and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

**b) Existing Customers**

i. RPs are required to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

ii. The CDD requirements entails that, if an RP has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

iii. An RP is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

iv. Where an RP is unable to complete and comply with CDD requirements as specified in the Regulations, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the RP shall terminate the relationship. Additionally, the RP shall consider making a STR to the FMU.

**c) Tipping-off & Reporting**

i. The Law prohibits tipping-off. However, a risk exists that customers could be unintentionally tipped off when the RP is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

ii. Therefore, if RPs form a suspicion of ML/TF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If the RP reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR. RPs should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

**d) No Simplified Due Diligence for Higher-Risk Scenarios**

RPs should not adopt simplified due diligence measures where the ML/TF risks are high. RPs shall identify risks and have regard to the risk analysis in determining the level of due diligence.

## 10. <u>On-going Monitoring of Business Relationships</u>

i. Once the identification procedures have been completed and the business relationship is established, the RP is required to monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened. RPs shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps RPs to

keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

ii. RPs shall conduct on-going due diligence which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer.

iii. RP should develop and apply written policies and procedures for taking reasonable measures to ensure that documents, data or information collected during the "Identification" process are kept up-to-date and relevant by undertaking routine reviews of existing records.

iv. RPs shall consider updating customer CDD records as a part its periodic reviews (within the timeframes set by the RP based on the level of risk posed by the customer) or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:

(1) Material changes to the customer risk profile or changes to the way that the account usually operates;
(2) Where it comes to the attention of the RP that it lacks sufficient or significant information on that particular customer;
(3) Where a significant transaction takes place;
(4) Where there is a significant change in customer documentation standards;
(5) Significant changes in the business relationship.

v. Examples of the above circumstances include:

(1) New products or services being entered into,
(2) A significant increase in a customer's salary being deposited,
(3) The stated turnover or activity of a corporate customer increases,
(4) A person has just been designated as a PEP,
(5) The nature, volume or size of transactions changes.

vi. RPs should be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

(1) transaction type
(2) frequency
(3) amount
(4) geographical origin/destination
(5) account signatories

vii. However, if an RP has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible

viii. It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring mechanism.

ix. Whilst some RPs may wish to invest in expert computer systems specifically designed to assist the detection of fraud and ML/TF, it is recognized that this may not be a practical option for many RPs for the reasons of cost, the nature of their business, or difficulties of systems integration. In such circumstances RPs will need to ensure they have alternative systems in place for conducting on-going monitoring.

## 11. Simplified Due Diligence Measures ("SDD")

i. RPs may conduct SDD in case of lower risks identified by the RP. However, the RP shall ensure that the low risks it identifies are commensurate with the low risks identified by the country or the Commission. While determining whether to apply

SDD, RPs should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity.

The simplified measures should be commensurate with the low risk factors.

ii. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.

iii. Where the risks are low and where there is no suspicion of ML/TF, the law allow the RPs to rely on third parties for verifying the identity of the applicants and beneficial owners.

iv. Where an RP decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

## 12. Enhanced CDD Measures ("EDD")

i. RPs should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose.

ii. Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, RPs should conduct enhanced CDD measures, consistent with the risks identified. In particular, RPs should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

iii. Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

(1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
(2) Updating more regularly the identification data of applicant/customer and beneficial owner.
(3) Obtaining additional information on the intended nature of the business relationship.
(4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.
(5) Obtaining additional information on the reasons for intended or performed transactions.
(6) Obtaining the approval of senior management to commence or continue the business relationship.
(7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

iv. In case of accounts where the accountholder has instructed the RP not to issue any correspondence to the accountholder's address. Such accounts do carry additional risk to RPs, and they should exercise due caution as a result. It is recommended on a best practice basis that evidence of identity of the accountholder should be obtained by the RP. "Hold Mail" accounts should be regularly monitored and reviewed and the RP should take necessary steps to obtain the identity of the account holder where such evidence is not already in the RP file.

### a) High-Risk Countries

i. Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to an RP. Conducting a business relationship with an applicant/customer from such a country exposes the RP to reputational risk and legal risk.

ii. RPs should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

iii. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

iv. RPs are advised to consult publicly available information to ensure that they are aware of the high-risk countries/territories. 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.

v. Useful websites include: FATF website at www.fatf-gafi.org and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

## 13. Politically Exposed Persons (PEPs)

i. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose RP to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons, commonly referred to as 'politically exposed persons' (PEPs) and defined in the Regulations, *inter-alia*, heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates.

ii. 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.

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

iv. Provision of financial services to corrupt PEPs exposes an RP to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of the whole financial system can be undermined.

v. RPs are encouraged to be vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. RPs should, in relation to PEPs, in addition to performing normal due diligence measures:

(1) have appropriate risk management systems to determine whether the customer is a politically exposed person;
(2) obtain senior management approval for establishing business relationships with such customers;
(3) take reasonable measures to establish the source of wealth and source of funds; and
(4) conduct enhanced ongoing monitoring of the business relationship.

vi. RPs should obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.

vii. RPs shall take a risk based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, the RP shall consider factors such as whether the customer who is a PEP:

(1) Is from a high risk country;
(2) Has prominent public functions in sectors known to be exposed to corruption;
(3) Has business interests that can cause conflict of interests (with the position held).

viii. The other red flags that the RPs shall consider include (in addition to the above and the red flags that they consider for other applicants):

(1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
(2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
(3) A PEP uses multiple bank accounts for no apparent commercial or other reason;
(4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

ix. RPs shall take a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:

(1) the level of (informal) influence that the individual could still exercise; and

(2) whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

x. In the case of insurance policies, RPs shall take steps to determine whether the beneficiary or beneficial owner of a beneficiary is a PEP. This determination should be done at least at the time of pay-out. Where high risks are identified, RPs shall inform the senior management before the pay-out of the policy and conduct EDD on the whole business relationship. Additionally, where appropriate, RPs shall consider filing a STR.

## 14. Record-Keeping Procedures

i. RPs should ensure that all information obtained in the context of CDD is recorded. This includes both;

a. recording the documents the RP is provided with when verifying the identity of the customer or the beneficial owner, and
b. transcription into the RP's own IT systems of the relevant CDD information contained in such documents or obtained by other means.

ii. RP should maintain, for at least 5 years after termination, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity.

iii. Where there has been a report of a suspicious activity or the RP is aware of a continuing investigation or litigation into ML/TF relating to a customer or a transaction, records relating to the transaction or the customer should be retained until confirmation is received that the matter has been concluded.

iv. RPs should also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of 5 years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to relevant competent authorities upon request.

v. 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.

vi. Records relating to verification of identity will generally comprise:

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

vii. Records relating to transactions will generally comprise:

1) details of personal identity, including the names and addresses, of:
   a) the customer;
   b) the beneficial owner of the account or product; and
   c) Any counter-party

2). details of securities and investments transacted including:
   a. the nature of such securities/investments;
   b. valuation(s) and price(s);
   c. memoranda of purchase and sale;
   d. source(s) and volume of funds and securities;
   e. destination(s) of funds and securities;
   f. memoranda of instruction(s) and authority(ies);
   g. book entries;
   h. custody of title documentation;
   i. the nature of the transaction;
   j. the date of the transaction;
   k. the form (e.g. cash, cheque) in which funds are offered and paid out.

## 15. Internal Controls (Audit Function, outsourcing, employee Screening and Training)

i. RPs are expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF risks they identified. RPs should establish and maintain internal controls in relation to:

(1) an audit function to test the AML/CFT systems, policies and procedures;
(2) outsourcing arrangements;
(3) employee screening procedures to ensure high standards when hiring employees; and
(4) an appropriate employee training program.

ii. The type and extent of measures to be taken should be appropriate to the ML/TF risks, and to the size of the RP.

### a) Audit Function

i. A RP should, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit should be commensurate with the RP's nature, size, complexity, and risks identified during the risk assessments. The AML/CFT audits should be conducted to assess the AML/CFT systems which include:

(1) test the overall integrity and effectiveness of the AML/CFT systems and controls;

(2) assess the adequacy of internal policies and procedures in addressing identified risks, including;

(a) CDD measures;
(b) Record keeping and retention;
(c) Third party reliance; and
(d) Transaction monitoring;

(3) assess compliance with the relevant laws and regulations;
(4) test transactions in all areas of the RP, with emphasis on high–risk areas, products and services;
(5) assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
(6) assess the adequacy, accuracy and completeness of training programs;
(7) assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and
(8) assess the adequacy of the RP's process of identifying suspicious activity including screening sanctions lists.

### b) Outsourcing

i. RPs should maintain policies and procedures in relation to outsourcing where they intend to outsource some of their functions. The RP shall conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the service provider ("OSP") is fit and proper to perform the activity that is being outsourced.

ii. Where the RP decides to enter into an outsourcing arrangement, the RP shall ensure that the outsourcing agreement clearly sets out the obligations of both parties. RPs entering into an outsourcing arrangement should develop a contingency plan and a strategy to exit the arrangement in the event that the OSP fails to perform the outsourced activity as agreed.

iii. The OSP should report regularly to the RP within the timeframes as agreed upon with the RP. The RP should have access to all the information or documents relevant to the outsourced activity maintained by the OSP. 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.

iv. 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.

### c) Employee Screening

i. RPs should maintain adequate policies and procedures to screen prospective and existing employees to ensure high ethical and professional standards when hiring. The extent of employee screening should be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the particular risks associated with the individual positions.

ii. Employee screening should be conducted at the time of recruitment, periodically thereafter, i.e., at least annually and where a suspicion has arisen as to the conduct of the employee.

iii. 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:

(1) Verify the references provided by the prospective employee at the time of recruitment
(2) Verify the employee's employment history, professional membership and qualifications
(3) Verify details of any regulatory actions or actions taken by a professional body
(4) Verify details of any criminal convictions; and
(5) Verify whether the employee has any connections with the sanctioned countries or parties.

### d) Employee Training

i. RPs should ensure that all appropriate staff, receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

ii. Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to the RP's business operations or customer base.

iii. RPs should provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of the RP's risk assessments. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.

iv. Staff should be aware on the AML/CFT legislation and regulatory requirements, systems and policies. They should know their obligations and liability under the legislation should they fail to report information in accordance with internal procedures and legislation. All staff should be encouraged to provide a prompt and adequate report of any suspicious activities.

v. All new employees should be trained on ML/TF know the legal requirement to report, and of their legal obligations in this regard.

vi. 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.

vii. Staff members who deal with the public such as sales persons are the first point of contact with potential money launderers, and their efforts are vital to an organization's effectiveness in combating ML/TF. 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.

viii. Staff involved in the processing of transactions should receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. 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.

ix. All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a customer with a personal account opening a business account. Whilst the RP may have previously obtained satisfactory identification evidence for the customer, the RP should take steps to learn as much as possible about the customer's new activities.

x. Although Directors and Senior Managers may not be involved in the handling ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML/CFT policies and procedures. Supervisors, managers and senior management (including Board of Directors) 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.

xi. 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.

# Reporting of Suspicious Transactions/ Currency Transaction Report

## 16. Reporting of Suspicious Transactions / Currency Transaction Report

i. A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and the RP should put "on enquiry". RPs should also pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

ii. Where the enquiries conducted by the RP do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the AML/CFT CO.

iii. Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented, and made available to the relevant authorities upon request. Activities which should require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

   (1) any unusual financial activity of the customer in the context of the customer's own usual activities;
   (2) any unusual transaction in the course of some usual financial activity;
   (3) any unusually-linked transactions;
   (4) any unusual method of settlement;
   (5) any unusual or disadvantageous early redemption of an investment product;
   (6) any unwillingness to provide the information requested.

iv. Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, RPs will need to approach such situations with caution and make further relevant enquiries. Depending on the type of business each RP conducts and the nature of its customer portfolio, each RP may wish to set its own parameters for the identification and further investigation of cash transactions.

v. Where the RP has been unable to satisfy that any cash transaction is reasonable, and therefore should be considered as suspicious. RP is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

vi. If the RP decides that a disclosure should be made, the law require the RP to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2008. The STR prescribed reporting form can be found on FMU website through the link below.

vii. http://www.fmu.gov.pk/docs/AML_Regulations-2008.pdf The process for identifying, investigating and reporting suspicious transactions to the FMU should be clearly specified in the reporting entity's policies and procedures and communicated to all personnel through regular training.

viii. RP is required to report total number of STRs filed to the Commission on bi-annual basis within seven days of close of each half year. The CO should ensure prompt reporting in this regard.

ix. Vigilance systems should require the maintenance of a register of all reports made to the FMU. Such registers should contain details of:

(1) the date of the report;
(2) the person who made the report;
(3) the person(s) to whom the report was forwarded; and
(4) reference by which supporting evidence is identifiable.

x. It is normal practice for an RP to turn away business that they suspect might be criminal in intent or origin. Where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF, that attempted transaction should be reported to the FMU.

xi. Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity RP should ensure that appropriate action is taken to adequately mitigate the risk of the RP being used for criminal activities. This may include a review of either the risk classification of the customer or account or of the entire relationship itself. Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

# Implementation of UN Security Council Resolutions

## 17. Sanctions Compliance- Implementation of UN Security Council Resolutions

i. Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them. There are also sanctions that target those persons and organizations involved in terrorism. The types of sanctions that may be imposed include:

(1) targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly;
(2) economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly;
(3) currency or exchange control;
(4) arms embargoes, which would normally encompass all types of military and paramilitary equipment;
(5) prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;
(6) import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.;
(7) visa and travel bans and
(8) Targeted financial sanctions relating to the prevention, suppression and disruption of proliferation of Weapons of Mass Destruction (WMD) and its financing.

ii. 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.

iii. The UNSC, acting under chapter VII of the United Nations Charter, adopts the Resolutions on counter terrorism measures and proliferation of WMD, in particular;

a. the UNSC Resolution 1267 (1999), 1989 (2011), 2253 (2015) and other subsequent resolutions, which impose sanctions covering; asset freeze, travel ban and arms embargo, against individuals and entities associated to Al-Qaida, Taliban, and the Islamic State in Iraq (Daésh) organizations. The regularly updated consolidated lists is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

b. the UNSC Resolution 1373 (2001), 1998 (2011) on terrorism and financing of terrorism requiring member states to proscribe individual and entities, who commit or attempt to commit terrorist act, freeze without delay the funds and other financial assets or economic resources, and prohibit making any funds or financial or other related services available to such proscribed persons and entities.

c. the UNSC Resolution 1718(2006), 2231(2015) and its successor resolutions [1] on proliferation of WMD and its financing, and Targeted Financial Sanctions (TFS) on countries and specifically identified individual and entities associated with it. The resolution require, inter-alia freezing without delay the funds or other assets of, any person or entity designated, or under the authority of UNSC. The regularly updated consolidated lists of person and entities designated under UNSCRR 1718(2006) and its successor resolutions (on the DPRK) and listed under UNSCR 2231 (2015) (on Iran) is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/1718/materials
https://www.un.org/sc/2231/list.shtml

iv. Government of Pakistan, Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 (Act No XIV of 1948) to give effect to the UNSC Resolutions and implement UNSC sanction measures in Pakistan. The said SROs are communicated to RPs, from time to time, and have a binding legal effect under the Act No. XIV of 1948. RPS should ensure compliance with the sanctions communicated through SROs. A list of such SROs issued by the Federal Government till date is also available at the following links:

UNSCR 1267

http://www.mofa.gov.pk/contentsro1.php
http://www.mofa.gov.pk/contentsro2.php

UNSCR 1718

http://www.secdiv.gov.pk/page/sro-unscr-sanctions

v. The Federal Government, Ministry of Interior issues Notifications of proscribed individuals /entities pursuant to the Anti-Terrorism Act, 1997, to implement sanction measures under UNSCR 1373(2001). The regularly updated consolidated list is available at the National Counter Terrorism Authority's website, at following link;

http://nacta.gov.pk/proscribed-organizations/

[1] The UNSC sanctions with respect to proliferation of WMD primarily encapsulates currently the Islamic Republic of Iran and the Democratic People's Republic of Korea's sanctions regime. The UNSC resolution on Iran is 2231 (2015). The UNSC resolution on Democratic People's Republic of Korea are 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), 2375 (2017) and 2397 (2017).

vi. The individuals and entities designated under the aforementioned resolutions are subject to sanctions including assets freeze, travel ban and ban on provision of any funds, financial assets or economic recourses. Such sanctions also extend to any funds, financial assets and economic resources indirectly owned by the designated individuals, and to individuals or entities acting on their behalf or on their direction.

vii. RPs shall, taking note of the circumstances where customers and transections are more vulnerable to be involved in TF and PF activities[2], identify high-risk customers and transections, and apply enhanced scrutiny. RP shall conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names in the abovementioned lists, to determine if the business relations involves any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

viii. RP is also required to screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list.
RP shall undertake reasonable efforts to collect additional information in order to identify, and avoid engaging in prohibited activities and, to enable follow-up actions.

ix. Where there is a true match or suspicion, RPs shall take steps that are required to comply with the sanctions obligations including immediately–

(a) freeze without delay[3] the customer's fund or block the transaction, if it is an existing customer;
(b) reject the customer, if the transaction has not commenced;
(c) lodge a STR with the FMU; and
(d) notify the SECP and the MOFA.

x. RP is required to submit a STR when there is an attempted transaction by any of the listed persons.

xi. RP must ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether it is a true match. 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.

xii. Notwithstanding the funds, properties or accounts are frozen, RP may continue receiving dividends, interests, or other benefits, but such benefits shall still remain frozen, so long as the individuals or entities continue to be listed.

xiii. 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).

xiv. The obligations/ prohibitions regarding proscribed entities and persons mentioned in the above lists are applicable, on an ongoing basis, to proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed/ designated name or with a different name.

[2] The circumstances that the RPs shall take note of where customers and transections are more vulnerable to be involved in PF activities relating to both DPRK and Iran sanction regime are listed on Annexure 4 as PF Warning Signs/Red Alerts.

[3] According to FATF , without delay is defined to be ideally within a matter of hours of designation by the UNSC

xv. 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.

xvi. 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.

xvii. RPs may also educate their customers that in case of wrongful or inadvertent freezing, they may apply in writing for de-listing to Federal Government through relevant Ministry or to the UN's Ombudsman, as the case may be.

# Risk Assessment and Applying a Risk Based Approach

*(Please refer to Annex 1 for Risk Assessment Tables)*

## 18. Risk Assessment and Applying a Risk Based Approach

i. The SECP AML/CFT Regulations shift emphasis from one-size-fits-all approach to Risk Based Approach ('RBA'), requiring RPs to carryout ML/TF risk assessment and apply RBA to prevent or mitigate ML and TF.

ii. The RBA enables RPs to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. RPs should develop an appropriate RBA for their particular organization, structure and business activities and apply the RBA on a group-wide basis, where appropriate. As a part of the RBA, RPs shall:

1) Identify ML/TF risks relevant to them;
2) Assess ML/TF risks in relation to-
    a. Customers (including beneficial owners);
    b. Country or geographic area in which its customers reside or operate and where the RP operates;
    c. Products, services and transactions that the RP offers; and
    d. Delivery channels.
3) Design and implement policies, controls and procedures approved by its Board of Directors;
4) Monitor and evaluate the implementation of mitigating controls;
5) Keep their risk assessments current through ongoing reviews;
6) Document the RBA including implementation and monitoring procedures and updates to the RBA; and
7) Have appropriate mechanisms to provide risk assessment information to the Commission.

iii. Under the RBA, where there are higher risks, RPs are required to take enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures may be permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF. In the case of some very high-risk situations or situations which are outside the RP's risk tolerance, the RP may decide not to take on the accept the customer, or to exit from the relationship.

iv. In view of the fact that the nature of the TF differs from that of ML, the risk assessment must also include an analysis of the vulnerabilities of TF. Many of the CFT measures entities have in place will overlap with their AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison relationships with the authorities. The guidance provided in these guidelines, therefore, applies to CFT as it does to AML, even where it is not explicitly mentioned.

v. The process of ML/TF risk assessment has four stages:

1) Identifying the area of the business operations susceptible to ML/TF;
2) Conducting an analysis in order to assess the likelihood and impact of ML/TF;
3) Managing the risks; and
4) Regular monitoring and review of those risks.

**a) <u>Identification, Assessment and Understanding Risks</u>**

i. The first step in assessing ML/TF risk is to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels that are specific to the RP. Depending on the specificity of the operations of RP, other categories could be considered to identify all segments for which ML/TF risk may emerge. The significance of different risk categories may vary from institution to institution, i.e. RP may decide that some risk categories are more important to it than others.

ii. In the second stage, the ML/TF risks that can be encountered by the RP need to be assessed, analyzed as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the RP from the crime, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself. The analysis of certain risk categories and their combination is specific for each RP so that the conclusion on the total risk level must be based on the relevant information available.

iii. For the analysis, RPs should identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, moderate if it can occur two to three per year and low if it is unlikely, but not possible. In assessing the impact, RPs can, for instance, look at the financial damage by the crime itself or from regulatory sanctions or reputational damages that can be caused. The impact can vary from low if there is only short-term or there are low-cost consequences, to high when there is cost inducing long-term consequences, affecting the proper functioning of the institution.

iv. The following is an example of a likelihood scale with 3 risk ratings as an example. RP's can customize their own as applicable to their operation with more details, if preferable.

| ***Likelihood Scale*** | | | |
|---|---|---|---|
| ***Consequence Scale*** | ***Low*** | ***Moderate*** | ***High*** |
| Almost Certain | Moderate | Moderate | High |
| Possible | Moderate | Moderate | High |
| Unlikely | Low | Moderate | Moderate |

v. RPs should allow for the different situations that currently arise in their business or are likely to arise in the near future. For instance, risk assessment should consider the impact of new products, services or customer types, as well as new technology. In addition, ML/TF risks will often operate together and represent higher risks in combination. Potential ways to assess risk include but are not limited to:

1) How likely an event is;
2) Consequence of that event;
3) Vulnerability, threat and impact;
4) The effect of uncertainty on an event;

vi. The assessment of risk should be informed, logical and clearly recorded. For instance, if a RP has identified gatekeepers as presenting higher inherent risk in relation to the delivery of a product, the risk assessment should indicate how RP has arrived at this rating (domestic guidance, case studies, direct experience).

***Risk Assessment (lower complexity)***

In line with this guidance, RPs may want to assess risk by only considering the likelihood of ML/TF activity. This assessment should involve considering each risk factor that have been identified, combined with business experience and information published by the Commission and international organizations such as the FATF. The likelihood rating could correspond to:

1) Unlikely - There is a small chance of ML/FT occurring in this area of the business;
2) Possible - There is a moderate chance of ML/FT occurring in this area of the business;
3) Almost Certain - There is a high chance of ML/FT occurring in this area of the business

For example, a RP may have identified that one of its products is vulnerable to ML/TF due to the potential for cross-border movement of funds. The risk assessment highlights the product is easily accessible, that many customers are using it, and it is used in higher-risk jurisdictions. Combined with domestic and international guidance, the RP assesses that the inherent risk rating of this product as high. The program should then address this likely risk with appropriate control measures. RPs will need to do this with each of the identified risks.

***Risk Assessment (moderate complexity)***

Another way to determine the level of risk is to work out how likely the risk is going to happen and cross-reference that with the consequence of that risk.

Using likelihood ratings and consequence ratings can provide you with a more comprehensive understanding of the risk and a robust framework to help arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist you in applying the appropriate risk management measures as detailed in the program.

For example, RPs may have identified that one of its products is vulnerable to ML/TF and RP assesses that the likelihood of this product being used in ML/TF activity is probable. RP judge the impact of the identified risk happening in terms of financial loss and assess the consequence as moderate.

Cross-referencing possible with moderate risk results in a final inherent risk rating of moderate. The program should then address this moderate risk with appropriate control measures. RPs will need to undertake this exercise with each of the identified risks.

***Risk Assessment (higher complexity)***

RP could assess risk likelihood in terms of threat and vulnerability. For example, you may consider domestic tax evasion criminals as the threat, and accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method you use, this could result in an inherent risk rating of almost certain. RP may then want to assess the impact of this event on the business and the wider environment.

Determining the impact of ML/TF activity can be challenging but can also help focus AML/CFT resources in a more effective and targeted manner. When determining impact, you may want to consider a number of factors, including:

1) Nature and size of your business (domestic and international);
2) Economic impact and financial repercussions;
3) Potential financial and reputational consequences;
4) Terrorism-related impacts;
5) Wider criminal activity and social harm;
6) Political impact;
7) Negative media.

RP may want to give more weight to certain factors to provide a more nuanced understanding of your ML/TF risk.

In addition, RPs may want to consider how your risks can compound across the various risk factors. For example, you may identify that one of these products is high risk and is being used in a high-risk jurisdiction that is directly involved in the production or transnational shipment of illicit drugs. As such, you assess the compounded risk of this scenario as presenting an inherent risk rating of severe. RPs would be expected to prioritize and allocate the resources accordingly.

### *Applying the Risk Assessment*

The risk assessment should help rank and prioritize risks and provide a framework to manage those risks. The risk assessment must enable RPs to prepare a comprehensive program. It should enable to meet relevant obligations under the regulations, including obligations to conduct CDD, monitor accounts and activities and report suspicious activity.

The assessment should help in determining suspicion and consequently assist in the decision to submit an STR to the FMU. RP must submit an STR to the FMU if it think activities or transactions are suspicious. For instance, RPs may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and submit an STR.

RPs must conduct ongoing CDD. The risk assessment will help target and prioritize the resources needed for ongoing CDD. For instance, RPs may want to undertake ongoing CDD on high-risk customers on a more regular basis than on lower-risk customers.

RPs must undertake account monitoring. The risk assessment will help you design the triggers, red flags and scenarios that can form part of account monitoring. For instance, you may want the activity of a high-risk customer in a high-risk jurisdiction (as identified in the risk assessment) to be subject to more frequent and in-depth scrutiny.

### *New and Developing Technologies and Products*

New and developing technologies and products can present unknown ML/TF risks and vulnerabilities. In addition, new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership. The risk assessment should consider whether the business is, or may be, exposed to customers involved in new and developing technologies and products. The program should detail the procedures, policies and controls that RPs will implement for this type of customer and technology.

### *Material Changes and Risk Assessment*

The risk assessment should adapt when there is a material change in the nature and purpose of the business or relationship with a customer. A material change could present an increase, or decrease, in ML/TF risk.

Material change could include circumstances where RPs introduce new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when RPs start using new methods of delivering services or have new corporate or organizational structures. It could result from deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, RPs may need to refresh their risk assessment.

vii. RPs should document their risk assessment in order to be able to demonstrate their allocation of compliance resources. An effective risk assessment is an ongoing process. Risk levels may change as new products are offered, as new markets are entered, as high-risk customers open or close accounts, or as the products, services, policies, and procedures change. The RP should therefore update its risk assessment every 12 to 18 months to take account of these changes. RP should also have appropriate mechanisms to provide risk assessment information to the Commission, if required.

**Examples of Risk Classification Factors**

Below are some examples that can be helpful indicators of risk factors/indicators that may be considered while assessing the ML/TF risks for different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

**High-Risk Classification Factors**

(1) ***Customer risk factors***: The institution will describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the RP for ML or TF, and the consequent impact if indeed that occurs. Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

(a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the RP and the customer).
(b) Non-resident customers.
(c) Legal persons or arrangements
(d) Companies that have nominee shareholders.
(e) Business that is cash-intensive.
(f) The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons;
(g) Politically exposed persons
(h) shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
(i) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
(j) Requested/Applied quantum of business does not match with the profile/particulars of client
(k) real estate dealers,
(l) dealers in precious metal and stones, and
(m) lawyers/notaries

**Example Scenarios of Customer Types**

**Small and Medium Sized Enterprises:**
*Small and medium business enterprise customers usually entail domestic companies with simple ownership structures. Most of these businesses deal with cash and multiple persons that can act on its behalf. The likelihood that funds deposited are from an illegitimate source is HIGH, since it can't be easily be identified and can have a major impact on a large number of SME customers. Thus, the risk assessment and risk rating result is HIGH.*

**International corporations:**
*International corporate customers have complex ownership structures with foreign beneficial ownership (often). Although there are only a few of those customers, it is often the case that most are located in offshore locations. The likelihood of Money Laundering is High because of the limited number of customers of this type and the beneficial ownership could be questionable, with two criteria that in this scenario result in a possible risk impact of moderate and a moderate risk assessment.*

As an example, these descriptions can result in a table as depicted below:

| ***Customer Type*** | ***Likelihood*** | ***Impact*** | ***Risk Analysis*** |
|---|---|---|---|
| Retail Customer/ Sole Proprietor | Moderate | Moderate | Moderate |
| High Netwoth Individuals | High | High | High |
| NGO/NPO | High | High | High |
| International Corporation | High | Moderate | Moderate |
| PEP | High | High | High |
| Company Listed on Stock Exchange | Low | Low | Low |

***Note: The above risk analysis is a general one for types or categories of customers. It is the starting point for the risk classification of an individual customer. Based on the circumstances of an individual customer, such as its background or information provided, the risk classification of an individual customer can be adjusted. Based on that individual risk classification, customer due diligence measures should be applied.***

(2) ***Country or geographic risk factors***: Country or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of the RP itself, its location and the location of its geographical units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to ML/TF. The factors that may indicate a high risk are as follow:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems.
(b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity.
(d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.
(e) Jurisdictions in which the customer and beneficial owner are based;
(f) Jurisdictions that are the customer's and beneficial owner's main places of business.

(3) ***Product, service, transaction or delivery channel risk factors***: A comprehensive ML/TF risk assessment must take into account the potential risks arising from the products, services, and transactions that the RP offers to its customers and the way these products and services are delivered. In identifying the risks of products, services, and transactions, the following factors should be considered:

(a) Anonymous transactions (which may include cash).
(b) Non-face-to-face business relationships or transactions.
(c) Payments received from unknown or un-associated third parties.
(d) The surrender of single premium life products or other investment-linked insurance products with a surrender value.
(e) International transactions, or involve high volumes of currency (or currency equivalent) transactions
(f) New or innovative products or services that are not provided directly by the RP, but are provided through channels of the institution;
(g) Products that involve large payment or receipt in cash; and
(h) One-off transactions.
(i) To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions.
(j) Any introducers or intermediaries the firm might use and the nature of their relationship with the RP.
(k) Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?
(l) Has the customer been introduced by another part of the same financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk? What has the firm done to satisfy itself that the group entity applies CDD measures?
(m) Has the customer been introduced by a third party, for example, a Financial Institution that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision? What has the firm done to be satisfied that:
(n) The third party applies CDD measures and keeps records to standards and that it is supervised for compliance with comparable AML/CFT obligations;

**<u>Low Risk Classification Factors</u>**

(1) Customer risk factors:
A customer that satisfies the requirements under regulation 11 (2) (a) and (b) of the SECP AML/CFT Regulations.

(2) Product, service, transaction or delivery channel risk factors:
The product, service, transection or delivery channel that satisfy the requirement under regulation 11(2) (c) to (g) of the SECP AML/CFT Regulations

(3) Country risk factors:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
(b) Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, RP could, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

<u>Example Scenarios of Product Types, Services and Transactions</u>

**Group Life Insurance:**

*The group life insurance products are simple and premiums tend to be very low. Premiums can only be paid through a bank account and no cash is involved. The life insurance products are only sold to resident persons. The likelihood that insurance products are used for ML/TF is LOW, with minor impact, and can result in a LOW risk assessment.*

As an example, these descriptions can result in a table as depicted below:

| *Transaction Type* | *Likelihood* | *Impact* | *Risk Analysis* |
|---|---|---|---|
| Intermediaries | High | Moderate | Moderate |
| Online Transaction | High | High | High |
| Bank Transfer | Moderate | Moderate | Moderate |

**Risk Matrix**

In assessing the risk of money laundering and terrorism financing, RPs are to establish whether all identified categories of risks pose a low, moderate, high or unacceptable risk to the business operations. The RPs must review different factors, e.g., number and scope of transactions, geographical location, and nature of the business relationship. In doing so, the RPs must also review the differences in the manner in which the RP establishes and maintains a business relationship with a customer (e.g., direct contact or non-face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from institution to institution. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk. Thus, for example, a low-risk product in combination with a customer from a high-risk country will combine carry a higher risk.

RPs can use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, the RPs take into account its specificities, may also define additional levels of ML/TF risk.

The development of a risk matrix can include the consideration of a wide range of risk categories, such as the products and services offered by the RP, the customers to whom the products and services are offered, the RPs size and organizational structure, etc. A risk matrix is not static: it changes as the circumstances of the RPs change. A risk analysis will assist RPs to recognize that ML/TF risks may vary across customers, products, and geographic areas and thereby focus its efforts on high-risk areas in its business.

The following is an example of a risk matrix of client product combination, but RPs should develop their own risk matrix based on their own risk analysis. Example only:

| *Customer Transaction* | *Intermediaries* | *Online Transactions* | *Domestic Transfers* | *Deposit or Investment* | *Life Insurance* | *Securities Account* |
|---|---|---|---|---|---|---|
| Domestic Retail Customer | Moderate | Moderate | Moderate | Moderate | Low | Low |
| High Networth Customers | N/A | High | Moderate | High | N/A | Moderate |
| SME Business Customer | High | High | Moderate | High | Moderate | Moderate |
| International Corporation | Moderate | High | Moderate | High | Moderate | Moderate |
| Company Listed on Stock Exchange | Moderate | Moderate | Low | Moderate | Low | Low |
| PEP | High | High | Moderate | High | Moderate | Moderate |
| Mutual Fund Transactions | Moderate | High | Moderate | High | N/A | N/A |

***Note: When conducting risk assessment, RP does not have to follow the processes in this guideline. As long as you comply with your obligations under the Act and any other applicable laws or regulations, you can choose the method of risk***

***assessment that best suits your business. For example, large financial institutions may have their own systems and methodology for conducting a risk assessment. However, it should be prepared to explain and demonstrate to the Commission, the adequacy and effectiveness of procedures, policies and controls.***

**b) Risk Management**

**Risk Mitigation**

i. RPs should have appropriate policies, procedures and controls that enable them to manage and mitigate effectively the inherent risks that they have identified, including the national risks. They should monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with legal and regulatory requirements.

ii. The nature and extent of AML/CFT controls will depend on a number of aspects, which include:

1) The nature, scale and complexity of the RP's business
2) Diversity, including geographical diversity of the RP's operations
3) RP's customer, product and activity profile
4) Volume and size of transactions
5) Extent of reliance or dealing through third parties or intermediaries.

iii. Some of the risk mitigation measures that RPs may consider include:

1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;
2) setting transaction limits for higher-risk customers or products;
3) requiring senior management approval for higher-risk transactions, including those involving PEPs;
4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;
5) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

**Evaluating Residual Risk and Comparing with the Risk Tolerance**

iv. Subsequent to establishing the risk mitigation measures, RPs should evaluate their residual risk, the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the RP's overall risk tolerance.

v. Where the RP finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high-risks, the RP should enhance the risk mitigation measures that are in place.

**Annex 1**

## Preparing AML/CFT Risk Assessment

*"Establish KYC-CDD and customer risk profiling prior to Risk Assessment process"*

### *Step 1 – Identify Customer Risk*

| Customer Risk Type | | | | | |
|---|---|---|---|---|---|
| Customer Type | Number of Customers/Policyholders | Total Amount on Deposit/Value of Trade (Buy and Sale)/Gross Premium | Internal Risk Rating by RP | | |
| | | | Total Number Classified as Low Risk | Total Number Classified as Medium Risk | Total Number Classified as High Risk |
| 1. Natural Persons | | | | | |
| Resident | | | | | |
| Non-Resident | | | | | |
| Total Natural Persons | 0 | 0.00 | 0 | 0 | 0 |
| 2. Legal Persons | | | | | |
| Resident | | | | | |
| Non-Resident | | | | | |
| Total Legal Persons | 0 | 0.00 | 0 | 0 | 0 |
| Total Exposure | 0 | 0 | 0 | 0 | 0 |

### *Step 2- Politically Exposed Persons and High Net worth Individuals*

| Politically Exposed Persons ('PEP's), and or, High Net Worth Individuals | | | | |
|---|---|---|---|---|
| Customer Risk | Politically Exposed Persons and or Related Companies | | High Net Worth Individuals | |
| Type | Total Number | | Total Number | |
| | Domestic PEP | Foreign PEP | Domestic | Foreign |
| Product 1 | | | | |
| Product 2 | | | | |
| Product 3 | | | | |
| Other (specify) | | | | |
| Total | 0.00 | 0.00 | 0.00 | 0.00 |

## Step 3 - Identify Risk by Product, Services and Transactions

| Products and Services | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Business Risk | Domestic | | | | | Foreign | | | | |
| Type | Total Deposits/Securities Purchashed/Policies Issued (Gross Premium) | | Total Withdrawals/Securities Sold/Claims & Maturities Paid | | Total Exposure/Value of Customers Assets in hand/ Net Premium | Total Deposits/Securities Purchashed/Policies Issued (Gross Premium) | | Total Withdrawals/Securities Sold/Claims & Maturities Paid | | Total Exposure/Value of Customers Assets in hand/ Net Premium |
| | Number | Value in Rs. | Number | Valuein Rs. | (on cutoff date) | Number | Value in Rs. | Number | Value in Rs. | (on cutoff date) |
| Products and Services | | | | | | | | | | |
| Product 1 | | | | | | | | | | |
| Product 2 | | | | | | | | | | |
| Product 3 | | | | | | | | | | |
| Product 4 | | | | | | | | | | |
| Other (specify) | | | | | | | | | | |
| Other (specify) | | | | | | | | | | |
| Transactions | | | | | | | | | | |
| Customer Type 1 | | | | | | | | | | |
| Customer Type 2 | | | | | | | | | | |
| Customer Type 3 | | | | | | | | | | |
| Customer Type 4 | | | | | | | | | | |
| Other (specify) | | | | | | | | | | |
| Other (specify) | | | | | | | | | | |
| Total | 0.00 | | 0.00 | | 0.00 | 0.00 | | | 0.00 | 0.00 |

## Step 4- Identify Wire Transfer Activity

| Type | Number of Incoming Transfers over the Period | Total Value | Number of Outgoing Transfers over the Period | Total Value |
|---|---|---|---|---|
| Wire Transfers (SWIFT) | | | | |
| Domestic Payments | | | | |
| Total | 0.00 | 0.00 | 0.00 | 0.00 |

## Step 5 – Identify Customer Type by Geographic Location

| Types of Customers | Number of Customers | Total Deposits/Value of Trade/Gross Premium |
|---|---|---|
| Natural Persons | | |
| Of which, non-resident customers from 'High risk Jurisdictions' as identified by the FATF | | |
| Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions | | |
| Legal Persons | | |
| Of which, non-resident customers from 'High risk Jurisdictions' as identified by the FATF | | |
| Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions | | |
| Total | 0.00 | 0.00 |

***Step 6 - Develop Risk Likelihood Table***

| ***Customer Risk Likelihood Table*** | | | |
|---|---|---|---|
| ***Type of Customer*** | ***Customer*** | ***Transaction*** | ***Geography*** |
| | *Rating: (High/ Moderate/Low)* | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| ***Product Risk Likelihood Table*** | | | |
|---|---|---|---|
| ***Product Type*** | ***Customers*** | ***Transactions*** | ***Geography*** |
| | *Rating (High/Moderate/Low)* | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| ***Delivery Channels Risk Likelihood Table*** | | | |
|---|---|---|---|
| ***Delivery Channels*** | ***Customer*** | ***Transactions*** | ***Geography*** |
| | *Rating (High/Moderate/Low)* | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| ***Overall Entity Level AML/CFT Risk Assessment*** | |
|---|---|
| *Rating (High/Moderate/Low)* | |
| ***Customer Type*** | |
| ***Product Type*** | |
| ***Delivery Channels*** | |
| ***Geography*** | |
| ***Overall AML/CFT Risk Rating*** | |

## AML/CFT Compliance Assessment Checklist

| *Anti-Money Laundering Compliance Assessment* | | | |
|---|---|---|---|
| | | | |
| *Name of the Financial Institution* | | | |
| *Checklist completed by (Name)* | | | |
| *(Designation)* | | | |
| *Date* | | | |
| **The AML / CFT Self-Assessment Checklist has been designed to provide a structured and comprehensive framework for RFIs and their associated entities to assess compliance with key AML / CFT requirements. RFIs are advised to use this as part of their regular review to monitor their AML/CFT compliance. The frequency and extent of such review should be commensurate with the risks of ML/TF and the size of the firm's business.**<br>**Note: *This AML / CFT Self-Assessment Checklist is neither intended to, nor should be construed as, an exhaustive list of all AML/CFT requirements.*** | | | |
| | | | |
| ***Sr No.*** | ***Question*** | ***Yes/No (N/A)*** | ***If No, provide explanation and plan of action for remediation.*** |
| ***(A) AML/CFT Systems*** | | | |
| | | | |
| ***1*** | RPs are required to assess their ML / TF risk and then implement appropriate internal policies, procedures and controls to mitigate risks of ML/TF. | | |
| | Have you taken into account the following risk factors when assessing your own ML / TF risk? | | |
| | (a) Product / service risk | | |
| | (b) Delivery / distribution channel risk | | |
| | (c) Customer risk | | |
| | (d) Country risk | | |
| | | | |
| ***2*** | RPs are required to have effective controls to ensure proper implementation of AML/CFT policies and procedures | | |
| | Does your AML/CFT systems cover the following controls? | | |
| | (a) Board of Director and Senior management oversight | | |
| | (ii) Have you appointed an appropriate staff as a Compliance Officer ('CO') ? | | |
| | (iii) Do you ensure that CO is: | | |
| | 1. the focal point for the oversight of all activities relating to the prevention and detection of ML/TF | | |
| | 2. independent of all operational and business functions as far as practicable within any constraint of size of your institution | | |
| | 3. of a sufficient level of seniority and authority within your institution | | |
| | 4. provided with regular contact with and direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and the measures against the risks of ML/TF is sufficient and robust | | |
| | 5. fully conversant in the statutory and regulatory requirements and ML/TF risks arising from your business | | |
| | 6. capable of accessing on a timely basis all required available information to undertake its role | | |

| | | | |
|---|---|---|---|
| | 7. equipped with sufficient resources, including staff | | |
| | 8. overseeing your firm's compliance with the relevant AML requirements in Pakistan and overseas branches and subsidiaries | | |
| | | | |
| | (b) Audit function | | |
| | (I) Have you established an independent audit function? | | |
| | (II) If yes, does the function regularly review the AML/CFT systems to ensure effectiveness? | | |
| | (III) If appropriate, have you sought review assistance from external sources regarding your AML/CFT systems? | | |
| | (c) Staff screening | | |
| | (I) Do you establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees? | | |
| | | | |
| 3 | RP with overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure an overall compliance with the CDD and record-keeping requirements. | | |
| | Does your firm have overseas branches and subsidiary undertakings? | | |
| | Do you have a group AML/CFT policy to ensure that all overseas branches and subsidiary undertakings have procedures in place to comply with the CDD and record-keeping requirements similar to those set under the AML Regulations? | | |
| | | | |
| | If yes, is such policy well communicated within your group? | | |
| | | | |
| | In the case where your overseas branches or subsidiary undertakings are unable to comply with the above mentioned policy due to local laws' restrictions, have you done the following? | | |
| | (a) Inform the SECP of such failure | | |
| | (b) take additional measures to effectively mitigate ML/TF risks faced by them | | |
| | | | |
| | ***(B) Risk-Based Approach ('RBA')*** | | |
| 4 | RPs are required to determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction or service used by that customer. | | |
| | Does your RBA identify and categorize ML/TF risks at the customer level and establish reasonable measures based on risks identified? | | |
| | Do you consider the following risk factors when determining the ML/TF risk rating of customers? | | |
| | (a) Country risk - customers with residence in or connection with the below high-risk jurisdictions | | |
| | (I) countries identified by the FATF as jurisdictions with strategic AML/CFT deficiencies | | |
| | (II) countries subject to sanctions, embargoes or similar measures issued by international authorities | | |
| | (III) countries which are vulnerable to corruption | | |
| | (Iv) countries that are believed to have strong links to terrorist activities | | |
| | | | |
| | (b) Customer risk - customers with the below nature or behaviour might present a higher ML/TF risk | | |
| | (I) the public profile of the customer indicating involvement with, or connection to, politically exposed persons ("PEPs") | | |
| | (II) complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial rationale | | |

| | | | |
|---|---|---|---|
| | (iii) request to use numbered accounts or undue levels of secrecy with a transaction | | |
| | (iv) involvement in cash-intensive businesses | | |
| | (v) nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities | | |
| | (vi) the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified | | |
| | | | |
| | (c) Product/service risk - product/service with the below factors might present a higher risk | | |
| | (i) services that inherently have provided more anonymity | | |
| | (ii) ability to pool underlying customers/funds | | |
| | | | |
| | (d) Distribution/delivery channels | | |
| | (i) a non-face-to-face account opening approach is used | | |
| | (ii) Business sold through third party agencies or intermediaries | | |
| | | | |
| | Do you adjust your risk assessment of customers from time to time or based upon information received from a competent authority, and review the extent of the CDD and ongoing monitoring to be applied? | | |
| | | | |
| | Do you maintain all records and relevant documents of the above risk assessment? | | |
| | If yes, are they able to demonstrate to the SECP the following? | | |
| | (a) how you assess the customer | | |
| | (b) the extent of CDD and ongoing monitoring is appropriate based on that customer's ML/TF risk | | |
| | | | |
| | ***(C) - Customer Due Diligence ('CDD')*** | | |
| **5** | RPs are required to carry out CDD, which is a vital tool for recognizing whether there are grounds for knowledge or suspicion of ML/TF. | | |
| | Do you conduct the following CDD measures? | | |
| | (a) identify the customer and verify the customer's identity using reliable, independent source documents, data or information | | |
| | (b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity, including in the case of a legal person or trust, measures to enable you to understand the ownership and control structure of the legal person or trust | | |
| | (c) obtain information on the purpose and intended nature of the business relationship established with you unless the purpose and intended nature are obvious | | |
| | (d) if a person purports to act on behalf of the customer: | | |
| | (i) identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information | | |
| | (ii) verify the person's authority to act on behalf of the customer (e.g. written authority, board resolution) | | |
| | | | |
| | Do you apply CDD requirements in the following conditions? | | |
| | (a) at the outset of a business relationship | | |
| | (b) when you suspect that a customer or a customer's account is involved in ML/TF | | |
| | (c) when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity | | |
| | | | |
| **6** | RPs are required to identify and take reasonable measures to verify the identity of a beneficial owner. | | |
| | | | |

| | | | |
|---|---|---|---|
| | When an individual is identified as a beneficial owner, do you obtain the following identification information? | | |
| | (a) Full name | | |
| | (b) Date of birth | | |
| | (c) Nationality | | |
| | (d) Identity document type and number | | |
| | | | |
| | Do you verify the identity of beneficial owner(s) with reasonable measures, based on its assessment of the ML/TF risks, so that you know who the beneficial owner(s) is? | | |
| | | | |
| 7 | RPs are required to identify and take reasonable measures to verify the identity of a person who purports to act on behalf of the customer and is authorized to give instructions for the movement of funds or assets. | | |
| | | | |
| | When a person purports to act on behalf of a customer and is authorized to give instructions for the movement of funds or assets, do you obtain the identification information and take reasonable measures to verify the information obtained? | | |
| | | | |
| | Do you obtain the written authorization to verify that the individual purporting to represent the customer is authorized to do so? | | |
| | | | |
| | Do you use a streamlined approach on occasions where difficulties have been encountered in identifying and verifying signatories of individuals being represented to comply with the CDD requirements? | | |
| | If yes, do you perform the following: | | |
| | (a) adopt an RBA to assess whether the customer is a low risk customer and that the streamlined approach is only applicable to these low risk customers | | |
| | (b) obtain a signatory list, recording the names of the account signatories, whose identities and authority to act have been confirmed by a department or person within that customer which is independent to the persons whose identities are being verified | | |
| | | | |
| 8 | RPs are required to take appropriate steps to verify the genuineness of identification provided if suspicions are raised. | | |
| | | | |
| | In case of suspicions raised in relation to any document in performing CDD, have you taken practical and proportionate steps to establish whether the document offered is genuine, or has been reported as lost or stolen? (e.g. search publicly available information, approach relevant authorities) | | |
| | | | |
| | Have you rejected any documents provided during CDD and considered making a report to the authorities (e.g. FIU, police) where suspicion on the genuineness of the information cannot be eliminated? | | |
| | | | |
| 9 | RPs are required to understand the purpose and intended nature of the business relationship established. | | |
| | | | |
| | Unless the purpose and intended nature are obvious, have you obtained satisfactory information from all new customers (including non-residents) as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the relevant account opening documentation? | | |
| | | | |
| 10 | RPs are required to complete the CDD before establishing business relationships. | | |
| | | | |
| | Do you always complete the CDD process before establishing business relationships? If you always complete CDD process before establishing a business relationship | | |

| | | | |
|---|---|---|---|
| | | | |
| | If you are unable to complete the CDD process, do you ensure that the relevant business relationships must not be established and assess whether this failure provides grounds for knowledge or suspicion of ML/TF to submit a report to the FMU as appropriate? | | |
| | | | |
| | If the CDD process is not completed before establishing a business relationship, would these be on an exception basis only and with consideration of the following: | | |
| | (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed. | | |
| | (b) it is necessary not to interrupt the normal course of business with the customer (e.g. securities [illegible]) | | |
| | (c) verification is completed as soon as reasonably practicable. | | |
| | (d) the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable. | | |
| | | | |
| | Have you adopted appropriate risk management policies and procedures when a customer is permitted to enter into a business relationship prior to verification? | | |
| | | | |
| | If yes, do they include the following? | | |
| | (a) establishing timeframes for the completion of the identity verification measures and that it is carried out as soon as reasonably practicable | | |
| | (b) placing appropriate limits on the number of transactions and type of transactions that can be undertaken pending verification | | |
| | (c) ensuring that funds are not paid out to any third party | | |
| | (d) other relevant policies and procedures | | |
| | | | |
| | When terminating a business relationship where funds or other assets have been received, have you returned the funds or assets to the source (where possible) from which they were received? | | |
| | | | |
| **11** | RPs are required to keep the customer information up-to-date and relevant. | | |
| | | | |
| | Do you undertake reviews of existing records of customers to ensure that the information obtained for the purposes of complying with the AML requirements are up-to-date and relevant when one of the following trigger events happen? | | |
| | (a) when a significant transaction is to take place | | |
| | (b) when a material change occurs in the way the customer's account is operated | | |
| | (c) when your customer documentation standards change substantially | | |
| | (d) when you are aware that you lack sufficient information about the customer concerned | | |
| | (e) if there are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box | | |
| | | | |
| | Are all high-risk customers subject to a review of their profile? | | |
| | | | |
| **12** | RPs are required to identify and verify the true and full identity of each natural person by using reliable and independent sources of information. | | |
| | Do you have customers which are natural persons? | | |
| | | | |
| | Do you collect the identification information for customers: | | |
| | (I) Residents | | |
| | (II) Non-residents | | |
| | (III) Non-residents who are not physically present | | |

| | | | |
|---|---|---|---|
| | | | |
| | Do you document the information? | | |
| | | | |
| | If yes, please provide a list of acceptable documents that you obtain for verifying residential address (e.g. utility bills or bank statements). For the avoidance of doubt, please note according to the Guideline on AML and CFT that certain types of address verification should not be considered sufficient, e.g. a post office box address, for persons residing in Pakistan or corporate customers registered and/or operating in Pakistan. | | |
| | | | |
| | In cases where customers may not be able to produce verified evidence of residential address have you adopted alternative methods and applied these on a risk sensitive basis? | | |
| | | | |
| | Do you require additional identity information to be provided or verify additional aspects of identity if the customer, or the product or service, is assessed to present a higher ML/TF risk? | | |
| | | | |
| **13** | RPs are required to identify and verify the true and full identity of each legal person and trust and its beneficial owners by using reliable and independent sources of information. | | |
| | | | |
| | Do you have measures to look behind each legal person or trust to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets? | | |
| | | | |
| | Do you fully understand the customer's legal form, structure and ownership, and obtain information on the nature of its business, and reasons for seeking the product or service when the reasons are not obvious? | | |
| | | | |
| **14** | Corporation | | |
| | | | |
| | Do you have customers which are corporations? | | |
| | | | |
| | Do you obtain the following information and verification documents in relation to a customer which is a corporation? | | |
| | | | |
| | For companies with multiple layers in their ownership structures, do you have an understanding of the ownership and control structure of the company and fully identify the intermediate layers of the company? | | |
| | | | |
| | Do you take further measures, when the ownership structure of the company is dispersed/ complex/multi-layered without an obvious commercial purpose, to verify the identity of the ultimate beneficial owners? | | |
| | | | |
| | | | |
| **15** | Partnerships and unincorporated bodies | | |
| | | | |
| | Do you have customers which are partnerships or unincorporated bodies? | | |
| | | | |
| | Do you take reasonable measures to verify the identity of the beneficial owners of the partnerships or unincorporated bodies? | | |
| | | | |
| | Do you obtain the information and verification documents in relation to the partnership or unincorporated body? | | |
| | | | |
| | Do you have customers which are in the form of trusts? | | |

| | | | |
|---|---|---|---|
| | | | |
| | Do you obtain the information and verification documents to verify the existence, legal form and parties to a trust? | | |
| | | | |
| | Have you taken particular care in relation to trusts created in jurisdictions where there is no or weak money laundering legislation? | | |
| | | | |
| | | | |
| **16** | RPs may conduct simplified 'Know Your Customer' due diligence ('SDD') process instead of full CDD measures given reasonable grounds to support it. Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing. SDD is a condition where the timing of the actual verification of a particular customer is deferred until such time the entire CDD process is completed, rather than reducing what needs to be obtained, under a risk-based approach. | | |
| | Have you conducted SDD instead of full CDD measures for your customers? | | |
| | | | |
| | Do you refrain from applying SDD when you suspect that the customer, the customer's account or the transaction is involved in ML/TF, or when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying or verifying the customer? | | |
| | | | |
| | Before the application of SDD on any of the customer categories, have you performed checking on whether they meet the criteria of the respective category? | | |
| | | | |
| **17** | RPs are required, in any situation that by its nature presents a higher risk of ML/TF, to take additional measures to mitigate the risk of ML/TF. | | |
| | Do you take additional measures or enhanced due diligence ('EDD') when the customer presents a higher risk of ML/TF? | | |
| | | | |
| | If yes, do they include the following? | | |
| | (a) obtaining additional information on the customer and updating more regularly the customer profile including the identification data | | |
| | (b) obtaining additional information on the intended nature of the business relationship, the source of wealth and source of funds | | |
| | (c) obtaining the approval of senior management to commence or continue the relationship | | |
| | (d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination. | | |
| | | | |
| **18** | RPs are required to apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview. | | |
| | Do you accept customers that are not physically present for identification purposes to open an account? | | |
| | | | |
| | If yes, have you taken additional measures to compensate for any risk associated with customers not physically present (i.e. face to face) for identification purposes? | | |
| | | | |
| | If yes, do you document such information? | | |
| | | | |
| **19** | RPs are required to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person ('PEP') and to adopt EDD on PEPs. | | |
| | | | |

| | | | |
|---|---|---|---|
| | Do you define what a PEP (foreign and domestic) is in your AML/CFT policies and procedures? | | |
| | | | |
| | Have you established and maintained effective procedures for determining whether a customer or a beneficial owner of a customer is a PEP (foreign and domestic)? | | |
| | | | |
| | If yes, is screening and searches performed to determine if a customer or a beneficial owner of a customer is a PEP? (e.g. through commercially available databases, publicly available sources and internet / media searches etc) | | |
| | | | |
| 20 | Foreign PEPs | | |
| | | | |
| | Do you conduct EDD at the outset of the business relationship and ongoing monitoring when a foreign PEP is identified or suspected? | | |
| | | | |
| | Have you applied the following EDD measures when you know that a particular customer or beneficial owner is a foreign PEP (for both existing and new business relationships)? | | |
| | (a) obtaining approval from your senior management | | |
| | (b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds | | |
| | (c) applying enhanced monitoring to the relationship in accordance with the assessed risks | | |
| | | | |
| 21 | Domestic PEPs | | |
| | | | |
| | Have you performed a risk assessment for an individual known to be a domestic PEP to determine whether the individual poses a higher risk of ML/TF? | | |
| | | | |
| | If yes and the domestic PEP poses a higher ML/TF risk, have you applied EDD and monitoring specified in question C.40 above? | | |
| | If yes, have you retained a copy of the assessment for related authorities, other authorities and auditors and reviewed the assessment whenever concerns as to the activities of the individual arise? | | |
| | | | |
| | For foreign and domestic PEPs assessed to present a higher risk, are they subject to a minimum of an annual review and ensure the CDD information remains up-to-date and relevant? | | |
| | | | |
| 22 | RPs have the ultimate responsibility for ensuring CDD requirements are met, even intermediaries were used to perform any part of the CDD measures. | | |
| | Have you used any intermediaries to perform any part of your CDD measures? | | |
| | | | |
| | When intermediaries (not including those in contractual arrangements with the RFI to carry out its CDD function or business relationships, accounts or transactions between RFI for their clients) are relied on to perform any part of the CDD measures, do you obtain written confirmation from the intermediaries that: | | |
| | (a) they agree to perform the role | | |
| | (b) they will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of you upon request. | | |
| | | | |
| | When you use an intermediary, are you satisfied that it has adequate procedures in place to prevent ML/TF? | | |
| | | | |
| | When you use overseas intermediaries, are you satisfied that it: | | |
| | (a) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction | | |
| | (b) has measures in place to ensure compliance with requirements | | |

| | | | |
|---|---|---|---|
| | (c) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities in PK | | |
| | | | |
| | In order to ensure the compliance with the requirements set out above for both domestic or overseas intermediaries, do you take the following measures? | | |
| | (a) review the intermediary's AML/CFT policies and procedures | | |
| | (b) make enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited | | |
| | | | |
| | Do you immediately (with no delay) obtain from intermediaries the data or information that the intermediaries obtained in the course of carrying out the CDD measures? | | |
| | | | |
| | Do you conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay? | | |
| | | | |
| | Have you taken reasonable steps to review intermediaries' ability to perform its CDD whenever you have doubts as to the reliability of intermediaries? | | |
| | | | |
| **23** | RPs are required to perform CDD measures on pre-existing customers when trigger events occur. | | |
| | | | |
| | Have you performed CDD measures on your pre-existing customers when one of the following trigger events happens? | | |
| | (a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is inconsistent with your knowledge of the customer or the customer's business or risk profile, or with your knowledge of the source of the customer's funds | | |
| | (b) a material change occurs in the way in which the customer's account is operated | | |
| | (c) you suspect that the customer or the customer's account is involved in ML/TF | | |
| | (d) you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying and verifying the customer's identity | | |
| | (e) Are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box | | |
| | | | |
| **24** | RPs are not allowed to maintain anonymous accounts or accounts in fictitious names for any new or existing customers. | | |
| | | | |
| | Do you refrain from maintaining (for any customer) anonymous accounts or accounts in fictitious names? | | |
| | | | |
| **25** | RPs are required to assess and determine jurisdictional equivalence as this is an important aspect in the application of CDD measures. | | |
| | | | |
| | When you do your documentation for assessment or determination of jurisdictional equivalence, do you take the following measures? | | |
| | (a) make reference to up-to-date and relevant information | | |
| | (b) retain such record for regulatory scrutiny | | |
| | (c) periodically review to ensure it remains up-to-date and valid | | |
| | | | |
| | ***(D) - Ongoing monitoring*** | | |
| **26** | RPs are required to perform effective ongoing monitoring for understanding customer's activities and it helps the firm to know the customers and to detect unusual or suspicious activities. | | |
| | | | |
| | Do you continuously monitor your business relationship with a customer by: | | |
| | (a) monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds. | | |

| | | | |
|---|---|---|---|
| | (b) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF | | |
| | | | |
| | Do you monitor the following characteristics relating to your customer's activities and | | |
| | (a) the nature and type of transaction (e.g. abnormal size of frequency) | | |
| | (b) the nature of a series of transactions (e.g. a number of cash deposits) | | |
| | (c) the amount of any transactions, paying particular attention to substantial transactions | | |
| | (d) the geographical origin/destination of a payment or receipt | | |
| | (e) the customer's normal activity or turnover | | |
| | | | |
| | Do you regularly identify if the basis of the business relationship changes for customers when the following occur? | | |
| | (a) new products or services that pose higher risk are entered into | | |
| | (b) new corporate or trust structures are created | | |
| | (c) the stated activity or turnover of a customer changes or increases | | |
| | (d) the nature of transactions change or the volume or size increases | | |
| | (e) If there are other situations, please specify and further elaborate in the text box | | |
| | | | |
| | In the case where the basis of a business relationship changes significantly, do you carry out further CDD procedures to ensure that the ML/TF risk and basis of the relationship are fully understood? | | |
| | | | |
| | Have you established procedures to conduct a review of a business relationship upon the filing of a report to the FMU and do you update the CDD information thereafter? | | |
| | | | |
| 27 | RPs are required to link the extent of ongoing monitoring to the risk profile of the customer determined through RBA. | | |
| | | | |
| | Have you taken additional measures with identified high risk business relationships (including PEPs) in the form of more intensive and frequent monitoring? | | |
| | | | |
| | If yes, have you considered the following: | | |
| | (a) whether adequate procedures or management information systems are in place to provide relevant staff with timely information that might include any information on any connected accounts or relationships | | |
| | (b) how to monitor the sources of funds, wealth and income for higher risk customers and how any change in circumstances will be recorded | | |
| | | | |
| | Do you take into account the following factors when considering the best measures to monitor customer transactions and activities? | | |
| | (a) the size and complexity of its business | | |
| | (b) assessment of the ML/TF risks arising from its business | | |
| | (c) the nature of its systems and controls | | |
| | (d) the monitoring procedures that already exist to satisfy other business needs | | |
| | (e) the nature of the products and services (including the means of delivery or communication) | | |
| | | | |
| | In the case where transactions are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, do you examine the background and purpose, including where appropriate the circumstances of the transactions? | | |
| | | | |
| | If yes, are the findings and outcomes of these examinations properly documented in writing and readily available for the SECP, competent authorities and auditors? | | |
| | | | |

| | | | |
|---|---|---|---|
| | In the case where you have been unable to satisfy that any cash transaction or third party transfer proposed by customers is reasonable and therefore consider it suspicious, do you make a suspicious transaction report to the FMU? | | |
| | | | |
| | ***(E) - Financial sanctions and terrorist financing*** | | |
| 28 | RPs have to be aware of the scope and focus of relevant financial/trade sanctions regimes. | | |
| | | | |
| | Do you have procedures and controls in place to: | | |
| | (a) ensure that no payments to or from a person on a sanctions list that may affect your operations is made | | |
| | (b) screen payment instructions to ensure that proposed payments to designated parties under applicable laws and regulations are not made | | |
| | | | |
| | If yes, does this include: | | |
| | (a) drawing reference from a number of sources to ensure that you have appropriate systems to conduct checks against relevant lists for screening purposes | | |
| | (b) procedures to ensure that the sanctions list used for screening are up to date | | |
| | | | |
| | Do you take the following measures to ensure compliance with relevant regulations and legislation on TF? | | |
| | (a) understand the legal obligations of your institution and establish relevant policies and procedures | | |
| | (b) ensure relevant legal obligations are well understood by staff and adequate guidance and training are provided | | |
| | (c) ensure the systems and mechanisms for identification of suspicious transactions cover TF as well as ML | | |
| | | | |
| | Do you maintain a database (internal or through a third party service provider) of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have been made known to it? | | |
| | | | |
| | If yes, have you also taken the following measures in maintaining the database? | | |
| | (a) ensure that the relevant designations are included in the database. | | |
| | (b) the database is subject to timely update whenever there are changes | | |
| | (c) the database is made easily accessible by staff for the purpose of identifying suspicious transactions | | |
| | | | |
| | Do you perform comprehensive screening of your complete customer base to prevent TF and sanction violations? | | |
| | | | |
| | If yes, does it include the following? | | |
| | (a) screening customers against current terrorist and sanction designations at the establishment of the relationship | | |
| | (b) screening against your entire client base, as soon as practicable after new terrorist and sanction designation are published by the SECP | | |
| | | | |
| | Do you conduct enhanced checks before establishing a business relationship or processing a transaction if there are circumstances giving rise to a TF suspicion? | | |
| | | | |
| | Do you document or record electronically the results related to the comprehensive ongoing screening, payment screening and enhanced checks if performed? | | |
| | | | |
| | Do you have procedures to file reports to the FMU if you suspect that a transaction is terrorist-related, even if there is no evidence of a direct terrorist connection? | | |
| | | | |

| | | | |
|---|---|---|---|
| | **(F) - Suspicious Transaction reports** | | |
| 29 | RPs are required to adopt on-going monitoring procedures to identify suspicious transactions for the reporting of funds or property known or suspected to be proceeds of crime or terrorist activity to the Joint Financial Intelligence Unit ("FMU"). | | |
| | | | |
| | Do you have policy or system in place to make disclosures/suspicious transaction reports with the FMU? | | |
| | | | |
| | | | |
| | Do you apply the following principles once knowledge or suspicion has been formed? | | |
| | (a) In the event of suspicion of ML/TF, a disclosure is made even where no transaction has been conducted by or through your institution | | |
| | (b) Internal controls and systems are in place to prevent any directors, officers and employees, especially those making enquiry with customers or performing additional or enhanced CDD process,committing the offence of tipping off the customer or any other person who is the subject of the disclosure | | |
| | | | |
| | Do you provide sufficient guidance to your staff to enable them to form a suspicion or to recognise when ML/TF is taking place? | | |
| | | | |
| | If yes, do you provide guidance to staff on identifying suspicious activity taking into account the following: | | |
| | (a) the nature of the transactions and instructions that staff is likely to encounter | | |
| | (b) the type of product or service | | |
| | (c) the means of delivery | | |
| | | | |
| | Do you ensure your staff are aware and alert with the SECP's guidelines with relation to: | | |
| | (a) potential ML scenarios using Red Flag Indicators | | |
| | (b) potential ML involving employees of RPs. | | |
| | | | |
| | | | |
| | Subsequent to a customer suspicion being identified, have you made prompt disclosures to the FMU if the following additional requests are made by the customer: Note: RPs are required to make prompt disclosure to FMU in any event, but the following requests are considered to be more urgent. | | |
| | (a) Instructed you to move funds | | |
| | (b) close the account | | |
| | (c) make cash available for collection | | |
| | (d) carry out significant changes to the business relationship | | |
| | | | |
| | **(G) - Record Keeping and Retention of Records** | | |
| 30 | RPs are required to maintain customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements. | | |
| | | | |
| | Do you keep the documents/ records relating to customer identity? | | |
| | | | |
| | If yes to the above documents/ records, are they kept throughout the business relationship with the customer and for a period of six years after the end of the business relationship? Note: While the AMLO identifies relevant documents to be retained for 6 years, the RFI should consider other SECP requirements when determining the record keeping and retention period of each document. | | |
| | | | |
| | Do you keep the following documents/ records relating to transactions? | | |
| | (a) the identity of the parties to the transaction | | |
| | (b) the nature and date of the transaction | | |

| | | | |
|---|---|---|---|
| | (c) the type and amount of currency involved | | |
| | (d) the origin of the funds | | |
| | (e) the form in which the funds were offered or withdrawn | | |
| | (f) the destination of the funds | | |
| | (g) the form of instruction and authority | | |
| | (h) the type and identifying number of any account involved in the transaction | | |
| | | | |
| | Are the documents/ records, they kept for a period of five years after the completion of a transaction, regardless of whether the business relationship ends during the period as required under the AML/CFT Regulations? | | |
| | | | |
| | In the case where customer identification and verification documents are held by intermediaries, do you ensure that the intermediaries have systems in place to comply with all the record-keeping requirements? | | |
| | | | |
| | ***(H) - Staff Training*** | | |
| **31** | RPs are required to provide adequate ongoing training for staff in what they need to do to carry out their particular roles with respect to AML/CFT. | | |
| | | | |
| | Have you implemented a clear and well articulated policy to ensure that relevant staff receive adequate AML/CFT training? | | |
| | | | |
| | Do you provide AML/CFT training to your staff to maintain their AML/CFT knowledge and competence? | | |
| | | | |
| | If yes, does the training program cover the following topics? | | |
| | (a) your institution's and the staff's own personal statutory obligations and the possible consequences for failure to report suspicious transactions under relevant laws and regulations | | |
| | (b) any other statutory and regulatory obligations that concern your institution and the staff under the relevant laws and regulations, and the possible consequences of breaches of these obligations | | |
| | (c) your own policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting | | |
| | (d) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by your staff to carry out their particular roles in your institution with respect to AML/CFT | | |
| | | | |
| | Do you provide AML/CFT training for all your new staff, irrespective of their seniority and before work commencement? | | |
| | | | |
| | If yes, does the training program cover the following topics? | | |
| | (a) an introduction to the background to ML/TF and the importance placed on ML/TF by your institution | | |
| | (b) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of 'tipping-off' | | |
| | | | |
| | Do you provide AML/CFT training for your members of staff who are dealing directly with the public? | | |
| | | | |
| | If yes, does the training program cover the following topics? | | |
| | (a) the importance of their role in the institution's ML/TF strategy, as the first point of contact with potential money launderers | | |
| | (b) your policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities | | |

| | | | |
|---|---|---|---|
| | (c) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required | | |
| | | | |
| | Do you provide AML/CFT training for your back-office staff? | | |
| | If yes, does the training program cover the following topics? | | |
| | (a) appropriate training on customer verification and relevant processing procedures | | |
| | (b) how to recognise unusual activities including abnormal settlements, payments or delivery instructions | | |
| | | | |
| | Do you provide AML/CFT training for managerial staff including internal audit officers and COs? | | |
| | | | |
| | If yes, does the training program cover the following topics? | | |
| | (a) higher level training covering all aspects of your AML/CFT regime | | |
| | (b) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the FMU | | |
| | | | |
| | Do you provide AML/CFT training for your MLROs? | | |
| | | | |
| | If yes, does the training program cover the following topics? | | |
| | (a) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the FMU | | |
| | (b) training to keep abreast of AML/CFT requirements/developments generally | | |
| | | | |
| | Do you maintain the training record details for a minimum of 3 years? | | |
| | | | |
| | If yes, does the training record include the following details: | | |
| | (a) which staff has been trained | | |
| | (b) when the staff received training | | |
| | (c) the type of training provided | | |
| | | | |
| | Do you monitor and maintain the effectiveness of the training conducted by staff by: | | |
| | (a) testing staff's understanding of the LC's / AE's policies and procedures to combat ML/TF | | |
| | (b) testing staff's understanding of their statutory and regulatory obligations | | |
| | (c) testing staff's ability to recognize suspicious transactions | | |
| | (d) monitoring the compliance of staff with your AML/CFT systems as well as the quality and quantity of internal reports | | |
| | (e) identifying further training needs based on training / testing assessment results identified | | |
| | | | |
| | ***(I) Wire Transfers*** | | |
| | Do you ask for further explanation of the nature of the wire transfer from the customer if there is suspicion that a customer may be effecting a wire transfer on behalf of a third party? | | |
| | | | |
| | Do you have clear policies on the processing of cross-border and domestic wire transfers? | | |
| | | | |
| | If yes, do the policies address the following? | | |
| | (a) record-keeping | | |
| | (b) the verification of originator's identity information | | |
| | | | |
| | Do you include wire transfers in your ongoing due diligence on the business relationship with the originator and the scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with your knowledge of the customer, its business and risk profile? | | |

**Annex 3**

## ML/TF Warning Signs/ Red Flags

The following are some of the warning signs or "red flags" to which RPs should be alerted. The list is not exhaustive, but includes the following:

**Insurance entities**

(1) Requests for a return of premium to be remitted to persons other than the policy holder.
(2) Claims payments paid to persons other than policyholders and beneficiaries.
(3) Unusually complex holding company or trust ownership structure.
(4) Making a false claim.
(5) A change in beneficiaries (for instance, to include non-family members).
(6) 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).
(7) Use of cash and/or payment of large single premiums.
(8) Payment/surrender by a wire transfer from/to foreign parties.
(9) Payment by banking instruments that allow anonymity of the transaction.
(10) Payment from third parties.
(11) Change of address and/or place of residence of the policyholder.
(12) Lump sum top-ups to an existing life insurance contract.
(13) Lump sum contributions to personal pension contracts.
(14) Requests for prepayment of benefits.
(15) 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).
(16) Change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment).
(17) Early surrender of the policy or change of the duration (particularly where this results in penalties).
(18) Requests for multiple policies to be taken out for premiums slightly below any publicised limits for performing checks, such as checks on the source of wealth or cash payments.

**Lending NBFCs**

(1) Loans secured by pledged assets held by third parties unrelated to the borrower.
(2) Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
(3) Borrower defaults on cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
(4) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
(5) 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.
(6) 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).

**Mutual Funds**

(1) When an investor is more concerned about the subscription and redemption terms of the Mutual Fund than with other information related to the investment strategy, service providers, performance history of the investment manager, etc.
(2) Lack of concern by an investor regarding losses or (large) fees or offering to pay extraordinary fees for early redemption;
(3) Sudden and unexplained subscriptions and redemptions;
(4) Quick purchase and redemption of units despite penalties;
(5) Requests to pay redemptions proceeds to a third (unrelated) party; and
(6) Customer that exhibits unusual concern with compliance with AML/CFT reporting requirements or other( AML/CFT) policies and procedures.

**Brokerage Houses**

(1) Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
(2) Customers who wish to deal on a large scale but are completely unknown to the broker;
(3) Customers who wish to invest or settle using cash;
(4) Customers who use a cheque that has been drawn on an account other than their own;
(5) Customers who change the settlement details at the last moment;
(6) Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
(7) Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
(8) Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
(9) Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
(10) Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
(11) 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;
(12) Customer trades frequently, selling at a loss
(13) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
(14) 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;
(15) Any transaction involving an undisclosed party;
(16) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
(17) Significant variation in the pattern of investment without reasonable or acceptable explanation
(18) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
(19) Transactions involve penny/microcap stocks.
(20) 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.

(21) Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
(22) Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
(23) Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
(24) Customer conducts mirror trades.
(25) Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

**Annex 4**

## Proliferation Financing Warning Signs/Red Alerts

RPs should take note of the following circumstances where customers and transactions are more vulnerable to be involved in proliferation financing activities relating to both DPRK and Iran sanctions regimes:

(a) customers and transactions associated with countries subject to sanctions;

(b) instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;

(c) customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;

(d) reasonableness of invoiced goods against market value, inconsistency or discrepancies in trade-related documentation.

In particular, RPs should be alert to the following non-exhaustive list of factors that are relevant to the DPRK sanctions regime:

(a) significant withdrawals or deposits of bulk cash that could potentially be used to evade targeted financial sanctions and activity-based financial prohibitions;

(b) opening of banking accounts by DPRK diplomatic personnel, who have been limited to one account each under relevant UNSCRs (including number of bank accounts being held, holding of joint accounts with their family members);

(c) clearing of funds, granting of export credits or guarantees to persons or entities that are associated with trading transactions relating to the DPRK;

(d) providing insurance or re-insurance services to maritime vessels owned, controlled or operated, including through illicit means, by the DPRK or classification services to vessels which there are reasonable grounds to believe were involved in activities, or the transport of items, prohibited by UNSCRs concerning the DPRK, unless the Security Council 1718 Committee determines otherwise on a case-by-case basis;

(e) direct or indirect supply, sale or transfer to the DPRK of any new or used vessels or providing insurance or re-insurance services to vessels owned, controlled, or operated, including through illicit means, by the DPRK, except as approved in advance by the Security Council 1718 Committee on a case-by-case basis; or

(f) the leasing, chartering or provision of crew services to the DPRK without exception, unless the Security Council 1718 Committee approves on a case-by-case basis in advance;38 or

(g) using real property that DPRK owns or leases in Pakistan for any purpose other than diplomatic or consular activities.

In case of any clarification/ enquiry, kindly contact Anti-Money Laundering Department, Securities and Exchange Commission of Pakistan at the following address:

Service Desk,
Securities and Exchange Commission of Pakistan
NIC Building, 63 Jinnah Avenue,
Islamabad
Telephone: +92-51-9100422
PABX: +92-51-9100496 Ext: 422
Email: aml.dept@secp.gov.pk