GUIDELINES

ON

SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

(ANTI-MONEY LAUNDERING AND

COUNTERING FINANCING OF TERRORISM)

REGULATIONS, 2018

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.

5. 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. RPs shall, before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied, take into account all the relevant risk factors, such as geography, products and services, delivery channels, types of customers, or jurisdictions within which it or its customers do business. As is the case for an RPs' overall risk management, RPs' senior management should understand the nature and level of the risks that they are exposed to and ensure that systems and processes are in place to identify, assess, monitor, manage and mitigate ML/TF risks.

iii. 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. Their 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. Their delivery channels.
3) Design and implement policies, controls and procedures that are approved by its Board of Directors to manage and mitigate the ML/TF risks identified and assessed;
4) Monitor and evaluate the implementation of mitigating controls and improve systems where necessary;
5) Keep their risk assessments current through ongoing reviews and, when necessary, updates;
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.

iv. 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.

v. 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. Since the funds used for TF may emanate from legal sources, the nature of the sources may vary when the source of the TF originate from criminal activities, the risk assessment related to ML is also applicable to TF.

vi. 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.

vii. 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. RPs should understand, identify and assess the inherent ML/TF risks posed by its customer base, products and services offered, delivery channels and the jurisdictions within which it or its customers do business, and any other relevant risk category. The risk assessment policies and procedures adopted by RPs should be appropriate to their size, nature and complexity.

ii. ML/TF risks may be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk for determining the overall risk classification (e.g. high, medium or low). RPs should make their own determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, RPs should take into consideration the relevance of different risk factors in the context of a particular customer relationship.

iii. 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.

iv. For the analysis, the RP 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, medium if it can occur once 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 minor if they is an only short-term or there are low-cost consequences, to very major, when they are found to be very costly inducing long-term consequences that affect the proper functioning of the institution.

v. The following is an example of a risk probability likelihood matrix with 5 risk ratings as an example. RP's can customize their own as applicable to their operation with more details, if preferable.

Probability and Likelihood Risk Rating Matrix

					Consequences					
					Customers	Few or isolated instances of reportable suspicious activity.	Minimal instances of reportable suspicious activity.	Single or a few instances of suspicious activity.	Single or multiple instances of suspicious activity.	Excessive, uncontrollable and manageable instances of suspicious activity.
					Countries	Few or isolated instances of technical exceptions related the organizations operational infrastructure.	Minor compromise of information sensitive to the operations of internal or departmental units.	Compromise of information sensitive to the organization's use of its operations.	Systemic compromise of information sensitive to the organization's use of its operations.	Porous and uncontrollable comprise of the organization's operations management.
					Products	Minimal losses.	Some losses.	Significant losses.	Extensive damage or losses.	Serious damages and losses.
					Services	Freedom to operated is primarily unaffected. Self assessment and improvements should suffice.	Scrutiny by the Executive, internal communication or internal audit to prevent short term or low cost consequences.	Persistent concerns, scrutiny required. Medium term consequences with some costs.	Persistent intense long term, high cost consequences affecting operations.	Significant losses to the organization's 'Brand' significantly affects its growth and abilities.
					Delivery Channels	Minimal impact on non-core operations. Technical exceptions can be addressed by routine day-to-day operations.	Some impact on the organization's capability in terms of delays and management's performance of controls.	Impact on the organization resulting in reduced performance.	Breakdown of key activities leading to reduction in service and performance.	Protracted unavailability of individuals with critical skills. Critical failure(s) preventing core activities from being performed. Survival of the entity is at risk.
						1	2	3	4	5
	Chance	Probability	Frequency			Insignificant	Minor	Moderate	Major	Significant
Likelihood	Is expected to occur in most circumstances	>95%	Occurs many times a year	E	Almost Certain	M	H	H	VH	VH
	Will probably occur in most circumstances	>65%	Probably occurs several times a year	D	Likely	L	M	H	H	VH
	Might occur at some time	>35%	Probably occurs once a year	C	Possible	L	L	M	H	H
	Could occur at some time	<35%	Unlikely to occur but not impossible	B	Unlikely	VL	L	L	M	H
	May occur in exceptional circumstances	<5%	Rare and unusual probability to occur	A	Rare	VL	VL	L	L	M

Very High	Immediate action required by the Executive with detailed planning, allocation of resources and regular monitoring.
High	Senior management's attention required
Medium	Management's responsibility must be specified
Low	Minor and managed by routine supervisory procedures
Very Low	Managed by routine procedure

vi. 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

(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.

(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.

Low Risk Classification Factors

(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.

Risk Matrix

RPs may use a risk matrix (Annex 1) 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 RP, taking into account its specificities, may also define additional levels of ML/TF risk.

b) Risk Management

Risk Tolerance

i. Risk tolerance is the amount of risk that the RP is willing and able to accept. An RP's risk tolerance impacts its decisions about risk mitigation measures and controls. For example, if an RP determines that the risks associated with a particular type of customer exceed its risk tolerance, it may decide not to accept or maintain that particular type of customer(s). Conversely, if the risks associated with a particular type of customer are within the bounds of an RP's risk tolerance, the RP must ensure that the risk mitigation measures it applies are commensurate with the risks associated with that type of customer(s).
ii. RPs should establish their risk tolerance. Such establishment should be done by senior management and the Board. In establishing the risk tolerance, the RP should consider whether it has sufficient capacity and expertise to effectively manage the risks that it decides to accept and the consequences such as legal, regulatory, financial and reputational, of an AML/CFT compliance failure.
iii. If an RP decides to establish a high-risk tolerance and accept high risks then the RP should have mitigation measures and controls in place commensurate with those high risks.

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.

6. 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.

7. 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 Control Assessment Template (Annex 2) within the period as required by the Commission from time to time.

8. 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.

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.

9. 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.

10. 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 (Annex 3), 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 4 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.

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.

11. <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.

12. 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.

13. 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.

14. 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.

15. 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.

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 2015. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.

vii. 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.

17. Sanctions Compliance

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.; and

(7) visa and travel bans.

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 Sanctions Committee, maintains the consolidated list of individuals and entities subject to the sanctions covering assets freeze, travel ban and arms embargo set out in the UNSC Resolution 1267 (1999) and other subsequent resolutions, concerning ISIL (Daésh)/ Al-Qaida and Taliban and their associated individuals.

iv. Government of Pakistan publishes Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 in the official Gazettes to give effect to the decisions of the UNSC Sanctions Committee and implement UNSC sanction measures in Pakistan. The regularly updated consolidated lists is available at the UN sanctions committee's website, at following link;

www.un.org/sc/committees/1267/aq_sanctions_list.shtml
https://www.un.org/sc/suborg/en/sanctions/1988/materials
https://www.un.org/sc/suborg/en/sanctions/1718/materials
http://www.un.org/en/sc/2231/list.shtml
https://www.un.org/sc/suborg/en/sanctions/1718/prohibited-items

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

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

vi. 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.

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

viii. RPs shall screen customers, beneficial owners, transactions, and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to the relevant sanctions lists, RPs may discover that certain sanctions are applicable to one or more of their customers, existing or new.

ix. Where there is a true match or suspicion, RPs shall take steps that are required to comply with the sanctions obligations including freeze without delay and without prior notice, the funds or other assets of designated persons and entities and reporting to the Commission, if they discover a relationship that contravenes the UNSCR sanction or a proscription.

x. 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.

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.

xi. 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.

xii. 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.

18. AML/CFT Program in a Group-Wide and Cross-Border Context

i. The Regulations require a financial group to have group-wide AML/CFT policies and procedures that are consistently applied and supervised across the group. The group-wide policies should be appropriate to all branches and majority owned subsidiaries of the RP, even though reflecting host jurisdiction (i.e., countries in which a branch or a subsidiary of an RP is located) requirements.

ii. Where the minimum regulatory or legal requirements of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two. In cases where the host jurisdiction requirements are stricter than the group's, RPs should allow the relevant branch or subsidiary to adopt and implement the host jurisdiction local requirements.

iii. Where the AML/CFT requirements of host jurisdiction are less strict than those of Pakistan, RPs shall ensure to have AML/CFT measures consistent with the requirements of Pakistan. Where the host jurisdiction do not permit the proper implementation of AML/CFT measures consistent with those of Pakistan, the RP shall inform the same to the Commission along with the appropriate additional measures that they wish to apply to manage ML/TF risks. Where the proposed additional measures are not sufficient to mitigate the risks, the Commission may make recommendations to the RP on further action.

iv. Policies and procedures should be designed not merely to comply strictly with all relevant laws and regulations, but more broadly to identify, monitor and mitigate group-wide risks. Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global AML/CFT policies and procedures is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements. In this regard, RPs should have robust information-sharing among the head office and all of its branches and subsidiaries. RP's' compliance and internal audit staff, in particular the CO, should evaluate compliance with all aspects of their group's policies and procedures, including the effectiveness of centralized CDD policies and the requirements for sharing information and responding to queries from head office.

19. 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.

Annex 1

AML/CFT Risk Assessment Matrix

This assessment characterizes the threats and areas of vulnerability while identifying management's accountability to effectively manage, assess mitigation, classify the anticipated trends, and evaluate risks. The following is a ratings guide or 'heat map' to assist in clarifying the levels of risk and scores for each identified criteria:

THREATS AND VULNERABLITY RATING		
AML and CFT compliance risk is the current and prospective risk to earnings or capital arising from violations of, or nonconformance, with rules, regulations, prescribed practices, and internal policies and procedures. AML and CFT compliance risk also arises in situations where the laws or rules governing certain financial products or activities of the institution's customers may be ambiguous or untested. This risk exposes the institution to potential civil and criminal prosecution, heavy monetary penalties, payment of damages and asset forfeitures. This risk can lead to diminished reputation, reduced franchise value, limited business opportunities, inability to enforce contracts, reduced expansion potential, and loss of the Financial Institution charter. Therefore all characterized threats and vulnerabilities are considered inherently a High level of risk.		
LEVEL	**SCORE**	**CRITERIA**
♦ High	3	Where activity is significant or positions are large in relation to the Financial institution's resources or to its peer group, where there are higher volumes of currency, difficult in determining source of funds, international transfers, or where the nature of the activity is inherently more complex than normal. The activity potentially could result in significant money laundering or establish a conduit for terrorist financing.
♦ Medium	2	Where positions are average in relation to the Financial institution's resources or to its peer group, where the volume of transactions is average, and where the activity is more typical or traditional. Thus while the activity potentially could result in money laundering activity or establish a conduit for terrorist financing, the risk could be absorbed by the Financial Institution in a normal course of business.
♦ Low	1	Where the volume, size, or nature of activity is such that even if the internal controls have weaknesses, the risk of money laundering or establishment of a conduit for terrorist financing is remote or, if money laundering or establishment of a conduit for terrorist financing were to occur, it would have little negative impact on the Financial institution's overall condition.
♦ None	0	Not applicable or not offered

PROBABILITY RATING		
The anticipated probability based upon, the financial institution's overall management of regulatory risks associated with growing expectations of AML or CFT compliance directly relating to the expansion of products and services offered, which provides a basis for determining risk focus and frequency of monitoring, and impacts to residual risk.		
LEVEL	**SCORE**	**CRITERIA**
♦ Increasing	3	Anticipated growth in volume of new products and services where positions are large in relation to the Financial institution's resources, where the nature of the activity is inherently more complex and management has an uncertain capacity to anticipate and respond to changing economic conditions. The activity potentially could lead to increase opportunities for money laundering or establishment of a conduit for terrorist financing if proper controls are not continually implemented or there are significant changes in key staff members.
♦ Stable	2	Improvement in economic conditions, anticipated growth in products and services where effective controls are in place, and/or there are sufficient staffing or no changes in key staff members that would have an negative effect that would likely lead to a significant opportunity for money laundering or establishment of a conduit for terrorist financing to occur. Products and services are not offered or is not conducted therefore poses no AML or CFT risk
♦ Decreasing	1	Level of risk decreases for opportunities available for money laundering or establishment of a conduit for terrorist financing due to positive economic conditions, reduction in products and services due to streamlining by the financial institution's strategic development, peer strategies or market conditions. Decrease in volume or values due to stagnant market conditions and little customer appetite for technology; or decreased volume of regulatory changes or changes with no significant value and minimal impact
♦ None	0	Not applicable or not offered

INHERENT RISK RATING		
Inherent risk is the risk to the Financial Institution in the absence of any actions management might take to alter either the risk's probability or impact (threats and vulnerability rating + probability rating = inherent risk).		
LEVEL	**SCORE**	**CRITERIA**
♦ High	5+	Significant risk to the Financial Institution and/or its customers through exposure to litigation, exposure to regulatory sanctions or fines, significant damage to the financial institution's reputation, or is a category continually identified as high risk by peers and/or regulators
♦ Medium	3 - 4	Moderate risk to the Financial Institution and/or its customers through undesirable but not significant damage to the financial institution's reputation, or is a category identified as a moderate risk by peers and/or regulators
♦ Low	1 - 2	There are little to no risk to the Financial Institution and/or its customers or is a category identified as a low risk by peers and/or regulators
♦ None	0	Not applicable or not offered

PREVENTIVE CONTROLS RATING		
Description of preventative measures that are in place which ensure that the inherent high risk associated with money laundering and terrorist financing is identified and controlled.		
LEVEL	**SCORE**	**CRITERIA**
♦ Strong	3	Management effectively identifies and controls all major types of risk posed by the relevant product/service. The employees participate in managing risk and ensures that appropriate policies and limits exist, and the board understands, reviews, and approves them.. Policies and limits are supported by risk monitoring procedures, reports, and management information systems that provide necessary information and analyses to make timely and appropriate responses to changing conditions. Internal controls and audit procedures are appropriate to the size and activities of the institution. There are few recommendations to change established policies and procedures, where none would likely lead to a significant opportunity for money laundering or establishment of a conduit for terrorist financing.
♦ Adequate	2	The mitigating factors and controls, although largely effective, may be lacking to some modest degree and are being addressed. Overall, employee oversight, policies and limits, risk monitoring procedures, reports and management information systems are considered effective in maintaining a safe and sound Financial Institution
♦ Weak	1	There are no policy, procedures, or processes in place. The lack of a internal control system is continually indicated by auditors and/or examiners as an exception. The safety and soundness of the Financial Institution is likely in jeopardy if not addressed immediately.
♦ None	0	Not applicable or not offered

RESIDUAL RISK RATING		
Residual risk is the risk which remains from inherent risk after all mitigating controls have been considered. Procedures, policies, processes, or other measures are in place and applied to current environment to mitigate risk associated with the threat or vulnerability. (inherent risk – preventive controls rating = residual risk).		
LEVEL	**SCORE**	**CRITERIA**
♦ High	4+	Mitigating risk factors and preventive controls have not been established and/or have significant weaknesses to effectively preclude the possibility of money laundering activities, or the establishment of a conduit for terrorist financing, resulting in an extremely negative impact on the condition of the Financial Institution.
♦ Medium/High	3	Mitigated risk where current factors have minor weaknesses and where the increase in probability if not properly controlled may result in the likelihood of money laundering activity or a conduit for terrorist financing occurring, which could have a moderate negative impact on the condition of the Financial Institution.
♦ Medium	2	Mitigating risk factors and preventive controls appropriately diminish the risk but where there is still a small possibility of potential money laundering activity or a conduit for terrorist financing occurring, that would have a minor negative impact on the condition of the Financial Institution.
♦ Low (None)	0 - 1	Preventive controls are strong and mitigating risk factors are effective in deterring money laundering activity or a conduit for terrorist financing risk. Products and/or services are not currently offered or will be discontinued in the near future, therefore there will be no existing risk.

#	Risk Category	Characterized Threats and Vulnerabilities (Volume Activity)	Threats and Vulnerability Rating		Probability Rating		Inherent Risk Rating		Mitigating Controls	Preventive Controls Rating		Residual Risk Rating	
			High = Medium = Low = None =	3 2 1 0	Increasing = Stable = Decreasing = None =	3 2 1 0	High = Medium = Low = None =	5+ 3-4 1-2 0		Strong= Adequate = Weak = None =	3 2 1 0	High = Med/High = Medium = Low =	4+ 3 2 0-1
INFRASTRUCTURE													
1	Date of Risk Assessment								Reviewer:				
2	Assessment Period								Reviewer:				
3	Name of Financial Institution								Compliance Officer:				
4	Type of Financial Institution												
5	Total Assets / Asset Size				Number of Employees								
CUSTOMER RISK													
1	Politically Exposed Persons (PEP)												
2	Non resident arrangements												
3	Trusts and legal arrangements												
4	*Additional Customer Categories*												
PRODUCTS AND SERVICES													
1	*Products and Services*												
2	*Products and Services*												

#	Risk Category	Characterized Threats and Vulnerabilities (Volume Activity)	Threats and Vulnerability Rating		Probability Rating		Inherent Risk Rating		Mitigating Controls	Preventive Controls Rating		Residual Risk Rating	
			High = Medium = Low = None =	3 2 1 0	Increasing = Stable = Decreasing = None =	3 2 1 0	High = Medium = Low = None =	5+ 3-4 1-2 0		Strong= Adequate = Weak = None =	3 2 1 0	High = Med/High = Medium = Low =	4+ 3 2 0-1
TRANSACTION RISK													
1	Non Face to Face delivery channel												
2	Unusual patterns of transactions that have no apparent economic purpose												
3	*Additional Transaction Risk Categories*												
GEOGRAPHY													
1	Countries subject to sanctions, embargoes by international authorities												
2	Countries/geographies identified by recognized sources as providing funding for terrorist activities												
3	*Additional Categories*												
Total													

Annex 2

Controls Assessment Template

Sr No.	Controls	Weak	Satisfactory	Strong
1.	**Governance Arrangements and Three Lines of Defense**			
1.1	Written AML/CFT policies and procedures approved by Board of Directors			
1.2	Risk assessment reviewed and updated periodically			
1.3	Are policies, procedures and compliance program updated periodically?			
1.4	Oversight by the Board of Director and senior management			
2.	**Three Lines of Defense**			
2.1	AML/CFT Chief Compliance Officer appointed			
2.2	Internal Audit Function			
2.3	Written policies and procedures communicated to all personnel			
2.4	Employee due diligence program			
2.5	Ongoing Employee Training Programs			
3.	**Program and Systems**			
3.1	AML/CFT in a Group-Wide and Cross-Border Context			
3.2	Internal Procedures/system for Detecting and Reporting Suspicious Transactions			
3.3	Appropriate integrated management information systems			
3.4	Review of Exception Reports to alert Senior Management/ Board of Directors			
3.5	Mechanism for asset freezing and sanction compliance			
3.6	Secrecy Privacy Of Information (Tip Off) ensured			
3.7	STR/CTR Cash generated and reported on timely basis			
3.8	Is there a procedure for independent review of AML/CFT program?			
4.	**Customer Identification, Verification and Acceptance Policy**			
4.1	Written policies and procedures for CDD/KYC			
4.2	Approval by senior management before establishing business relationships with high-risk customers			
4.3	Customer due diligence programs			

4.4	Enhanced due diligence program for high risk customers			
4.5	Customer Risk Profiling			
4.6	Mechanism to review/update risk rating and profile of customers			
4.7	Systematic Procedure for Identifying and Verifying: a) Customers b) Beneficial Owners c) PEPs d) Person acting on behalf			
4.8	Outsourcing customer identification/verification or reliance on others to perform customer identification			
4.9	Due diligence assessment of correspondent relationship			
5.	**Ongoing Monitoring**			
5.1	Transaction monitoring mechanism in place to detect unusual or suspicious transactions			
5.2	Screening of customer with database and changes to sanction lists			
5.3	Is transaction Monitoring System automated?			
5.4	Customer due diligence for existing customers			
6.	**Management of Information**			
6.1	Customer identification, verification and due diligence information			
6.2	Record-keeping procedures allow for tracing transactions and provide a clear audit trail			
6.3	Are records maintained electronically?			

Annex 3

RISK PROFILING OF CUSTOMER

The following sets out examples of factors that RPs should consider when performing risk assessment. Where there is one or more "yes" responses, professional judgement must be exercised, with reference to the policies and procedures of the RPs, as to the nature and extent of customer due diligence to be carried out.

For Internal Use

Section A: *If the response to any of the statements in Section A is "Yes", the entity shall NOT establish business relationship with the client*		**Yes/No**	**Remarks**
1	Customer unable to provide all the required information in relevant forms		
2	Information required to be verified as per the regulations, cannot be verified to independent and reliable documents		
3	Customer, Beneficial Owner of the customer, person acting on behalf of the customer, or connected party of the customer matches the details in the following lists: a. Proscribed under the united nations security council resolutions and adopted by the government of Pakistan; b. Proscribed under the Anti-Terrorism Act, 1997		
4	There is suspicion of money laundering and/or terrorist financing		
Section B: Customer Risk Factor			
1	Is the customer, any of the beneficial owner of the client or person acting on behalf of the customer a politically exposed person (PEP), family member of a PEP or close associate of a PEP?		
2	Is the customer non-resident Pakistani?		
3	Is the customer foreign national?		
4	Is the customer High net worth individual?		
5	Legal persons: • Companies – Local • Companies – Foreign • Foreign Trust or Legal arrangements • Local Trust or Legal arrangements • Partnerships • NGOs and Charities • Cooperative societies		
6	Intermediaries eg. Third parties acting on behalf of customers (Lawyers, Accountants etc.).		
7	Performed further screening of details of customer, beneficial owner of the customer, person acting on behalf of the customer, or		

	connected party of the customer against other information sources, for example, google, the sanctions lists published and/or other third party screening database. Are there adverse news or information arising?		
8	Customer's source of wealth/ income is high risk/ cash intensive		
9	Does the customer have nominee shareholder(s) in the ownership chain where there is no legitimate rationale?		
10	Is the customer a shell company?		
11	Does the customer have unusual or complex shareholding structure (e.g. involving layers of ownership structure, different jurisdictions)?		
12	Does the stated source of wealth / source of funds and the amount of money involved correspond with what you know of your customer?		
Section C: Country / Geographic Risk Factors			
1	Is the customer, beneficial owner of the customer or person acting on behalf of the customer from or based in a country or jurisdiction: a. Identified as High-risk jurisdiction by the FATF and for which financial institutions should give special attention to business relationships and transactions. (Countries having weak governance, law enforcement, and regulatory regimes). b. Countries subject to sanctions, embargos or similar measures issued by international authorities (E.G. UN, WB, IMF) c. Countries where protection for customers privacy prevents effective implementation of AML/CFT requirements and/or facilitates the framework for establishment of shell-companies. d. Countries/ Geographies identified by recognized sources as having significant levels of organized crime, corruption or criminal activity. e. Countries/ Geographies identified by recognized sources as providing funding or support for terrorist activities or have terrorist organizations operating within them.		
Section D: Services / Transactions Risk Factors			
1	Is the business relationship with the customer established through non face-to-face channel?		

2	Has the customer given any instruction to perform a transaction (which may include cash) anonymously?		
3	Has the customer transferred any funds without the provision of underlying services or transactions?		
4	Are there unusual patterns of transactions that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)?		
5	Are there unaccounted payments received from unknown or un-associated third parties for services and/or transactions provided by the customer?		
6	Does the value of the transaction appear to fall within the financial means of your customer, given their income and savings?		
7	Is there any divergence in the type, volume or frequency of services and/or transactions expected in the course of the business relationship with the customer?		
8	Significant and unexplained geographic distance between residence or business location of the customer and the location where the product sale took place (or the location of the insurer's representative)		
9	Customers seek or accept very unfavorable account/policy/contract provisions or riders and rely on free look up provisions		
10	Customers transfer the benefit of a product to an apparently unrelated third party		
11	Customer uses brokerage accounts as long term depository accounts for funds		
12	Customer is conducting transactions that do not have apparent economic rationale		
13	Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting Thresholds		
14	Transactions involve penny/microcap stocks		
15	Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation		
16	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		
17	Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason		
18	Customer trades frequently, selling at a loss		
19	Customer invests in securities suddenly in large volumes, deviating from previous transactional activity		
20	Cross border correspondent financial institutions relationships		
21	Products/ Services		
22	Transaction Amount		

Section E: Customer Risk Assessment

☐ Low – Simplified CDD ☐ Medium – Standard CDD ☐ High – Enhanced CDD

Document reasons for customer risk rating:

Section F: Recommendation

☐ Accept customer ☐ Reject customer

Assessed By: Designation: Signature: Date:	Approved By: Designation: Signature: Date:

Annex 4

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.

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