MAAN Securities (Private) Limited
POLICY OF ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM AND PROLIFERATION FINANCING BASED ON GUIDELINES ISSUED BY SECP

(Updated April, 2020)

Table of Contents

AML/CFT Framework under the SECP Guidelines
Man Securities (Private) Limited (AML/CFT Regulations, 2018)

1. Introduction, Purpose and Scope

i Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime requires financial institutions to understand their Money Laundering ("ML"), Terrorist Financing ("TF") and Proliferation Financing ("PF") risks, adopt and effectively implement an appropriate risk-based ML/TF/PF control framework. By aligning Pakistan's AML and CTF control framework with FATF recommendations, Pakistan's integration into the global financial system will be facilitated. This is an essential contribution that all RPs can make to the lawfulness, transparency, and long-term solid growth of Pakistan's financial sector supported by strong a capital market and the economy as a whole.

ii Maan Securities (Private) Limited in order to maintain the integrity of its regulated financial sector that includes the brokers, insurers, NBFCs and Modarabas notified the Maan Securities (Private) Limited AML/CFT Regulations, 2018 ("the Regulations"). The AML/CFT Regulations require Regulated Persons (RPs) to establish policies, systems and internal controls to detect and combat ML and TF for preventing the abuse of their financial products and services.

These Guidelines supplement the Regulations and the AML/CFT regime by clarifying and explaining the general requirements of the regulatory framework to help RPs in applying national AML/CFT measures. The 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") and relevant international best practices.

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

i. RPs should understand their ML/FT/PF risk exposure and their obligation of establishing an effective AML/CFT regime to deter criminals from using their financial system for illicit purposes. RPs need to develop their own comprehensive risk-based AML/CFT compliance program to comply with all relevant and applicable laws and obligations.

ii. RPs' Board of Directors and senior management must be engaged in decision making on AML/CFT policies, procedures and controls, and take ownership of their risk-based compliance program. They must be aware of the level of ML/TF/PF risk the RP is exposed to and evaluate whether it is equipped to mitigate that risk effectively. Directors and senior management are required to proactively guide the RP with respect to appropriate actions and changes needed in the risk control environment for adequately mitigating ML/TF/PF risks identified.

iii. RP must give due priority to establishing and maintaining an effective AML/CFT compliance culture with written internal procedures. It must adequately train its staff to identify suspicious activities and adhere with the internal reporting chain and procedures that needs to be followed. Such procedures should be updated to reflect changes in regulatory requirements and RP's control environment.

iv. To oversee the compliance function, the Regulations require RP to appoint a Compliance Officer ("CO") at the management level. Compliance officer shall have all necessary powers and access to information in the RP, and will be the point of contact both internally in Compliance matters as well as with the supervisory authorities, including the Commission and the Financial Monitoring Unit ("FMU").

3. Program and Systems to prevent ML/TF/PF

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

(a) Policies and procedures to undertake a Risk Based Approach ("RBA");
(b) Internal policies, procedures and controls to combat ML/TF/PF, including appropriate risk management arrangements;
(c) Adequate systems to identify and assess ML/TF/PF risks relating to customers, products/services, delivery channels and geography (such as higher risk countries or regions within a country);
(d) Customer due diligence measures (enhanced or simplified due diligence) including identifying customers, beneficial owners and politically exposed person and verifying their identity;
(e) Ensure screening against all applicable sanctions lists;
(f) Ongoing monitoring of customers and transactions;
(g) Record keeping procedures;
(h) Group-wide AML/CFT programs;
(i) Audit function to test the AML/CFT system;
(j) Screening procedures to ensure high standards, when hiring employees; and (k) an appropriate employee-training program.

Applying a Risk Based Approach (RBA)

4. Applying a Risk Based Approach (RBA)

i. RPs need to analyses the risk environment of their sector to estimate the likelihood of ML/TF/PF occurring based on sub-factors such as customers, products and services and distribution channels.

ii. The RBA enables RPs to ensure that AML/CFT measures are commensurate to the risks identified and enables efficient allocation of resources. 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:
   (a) Conduct a risk assessment to identify and determine the ML/TF/PF relevant to RP;
   (b) Develop and implement a programmer containing the procedures, policies and controls used to manage and mitigate those risks.

iii. Under the RBA, where there are higher risks, RPs are required to take enhanced measures to manage and mitigate those risks; and where the risks are lower, simplified measures may be permitted.

iv. 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, and escalation of suspicions and liaison relationships with the authorities. The guidance provided in these guidelines applies to CFT as well as AML, even where it is not explicitly mentioned.

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

(a) Identifying the area of the business operations susceptible to ML/TF/PF;
(b) Conducting an analysis in order to assess the likelihood and impact of ML/TF/PF;
(c) Managing the risks; and
(d) Regular monitoring and review of those risks.

5. Risk Assessment of the Entity

Every RP shall regularly create and maintain an updated document that describes its current assessment of its ML/TF/PF risk in light of the latest National Risk Assessment. This document will be formally approved by the management and board of directors of the RP and must provide a list of proposed actions needed to address any deficiencies in risk mitigants, controls processes and procedures identified by the assessment. In addition, the document must include a view on the AML/CFT risks with respect to its customers, products, delivery channels, geography and the quality of the RPs risk mitigants, such as controls processes and procedures involving more detailed steps.

ii. The ML/TF/PF risk assessment is not a one-time exercise and is required to be carried out annually (or as directed by). Further, the RP management should review the risks w.r.t to new products or services, opening or closing accounts with high-risk customers and mergers and acquisitions.

iii. RP should be able to demonstrate to the Commission, the adequacy of its assessment, management and mitigation of ML/TF/PF risks, and of the measures taken in the context of AML/CFT. Documentation should include:
   (a) Risk assessment systems including details of the implementation of appropriate systems and procedures, due diligence requirements, and how the RP assesses ML/TF/PF risks;
   (b) Customer acceptance policy; procedures and policies concerning customer identification and verification; and its ongoing monitoring and procedures for reporting suspicious transactions;
   (c) The arrangements for monitoring and reporting to senior management on the results of ML/TF/PF risk assessments and the implementation of its ML/TF/PF risk management systems and control processes.

iv. Risk Assessment must be sufficiently precise to allow the development of a Risk Matrix that grades customers, products, geography, and delivery channels into risk categories. Each customer must receive an initial AML/CFT risk rating at the beginning of the business relationship, and it must be kept current based on updates and changes in the relationship. For example, if a customer is inactive over a longer period of time, his risk rating may need to be revised.

v. For guidance to prepare entities Internal AML/CFT Risk Assessment, please refer to Section 20 - Risk Assessment and Applying a Risk Based Approach.

6. Monitoring AML/CFT Systems and Controls

i. RPs shall monitor the AML/CFT risks as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, products offered and their characteristics, development of new technologies in the markets or there use by the RP itself and new sanctions.

ii. Additionally, RPs shall assess the effectiveness of their risk mitigation procedures and controls, identify areas for improvement and update their systems as appropriate to suit the change in risks. This allows them to manage their AML/CFT risk effectively. For this purpose, the RP monitors:

(a) changes in customer profile or transaction activity/behavior in the normal course of business including incidents related to suspicious transactions and terrorist financing sanctions (TFS);
(b) changes in risk relative to countries and regions to which the RPs or its customers are exposed;
(c) the potential for abuse of products and services because of their size, unusual patterns, ambiguity and complexity;
(d) deficiencies in internal cooperation and coordination mechanisms, and employee awareness of their roles in AML/CFT compliance and other functions/areas; and
(e) the selection, training and performance of agents, intermediaries and third parties who are in any way involved in the AML/CFT processes of the RP.

iii. RP should also take into account the quality of systems, qualification and experience of designated compliance officer, number and qualification of employees in compliance function.

7. New Products and Technologies

RPs in coordination with compliance function should have systems in place to identify and assess ML/TF/PF risks that may arise from new and pre-existing product such as:

(a) New products, markets or sales channels;
(b) New internal organization or new offices and departments;
(c) New data and transaction screening systems and verification of documentation:
(d) the use of virtual or digital currencies and assets;

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, and avoid or mitigate all technologies that favour anonymity. Limitations on the use of non-face to face business, or on virtual business, may be adequate to avoid opening up of alternative possibilities for ML/TF and fraud, especially in industries of higher risk according to National Risk Assessment, such as brokerage.

iv. Use of modern technology can strengthen AML/CFT measures, e.g. initial application forms completed online and then followed up with appropriate identification checks before a relationship goes into full operation. This will allow more time to check the customer and lead to better prevention of ML/TF/PF.

8. Customer Due Diligence (CDD)

i RPs shall take steps to know who all 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.

ii RPs shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer.

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

iv The Regulations require RPs to identify and verify the identity of any person that is purporting to act on behalf of the customer. Additionally, RPs shall ascertain the reason for such authorization and obtain a copy of the authorization document.

v 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.

vi RP must assess each customer's risk to allow for correct application of enhanced due diligence, standard, simplified or special measures for PEPs and other designated categories as per the Regulations. Necessary minimum customer risk rating categories are:

(a) High
(b) Standard
(c) Low
(d) PEP

vii RPs are entitled to ask customers all relevant CDD questions and may refuse business if the necessary questions are not answered, or the necessary data and documents are not provided.

viii If an RP has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report (STR).

9. Timing of Due Diligence

a) Establishment of a Business Relationship

i. Customer Due Diligence and verification measures should be undertaken when establishing the business relationship and before any financial service or transaction occurs.

ii. However, as provided in the Regulations RPs may complete verification after the establishment of the business relationship as soon as is practicable where the risks of ML/TF/PF are low.

iii. Examples of the types of circumstances 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: (a) Non face-to-face business;

(b) 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.

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.

b) Due Diligence of Existing Customers

i. Existing customers must be assigned a risk rating based on the Risk Matrix which RP has created together with RP's Risk Assessment in its Risk based Approach.

ii. 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.

iii. The CDD requirements entails that if an RP has a suspicion of ML/TF/PF 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.

iv. 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.

v. Finally, RPs should entertain filing a suspicious transaction report if there are any indicators that support such an action.

c) Tipping-off and Reporting

The Law prohibits tipping-off. If RPs form a suspicion of ML/TF/PF 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 customer, it may choose not to pursue that process and should file a STR. RPs should ensure that their employees are aware of these issues when conducting CDD or ongoing CDD.

10. Beneficial Ownership (BO)

i The Beneficial Owner is the natural person at the end of the chain who ultimately owns or controls the customer. The definition of BO in the Regulations is as below:
"beneficial owner" in relation to a customer of a regulated person means, the natural person who ultimately owns or control a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement".

ii For legal persons or arrangements, it is essential to understand the ownership and control structure of the customer. This may be done based on plausibility and records. In any case of lack of transparency or doubt, or higher risk, verification is needed. For legal persons, the primary source for verification of ultimate beneficial ownership is the Register of Ultimate Beneficial Ownership.

iii For complex structures, foreign entities or foreign owned entities, RPs are required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet.

iv RPs may adopt a risk-based approach to the verification of beneficial ownership of a customer. Identifying beneficial ownership of a customer is an obligation that must be satisfied, regardless of the level of risk associated with that customer. However, the reasonable steps to take to verify the identity and information depends upon on the risk assessment of the customer.

v RPs should assess different levels of money laundering/terrorism financing risks posed by their customers' beneficial owners. For example, RPs should consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.

vi If an RP has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report to FMU.

11. Enhanced CDD Measures ("EDD")

i. Where the risks of ML/TF/PF 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.

ii. In all cases where the connection between a customer and his source of income or wealth is very disparate, consider whether the customer is acting on his own behalf or may be a close associate acting for another party, e.g. a PEP. This is particularly relevant for any person with no discernible source of income and a high living

standard, such as housewives, children or students. Close Associate is defined as: "Close Associates" means any natural person who is known to hold,-

(i) Joint ownership or control of a legal instrument with a politically exposed person, or

(ii) any other close business or personal relationship with a politically exposed person, or

(iii) Ownership or control of a legal instrument or a person which is set up for the benefit of a politically exposed person.

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

(a) Obtaining additional information on customer (e.g. occupation, intended nature of business, volume of assets, information available through public databases, internet, etc.);
(b) Updating more regularly the identification data of applicant/customer and beneficial owner.
(c) Obtaining additional information on the intended nature of the business relationship, source of funds or source of wealth, reasons for intended or performed transactions;
(d) Obtaining the approval of senior management to commence or continue the business relationship.

a) Source of Funds and Source of Wealth

i. The RP has to establish that the transaction is within the financial means of the customer. The information that should be obtained should give an indication as to the volume of wealth the customer is reasonably expected to have, and how it was acquired.

ii. Once the client's net worth is established, information should be obtained on where it came from i.e. inheritance, employment, business, investment etc. RPs may rely on publicly disclosed information if such information is available to verify the information.

iii. Understanding the customer's source of funds and their overall financial situation does not mean full proof of all monies, but it does mean that the RP has asked and validated the financial position. The same applies to housewives and students, where the income of the person or family that sustains them must be documented, otherwise the due diligence is not complete.

iv. For PEPs, and other HNWI, as well as higher risk customers, the requirement covers source of wealth. This means that not only the source of the funds for the current specific transaction should be understood, but that the overall wealth of the customer needs to be understood. This means a view of the overall ownerships and earnings of the client, to understand his assets and holdings in a complete overview, and be able to estimate his total wealth to some extent. This is an onerous requirement which may lead some RPs to consider whether contracting with such high-risk customers is possible for them.

12. Special Cases of Higher Risk & Enhanced Due Diligence

a) **Politically Exposed Persons (PEPs)**

i. PEPs are defined in the Regulations, inter-alia, as heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates.

ii. Business relationships with PEPs holding important public positions may expose RP to significant reputational and/or legal risk. In addition, PEPs because of their position, may expose RPs and their business partners to a high degree of public expectation and scrutiny.

iii. Family members of a PEP are individuals who are related to a PEP either directly or through marriage. Close associates are individuals who are closely connected to PEP, either socially or professionally. Close associates have in many cases been used to provide a cover for the financial activities of a PEP, and may Not be in any way connected to the PEP in an official capacity. The CDD done by RPs on the source of funds or source of wealth of a customer may be the first clear documentation of a close association.

iv. The AML/CFT National Risk Assessment of Pakistan has determined the risk of corruption and therefore the risk of providing financial services to PEPs is high. This means that all domestic PEPs must be scrutinized, particularly for their source of funds wealth and assets.

v. RPs are obliged to ascertain whether their customer is a PEP. In assessing the ML/TF risks of a PEP, the RP shall consider factors such as whether the customer who is a PEP:

(a) Has prominent public functions in sectors known to be exposed to corruption;
(b) Has business interests that can cause conflict of interests (with the position held); (c) has been mentioned in media related to illicit financial behavior; and (d) is from a high risk country.

vi. In very low risk scenarios declaration may be sufficient. In higher risk scenario, a search of publicly available information, such as internet public sources or commercial databases is necessary.

vii. The PEP red flags that the RPs shall consider include:

(a) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
(b) A family member of a PEP without own financial means is transacting with the RP without declaring the relationship to a PEP, or the origin of the funds transacted;
(c) The PEP is associated with, or owns, or signs for, complex legal structures that are commonly used to hide Beneficial Ownership;
(d) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
(e) A PEP uses multiple bank accounts for no apparent commercial or other reason;
(f) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

viii. 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 RPs should consider include:

(a) the level of (informal) influence that the individual could still exercise; and
(b) 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, or through continued strong ties within a party, family or institution).

ix. RPs are encouraged to be vigilant in relation to domestic PEPs and PEPs from other jurisdictions, who are seeking to establish business relationships. RPs, in addition to performing normal due diligence measures should also:

(a) have appropriate risk management systems to determine whether the customer is a PEP;
(b) Obtain senior management approval for establishing business relationships; (c) take reasonable measures to establish the source of wealth and source of funds; and (d) conduct enhanced ongoing monitoring of the business relationship.

b) **Non-Profit Organizations (NPOs)**

i. Both by international standards and in Pakistan's National Risk Assessment, NPOs are classified as a High Risk Sector for TF.

ii. The objective of Enhanced Customer Due Diligence for NPOs is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes.

iii. RPs who transact with NPOs should understand:
   a. Beneficiaries and Beneficial Owners including certain donors that maintain decision rights;
   b. Flow of funds, in particular the use of funds by an NPO.

c) **High Net worth Individuals (HNWI)**

i. High net worth individuals while an attractive customer for RPs, can expose the RP to higher risk of financial transactions that may be illicit. There is no standard size of HNWI. Every RP knows to whom it is offering its products and services, and can establish criterion for HNWI applicable to their particular business.

ii. RP should scrutinize HNWI customers to determine, whether they carry a higher risk of ML/FT and require additional due diligence measures. Such scrutiny must be documented and updated as part of the Risk Assessment of the RP.

d) **High-Risk Countries & Higher Risk Regions within a country**

i. Certain countries, or regions within countries have a specific higher AML/CFT risk profile. Examples are border regions, large goods transit points such as ports, or regions experiencing social unrest, that can be associated with specific crime patterns such as cash or people smuggling, drug trafficking, violent crimes, fraud and corruption, and consequently pose a higher potential risk to the RP. Conducting a business relationship with a customer from such a country/region exposes the RP to risk of channelling illicit money flows.

ii. RPs should exercise additional caution, and conduct enhanced due diligence on individuals and/or entities based in high-risk countries / regions. RPs are advised to consult publicly available information to ensure that they are aware of the high-risk countries/territories. RPs should 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 (TI CPI).

iii. Complex legal structures may be created in jurisdictions specializing in obscuring the trail to Beneficial Owners and allowing easy creation of complex corporate vehicles, so called offshore jurisdictions. RPs engaging with foreign complex legal structures, or with local companies owned by such foreign legal structures, need to educate themselves on offshore financial centres and acquire adequate expertise to understand their customers' ownership structure up to the Beneficial Owner and be able to assess documents presented to them.

13. Simplified Due Diligence Measures (SDD)

i. RPs may conduct SDD in case of lower risks identified by the RP in line with latest National Risk Assessment. 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 as mentioned in the latest National Risk Assessment.

ii. Using SDD measures may include:
   (a) reducing the frequency of customer identification updates;
   (b) reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold;
   (c) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established;
   (d) undertaking verification after establishment of the business relationship; (e) less stringent steps to verify the Beneficial Owner.

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

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

14. Reliance on Third Parties (Cooperation within Financial Sector)

i. When another domestic financial sector entity, e.g. a bank or an RP, has already established a relationship with a customer, the RP may rely on the CDD performed by that other party. This only applies if the information and CDD is shared directly between the RP and the other entity.

ii. RP may rely on the initial CDD information provided by another financial institution in Pakistan, where the third party is regulated and supervised by SPB or and where RP can immediately obtain necessary information from the third party.

iii. The ultimate responsibility for the CDD and the other AML/CFT obligation remains with the RP for the business they conduct with the customer, and covers all other obligations mentioned in this guideline.

15. On-going Monitoring of Business Relationships

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.

ii. In all cases, the transactions of the customers must be monitored, scrutinizing the transactions undertaken throughout the course of the business relationship by recognizing unusual patterns or large transactions and unusual money flows.

iii. RP should develop and apply written policies and procedures for taking reasonable measures to ensure that CDD data or information is kept up-to-date by undertaking routine reviews of existing records. RPs shall consider updating customer CDD records within the time frames 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:

(a) Material changes to the customer risk profile or the way that account usually operates;
(b) RP lacks sufficient or significant information on a particular customer;
(c) Where a significant transaction takes place;
(d) Where there is a significant change in customer documentation standards;
(e) Significant changes in the business relationship;
(f) Transaction restructuring to circumvent the applicable threshold.

iv. Annex 3 and 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF/PF, enabling RPs to recognize possible ML/TF/PF schemes. 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.

v. In case a customer has no active business with the RP, and cannot be reached, or refuses to engage in updating because there is no active business, account should be marked inactive with the instruction that relationship cannot be re-activated without full CDD.

vi. In case due diligence cannot be updated, a formal ending of the relationship should be done by following the legal process for ending a customer relationship under the applicable laws.

vii. RPs are required to apply ongoing 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 CDD measures previously undertaken, and the adequacy of data obtained.

viii. RPs are encouraged to invest in computer systems for transactions monitoring specifically designed to assist the detection of ML/TF/PF. It is recognized that this may not be necessary in a risk-based approach. In such circumstances, RPs will need to ensure they have alternative systems in place for conducting on-going monitoring.

vi. Alternate or manual systems of ongoing monitoring may rely on Compliance Officer generated lists or instructions and regular lists generated from IT system such as:
(a) High transaction list for each day;
(b) Periodic list of transactions over determined thresholds;
(c) Periodic list of new clients and relations closings;
(d) Monthly or yearly lists of inactive clients;
(e) Ad Hoc reviews, meaning reviews triggered by an event, new information from supervisors and media reports.

16. Record-Keeping Procedures

i. RPs should ensure that all information obtained in the context of CDD is recorded. This includes:
(a) Documents provided to the RP when verifying the identity of the customer or BO;
(b) Verification of CNIC through NADRA Verisys/ Biometric;
(c) Transcription into the RP's own IT systems of the relevant CDD information.

ii. RP should maintain, for at least 10 years after termination of the business relationship, all necessary records on the customer and their 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.

17. Reporting of Suspicious Transactions

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. Activities requiring further enquiry may fall into one or more of the following:
   (a) any unusual financial activity of the customer not in line with the customer's profile;
   (b) any unusual transaction in the course of some usual financial activity;
   (c) any unusually-linked transactions;
   (d) any unusual method of settlement;
   (e) Unusual or disadvantageous early redemption of an investment product; (f) unexplained unwillingness to provide the information requested.

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 escalation of matters to the CO. Ultimately, RP must decide whether to file a suspicious transaction report based on the above. If it decides not to file, reasons must be documented for this decision.

iii. RP may refuse business that they suspect, might be criminal in intent or origin. Where a customer is hesitant/fails to provide adequate documentation, consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF/PF, that attempted transaction should be reported to the FMU.

iv. If the RP decides that a disclosure should be made, the law require the RP to report STR without delay to the FMU. The STR should be filed through GoAML portal of the FMU.

v. After concluding an internal enquiry, or making an STR, the RP has to decide whether to close the enquiry, take additional steps such as higher risk rating of customer, or ending the business relationship. This decision must be documented with an explanation for the reasoning behind it.

vi. 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.

vii. RPs should maintain a comprehensive record of AML/CFT reports w.r.t. internal enquiries and reporting to FMU. Such documentation may include:
   (a) the report itself and all its attached information / documents in copy;
   (b) the date of the report;
   (c) the person who made the report and the recipient;
   (d) any decision based on the STR for the specific customer or a group of customers; (e) any updating or additional documentation taken based on the report ; and (f) the reasoning underlying the decisions taken.

18. Implementation of UN Security Council Resolutions

i. Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities, or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them.

ii. 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 United Nations Security Council's (UNSC) relevant Committee established in pursuance of Resolution 1267 (1999) and successor resolutions concerning ISIL (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities, approves the addition, amendments and deletion of individuals and entities subject to assets freeze, travel ban and arms embargo as set out in the UNSC resolutions adopted under Chapter VII of the UN Charter.

iv. The Government of Pakistan under the United Nations (Security Council) Act, 1948 gives effect to the decisions of UNSC whenever the Consolidated List maintained by the relevant Sanctions Committee is updated. The Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) to provide legal cover for implementing sanction measures under UNSC resolutions. These SROs in respect of designated individuals/ entities require assets freeze (including funds and other financial assets or economic resources), travel ban and arms embargo, in addition to other measures in accordance with the UNSC resolutions. These SROs are available at the following links:

(a) http://mofa.gov.pk/unsc-sanctions/

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

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

vi. Each RP is required to immediately scan its customer data bases and their Beneficial Owners /associates for any matches with the stated designated/proscribed person(s)/entity(ies) on the receipt of notifications; issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/ Home Departments of Provinces/Ministry of Interior regarding updates in list of proscribed persons under the Anti- Terrorism Act, 1997. In case of a true match or suspicion of a proscribed/designated person the following actions shall be immediately taken by the RP:

(a) if it is an existing customer, freeze without delay the customer's fund and other financial assets or economic resources / policy or block the transaction, without prior notice;

(b) Reject the customer, if the relationship has not commenced;

(c) Lodge a STR with the FMU, and simultaneously notify and the Ministry of Foreign Affairs in case that person is designated under United Nations Security Council Resolutions, or the National Counter Terrorism Authority ("NACTA") in case that person is designated under the Anti-Terrorism Act, 1997.

vii. RP must ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether it is a true match. In case there is not 100% match, but sufficient grounds for suspicion that customer/ funds belong to sanctioned entity/ individual, the RPs may consider raising an STR to FMU.

viii. 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 place w.r.t to sanctions compliance. RPs shall provide adequate sanctions related training to their staff. When conducting risk assessments, RPs shall, take into account any sanctions that may apply (to customers or countries).

ix. RPs should not provide any services to proscribed/ designated entities and individuals or their associated persons as required under the Regulations. For this purpose, necessary measures should be taken including but not limited to the following controls:

(a) In case of entity accounts, it should be ensured that their beneficial owners, directors, members, trustees and authorized signatories are not linked with any proscribed/ designated entities and individuals, whether under the same name or with a different name.

(b) The association of individuals/entities with proscribed/designated entities and individuals may be determined on the basis of appropriate screening of sanctions lists, publicly known information or linkages (on the basis of Government or regulatory sources, reliable media information, etc.)

(c) While opening new accounts or extending services to customers, any similarity between the identifying information of the customer and that of proscribed/ designated entities and individuals including national identification number, address, etc. may be viewed with suspicion and properly investigated for necessary action as per requirements.

(d) RPs should monitor their relationships on a continuous basis and ensure that no such relationship exists.

If any such relationship is found, immediate action shall be taken as per law, including reporting to the FMU.

(e) RPs shall report to the FMU and the Commission immediately, all attempted or rejected transactions or account opening requests pertaining to proscribed/ designated entities and individuals and their associates.

(f) RPs shall maintain up to date data/MIS of all frozen assets/ funds, attempted or rejected transactions or account opening requests, and the same shall be made available to the Commission as and when required.

x. RPs shall, taking note of the circumstances where customers and transections are more vulnerable to be involved in TF and PF activities by identifying high-risk customers and transections, and applying enhanced scrutiny. RP shall carry out checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names

in the abovementioned lists, to determine if the business relationship involves any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

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. The Consolidated Lists available at NACTA's and the UNSC Sanctions Committees' websites, are regularly updated and can be accessed at the following links:

(a) https://www.un.org/securitycouncil/content/un-sc-consolidated-list

(b) https://scsanctions.un.org/search/

(c) https://www.un.org/securitycouncil/sanctions/1267

(d) https://www.un.org/securitycouncil/sanctions/1988

(e) https://www.un.org/securitycouncil/sanctions/1718

(f) https://www.un.org/securitycouncil/content/2231/background

(g) https://nacta.gov.pk/proscribed-organizations-3/

(h) https://nacta.gov.pk/pp/

(i) https://nfs.punjab.gov.pk/

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

19. Internal Controls (Compliance Function, Audit Function, Employee Screening, Ongoing Training Program and Outsourcing)

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/PF risks identified. RPs should establish and maintain internal controls in relation to:

(a) compliance management arrangements;

(b) screening procedures to ensure high standards when hiring employees; (c) an ongoing employee training programme; and (d) an independent audit function to test the system.

ii. RPs should establish the following three lines of defence to combat ML/TF/PF:

a) First line of defence: Business units

Business unit that directs the sales force (e.g. front office, customer-facing activity, front-line and mid-line managers, who have day-to-day ownership of management of risks and controls) is the first line of defence. For each decision or approval, they need to determine and ensure that sufficient resources are provided for carrying out policies and procedures related to AML/CFT due diligence.

As part of first line of defence, management must create and approve policies and procedures that are clearly specified in writing, and communicated to all employees. They should clearly describe obligations and instructions for employees, as well as guidance on compliance with the Regulations. There should be internal procedures for detecting, monitoring and reporting suspicious transactions.

b) Second line of defence: Compliance Officer and Compliance Function

Compliance Officer, back office, internal control and risk management functions, the compliance function and human resources or technology are the second line of defence.

As part of second line of defence, the CO must have the authority and ability to oversee the effectiveness of RP's AML/CFT systems. His responsibilities include compliance with applicable AML/CFT legislation, reporting of suspicious and currency transactions, and providing guidance in day-to-day operations of the AML/CFT policies and procedures, including freezing of accounts/funds if subsequently identified on proscribed lists. CO must be a person who is fit and proper to assume the role and who:

(a) has sufficient skills and experience to develop and maintain systems and controls (including submitting written policies and procedures for management's approval);

(b) reports directly and periodically to the Board of Directors, Chief Executive or equivalent competent authority on AML/CFT systems and controls;

(c) has sufficient resources and access to all information and data within the RP necessary for performing the AML/CFT compliance function;

(d) ensures independent audit of the AML/CFT program;

(e) maintains or ensures maintenance of various logs, as necessary, with respect to declined business/rejected transactions, internal investigations, suspicious transaction reports, and freezing or blocking of payments under Sanction Regime;

(f) responds promptly to requests for information by the /LEAs.

c) Third line of defence: Internal Audit Function

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 assess:

(a) overall governance structure of the RP for AML/CFT, including the role, duties and responsibilities of the Compliance Officer/function;

(b) ownership taken by management and board of directors (where applicable), in particular Risk Assessment, Risk Based Approach, AML/CFT related internal enquiries, suspicious transaction reports and regulatory compliance;

(c) integrity and effectiveness of the AML/CFT systems and controls and the adequacy of internal policies and procedures in addressing identified risks, including:

- CDD measures including monitoring and updating of customer data;
- Screening process for TFS, and test its functionality;
- testing transactions with emphasis on high–risk customers, geographies, products and services;
- Record keeping and documentation.

(d) the effectiveness of parameters for automatic alerts and the adequacy of RP's process of identifying suspicious activity, internal investigations and reporting;

(e) the adequacy and effectiveness of training programs and employees' knowledge of the laws, regulations, and policies & procedures.

iii. **Employee Screening**

(1) RPs should maintain adequate policies and procedures to screen prospective and existing employees to ensure high ethical and professional standards. 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.

(2) Employee screening should be conducted periodically where a suspicion has arisen as to the conduct of the employee. 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 should verify:

- references provided by the prospective employee at the time of recruitment;
- employee's qualifications, employment history, and professional memberships;
- details of any regulatory actions or actions taken by a professional body and the existence of any relevant criminal convictions.

(3) RPs should screen all employees periodically against proscribed and Targeted Financial Sanctions lists.

iv. **Employee Training**

(1) RPs should ensure that all concerned staff receive training on ML/TF/PF prevention on a regular basis, at least annually or more frequently where there are changes to the regulatory requirements or where there are significant changes to the RP's business operations or customer base. RP must ensure that all staff fully understand the procedures and need for compliance with the regulations.

(2) 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 laws.

(3) 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 noncompliance with relevant laws.

(4) The CO should receive in-depth training on all aspects of AML/CFT laws and regulations. They should also receive ongoing training on new trends of criminal activity determination, investigation and reporting of suspicious activities.

v. **Outsourcing to Third Parties**

(1) RPs should maintain policies and procedures in relation to outsourcing some of their functions to third parties. The RP shall conduct due diligence on the proposed service provider and also ensure that the service provider (OSP) is fit and proper to perform the activity that is being outsourced.

(2) RP shall ensure that a written 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. The ultimate responsibility for meeting AML/CFT requirements always remains with the RP for outsourcing arrangements.

(3) The function of Compliance Officer cannot be outsourced, only limited functions such as screening or database checks can be performed by another entity, except where the third party is part of a group and is properly supervised by a competent authority.

(4) 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.

20. Risk Assessment and Applying a Risk Based Approach - (Please refer to Annex 1 for Risk Assessment Tables)

Identification, Assessment and Understanding Risks

i. Before undertaking an ML/TF/PF risk assessment, RP must consider the following guidance material to determine the level of risk involved in relation to customers, products/services, delivery channels and countries/regions:
   (a) Latest National Risk Assessment;
   (b) Sector Risk Assessment guidance by the ;
   (c) Any applicable guidance by relevant authorities (such as FMU, SBP, MoFA, NACTA etc.); (d) information and guidance published by international organizations such as the FATF, APG; (e) RPs business experience in relation to certain risks.

ii. As part of assessing risk, RP must address inherent risks. These are the ML/TF/PF risks present before any controls and mitigations. RP may assess residual risk (the risk after your controls and mitigations) as part of risk assessment.

The first step in assessing ML/TF/PF risk is to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels that are specific to the RP. The significance of different risk categories may vary from institution to institution, i.e. RP may decide that some risk categories are more important to it than others.

iii. In the second stage, RP should assess and analyse the ML/TF/PF risks that can be encountered as a combination of the likelihood that the risks will result in an ML/TF/PF event taking place and the impact of cost or damages resulting from the event. The impact can consist of financial loss to the RP from the crime, monetary penalties from regulatory authorities or the cost of enhanced mitigation measures.

iv. The likelihood for certain types or categories of risk can be high, if it can occur several times per year, moderate if it can occur two to three per year and low if it is unlikely, but not impossible.

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

(a) How likely an event is;
(b) Consequence of that event;
(c) Vulnerability, threat and impact;
(d) The effect of uncertainty on an event.

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

Approaches to Risk Assessment

i. The size and complexity of your business plays an important role in how attractive or susceptible it is for ML/TF/PF risk. For example, because a large business is less likely to know its customers individually, it could offer a greater degree of anonymity than a small business. Likewise, a business that conducts complex transactions across domestic and international jurisdictions could offer greater opportunities to money launderers.

ii. For low risk environment, RPs may want to assess risk by only considering the likelihood of ML/TF/PF activity. This assessment should involve considering each risk factor that has been identified, combined with business experience, and guidance available through, latest National Risk Assessment (NRA) for Pakistan, and international organizations such as the FATF. The likelihood rating could correspond to:

(a) Unlikely - There is a small chance of ML/FT/PF occurring in this area of the business;
(b) Possible - There is a moderate chance of ML/FT/PF occurring in this area of the business;
(c) Almost Certain - There is a high chance of ML/FT/PF occurring in this area of the business

Notwithstanding the low risk environment the RP may have identified that one of its products is vulnerable to ML/TF/PF due to the potential for cross-border movement of funds. The risk assessment highlights this product as being easily accessible and is being used by many customers in higher-risk jurisdictions. Combined with domestic and international guidance, the RP assesses that the inherent risk rating of this product is high. The AML/CFT Compliance officer/department should then address this likely risk with appropriate control measures. RPs will need to do this with each of the identified risks.

iii. For a moderately complex risk environment, another approach to determining the level of risk is to estimate how likely the vulnerability to ML/TF/PF is going to be exploited and cross-reference that to s the consequence of that risk.

Using likelihood and consequence ratings can provide you with a more comprehensive understanding of the risk and developing an effective risk management framework to help you arrive at a final risk rating. For example, RPs may have identified that one of its products is vulnerable to ML/TF/PF, and RP assesses that

the likelihood of this product being used in ML/TF/PF activity is probable (i.e. it is likely to happen). The RP then judges the impact of the identified ML/TF/PF activity taking place in terms of financial loss and assesses the consequence as moderate.

iv. For a high risk environment the RP should assess risk likelihood in terms of threat and vulnerability. For example, you may consider customers from porous border areas as the threat, and accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method you use, the inherent risk rating for this scenario would be high. RP may then want to assess the impact of this event on the business and the wider AML/CFT environment.

v. Determining the impact of ML/TF/PF activity can be challenging but it can also help you allocate your AML/CFT enforcement resources more efficiently and in a more effective and targeted manner. When determining impact of AML/CFT activity RP may consider a number of factors, including:

(a) Nature and size of your business (domestic and international);
(b) Potential financial and reputational consequences;
(c) Terrorism-related impacts;
(d) Wider criminal activity and social harm; (e) Political impact; (f) Negative media.

RP may want to give more weight to certain factors to provide a more nuanced understanding of RP's ML/TF/PF risk. In addition, RPs may want to consider how your risks can compound across the various risk scenarios. For example, RP may identify that one of the products is high risk and is being used in a highrisk jurisdiction that is directly involved in the production or transnational shipment of illicit drugs. Such compounded inherent risk scenario would be rated as severe, requiring appropriate allocation of resources.

Applying the Risk Assessment

i. The risk assessment should help rank and prioritize risks and provide a framework for managing those risks. The risk assessment must enable RPs to prepare a comprehensive program for meeting relevant obligations under the regulations, including obligations to conduct CDD, monitor accounts and activities and report suspicious activity. For instance, RPs may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and should submit an STR.

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

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

New and Developing Technologies and Products

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

Material Changes and Risk Assessment

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

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

iii. 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 the risk assessment every 12 months to take account of these changes. RP should also have appropriate mechanisms to provide risk assessment information to the Commission, as 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/PF risks for different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

i. **Customer risk factors**: The institution must list and 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/TF/PF 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) 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 amount of business does not match the profile/particulars of client.
   (k) Designated Non-Financial Business and Professions: real estate dealers, dealers in precious metal and stones, accountants and lawyers/ notaries.

Risk analysis for types or categories of customers is the starting point for the risk classification of an individual customer. Based on the circumstances of an individual customer, such as its background or information provided, the risk classification of an individual customer can be adjusted. For illustration purposes only, a sample risk classification for customer type is presented below.

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

ii. **Country or geographic risk factors**: These may arise because of RPs business location and location of its branch offices together with its customer's geographic presence and jurisdiction in which the customer is operating. The factors that may indicate a high risk are as follow:

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

iii. **Product, service, transaction or delivery channel risk factors**: A comprehensive ML/TF/PF 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) Surrender of single premium life products or other investment-linked insurance (e) Products with a surrender value.
(f) International transactions, or transactions involving high volumes of currency (or currency equivalent) transactions
(g) New or innovative products or services that are not provided directly by the RP, but are provided through channels of the institution;
(h) Products that involve large payment or receipt in cash; and (i) One-off transactions.
(j) Complex transactions that involves multiple parties or multiple jurisdictions.
(k) Any introducers or intermediaries the RP might use and the nature of their relationship with the RP.
(l) Physical presence of the customer for identification purposes. If they are not present, has the RP used a reliable form of non-face-to-face CDD (Has it taken steps to prevent impersonation or identity fraud).
(m) The customer being introduced by another part of the same financial group and to what extent can the RP rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF/PF risk (what has the RP done to satisfy itself that the group entity applies CDD measures).

iv. **Risk Matrix**

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

RPs can use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing.

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

The following is an example of a sample risk matrix of client product combination, but RPs should develop their own risk matrix based on their own risk analysis of their particular risk environment. This is being presented for illustration purposes only:

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

Note: When conducting risk assessment, RP does not have to follow the processes in this guideline. As long as you comply with your obligations under the Act and any other applicable laws or regulations, you can choose the method of risk assessment that best suits your business. For example, large financial institutions may have their own systems and methodology for conducting a risk assessment. However, it should be prepared to explain and demonstrate to the Commission, the adequacy and effectiveness of procedures, policies and controls.

v. **Risk Management**

RPs should have appropriate policies, procedures and controls that enable them to manage and mitigate effectively the inherent risks that they have identified, including risks identified in the latest National Risk Assessment. RPs should continuously monitor the implementation of the controls and enhance them, if necessary. The policies, controls and procedures should be approved by the board of directors and senior management, and the measures taken to manage and mitigate the risks should be consistent with legal and regulatory requirements. The nature and extent of AML/CFT controls will depend on a number of aspects that include:

(a) The nature, scale and complexity of the RP's business.
(b) Diversity, including geographical diversity of the RP's operations, proximity to porous border areas and areas with terrorist activity/threat.
(c) RP's customer, product and activity profile
(d) Volume and size of transactions
(e) Extent of reliance or dealing through third parties or intermediaries.

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

(a) determining the scope of the identification and verification requirements based on the risks posed by particular customers;
(b) setting transaction limits for higher-risk customers or products;
(c) requiring senior management approval for higher-risk transactions, including those involving PEPs;
(d) determining the circumstances under which the RP may refuse to take on or terminate high risk customers/products or services;
(e) Determining the circumstances requiring senior management approval (e.g. high risk or large transactions, and establishing relationship with high risk customers such as PEPs).
(f) Quality of systems in place,
(g) Qualification and experience of designated compliance officer,
(h) Number and qualification of employees in compliance function and quality of systems, functioning)

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

ANNEX 1 Preparing AML/CFT Risk Assessment

Note: It is important to *establish KYC-CDD and customer risk profiling prior to undertaking the Risk Assessment process.*

Step 1 – Identify Customer Risk by Customer Type

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

Step 2- Politically Exposed Persons and High Net worth Individuals

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

Step 3 - Identify Risk by Product, Services and Transactions

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

Step 4– Identify Customer Type by Geographic Location

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

Of which, non-resident customers from 'High risk Jurisdictions/region' identified by the financial institutions as per NRA		
Total	0.00	0.00

Step 5- Develop Risk Likelihood Tables

Customer Risk Likelihood Table			
Type of Customer	Customer	Transaction	Geography
	Rating: (High/ Medium/Low)		

Product Risk Likelihood Table			
Product Type	Customers	Transactions	Geography
	Rating (High/Medium/Low)		

Delivery Channels Risk Likelihood Table			
Delivery Channels	**Customer**	**Transactions**	**Geography**
	Rating (High/Medium/Low)		

Overall Entity Level AML/CFT Risk Assessment	
Rating (High/Medium/Low)	
Customer Type	
Product Type	
Delivery Channels	
Geography	
Overall AML/CFT RiskRating	

AML/CFT Compliance Assessment Checklist ANNEX 2

AML/CFT Compliance Assessment Checklist
Name of the Financial Institution
Checklist completed by (Name) **(Designation)**
Date

The AML / CFT Self-Assessment Checklist has been designed to provide a structured and comprehensive framework for RPs to assess compliance with AML/CFT requirements. RPs are advised to use this as part of their regular review to monitor their AML/CFT compliance.

Note: This AML / CFT Self-Assessment Checklist is neither intended to, nor should be construed as, an exhaustive list of all AML/CFT requirements.

Sr No.	Question	Yes/No (N/A)	If No, explain and provide action plan for remediation
	(A) AML/CFT Systems		
1	RPs are required to assess their ML/TF/PF risk and then implement appropriate internal policies, procedures and controls to mitigate risks of ML/TF/PF.		
	Have RP taken into account the following risk factors when assessing own ML / TF/PF risk?		
	(a) Product / service risk		
	(b) Delivery / distribution channel risk		
	(c) Customer risk		
	(d) Country risk		
2	RPs are required to have effective controls to ensure proper implementation of AML/CFT policies and procedures.		
	Does your AML/CFT system cover the following controls?		
	(a) Board of Director and Senior management oversight		
	(i) Do Any member of Board of Director have AML/CFT qualification or experience		
	(b) Have you appointed an appropriate person as a Compliance Officer?		
	i) Does Compliance Officer have a qualification/certification in the area of AML/CFT?		
	ii) Does a Compliance Officer have experience in the area of AML/CFT?		
	(iii) Do you ensure that CO/department is:		
	1. the focal point for the oversight of all activities relating to the prevention and detection of ML/TF/PF		
	2. independent of all operational and business functions as far as practicable within any constraint of size of your institution		
	3. of a sufficient level of seniority and authority within your institution		
	4. provided with regular contact with and direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and measures against the risks of ML/TF/PF are sufficient and robust		
	5. fully conversant in the statutory and regulatory requirements and ML/TF/PF risks arising from your business		
	6. capable of accessing on a timely basis all required available information in performing their role		
	7. equipped with sufficient resources, including staff		

	8. overseeing your firm's compliance with the relevant AML requirements in Pakistan and overseas branches and subsidiaries.		
	(b) Audit function		
	(i) Have you established an independent audit function?		
	(ii) If yes, does the function regularly review the AML/CFT systems to ensure effectiveness?		
	(iii) If appropriate, have you sought review assistance from external sources regarding your AML/CFT systems?		
	(c) Staff screening		
	(i) Do you establish, maintain and operate appropriate procedures in order to be satisfied with the integrity of any new employees?		
3	RP with local / overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure an overall compliance with the CDD and record-keeping requirements.		
	Does your firm have overseas branches and subsidiary undertakings?		
	Do you have a group AML/CFT policy to ensure that all local /overseas branches and subsidiary undertakings have procedures in place to comply with the CDD and record-keeping requirements similar to those set under the AML Regulations?		
	If yes, is such policy communicated within your group?		
	In the case where your overseas branches or subsidiary undertakings are unable to comply with the above mentioned policy due to local laws' restrictions, have you done the following?		
	(a) informed the of such failure		
	(b) taken additional measures to effectively mitigate ML/TF/PF risks faced by them		
3a	Transnational TR Risk Assessment Factor Review		
	A: SENIOR MANAGEMENT OVERSIGHT		
	Did the Financial Institution (FI) have an adequate understanding of the transnational TF risk generated by it?		
	Did the FI identify international jurisdictions which it considers riskier in perspective of transnational TF risk?		
	Did the FI identify domestic locations which it considers riskier in perspective of transnational TF risk?		
	Did the FI identify and assessed its customers / products / channels which involve transactions with overseas jurisdictions and are more risky with respect to transnational TF risk?		
	Did the FI file any STR suspecting a customer over transnational TF risk during the year?		
	B: POLICY & PROCEDURES		
	Did the FI's board approve AML/CFT policy adequately defines and covers the area of transnational TF risks posed by / to the FI?		
	Did the FI's policy cover methodology for identification, assessment, monitoring and mitigation of transnational TF risks?		
	Did the FI cover transnational TF aspect in their internal TF risk assessment and aligned it with the country's NRA TF?		
	C: TRANSNATIONAL TF RISK ARISING FROM CUSTOMER ONBOARDING		
	Did the FI maintain comprehensive listings of all persons and entities who are designated either by UNSC or ATA, 1997?		
	Did the FI name screen those customers who posed transnational TF risk before providing any financial services to them?		
	At the time of customer onboarding, did the FI properly identify the nationality of individual customers?		
	Where the nationality was assessed as 'Pakistani', did the FI identify whether the individual customer was a resident or non-resident Pakistani?		

	While onboarding Afghan nationals, did the FI seek information like profession, occupation, sources and jurisdiction of funds generation, utilization and jurisdiction of utilization and expected turnover in the account?		
	While onboarding nationals of FATF monitored jurisdictions (grey listed and black listed), did the FI seek information like profession, occupation, sources and jurisdiction of funds generation, utilization and jurisdiction of utilization and expected turnover in the account?		
	In case of entities, did the FI identify the actual country of origin of the entity?		
	In case of foreign entities, did the FI identify the ultimate beneficial ownership of the entity?		
	In case of domestic NPOs / NGOs, did the FI assess the validation of their registration, the terms of their licenses?		
	In case of domestic NPOs / NGOs (including but not limited to Madrassas & religious charitable organizations), did the FI assess the sources of their funds?		
	D: ON GOING MONITORING AND REVIEW		
	Did the FI ensure that it, on an ongoing basis, review all relationships of the FI posing transnational TF risk?		
	Did the FI specifically ensure that it, on an ongoing basis, reviewed the accounts of Afghan nationals, nationals of Iran and DPRK including the accounts of staff of their embassies with respect to transnational TF risk?		
	Did the FI put in place such name screening measures which screened all existing relationships on a continuous basis.		
	Did the FI adequately assess funding of domestic NPOs/NGOs (including but not limited to Madrassas & religious charitable organizations) by foreign NPOs/NGOs/individuals that have presence in jurisdictions maintaining hostile relationship with Pakistan, jurisdictions monitored by FATF as high risk, jurisdictions identified as high risk by the FI or have links with designated / proscribed entities or individuals?		
	F: OTHERS		
	Did the FI's staff have adequate understanding of the transnational TF risk emanating from financial operations?		
	Did the FI provide any trainings to its staff on transnational TF risk arising from financial operations?		
	Did the FI's Internal Audit include review of the FI's assessment of transnational TF risk in its reviews?		
	Was review of transnational TF risk assessment by internal audit adequate?		
(B) Risk-Based Approach ('RBA')			
4	RPs are required to determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction, or service used by that customer.		
	Does your RBA identify and categorize ML/TF/PF risks at the customer level and establish reasonable measures based on risks identified?		
	Do you consider the following risk factors when determining the ML/TF/PF risk rating of customers?		
	(a) Country risk - customers with residence in or connection with the below high-risk jurisdictions:		
	(i) countries identified by the FATF as jurisdictions with strategic AML/CFT deficiencies		
	(ii) countries subject to sanctions, embargoes or similar measures issued by international authorities		
	(iii) countries that are vulnerable to corruption		
	(iv) countries that are believed to have strong links to terrorist activities		
	(b) Customer risk - customers with the following nature or behaviour might present a higher ML/TF/PF risk		
	(i) the public profile of the customer indicates involvement with, or connection to, politically exposed persons ('PEPs')		
	(ii) complexity of the relationship, including use of corporate structures, trusts and the use of nominees **and bearer instruments (if applicable)** where there is no legitimate commercial rationale		

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

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

	If you are unable to complete the CDD process, do you ensure that the relevant business relationships must not be established and assess whether this failure provides grounds for knowledge or suspicion of ML/TF/PF to submit a report to the FMU as appropriate?		
	If the CDD process is not completed before establishing a business relationship, would this be on an exception basis only, and with consideration of the following:		
	(a) any risk of ML/TF/PF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed.		
	(b) it is necessary not to interrupt the normal course of business with the customer (e.g. securities transactions).		
	(c) verification is completed as soon as reasonably practicable.		
	(d) the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable.		
	Have you adopted appropriate risk management policies and procedures when a customer is permitted to enter into a business relationship prior to verification?		

	If yes, do they include the following?		
	(a) establishing timeframes for the completion of the identity verification measures and ensuring that they are carried out as soon as reasonably practicable		
	(b) placing appropriate limits on the number of transactions and type of transactions that can be undertaken, pending verification		
	(c) ensuring that funds are not paid out to any third party		
	(d) other relevant policies and procedures		
	When terminating a business relationship where funds or other assets have been received, have you returned the funds or assets to the source (where possible) from which they were received?		
11	RPs are required to keep the customer information up-to-date and relevant.		
	Do you undertake reviews of existing records of customers to ensure that the information obtained for the purposes of complying with the AML requirements are up-to-date and relevant when one of the following trigger events happen?		
	(a) when a significant transaction is to take place		
	(b) when a material change occurs in the way the customer's account is operated		
	(c) when your customer documentation standards change substantially		
	(d) when you are aware that you lack sufficient information about the customer concerned		
	(e) if there are other trigger events that you consider and are defined in your policies and procedures, please elaborate further in the text box		
	Are all high-risk customers subject to a review of their profile?		
12	RPs are required to identify and verify the true and full identity of each natural person by using reliable and independent sources of information.		
	Do you have customers who are natural persons?		
	Do you collect the identification information for customers:		
	(i) Residents		
	(ii) Non-residents		
	(iii) Non-residents who are not physically present		
	Do you document the information?		
	If yes, please provide a list of acceptable documents that you obtain for verifying residential address (e.g. utility bills or bank statements). Certain types of address verification should not be considered sufficient, e.g. a post office box address for persons residing in Pakistan or corporate customers registered and/or operating in Pakistan.		
	In cases where customers may not be able to produce verified evidence of residential address, have you adopted alternative methods and applied these on a risk sensitive basis?		
	Do you require additional identity information to be provided or verify additional aspects of identity if the customer, or the product or service, is assessed to present a higher ML/TF/PF risk?		
13	RPs are required to identify and verify the true and full identity of each legal person and trust and its beneficial owners by using reliable and independent sources of information.		
	Do you have measures to look behind each legal person or trust to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets?		
	Do you fully understand the customer's legal form, structure and ownership, and obtain information on the nature of its business, and reasons for seeking the product or service when the reasons are not obvious?		
14	Companies		
	Do you have customers that are companies?		

	Do you obtain the following information and verification documents in relation to a customer that is a company?		
	For companies with multiple layers in their ownership structures, do you have an understanding of the ownership and control structure of the company and fully identify the intermediate layers of ownership in the company?		
	Do you take further measures, when the ownership structure of the company is dispersed/complex/multilayered without an obvious commercial purpose, to verify the identity of the ultimate beneficial owners?		
15	Partnerships and unincorporated bodies		
	Do you have customers that are partnerships or unincorporated bodies?		
	Do you take reasonable measures to verify the identity of the beneficial owners of the partnerships or unincorporated entities?		
	Do you obtain the information and verification documents in relation to the partnership or unincorporated entity?		
	Do you have customers that are in the form of trusts?		
	Do you obtain the information and verification documents to verify the existence, legal form and parties to a trust?		
	Have you taken particular care in relation to trusts created in jurisdictions where there is no or weak money laundering legislation?		
16	RPs may conduct simplified 'Know Your Customer' due diligence ('SDD') process instead of full CDD measures given reasonable grounds to support it. Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate, where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing. SDD is a condition where the timing of the actual verification of a particular customer is deferred until such time the entire CDD process is completed, rather than reducing what needs to be obtained, under a risk-based approach.		
	Have you conducted SDD instead of full CDD measures for your customers?		
	Do you refrain from applying SDD when you suspect that the customer, the customer's account or the transaction is involved in ML/TF/PF, or when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying or verifying the customer?		
	Before the application of SDD on any of the customer categories, have you performed a review of whether they meet the criteria of the respective category?		
17	RPs are required, in any situation that by its nature presents a higher risk of ML/TF/PF, to take additional measures to mitigate the risk of ML/TF/PF.		
	Do you take additional measures or enhanced due diligence ('EDD') when the customer presents a higher risk of ML/TF/PF?		
	If yes, do they include the following?		
	(a) obtaining additional information on the customer and updating more regularly, the customer's profile including the identification data.		
	(b) obtaining additional information on the intended nature of the business relationship, the source of wealth and source of funds		
	(c) obtaining the approval of senior management to commence or continue the relationship		
	(d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.		
18	RPs are required to apply, the same equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes, as are used for customers who are available for interview.		
	Do you accept customers that are not physically present for identification purposes to open an account?		
	If yes, have you taken additional measures to compensate for any risk associated with customers not physically present (i.e. face to face) for identification purposes?		

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

	(b) make enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited		
	Do you immediately (with no delay) obtain from intermediaries the data or information that the intermediaries obtained in the course of carrying out the CDD measures?		
	Do you conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay?		
	Have you taken reasonable steps to review intermediaries' ability to perform its CDD , whenever you have doubts as to the reliability of intermediaries?		
23	RPs are required to perform CDD measures on pre-existing customers when trigger events occur.		
	Have you performed CDD measures on your pre-existing customers when one of the following trigger events happens?		
	(a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is inconsistent with your knowledge of the customer or the customer's business or risk profile, or with your knowledge of the source of the customer's funds		
	(b) a material change occurs in the way in which the customer's account is operated		
	(c) you suspect that the customer or the customer's account is involved in ML/TF/PF		
	(d) you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying and verifying the customer's identity		
	(e) Are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box		
24	RPs are not allowed to maintain anonymous accounts or accounts in fictitious names for any new or existing customers.		
	Do you refrain from maintaining (for any customer) anonymous accounts or accounts in fictitious names?		
25	RPs are required to assess and determine jurisdictional equivalence as this is an important aspect in the application of CDD measures.		
	When you do your documentation for assessment or determination of jurisdictional equivalence, do you take the following measures?		
	(a) make reference to up-to-date and relevant information		
	(b) retain such record for regulatory scrutiny		
	(c) periodically review to ensure it remains up-to-date and valid		
(D) - Ongoing monitoring			
26	RPs are required to perform effective ongoing monitoring for understanding customer's activities and it helps the RP to know the customers and to detect unusual or suspicious activities.		
	Do you continuously monitor your business relationship with a customer by:		
	(a) monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds.		
	(b) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and that may indicate ML/TF/PF		
	Do you monitor the following characteristics relating to your customer's activities and transactions?		
	(a) the nature and type of transaction (e.g. abnormal size or frequency)		
	(b) the nature of a series of transactions (e.g. number of cash deposits)		
	(c) the amount of any transaction, paying particular attention to substantial transactions		
	(d) the geographical origin/destination of a payment or receipt		
	(e) the customer's normal activity or turnover		

	Do you regularly identify if the basis of the business relationship changes for customers when the following occurs?		
	(a) new products or services that pose higher risk are entered into		
	(b) new corporate or trust structures are created		
	(c) the stated activity or turnover of a customer changes or increases		
	(d) the nature of transactions change or the volume or size increases		
	(e) if there are other situations, please specify and further elaborate in the text box		
	In cases, where the basis of a business relationship changes significantly, do you carry out further CDD procedures to ensure that the ML/TF/PF risk and basis of the relationship are fully understood?		
	Have you established procedures to conduct a review of the business relationship upon the filing of a report to the FMU, and do you update the CDD information thereafter?		
27	RPs are required to link the extent of ongoing monitoring to the risk profile of the customer determined through RBA.		
	Have you taken additional measures with identified high risk business relationships (including PEPs) in the form of more intensive and frequent monitoring?		
	If yes, have you considered the following:		
	(a) whether adequate procedures or management information systems are in place to provide relevant staff with timely information that might include any information on any connected accounts or relationships		
	(b) how to monitor the sources of funds, wealth and income for higher risk customers, and how any changes in circumstances will be recorded		
	Do you take into account the following factors when considering the best measures to monitor customer transactions and activities?		
	(a) the size and complexity of its business		
	(b) assessment of the ML/TF/PF risks arising from its business		
	(c) the nature of its systems and controls		
	(d) the monitoring procedures that already exist to satisfy other business needs		
	(e) the nature of the products and services (including the means of delivery or communication)		
	In the case where transactions are complex, large or unusual, or patterns of transactions that have no apparent economic or lawful purpose are noted, do you examine the background and purpose, including where appropriate the circumstances of the transactions?		
	If yes, are the findings and outcomes of these examinations properly documented in writing and readily available for , other competent authorities and auditors?		
	In the case where you have been unable to satisfy that any cash transaction or third party transfer proposed by customers is reasonable and therefore consider it suspicious, do you make a suspicious transaction report (STR) to the FMU?		
(E) - Financial sanctions and terrorist financing			
28	RPs have to be aware of the scope and focus of relevant financial/trade sanctions regimes.		
	Do you have procedures and controls in place to:		
	(a) ensure that no payments to or from a person on a sanctions list that may affect your operations is made		
	(b) screen payment instructions to ensure that proposed payments to designated parties under applicable laws and regulations are not made		
	If yes, does this include:		
	(a) drawing reference from a number of sources to ensure that you have appropriate systems to conduct checks against relevant lists for screening purposes		
	(b) procedures to ensure that the sanctions list used for screening are up to date		

	Do you take the following measures to ensure compliance with relevant regulations and legislation on TF?		
	(a) understand the legal obligations of your institution and establish relevant policies and procedures		
	(b) ensure relevant legal obligations are well understood by staff and adequate guidance and training is provided		
	(c) ensure that the systems and mechanisms for identification of suspicious transactions cover TF as well as ML		
	Do you maintain a database (internal or through a third party service provider) of names and particulars of terrorist suspects and designated parties that consolidates the various lists that have been made known to it?		
	If yes, have you also taken the following measures in maintaining the database?		
	(a) ensure that the relevant designations are included in the database.		
	(b)ensure that the database is subject to timely update whenever there are changes		
	(c) ensure that the database is made easily accessible by staff for the purpose of identifying suspicious transactions		
	Do you perform comprehensive screening of your complete customer base to prevent TF and sanction violations?		
	If yes, does it include the following?		
	(a) screening customers against current terrorist and sanction designations at the establishment of the relationship		
	(b) screening against your entire client base, as soon as practicable, after new terrorist and sanction designation are published by the MoFA/NACTA/MoI/CTD		
	Do you conduct enhanced checks before establishing a business relationship or processing a transaction if there are circumstances giving rise to a TF suspicion?		
	Do you document or record electronically the results related to the comprehensive ongoing screening, payment screening and enhanced checks if performed?		
	Do you have procedures to file reports to the FMU, if you suspect that a transaction is terrorist-related, even if there is no evidence of a direct terrorist connection?		
(F) - Suspicious Transaction reports			

29	RPs are required to adopt on-going monitoring procedures to identify suspicious transactions for the reporting of funds or property known or suspected to be proceeds of crime or terrorist activity to the Financial Monitoring Unit (FMU).		
	Do you have policy or system in place to make disclosures/suspicious transaction reports to the FMU?		
	Do you apply the following principles once knowledge or suspicion has been formed?		
	(a) in the event of suspicion of ML/TF/PF, a disclosure is made even where no transaction has been conducted by or through your institution		
	(b) internal controls and systems are in place to prevent any director, officer and employee, especially those making enquiry with customers or performing additional or enhanced CDD procedures, committing the offence of tipping off the customer, or any other person who is the subject of the disclosure		
	Do you provide sufficient guidance to your staff to enable them to form a suspicion or to recognize when ML/TF/PF is taking place?		
	If yes, do you provide guidance to staff on identifying suspicious activity taking into account the following:		
	(a) the nature of the transactions and suspicious activity that staff is likely to encounter		
	(b) the type of product or service		
	(c) the means of delivery		
	Do you ensure your staff are aware and alert with the 's guidelines with relation to:		

	(a) potential ML scenarios using Red Flag Indicators		
	(b) potential ML involving employees of RPs.		
	Subsequent to a customer suspicion being identified, have you made prompt disclosures to the FMU if the following additional requests are made by the customer:		
	(a) instructed you to move funds		
	(b) close the account		
	(c) make cash available for collection		
	(d) carry out significant changes to the business relationship		
	Note: RPs are required to make prompt disclosure to FMU in any event.		
(G) - Record Keeping and Retention of Records			
30	RPs are required to maintain customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements.		
	Do you keep the documents/ records relating to customer identity?		
	If yes, are records kept throughout the business relationship with the customer, and for minimum period of five years after the end of the business relationship as per regulations. ? Note: As per the regulations, Records may be maintained for a longer period where transactions , customers or accounts involve litigation or is required by court or other competent authority .		
	Do you keep the following documents/ records relating to transactions?		
	(a) the identity of the parties to the transaction		
	(b) the nature and date of the transaction		
	(c) the type(if applicable) and amount of currency involved		
	(d) the origin of the funds		
	(e) the form in which the funds were offered or withdrawn		
	(f) the destination of the funds		
	(g) the form of instruction and authority		
	(h) the type and identifying number of any account involved in the transaction		
	Are the records kept for a period of five years after the completion of a transaction, regardless of whether the business relationship ended during the period, as required under the AML/CFT Regulations?		
	In the case where customer identification and verification documents are held by intermediaries, do you ensure that the intermediaries have systems in place to comply with all the record-keeping requirements?		
(H) - Staff Training			
31	RPs are required to provide adequate ongoing training to staff in what they need to do to carry out their particular roles with respect to AML/CFT.		
	Have you implemented a clear and well articulated policy to ensure that relevant staff receive adequate AML/CFT training?		
	Do you provide AML/CFT training to your staff to maintain their AML/CFT knowledge and competence?		

	Do your Compliance officer have professional qualification/Certification in the field of AML/CFT?		
	If yes, does the training program cover the following topics?		
	(a) your institution's and the staff's own personal statutory obligations, and the possible consequences for failure to report suspicious transactions under relevant laws and regulations		
	(b) any other statutory and regulatory obligations that concern your institution and the staff under the relevant laws and regulations, and the possible consequences of breaches of those obligations		

	(c) your own policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting		
	(d) any new and emerging techniques, methods and trends in ML/TF/PF to the extent that such information is needed by your staff to carry out their particular roles in your institution with respect to AML/CFT		
	Do you provide AML/CFT training for all your new staff, irrespective of their seniority, and before commencement of work ?		
	If yes, does the training program cover the following topics?		
	(a) an introduction to the background to ML/TF/PF and the importance placed on ML/TF/PF by your institution		
	(b) the need for identifying and reporting of any suspicious transactions to the Compliance Officer, as well as for reporting the offence of 'tipping-off' to the compliance officer.		
	Do you provide AML/CFT training for your members of staff who are dealing directly with the public?		
	If yes, does the training program cover the following topics?		
	(a) the importance of their role in the institution's ML/TF/PF strategy, as the first point of contact with potential money launderers		
	(b) your policies and procedures in relation to CDD, and record-keeping requirements for staff members that are relevant to their job responsibilities		
	(c) training with respect to circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required		
	Do you provide AML/CFT training for your back-office staff?		
	If yes, does the training program cover the following topics?		
	(a) appropriate training on customer verification and relevant processing procedures		
	(b) how to recognize unusual activities including abnormal settlements, payments or delivery instructions		
	Do you provide AML/CFT training for managerial staff including internal audit officers and COs?		
	If yes, does the training program cover the following topics?		
	(a) higher level training covering all aspects of your AML/CFT regime		
	(b) specific training in relation to their responsibilities for supervising or managing staff, auditing the system, and performing random checks as well as reporting of suspicious transactions to the FMU		
	Do you provide AML/CFT training for your Compliance Officer?		
	If yes, does the training program cover the following topics?		
	(a) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them, and reporting of suspicious transactions to the FMU		
	(b) training to keep abreast of AML/CFT requirements/developments generally		
	Do you maintain the training record details for a minimum of 3 years?		
	If yes, does the training record include the following details:		
	(a) which staff have been trained		
	(b) when the staff received training		
	(c) the type of training provided		
	Do you monitor and maintain the effectiveness of the training conducted by staff by:		
	(a) testing staff's understanding of the RPs and associated entities policies and procedures to combat ML/TF/PF		
	(b) testing staff's understanding of their statutory and regulatory obligations		
	(c) testing staff's ability to recognize suspicious transactions		
	(d) monitoring the compliance of staff with your AML/CFT systems as well as the quality and quantity of internal reports		

	(e) identifying further training needs based on training / testing assessment results identified above		

Annex 3

ML/TF Warning Signs/ Red Flags

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

Insurance entities

(1) Requests for a return of premium to be remitted to persons other than the policyholder.
(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) Change in beneficiaries (for instance, to include non-family members).
(6) 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 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.

Mutual Funds

(1) When an investor is more concerned about the subscription and redemption terms of the Mutual Fund than with r information related to the investment strategy, service providers, or 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) Customer trades frequently, selling at a loss
(12) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
(13) 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;
(14) Any transaction involving an undisclosed party;
(15) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;
(16) Significant variation in the pattern of investment without reasonable or acceptable explanation
(17) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
(18) Transactions involve penny/microcap stocks.
(19) 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.
(20) Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
(21) Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
(22) Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
(23) Customer conducts mirror trades.
Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

Annex 4

Proliferation Financing Warning Signs/Red Alerts

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

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

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

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

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

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

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

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

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

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

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

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

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

In case of any clarification/ enquiry, kindly contact Maan Securities (Private) Limited at the following address:

Service Desk,
Maan Securities (Private) Limited
Address: 611، 6th Floor, Pakistan Stock Exchange Building, 19-Khyaban-e-Aiwan-e-Iqbal, Lahore, Punjab 54000
Telephone: (042) 36308000
Email: Maansecurities@gmail.com