GUIDELINES ON ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM AND PROLIFERATION FINANCING

(Updated January, 2021)

SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

Disclaimer

These Guidelines are intended to provide general guidance to SECP regulated persons in implementation of the SECP AML/CFT Regulatory Framework including SECP AML/CFT Regulations 2020 issued under the amended AML Act 2010.

It is not a full statement of the law and should, therefore, not be relied upon as a source of law. It must be read in conjunction with the applicable laws and does not absolve any person from legal obligations, including obligations under other statutory provisions relating to AML/CFT regulatory framework for SECP regulated entities.

IMPORTANT: These guidelines in no way alter a reporting entity's obligations under the SECP Anti money Laundering and Countering Financing of Terrorism Regulations 2020. Any reference to SECP Regulations and AMLA in this guideline is for reference purposes only.

ACRONYMS / TERMS

AMLA	Anti-Money Laundering Act, 2010
AML	Anti-Money Laundering
AML/CFT legislations	AMLA FBR AML/CFT Regulations for DNFBPs UNSC Act ATA AML/CFT Sanctions Rules Counter Measures for High Risk Jurisdiction Rules
AML/CFT Sanction Rules	AML/CFT Sanction Rules 2020 SRO NO 950(I)/2020
ATA	Anti-Terrorism Act 1997
ATA	Anti-Terrorism Act 1997
APG	Asia/Pacific Group on Money Laundering
BO	Beneficial Ownership
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
CTR	Currency Transaction Report
Counter Measures for High Risk Jurisdiction Rules	Counter Measures for High Risk Jurisdiction Rules, 2020
DNFBP	Designated Non-Financial Business or Profession
ECDD or EDD	Enhanced Customer Due Diligence
FBR	Federal Board of Revenue
FATF	Financial Action Task Force
FMU	Financial Monitoring Unit
ML	Money Laundering
PF	Financing of proliferation
NACTA	National Counter Terrorism Authority
NPO	Non-Profit Organisation
RBA	Risk-Based Approach
SECP	Securities and Exchange Commission of Pakistan

SECP AML/CFT Regulations, 2020	Securities and Exchange Commission of Pakistan Anti Money Laundering and Countering Financing of Terrorism Regulations
SRO	Statutory Regulatory Order
STR	Suspicious Transaction Report
TF	Terrorism Financing
UN	United Nations
UNSC Act	United Nations (Security Council) Act, 1948
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution

Table of Contents

Implementation of AML/CFT Framework under the Securities and Exchange Commission of Pakistan (AML/CFT Regulations, 2020)

1. Introduction Purpose and Scope

i. A robust Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime ensures that financial systems and the broader economy are protected from the threats of Money Laundering ("ML"), Terrorist Financing ("TF") and Proliferation Financing ("PF"), thereby strengthening financial sector integrity and contributing to safety and security.

ii. Anti-Money Laundering and Countering the Financing of Terrorism regime requires financial institutions to understand their Money Laundering, Terrorist Financing and Proliferation Financing risks, adopt and effectively implement an appropriate risk-based ML/TF/PF control framework.

iii. In September 2020, the AML Act 2010 ("AMLA") has been amended under the (Anti-Money Laundering (Second Amendment) Act, 2020. Under section 6(A) (1) and Schedule IV of the Amended AML Act 2010, SECP has been designated as the AML/CFT Regulatory Authority for reporting entities regulated by SECP under the administered laws.

iv. Pursuant to the consequential alignment of SECP AML/CFT Regulatory Framework in line with the amended AMLA, the SECP issued SECP AML/CFT Regulations, 2020 (Regulations) in September 2020.

v. 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 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.

vi. These guidelines are applicable to all SECP Regulated Persons as defined in sub regulation 3(r) of SECP AML/CFT Regulations 2020 to mean: securities brokers, futures brokers, Insurers, Takaful Operators, NBFCs and Modarabas regulated by SECP under the administered legislation.

vii. The guidance provided in these guidelines applies to AML as well as CFT, even where it is not explicitly mentioned. Many of the AML measures entities have in place will overlap with their CFT measures. These may cover for example risk assessment, CDD checks, transaction monitoring, and escalation of suspicions and liaison relationships with the authorities.

2. Background

i. Financial Action Task Force (FATF)

The FATF is an international task force established in 1989 to develop international standards to combat ML, TF and PF. The FATF published a revised set of 40 Recommendations on AML/CFT measures in 2012, which are being continuously updated. Further information on the FATF is available at http://www.fatf-gafi.org/.

ii. Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is a FATF Style Regional Body. The APG is an associate member of FATF. It is an international organisation, consisting of 41 member jurisdictions. The APG is focused on ensuring that its members effectively implement the FATF Recommendations against ML, TF and PF. (For further information on the APG, visit: http://www.apgml.org/.)

Pakistan is not a member of the FATF, but is a member of the APG. The APG undertook a mutual evaluation of Pakistan in 2019. A copy of the Mutual Evaluation Report of Pakistan 2019 is available at http://www.apgml.org/documents/

iii. Money laundering

ML is the method by which criminals disguise or attempt to disguise the illegal origins of their wealth and protect their asset bases, so as to avoid the suspicion of law enforcement agencies and prevent leaving a trail of incriminating evidence. The term "Offence of money laundering" is defined in section 3 of the AMLA.

Money is the foremost reason for engaging in any type of criminal activity that generates funds. A predicate offence is the underlying crime that generates the funds to be laundered. The examples of predicate offences include inter-alia corruption, bribery, fraud, forgery, counterfeiting, kidnapping and corporate and fiscal offences. The offences listed in the Schedule to the AMLA have been declared as predicate offences.

iv. Terrorism financing

Terrorists and terrorist organizations rely on money to sustain themselves and to carry out terrorist acts. Money for terrorists is derived from a wide variety of sources. Generally, individual terrorists or entities are not greatly concerned with disguising the origin of money, they are concerned with concealing its destination and the purpose for which it has been collected. Terrorists and terrorist organizations therefore employ techniques similar to those used by money launderers to hide their money, which may be from legitimate or illegal sources. Section 11 of the ATA defines and criminalises TF.

3. Pakistan AML/CFT Regulatory Regime

i. Role of Government authorities

(a) The SECP is the designated AML/CFT Regulatory Authority for reporting entities regulated by SECP under the administered laws.
(b) The Financial Monitoring Unit (FMU) is the Financial Intelligence Unit of Pakistan. It is mandated to receive and analyse STRs and CTRs. All RPs must submit STRs and CTRs to the FMU.
(c) The Ministry of Foreign Affairs is responsible for issuing SROs on TF and PF. These resolutions are implemented in Pakistan through the United Nations (Security Council) Act, 1948. Under this Act the Ministry of Foreign Affairs issues SROs to give legal effect in Pakistan these decisions of the Security Council.
(d) The Ministry of Interior/NACTA issues Proscribed Organizations and Persons under the ATA for domestic designations on terrorism and TF.

ii. Legislative Framework

The relevant laws and regulations applicable to Financial Institutions are contained in the following laws and regulations:

(a) Anti-Money Laundering Act, 2020 (AMLA);
(b) SECP AML/CFT Regulations, 2020;
(c) The United Nations (Security Council) Act 1948 (UNSC Act);
(d) The Anti-Terrorism Act 1997 (ATA);
(e) United Nations Security Council (Freezing and Seizure) Order, 2019;
(f) UNSC Act Statutory Regulatory Orders (UN SROs) by the Ministry of Foreign Affairs;
(g) Ministry of Interior/National Counter Terrorism Authority (NACTA) Proscribed Organizations under Schedule-1 and Proscribed individuals under Schedule-4 of ATA;
(h) AML/CFT Sanction Rules 2020;
(i) Counter Measures for High Risk Jurisdiction Rules, 2020.

Sanctions for non-compliance

AMLA: Section 7I AMLA provides that if any reporting entity or natural person contravenes any of the provisions of sections 7(1), 7(3) to 7(6) and 7A to 7H, it may be subjected to sanctions, as mentioned under clause (h) of section 6A of this Act and as may be prescribed.

SECP AML/CFT Regulations: Section 31 provides that a violation of any of the provisions of the Regulations will be subject to sanctions as provided under the section 6A of AMLA and liable to sanction provided in the AML/CFT Sanctions Rules, 2020.

AML/CFT Sanction Rules: Section 3 provides the powers for SECP to sanction RPs for non-compliance with Sections 7 and 7A-7H of the AMLA, and with the AML/CFT regulations and FMU regulations. Sections 4 and 6 outline the types of sanctions and penalty amounts.

Annexure 6 provides for the relevant provisions of AMLA, 2010

Annexure 7 provides a list of useful weblinks to other AML/CFT legislation and guidance documents.

4. Obligation of RP in Establishing an Effective AML /CFT Governance and Compliance Program

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 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.

Statutory requirements under AML/CFT Legislation

AMLA: Under sections 7G-H, FIs shall implement compliance management arrangements and AML/CFT policies and procedures.

SECP AML/CFT Regulations: Section 5 on risk-based approach states the RPs shall:

(a) have policies, controls and procedures, which are approved by its board of directors, to enable them to manage and mitigate the risks that have been identified in its own risk assessment and any other risk assessment publicly available or provided by the Commission;
(b) monitor the implementation of those policies, controls and procedures and to enhance them if necessary; and
(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

Section 27 specifically states that in order to implement compliance programs as set out in 7G of the AMLA.

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. 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, procedures and controls to undertake a Risk Based Approach ("RBA");
   (b) Monitoring the implementation of policies, controls and procedures;

(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) Adequate 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.

iv. 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.

5. Risk Mitigation and Applying a Risk-based Approach (Regulation 5)

i. 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 programme containing the procedures, policies and controls to manage and mitigate those risks.
(c) Regular monitoring and review of those risks.

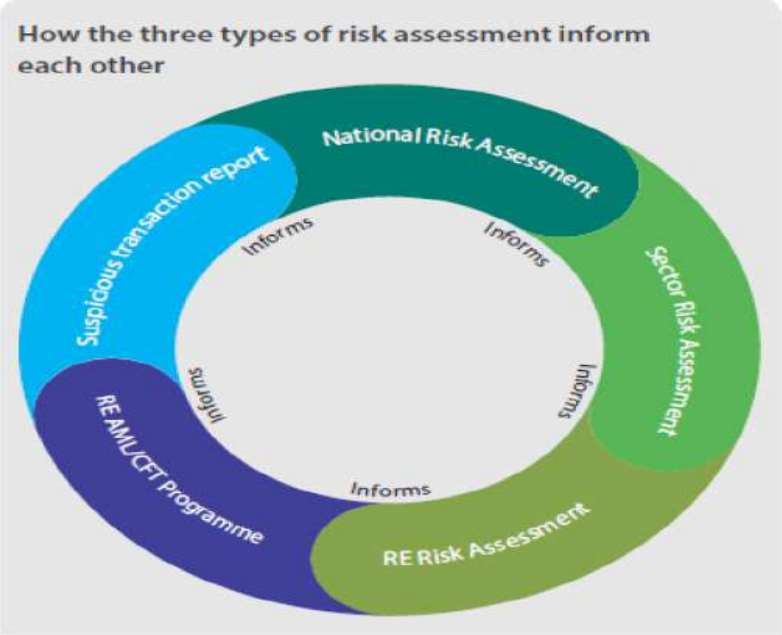
Statutory requirements under AML/CFT Legislation

AMLA: Section 7F requires the FIs to take appropriate steps to identify, assess and understand the risks to which its business is subjected to.

SECP AM/CFT Regulations: Section 4 refers to the requirement in the AMLA that RPs must identify, assess and understand its money laundering, and terrorism financing risks for customers, countries or geographic areas and products, services, transactions or delivery channels. The regulated person shall:
(a) document their risk assessments;
(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
(c) keep their risk assessments up to date;
(d) categorize its own overall entity level risk as high, medium or low based on the result of risk assessment; and
(e) have appropriate mechanisms to provide risk assessment information to the Commission.

ii. 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.

a. Risk Assessment and the RBA in relation to NRA findings



b. ML/TF Risk Assessment

There are three levels of risk assessment, which review ML/TF risks from different perspectives. Together, the three assessments inform RPs of potential risks to help combat ML/TF. The three risk assessments inform each other and combined provide a picture of the ML/TF risks Pakistan faces. The three levels of risk assessments are:

c. National Risk Assessment (NRA)

The NRA reviews ML/TF issues affecting the whole of Pakistan. It is based on information from suspicious transaction reports (STRs) and proceeds of crime asset recovery data. Information from government organizations, both domestic and international, also contribute to the NRA, and it provides a comprehensive overview of threats and crime trends. SECP encourages RPs to use the NRA to stay informed about emerging threats and trends.

d. Sector Risk Assessment (SRA)

SECP produce a risk assessment for the sectors it regulates aiming to improve RPs' understanding of the ML/TF sector risks, and to inform them of the risk indicators, trends and emerging issues. The SRA is reviewed from time to time to check how ML/TF risks affect the regulated sectors.

e. Risk assessments by RPs

i. RPs must carry out a risk assessment of ML/TF in their business. taking into account guidance material from SECP and the Financial Monitoring Unit. The entity risk assessment is part of SECP anti-money laundering and countering financing of terrorism guidance materials.

ii. 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.

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. The ML/TF/PF risk assessment is not a one-time exercise and is required to be carried out annually and as required under SECP SRO 920(1)2020 on TFS Obligation and reporting. https://www.secp.gov.pk/laws/directives/.

For guidance to prepare Internal AML/CFT Risk Assessment, please refer to Section 13 - Risk Assessment and Applying a Risk Based Approach.

6. New Products and Technologies (Regulation 7)

i. 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.

iv. Use of modern technology can strengthen AML/CFT measures, e.g. initial application forms completed on-line 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

7. Customer Due Diligence (CDD) – (Regulation 8 – 24)

i. CDD is the process through which an RP develops an understanding regarding customers and the ML/TF/PF risks they pose to the business. 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.

Statutory requirements under AML/CFT legislations

AMLA: Under Section 7A the AMLA, requires every reporting entity to conduct CDD on the customer, its beneficial owner, understand the purpose and intended nature of the business relationship and monitor the business relationship on an ongoing basis.

Section 7B provides for reliance on third parties to perform CDD.

Section 7D requires CDD to be completed prior to providing the services or terminating the relationship if any. It also provides for ceasing the CDD process to avoid tipping off.

Section 7E prohibits anonymous business relationships and transactions.

SECP AML/CFT Regulations:

Section 8 –15 prescribe the mandatory CDD requirements on identifying and verifying the customer, beneficial owner and person purporting to act on behalf of the customer using reliable and independent documents, data or information.

Section 16-18 provide for delayed verification subject to certain conditions.

Section 19 require RPs to conduct ongoing due diligence including scrutinising transactions, reviewing and keeping CDD records up to date.

Section 20 require RPs to apply CDD on existing customers on the basis of materiality and risk.

Section 21 state that the RP shall apply enhanced due diligence when there is a higher risk, called upon by the FATF for designated countries and for PEPs, including their close associates and family members.

Section 22 states that the RPs shall apply counter measures against high risk countries.

Section 23 states that the RPs may apply simplified due diligence after lower risks have been identified through proper risk assessments, but not when there is suspicion of ML/TF.

Section 24 provides for reliance on a third party subject to certain conditions.

a. Conducting CDD (Regulation 8-10)

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 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.

iii. 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

iv. Standard CDD is likely to apply to most of the customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer. It also includes the verification of that information. For beneficial owners the verification is according to the level of risk involved.

v. Simplified CDD can only be conducted on a specified set of circumstances such as government departments, local authorities and certain listed companies.

vi. EDD must be conducted when RP considers that the level of risk involved is such that EDD should apply. EDD requires the collection and verification of the same information as standard CDD as well as, according to the level of risk involved, the collection and verification of information relating to the source of wealth (SoW) and source of funds (SoF) of the customer.

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).

ix. 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.

x. 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.

xi. 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.

b. Risk-based implementation of Beneficial Ownership (BO) obligations – (Regulation 11 – 15)

i. The Beneficial Owner is the natural person at the end of the chain who ultimately owns or controls the customer. BO as per AMLA means:

(a) natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted; or
(b) natural person who exercises ultimate effective control over a legal person or legal arrangement

ii. For the beneficial ownership in the context of natural person, where a natural person seeks to open an account in his/her own name, the RP should inquire whether such person is acting on his own behalf. However, in relation to student, senior citizens and housewife accounts (where doubt exists that the apparent account holder is acting on his own behalf) the RP may obtain a self-declaration for source and beneficial ownership of funds from the customer and perform further due diligence measures accordingly.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

Please refer to Annexure 3 for guidance on Ultimate Beneficial Ownership.

c. Timing of Due Diligence (Regulation 16 - 18)

i. Customer Due Diligence and verification measures should be undertaken when establishing the business relationship and before any financial service or transaction occurs (Regulation 8).

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 (Regulation 16). 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.

iii. RPs need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

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.

d. Ongoing Monitoring of Customers, Systems and Controls (Regulation 19)

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. The regulated person should conduct ongoing due diligence on the business relationship by:

a) scrutinizing transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the regulated person's knowledge of the customer, their business and risk profile, including where necessary, the source of funds;
b) Examining the background and purpose of all complex and unusual transactions that have no apparent economic or visible lawful purpose. The background and purpose of these transactions will be inquired and findings documented with a view to making this information available to the relevant competent authorities, when required.
c) Carrying out reviews of existing records and ensuring that documents, data or information collected for CDD purposes is kept up-to-date and relevant, particularly for higher risk categories of customers.
d) It is important to review and revise the profiles of customers identified in (b) that are involved in complex and unusual transactions that have no apparent economic or visible lawful purpose.

iii. Additionally, RPs will 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/behaviour 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) selection, training and performance of agents, intermediaries and third parties who are in any way involved in the AML/CFT processes of the RP.

iv. RP should 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

v. Annexure 4 and 5 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.

vi. 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.

vii. 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.

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.

ix. 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.

e. Due Diligence of Existing Customers (Regulation 20)

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.

vi. For existing customers who opened accounts with old NICs, the RP will ensure that attested copies of identity documents are present in the RP's records. The RP will block accounts without identity document (after serving one-month prior notice) for all withdrawals, until the subject regulatory requirement is fulfilled. However, upon submission of attested copy of identity document and verification of the same from NADRA or biometric verification the block from the accounts shall be removed.

vii. For customers whose accounts are dormant or in-operative, withdrawals will not be allowed until the account is activated on the request of the customer. For activation, the regulated person shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfil the regulatory requirements.

viii. 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.

f. Enhanced Due Diligence (Regulation 21)

i. In some higher ML/TF/PF risk or in cases of unusual or suspicious activity an increased level of CDD is required. This includes situations where the RP consider (based on risk assessment) that the level of risk involved is such that enhanced CDD should apply. In such situations the RP need to use increased or more sophisticated measures to obtain and verify customer's details, their beneficial ownership structure and take reasonable steps to do this according to the level of risk involved.

ii. RP should usually obtain and verify information relating to the source of wealth (SoW) or source of funds (SoF) of your customer. In particular, RPs should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

iii. In case of low risk customer, the regulated person should obtain information of source of income however, no specific evidence is required. In case of high-risk customers, where EDD is required, evidence of source of income may be requested from the customer.

iv. List of examples of appropriate information and/or supporting documentation required to establish source of wealth and funds is as follows (any one of the documents may be obtained):

a) <u>Employment Income:</u> • Last month/recent pay slip; • Annual salary and bonuses for the last couple of years; • Confirmation from the employer of annual salary; • Income Tax Returns/ Wealth Statement.	**b) <u>Business Income/ Profits / Dividends</u>** • Copy of latest audited financial statements; • Rental statements • Dividend statements
c) <u>Savings / deposits/ assets/property:</u> • Statement from financial institution • Bank Statement • Taxation returns • Accountant's statements • Property ownership certificate • Share certificates	**d) <u>Inheritance:</u>** • Succession Certificate.
e) <u>Sale of Property/ Business:</u> • Copy of sale agreement/Title Deed	**f) <u>Loan</u>** • Loan agreement
g) <u>Gift:</u> • Gift Deed; • Source of donor's wealth; • Certified identification documents of donor.	**h) <u>Other income sources:</u>** • Nature of income, amount, date received and from whom along with appropriate supporting documentation. • Where there nature of income is such that no supporting documentation is available (for eg. Agricultural Income) Bank Statement may be obtained.
<u>Note:</u> The extent to documentation required for EDD would depend on the level of risk involved. **Disclaimer:** This list is indicative only and non-exhaustive. The examples provided may serve only as guidance.	

v. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations.

vi. Examples of enhanced CDD measures that could be applied for high-risk business relationships include:
   (a) Obtaining additional information, for example, about the volume of assets and information available through public databases, internet, etc. and more regularly updating the identification data of customer and beneficial owner;
   (b) Obtaining additional information on the intended nature of the business relationship;
   (c) Obtaining information about source of funds or source of wealth of the customer;
   (d) Obtaining information on the reasons for intended or performed transactions;
   (e) Obtaining approval of senior management to commence or continue the business relationship;
   (f) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

vii. However, enhanced CDD could be required again as a result of any material changes in your business relationship with your customer or due to ongoing CDD and account monitoring.

viii. An insurer/ takaful operator will include the beneficiary of a life insurance policy as a relevant risk factor in determining whether EDD measures are applicable.

g. Special Cases of Higher Risk and Enhanced Due Diligence

- **Politically Exposed Persons (PEPs)**

i PEPs hold positions of power and influence, thus potentially making them and their close associates more susceptible to corruption. The proceeds of corruption could be routed through the financial sector for the purpose of ML.

ii Under Regulation 3(q) of the Regulations 2020 PEPs means an individual who is or has been entrusted with a prominent public function either domestically or by a foreign country, or in an international organization.

iii 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.

iv Family members of a PEP spouse of the PEP and lineal descendants and ascendants and siblings of the PEP. 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.

v 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.

vi 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 behaviour; and
(d) Is from a high risk country.

vii The PEP red flags that the RPs shall consider include:
The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;

(a) 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;
(b) The PEP is associated with, or owns, or signs for, complex legal structures that are commonly used to hide Beneficial Ownership;
(c) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
(d) A PEP uses multiple bank accounts for no apparent commercial or other reason;
(e) 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 and foreign PEPs who are seeking to establish business relationships. RPs, in addition to performing standard due diligence measures should also:

(a) have appropriate risk management systems to determine whether the customer a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
(b) obtain approval from senior management to establish or continue a business relationship where the customer or a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP; and
(d) conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as a PEP, close associate and family member of a PEP.
(e) An insurer/ takaful operator will take reasonable measures at the time of payout of a life insurance policy to determine whether the beneficiaries and/or, where applicable, the beneficial owner of the beneficiary are politically exposed persons.
(f) Where higher risks are identified at payout to a PEP, the insurer or takaful operator must inform senior management before the payout of the policy proceeds, conduct enhanced scrutiny and also consider making a suspicious transaction report.

x The RP should undertake an independent check which may include an internet search of the customer's or beneficial owner's background and databases and reports from commercial service providers. Commercial screening service providers do provide databases of PEPs. They may be good for foreign PEPs, but may not be as good for Pakistani PEPs and their family and close associates.

xi In low risk scenarios declaration may be sufficient. This should be in a signed declaration as part of the customer acceptance/application form. In higher risk scenario, a search of publicly available information, such as internet public sources or commercial databases is necessary.

xii During ongoing monitoring RP should later identify the customer and/or the beneficial owner as a PEP. This may occur if the individual customer is promoted into a more senior role, or a ownership of a company changes and an individual acquires 25% or more, or some other controlling interest, or for some other reasons.

- **Non-Profit Organizations**

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:
    (a) by posing as legitimate entities;
    (b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
    (c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, 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.

- **High Net worth Individuals (HNWIs)**

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.

h. High-risk Countries and Higher Risk Regions within country (Regulation 22)

i. Pursuant to recommendations by the National Executive Committee, when called upon to do so by FATF and as indicated by the Federal Government, regulated persons will apply appropriate counter measures and EDD against high risk countries that is proportionate to the risk indicated.

ii. 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.

iii. 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).

iv. 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.

i. Simplified Due Diligence Measures (Regulation 23)

i. Under Regulation 23(1), RPs may conduct SDD in case of lower risks identified through adequate analysis and assessment and in line with the 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. In addition, under Regulation 23(2) the decision to rate a customer as low risk will be justified in writing by the regulated person.

iii. Simplified measures may include the following measures:
   (a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
   (b) Reducing the degree of on-going monitoring and scrutinizing of transactions;
   (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 transactions or business relationship established.

iv. 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.

j. Reliance on Third Parties (Regulation 24)

i When another 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 SECP and where RP can immediately obtain necessary information from the third party.

iii. RP may rely on a third party to conduct CDD on its behalf, provided that the regulated person will:

(a) remain liable for any failure to apply such indicated CDD measures;
(b) immediately obtain from the Third Party the required information concerning CDD;
(c) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; and
(d) satisfy itself that the Third Party is supervised by an AML/CFT regulatory authority or an equivalent foreign authority and has measures in place for compliance with AML Act obligation of CDD and record keeping.

iv. Where a regulated person relies on a third party that is part of the same corporate group, the regulated person may deem the requirements of subsection 24(1) to be met if: (3) In addition to subsection 24(1), when determining in which country a third party may be based, the regulated person shall have regard to available information on the level of country risk

v. RP shall ultimately remain responsible for its AML/CFT obligations, including generating STRs and shall carry out ongoing monitoring of such customer itself.

8. Targeted Financial Sanctions (Regulation 25)

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 Targeted Financial Sanctions (TFS) means both assets and funds freezing and prohibitions to prevent assets or financial services from being made available, directly or indirectly, for the benefit of designated persons and entities, except as authorized by the Competent Authority i.e. Ministry of Foreign Affairs or Ministry of Interior/ National Counter Terrorism Authority (NACTA).

Statutory requirements under AML/CFT legislations

AMLA*:* Under Sections 7G reporting entities must have a compliance programme and have AML/CFT policies and procedures, including for targeted financial sanctions.

AML/CFT Regulations: Section 25 states that the RP must undertake the following:

(a) develop mechanisms, processes and procedures for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with the stated designated/proscribed persons in the SROs and notifications issued by MoFA, NACTA and MoI.

(b) If during the process of screening or monitoring of customers or potential customers the regulated person finds a positive or potential match, it shall immediately:
i. freeze the relevant funds and assets without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer in accordance with the respective SRO.
ii. prohibit from making any funds or other assets, economic resources, or financial or other related services and funds in accordance with the respective SRO
iii. Reject the transaction or attempted transaction or the customer, if the relationship has not commenced.

(c) In all cases referred to in (b), the regulated person shall file a suspicious transaction report to the FMU in case that person is designated under United Nations Security Council Resolutions, or proscribed under the Anti-Terrorism Act, 1997 and simultaneously notify the Commission in the manner as may be instructed from time to time by the Commission.
(d) implement any other obligation under the AML Act 2010, United Nations (Security Council) Act 1948 and Anti-Terrorism Act 1997 and any regulations made there under.

Section 25 (2) further states:

(2) The regulated person is prohibited, on an ongoing basis, from providing any financial services to proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed/ designated name or with a different name. The regulated person should monitor their business relationships with the entities and individuals on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the regulated person shall take immediate action as per law, including reporting to the FMU.

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 require assets freeze in respect of designated individuals/ entities (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.

v RPs must make their Targeted Financial Sanctions (TFS) 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.

vi RPs shall 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.

vii For identification and mitigation of TF risk, the SECP has directed RPs under SRO 920 (1)2020 to follow the requirements of Red Flags/ indicators for identification of persons or entities suspected to be acting on behalf of or at the direction of designated/proscribed individuals or entities. Regulated persons must comply with the reporting requirements of SECP directive under SRO 920(1) 2020 available at : https://www.secp.gov.pk/laws/directives/

viii 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, MoFA and the UNSC Sanctions Committees' websites, are available at the following links and are regularly updated:

- Ministry of Foreign Affairs SROs for UN Security Council sanctions: http://mofa.gov.pk/unsc-sanctions/
- UN Security Council ISIL (Da'esh) & Al-Qaida Sanctions Committee: https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list/summaries
- UN Security Council Taliban Sanctions Committee: https://www.un.org/securitycouncil/sanctions/1988 .
- Ministry of Interior/NACTA the formal notification of proscription of an organization or person.
  (a) https://nacta.gov.pk/proscribed-organizations-3/
  (b) https://nacta.gov.pk/pp/
  (c) https://nfs.punjab.gov.pk/
- Ministry of Foreign Affairs Strategic Export Control Division (SECDIV) SROs http://www.secdiv.gov.pk/page/sro-unscr-sanctions
- UN Security Council 1718 (North Korea) Sanctions Committee: https://www.un.org/securitycouncil/sanctions/1718/materials
- UN Security Council Resolution 2231 Iran Sanctions: https://www.un.org/securitycouncil/content/2231/background

ix To ensure prompt transmission of SROs issued by MOFA to relevant stakeholders, the MOFA has put in place an email subscription service. RPs are required to sign up for this service and update their credential in case of any change. The link to the MOFA's website is: http://202.83.172.66/app/signup/.

x Similarly, whenever an addition or deletion is made in Fourth Schedule, a system generated email alert is immediately disseminated to all registered stakeholders. Therefore, the RPs shall also register for this service for immediate receipt of the alert.

xi 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.

xii The SECP has issued frequently asked questions on targeted financial sanctions under UNSCRs. These are available via the link below:
https://www.secp.gov.pk/aml-cft-2/aml-cft-faqs/

9. Record Keeping Procedures (Regulation 26)

Statutory requirements under AML/CFT legislations

AMLA: The AMLA Section 2 defines record as follows:

(xxxii) "record" includes the records maintained in the form of books or stored in a computer or any electronic device, or such other form as may be prescribed.

The AMLA Section 7C states the general record keeping requirements:

Every reporting entity shall maintain a record of all transactions for a period of at least five years following the completion of the transaction, and records of account files, business correspondence, documents, of all records obtained through CDD and the results of any analysis undertaken for a period of at least five years following the termination of the business relationship.

Further, Section 7(4) requires the record to be maintained for a period of 10 years for submitted STRs and CTRs after reporting of the transaction:

"Every reporting entity shall keep and maintain all record related to Suspicious Transaction Reports and CTRs filed by it for a period of at least ten years after reporting of transaction under sub-sections (1), (2) and (3)."

SECP AML/CFT Regulations: Section 26 requires RPs to maintain the required records as stated in Section 7C of the AMLA.

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. The RP will maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification.

iii. RPs should maintain a comprehensive record of AML/CFT reports with respect to 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

iv. Where transactions, customers or instruments are involved in litigation or where relevant records are required by a court of law or other competent authority, the RP will retain such records until such time as the litigation is resolved or until the court of law or competent authority indicates that the records no longer need to be retained.

v. The RP will maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification.

vi. The regulated person will provide, when requested by the Commission, investigating or prosecuting agency and FMU, any record within 48 hours after the request has been made or such time as may be instructed by the relevant authority.

10. Reporting Suspicious Transactions

Statutory requirements under AML/CFT legislations

AMLA: Under Section 7 (1) of the AMLA, the reporting entity (as per Section 2 (xxxiv) and 2 (xii) of AMLA) must file an STR to the FMU promptly for a conducted or attempted transaction if the RP knows, suspects or has reason to suspect that the transaction or a pattern of transactions of which the transaction is a part:

(a) involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime;
(b) is designed to evade any requirements of this Act;
(c) has no apparent lawful purpose after examining the available facts, including the background and possible purpose of the transaction; or
(d) involves financing of terrorism, including fund collected, provided, used or meant for, or otherwise linked or related to, terrorism, terrorist acts or organizations and individuals concerned with terrorism:

Under Section 34 (1) Disclosure of information. The directors, officers, employees and agents of any reporting entity or intermediary which report an STR or CTR pursuant to this law or any other authority, are prohibited from disclosing, directly or indirectly, to any person that the transaction has been reported unless there are disclosure agreements for corporate groups in accordance with regulations made hereunder.

SECP AML/CFT Regulations: Section 19(4) merely reminds RPs of their filing obligations as prescribed under Section 7 of the AMLA.

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. 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.

v. If the RP decides that a disclosure should be made, the law require the RP to report STR without delay to the FMU. Under Section 7 (1) of the AMLA, the requirements is that the STR must be filed promptly by the RP with the FMU.

vi. As required by the FMU, all STR reporting is via the FMU's online goAML system. The RPs are required to get themselves registered on the GoAML system of the FMU. The link to this system is as follows: www.fmu.gov.pk/goaml

vii. In order to ensure quality reporting, the reason(s) for suspicion should be supported with proper analysis and should contain following elements:

(a) Information on the person/entity conducting the suspicious transaction/activity;
(b) Details of the transaction, such as the pattern of transactions, type of products or services and the amount involved;
(c) Description of the suspicious transaction or its circumstances
(d) Tax profile of person/entity (if available)
(e) If the reported subject (e.g. client/customer) has been the subject of a previous STR then the reference number with date should be provided.
(f) Information regarding the counterparties, etc.
(g) Any other relevant information that may assist the FMU in identifying potential offences and individuals or entities involved.

viii. There are two types of suspicious reports which can be submitted by the RP to FMU.

(a) STR- A is to be reported on parties (Person, Account or Entity) involved in any suspicious activity, which does not involve transaction (s) or transmission of funds, However, STR-F should be filed in case where the transactions have been conducted.

(b) STR-F is to be reported on parties (Person, Account or Entity) for reporting of transactions and/or financial activity in which funds are involved and appears to be suspicious. An activity/event in which funds transmitted from one party to another must be reported as STR-F.

ix. The link of the goAML registration guide is provided as follows: http://www.fmu.gov.pk/docs/RegistrationGuideFMU.pdf. The link of the goAML reporting guide is provided as follows: http://www.fmu.gov.pk/docs/Financial-Monitoring-Unit-FMU-goAML-Web-Users-Guide-Updated-2020.pdf.

11. Currency Transaction Report (CTR)

i. The purpose of Currency Transaction Report (CTR) is to identify cash transactions with the financial system, either directly or via financial institution. The aim is to provide additional information to the FMU to develop financial intelligence for law enforcement agencies to investigate potential ML, TF or other offences.

Statutory requirements under AML/CFT legislations

AMLA: Section 7 (3) specifies that every reporting entity should:

(3) All CTRs shall, to the extent and in the manner prescribed by the FMU, be filed by the reporting entities with the FMU immediately, but not later than seven working days, after the respective currency transaction.

Under Section 2 (xi): Definitions in the AMLA, a CTR is defined as:

"CTR" means report on currency transactions exceeding such amount as may be specified by the National Executive Committee by notification in the official Gazette;

Under Section 34 (1) Disclosure of information**.** The directors, officers, employees and agents of any reporting entity or intermediary which report an STR or CTR pursuant to this law or any other authority, are prohibited from disclosing, directly or indirectly, to any person that the transaction has been reported unless there are disclosure agreements for corporate groups in accordance with regulations made hereunder.

SECP AM/CFT Regulations: Section 19(4) merely reminds RPs of their filing obligations as prescribed under Section 7 of the AMLA.

ii. As per Gazette notification SRO 73 (I)/2015 dated 21-01-2015, the minimum amount for reporting a CTR to FMU is two million rupees. Accordingly, all cash-based transactions of two million rupees or above involving payment, receipt, or transfer are to be reported to FMU as CTR. Aggregation of cash transactions during the day for the purpose of reporting a CTR is not required. However, if there is a suspicion that the customer is structuring the transaction into several broken cash transactions to evade reporting of CTR, the same may be reported in the form of an STR.

iii. Section 5 of AML Regulations 2015 further explains that the CTR is filed on a prescribed format when a cash-based transaction involving payment, receipt, or transfer of an amount, as specified by the National Executive Committee, occurs.

iv. Under Section 7 (3) of the AMLA, the CTR must be filed by the RP with the FMU not later than seven working days, after the respective currency transaction.

v. Similar to STR reporting to the FMU, all CTR reporting is via the FMU's online goAML system – refer: https://goamlweb.fmu.gov.pk/PRD/Home.

12. Internal Controls (Compliance Function, Audit Function, Employee Screening, Ongoing Training Program and Outsourcing) – (Regulation 27)

Statutory requirements under AML/CFT Legislation

AMLA: Under Sections 7G-H, FIs must have a compliance programme and have AML/CFT policies and procedures. A compliance programme includes the appointment of a compliance officer at a management level and staff training.

SECP AML/CFT Regulations: Section 27 (1) specifically states that in order to implement compliance programs as set out in 7G of the AMLA, the RPs shall implement the following internal policies, procedures and controls:

(a) compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the regulated person's compliance with these Regulations, the AML Act and other directions and guidelines issued under the aforementioned regulations and laws;
(b) screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively;
(c) an ongoing employee training program; and
(d) an independent audit function to test the system.

Section 27 (2) includes reporting lines and terms of reference for the compliance officer.

Section 28 states the requirements on corporate group compliance, including safeguards for the confidentiality on the use of information exchanged within the group.

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:

- **First line of defence: Business units**

1) 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.

2) 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.

- **Second line of defence*:* Compliance Officer and Compliance Function**

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

2) As part of second line of defence, the Compliance Officer 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 SECP/LEAs.

- **Third line of defence: Internal Audit Function**

1) 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:
(d) CDD measures, monitoring and updating of customer data;
(e) Screening process for TFS, and test its functionality;
(f) testing transactions with emphasis on high–risk customers, geographies, products and services;
(g) Record keeping and documentation.
(h) the effectiveness of parameters for automatic alerts and the adequacy of RP's process of identifying suspicious activity, internal investigations and reporting;
(i) the adequacy and effectiveness of training programs and employees' knowledge of the laws, regulations, and policies & procedures.

iii. **Employee Screening**

(a) 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.

(b) 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.

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

iv. **Employee Training**

(a) 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.
(b)
(c) 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.
(d)
(e) 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 non-compliance with relevant laws.
(f)
(g) 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**

(a) 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 is fit and proper to perform the activity that is being outsourced.

(b) 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 service provider fails to perform the outsourced activity as agreed. The ultimate responsibility for meeting AML/CFT requirements always remains with the RP for outsourcing arrangements.

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.

(c) The service provider 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 service provider.

13. Risk Assessment and Applying a Risk Based Approach - (Please refer to Annexure 1 for preparing AML/CFT risk assessments)

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 SECP;
   (c) Any applicable guidance by relevant authorities (such as FMU, SBP, MoFA, NACTA etc.);
   (d) information and guidance published by international organisations 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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 SECP, 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.

iv. 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.

v. 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.

vi. 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 high-risk 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 when new products are offered, new markets are entered, high-risk customers open or close accounts, or when 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.

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 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 One-off transactions.
(i) Complex transactions that involve multiple parties or multiple jurisdictions.
(j) Any introducers or intermediaries the RP might use and the nature of their relationship with the RP.
(k) 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).
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/region 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 customer 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***.

Customer Transaction	*Intermediaries*	*Online Transactions*	*Domestic Transfers*	*Deposit or Investment*	*Life Insurance*	*Securities 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.

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.

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

i. Legal Person

Customer Risk Type - Legal Persons					
Customer Type	Number of Customers/Policyholders	Total Amount on Deposit/Value of Trade (Buy and Sale)/Gross Premium	Internal Risk Rating by RP		
			Total Number Classified as Low Risk	Total Number Classified as Medium Risk	Total Number Classified as High Risk
1. Non-Resident					
Foreign Company					
Total Non-Resident Legal/Natural Persons	0	0.00	0	0	0
Legal Persons					
Listed Companies					
Private Companies					
Limited Liability Partnerships					
Trusts/WAQF					
Cooperatives					
NGO's					
Mutual Funds					
Exchange Companies					
Gov Contractors					
Other(as may be defined by RP)					
Accountants/Auditors/Tax Consultants					
Lawyers					
Real Estate Agents					
Gems/Jewellery Dealers					
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' as identified by the FATF		
Of which, resident customers from 'High risk Jurisdictions' as identified by the Latest NRA		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions		
Legal Persons		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the FATF		
Of which, resident customers from 'High risk Jurisdictions' as identified by the Latest NRA		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions		
Total	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/Moderate/Low)	
Customer Type	
Product Type	
Delivery Channels	
Geography	
Overall AML/CFT Risk Rating	

AML/CFT Compliance Self-Declaration **Annexure 2**

Regulated Entities should submit their annual compliance assessment checklist to demonstrate adequacy and effectiveness of AML/CFT compliance framework in light of the Regulations, and are encouraged to use the checklist provided below.

SECP AML/CFT Compliance Self-Declaration			
Name of the Financial Institution			
Self-Declaration completed by (Name) ***(Designation)***			
Date			
The AML/CFT Compliance Self-Declaration 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 Compliance Self-Declaration 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 SECP 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 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 SECP 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/multi-layered without an obvious commercial purpose, to verify the identity of the ultimate beneficial owners?		
15	Partnerships and unincorporated bodies		
	Do you have customers 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	The RP may apply SDD only where low risk is identified through adequate analysis and assessment and any other risk assessment publicly available or provided by the Commission. In addition, the decision to rate a customer as low risk will be justified in writing by the regulated person. RPs may conduct simplified 'Know Your Customer' due diligence ('SDD') process instead of full CDD measures. This is appropriate, only 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, and justified this in writing?		
	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 and 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 SECP, 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 SECP's guidelines with relation to:		
	(a) potential ML scenarios using Red Flag Indicators		
	(b) potential ML involving employees of RPs.		
	Subsequent to a customer suspicion being identified, have you made prompt disclosures to the FMU if the following additional requests are made by the customer:		
	(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 SECP 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		

Annexure 3

Ultimate BENEFICIAL OWNERSHIP (UBO)

Introduction

Corporate vehicles, such as companies, foundations, partnerships, and other types of legal persons and arrangements play an important and essential role in supporting commercial and entrepreneurial activity. However, despite the essential and legitimate role that these corporate vehicles play in an economy, under certain conditions, they have been misused for illicit purposes, including money laundering (ML), bribery and corruption, insider dealings, tax fraud, and terrorist financing (TF),

The ease with which limited liability companies can be formed makes them particularly vulnerable, to being used for building complex legal ownership structures, often involving shell companies. Similarly Trust and company service providers frequently play a role in such structures. The use of nominee directors and shareholders, both formal and informal greatly increases the risks by creating barriers between the natural person, who is the UBO and laundered proceeds. In many cases professional intermediaries play an important role in helping create or operate the structures used to conceal beneficial ownership, either complicity or unwittingly.

What is an Ultimate Beneficial Owner (UBO)?

Definition of 'beneficial owner' from the Glossary to the FATF Recommendations is as follows: Beneficial owner refers to the natural person(s) who *ultimately owns or controls* a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise *ultimate effective control* over a legal person or arrangement.

Reference to "ultimately owns or controls" and "ultimate effective control" refers to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. This definition also applies to beneficial owner or a beneficiary under a life or other investment linked insurance policy.

In your business dealings the beneficial owner can be:

a) the person you are doing business with, who may be the legal owner of the entity, or
b) the person, or group of persons, who own/s or controls that business.

A company may have more than one beneficial owner or group of owners, to conceal the identity of absolute controlling person or interests. The "ultimate beneficial owner" of a legal entity is thus:

- one who holds 25% or more of share capital; or
- one who exercises 25% or more of the voting rights; or
- a beneficiary of 25% or more of the legal entity's capital; or
- a 'nominee director 'appointed on behalf of another person and used to conceal the identity of the true owner of the company or some illicit activity; or
- a company or other legal entity who is a 'corporate director', who may be used to construct complex and opaque corporate structures across multiple jurisdictions to facilitate illicit activity

Understanding Beneficial Ownership

I. Beneficial ownership is not legal ownership in all circumstances

The three key points to understand are:

a) legal ownership is not synonymous with beneficial ownership. People tend to assume that legal owners are the same as beneficial owners, and therefore do not differentiate between the two. In AML/CFT, this distinction is very important;
b) an individual can be an indirect owner of a company through another company in which the individual has ownership; and
c) the beneficial owner is always an individual who ultimately owns or controls a legal entity or arrangement, such as a company, a trust, a foundation, etc.

II. Natural persons :
In most instances the individual customer is buying for oneself, so the customer and beneficial owner are the same. However, this may not always be the case and confusion may arise whether the individual customer is also the beneficial customer.

III. Legal persons (e.g. company)

The separation of beneficial ownership from legal ownership occurs more frequently with legal persons and arrangements e.g. companies and trusts. In many cases, the legal owner of the legal person is the beneficial owner, but not in all circumstances. The Companies Act 2017 also provides a definition of beneficial ownership as stated in Section 123A, as follows:

"*For the purpose of this section, the term "ultimate beneficial owner" means a natural person who ultimately owns or controls a company, whether directly or indirectly, through at least twenty five percent shares or voting rights, or by exercising control in that company through other means, a may be specified.*"
This definition provides for 25% and above ownership, directly or indirectly, for the controlling ownership test. Essentially there are three tests for identifying the beneficial owner of a company as provided in the AML/CFT legislations: controlling ownership test, control through other means test and senior management test. The three tests are a cascading process, to be used in succession, when a previous test has been taken but has not resulted in the identification of the beneficial owner. These are explained in the Table below.

<table>
<tr><td colspan="2">Identifying Beneficial Ownership for Legal Persons –

Three Cascade Tests</td></tr>
<tr><td colspan="2">Limited Companies/ Corporations</td></tr>
<tr><td colspan="2">TEST 1: The Legal Ownership Test
This test is still about control, but control primarily through legal ownership. In general the threshold to use is 25% or more to determine controlling legal ownership, but there may be a need to use a lower threshold.</td></tr>
<tr><td>1. Ownership threshold approach: The natural person(s) who directly or indirectly holds a minimum percentage of ownership interest in the legal person, so that he/she can exercise controlling ownership interest (e.g. voting rights).</td><td>Any individual owning more than a certain percentage of the company i.e. 25%. If 25% is the threshold there can only be a maximum of 4 beneficial owner as provided in Section 123A of the Companies Act.

While 25% or more may be used for the controlling ownership test, If the 25% threshold does not identify any beneficial owners, or there are concerns or doubts that the 25% threshold has correctly identified all the beneficial owners , it is recommended that a lower threshold of 20% be used, and then 10%, if needed.

Individuals may not meet the ownership threshold (e.g. below 25%) but because they are connected (e.g. family or extended family), collectively they can exercise control – refer to Test 2.

These concepts will be explained in the examples following this table.</td></tr>
<tr><td colspan="2">TEST 2: The Control Test

This is normally the second test used to identify beneficial owner. This test is used when there is doubt that the person with the controlling ownership interest is the beneficial owner or where no natural persons exerts control through ownership interest. For example, no one owns more than 25% or more, or there are so many layers of indirect ownership that it is difficult to identify the individuals who own the company in the top layer</td></tr>
</table>

2. Majority interest approach: Shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity.	For example, to appoint or remove the majority of the board of directors, or its chair, or CEO of the company; This can be achieved by exercising 25% or more of the voting rights other than through legal ownership e.g. shareholders agreement to vote collectively to control a company even though individually they do not have 25% or more.
3. ***Connections or contractual relations approach:*** Natural persons who may control the legal person through other means	For example, the natural person(s) who exerts control of a legal person through other means such as personal connections to persons in positions described above or that possess ownership. The natural person(s) who exerts control without ownership by participating in the financing of the enterprise, or because of close and intimate family relationships, historical or contractual associations, or if a company defaults on certain payments.
4. ***Company director's position approach:*** The natural person(s) responsible for strategic decisions that fundamentally affect the business practices or general direction of the legal person.	The identification of the directors may still provide useful information.
TEST 3: The Senior Management Test In the event the beneficial owner cannot be identified or verified through Tests 1 and 2, the use of the senior management approach is an alternative test of beneficial ownership.	
5. *Senior management approach (alternative test):* The natural person(s) who exercises executive control over the daily or regular affairs of the legal person through a senior management position**.**	For example, Dispersed ownership; Multiple layers of ownership, including in overseas secrecy jurisdiction. The senior management test for, example, may include the chief executive officer (CEO), chief financial officer (CFO), managing or executive director, or president. It is the natural person(s) who has significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person.

To assist regulated person in identifying and verifying UBO, the following two documents will be useful:

(i) Register of Ultimate Beneficial Ownership Information of the Company, maintained under Section 123A of Companies Act 2017, relates to the Register of Ultimate Beneficial Ownership which may be beyond the first layer of shareholding of the company.

(ii) Register of Members of a Company, maintained under Section 119 of the Companies Act, 2017, provides information on shareholders/members of the company whether natural or legal persons

Basically for simple company structures where individuals own the company directly, the RP will need the information that the company is required to keep under Section 119 of the Companies Act. However, where another company owns your customer (company), then the RP will need the Register of Ultimate Beneficial Ownership maintained by the company under S123 (A) of the Companies Act 2017. The UBO register should identify beneficial ownership, even when the company (a shareholder of your customer) is owned by other companies through a chain of corporate ownership).

The Table below provides a summary of information in both documents.

Summary of information contained in the Register of Beneficial Ownership and Register of Members		
	Register of Beneficial Ownership Section 123 A	**Register of Members Section 119**
Applicability	A company shall maintain information of its beneficial owners in such form and manner, within such period and obtain such declaration from its members as may be specified. *Explanation.–* For the purpose of this section, the term "ultimate beneficial owner" means a natural person who ultimately owns or controls a company, whether directly or indirectly, through at least twenty five percent shares or voting rights or by exercising effective control in that company through such other means, as may be specified. (2) Every company shall, in such form and manner as may be specified, maintain a register of its ultimate beneficial owners and shall timely record their accurate and updated particulars, including any change therein, and provide a declaration to this effect to the registrar, and where any government owned entity is a member of a company such particulars of the relevant government owned entity shall be entered in the register of ultimate beneficial owners in the specified manner. The particulars of UBO have been specified through Regulation 19A of the Companies (General Provisions and Forms) Regulations, 2020. The same are available at; https://www.secp.gov.pk/UBO	Every company shall keep a register of its members. There must be entered in the register such particulars of each member as may be specified. The above specification is contained in Regulation 19 of the Companies (General Provisions and Forms) Regulations, 2018 which is available at https://www.secp.gov.pk/forms
Represents	Ultimate Ownership of the company	Basic/Legal Ownership
Information to be maintained by the company	Yes	Yes

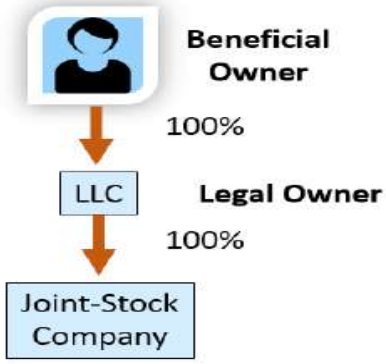
Information to be notified to the registrar or Commission	No, only Compliance Certificate is provided by the Company	Yes, through FORM A once a year and any Change up to and beyond 25% through Form 3A
Information is publicly available	No	Yes
Penal provision for non-compliance	Yes	Yes

Here are some examples to show how to identify beneficial ownership using the three tests.

Example 1: Direct Ownership (Test 1: Identifying the beneficial owner through controlling legal ownership)

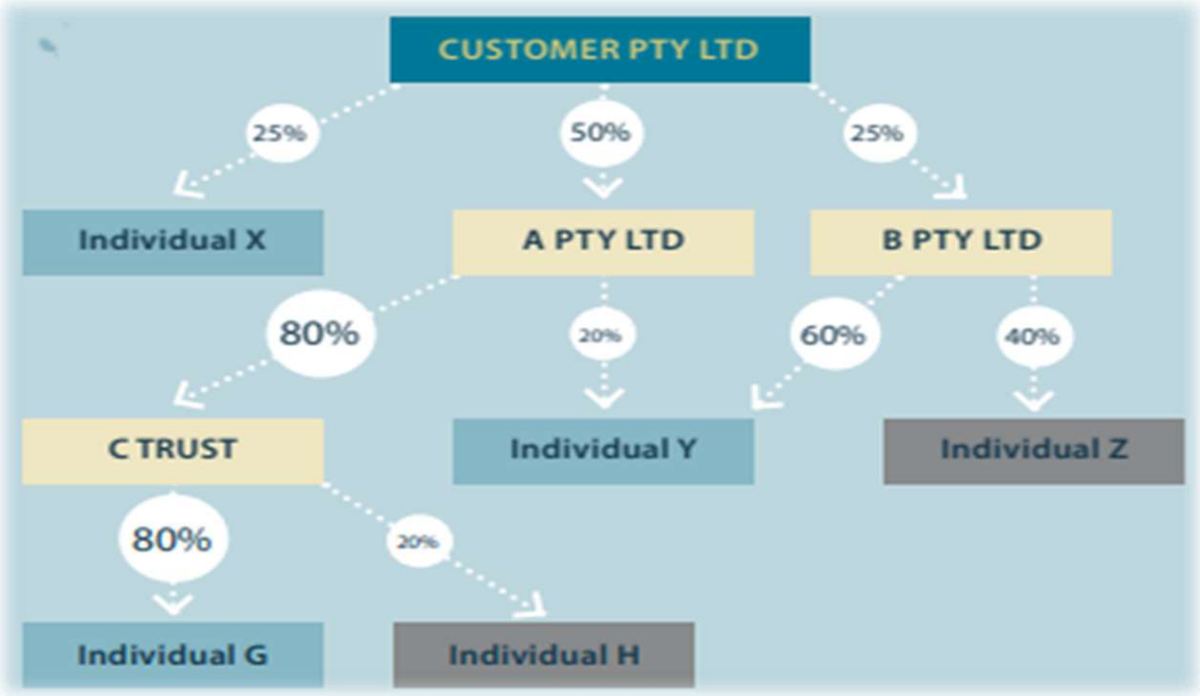
Example 1 below demonstrates a simple use of the ownership test to identify the beneficial owner, namely identify the person that owns 25% or more. In this example, there is one individual who is the sole shareholder (i.e. 100%). The person directly owns the company. Unless there is information to the contrary, this individual is also both the legal and the beneficial owner of the company.

Example 2: Indirect ownership with one layer (Test 1: Identifying the beneficial owner through controlling legal ownership)



Example 2 (Test 1) above shows an additional layer – the limited liability company (LLC) – between the legal vehicle (the Joint Stock Company) and its beneficial owner. This is indirect ownership. The LLC, as the shareholder of the Joint Stock Company, is its direct legal owner, while the beneficial owner indirectly controls the joint stock company through the LLC.

Example 3: Indirect ownership with multiple layers (Test 1: Identifying the beneficial owner through controlling legal ownership)



Example 3 above shows the following:

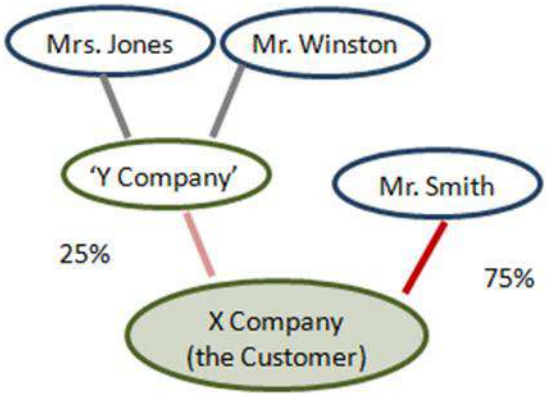
I. Individual X is a beneficial owner because they directly own 25% of CUSTOMER PTY LTD

II. Individual G is a beneficial owner because they hold 80% of the units in C TRUST (a unit trust) which in turn owns 80% of A PTY LTD, which owns 50% of CUSTOMER PTY LTD (meaning Individual G has an indirect .8 x .8 x .5 = 32% ownership of CUSTOMER PTY LTD).

III. Individual Y is a beneficial owner because they have two interests that collectively amount to an indirect 25% of CUSTOMER PTY LTD:

- The first is their 20% interest in A PTY LTD, which owns 50% of CUSTOMER PTY LTD (providing an indirect .2 x .5 = 10% ownership of CUSTOMER PTY LTD).
- The second is their 60% interest in B PTY LTD, which owns 25% of CUSTOMER PTY LTD (providing an indirect .6 x .25 = 15% ownership of CUSTOMER PTY LTD).
- Adding these together, Individual Y has a 10% + 15% = 25% interest in CUSTOMER PTY LTD

Example 4: Direct and indirect ownership of private company (Test 2: Identifying the beneficial owner through control by other means)



The point of example 4 above is to illustrate how to identify the beneficial owner through control by other means. If we use the ownership test with the 25% threshold, Mr Smith would be the sole beneficial owner as he owns 75%. While Mrs Jones and Mr Winston own 50% each of Y Company, and Y Company owns 25% of the customer – X Company, individually they own only 12.5% of the customer. This is below the 25% threshold.

However, the RP discovers after reviewing the company registration details of Y Company that Mrs Jones and Mr Winston both live in the same residential address and are married, but Mrs Jones has kept her maiden name. They could be working collectively to control Y Company which in turn would exercise its 25% control of X Company, the customer. Therefore both Mrs Jones and Mr Winston are deemed to be also beneficial owners based on the control test.

Example 5: Direct and indirect ownership by 10 shareholders (Test 3: Identifying the beneficial owner through control by other means/senior management)

The purpose of Example 5 is to highlight a situation of dispersed legal ownership and control. This simple example is of Company A which has 10 shareholders all owning 10% each. All are direct owners, and all 10 owners are on the board of directors.

Customer – Company A

Shareholder 1	10%
Shareholder 2	10%
Shareholder 3	10%
Shareholder 4	10%
Shareholder 5	10%
Shareholder 6	10%
Shareholder 7	10%
Shareholder 8	10%
Shareholder 9	10%
Shareholder 10	10%

In this case, there are no beneficial owners of Company A using Test 1 (ownership test) as no one owns 25% or more. Using Test 2 (control test) has not identified any owner that has control, as all are directors with equal voting rights. Assuming owners are not forming any alliances or voting blocs, Test 3 on senior management would be the best approach. The RP could apply Test 2 and work on the assumption there are 10 individuals that control the customer. This would require verifying the 10 individual directors.
Importance of identifying Ultimate Beneficial Owner (UBO)

IMPORTANT: Identification of UBO is essential for implementation and enforcement of an effective AML and CFT regime. In certain cases a legal person could be effectively controlled indirectly by a natural person through a chain of ownership for use in ML/TF activities and remain undetected.
The objective of regulatory framework for UBOs is to identify the ownership structures of legal persons, to identify the indirect methods deployed to exercise effective control over the legal persons, and to determine the UBO who is ultimately the natural person behind the transactions.

For further guidance please refer to SECP Guidelines on Ultimate Beneficial Ownership Framework for Legal Persons and Legal Arrangements:

Link: https://www.secp.gov.pk/laws/guidelines/

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.

Annexure 5

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.

(h) FMU has prepared red flags indicators to identify a suspicion that could be indicative of Proliferation Financing. The red flags can be accessed from FMU website at the following link:

http://www.fmu.gov.pk/docs/Red-Flag-Indicators-for-Proliferation-Financing.pdf

Relevant provisions of AMLA, 2010

7A. Conducting CDD.— (1) Every reporting entity shall conduct CDD in the manner as may be prescribed and in accordance with provisions of this Act in the following matters, namely:-
(a) entering into a business relationship;
(b) conducting an occasional transaction above the prescribed threshold;
(c) where there is a suspicion of money laundering or terrorist financing; or
(d) where there are doubts about the veracity or adequacy of previously obtained data.

(2) Every reporting entity shall—
(a) identify the customer and verify the customer's identity on the basis of documents, data or information obtained from reliable and independent sources;

(b) identify the beneficial owner and take reasonable measures to verify the beneficial owner's identity on the basis of documents, data or information obtained from reliable sources and be satisfied that it knows who the beneficial owner is;

(c) understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship; and
(d) monitor the business relationship on an ongoing basis.

7B. Reliance on third parties.— A reporting entity may rely on third party to perform CDD in the manner as may be prescribed.

7C. Record keeping.— Every reporting entity shall maintain a record of all transactions for a period of at least five years following the completion of the transaction, and records of account files, business correspondence, documents, of all records obtained through CDD and the results of any analysis undertaken for a period of at least five years following the termination of the business relationship.

7D. Inability to complete CDD and tipping off.— (1) Where a reporting entity is unable to complete CDD requirements, it—
(a) shall not open the account, commence business relations or perform the transaction; or shall terminate the business relationship if any ; and
(b) shall promptly consider filing a Suspicious Transaction Report in relation to the customer.

(2) Where a reporting entity forms a suspicion of money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the customer, the reporting entity shall not pursue the CDD process and shall file a STR.

7E. Anonymous business relationships and transactions.— No reporting entity shall enter into a business relationship or conduct any transaction with a customer who is anonymous or provides a fictitious name.

7F. Risk understanding.— Every reporting entity shall take appropriate steps to identify, assess and understand the risks to which its business is subjected to, in accordance with this Act and as prescribed.

7G. Compliance program.— Every reporting entity shall implement compliance management arrangements, including the appointment of a compliance officer at a management level and training programs, having regard to the money laundering and terrorism financing risks and the size of the business during the course of their activities subject to this Act and as prescribed.

7H. Policies and procedures.— Every reporting entity shall implement policies and procedures to ensure their compliance with the provisions of this Act and orders, rules or regulations made thereunder that impose TFS obligations upon reporting entities.

7I. Sanctions for reporting entities.– If any reporting entity or natural person contravenes any of the provisions of sections 7(1), 7(3) to 7(6) and 7A to 7H, it may be subjected to sanctions, as mentioned under clause (h) of section 6A of this Act and as may be prescribed.

Annexure 7

Useful Web links to publications /documents/information

Document	Web link
1. AMLA 2010	http://www.fmu.gov.pk/Anti-Money- Laundering-Act-2010-as-amended-upto-Feb.-2020.pdf
2. ATA	http://www.fmu.gov.pk/wp-content/uploads/2020/04/The-Anti-Terrorism-Act-1997-as-amended-upto-Feb-2017-1.pdf
3. Guidelines on filing of Suspicious Transaction Reports for the Reporting Entities	http://www.fmu.gov.pk/wp-content/uploads/2020/05/Circular-02-of-2020-.pdf http://www.fmu.gov.pk/wp-content/uploads/2020/05/Guidelines-on-filing-of-Suspicious-Transaction-Reports-for-the-Reporting-Entities.pdf
4. Guidelines on Reporting of Suspicious Transaction Reports (STRs) on Designated /Proscribed Individuals / Entities and their Associates	http://www.fmu.gov.pk/wp-content/uploads/2020/05/Guidelines-on-Reporting-of-Suspicious-Transaction-Reports-STRs-on-Designated-Proscribed-Individuals-Entities-and-their-Associates.pdf
5. Financial Monitoring Unit (FMU) goAML Web User's Guide For Stakeholders	http://www.fmu.gov.pk/docs/goAML-Userguide-for-Stakeholders-LEAs-Updated-Version.pdf
6. FMU reporting forms	http://www.fmu.gov.pk/reporting-forms/
7. FATF	http://www.fatf-gafi.org/.
8. APG	http://www.apgml.org/
9. Sanctions Rules 2020	https://AML-CFT-Sanction-Rules-2020-SRO-NO-950I-2020.pdf
10. Guidelines on Reporting of (STRs) on Designated/ Proscribed Individuals / Entities and their Associates	http://fmu.gov.pk/wp-content/uploads/2020/05/Guidelines-on-Reporting-of-Suspicious-Transaction-Reports-STRs-on-Designated-Proscribed-Individuals-Entities-andtheir-Associates.pdf
11. Red Flags for Misuse of Legal Persons	http://www.fmu.gov.pk/docs/Red_Flag_Indicators_for_Misuse_of_Legal_Persons.pdf
12. Red Flags for Misuse Legal Arrangements and NPOs	http://www.fmu.gov.pk/docs/Red_Flag_Indicators_for_Misuse_of_Legal_Arrangements_and_NPOs.pdf

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

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