OPTIMUS CAPITAL MANAGEMENT (PVT) LTD

AML, CFT AND KYC RISK MANAGEMENT POLICY

APPROVALS

Segment	Compliance, Sales and Settlement
Document	AML, CFT and KYC Risk Management Policy
Proposed By:	
Syed Ayaz Ahmed Head of Compliance	
Reviewed By:	
Mohammad Ovais Head of Equity Settlement	Mohammad Waqar EVP – Equity Sales
Faizan Sarmad Head of Accounts	
Approved By:	
Mohammad Ovais Ahsan Chief Executive Officer	

ACRONYMS

Term	Description
OCM	Optimus Capital Management (Pvt.) Ltd
Policy	AML, CFT and KYC Risk Management Policy
ML	Money Laundering
TF	Terrorist Financing
KYC	Know Your Customer
RBA	Risk Based Approach
CE	Chief Executive
BOD	Board of Directors
IA	Internal Audit
CD	Compliance Department
ESD	Equity Settlement Department
SD	Sales Department
SECP	Securities and Exchange Commission of Pakistan
STR	Suspicious Transaction Reporting
CTR	Currency Transaction Reporting
FMU	Financial Monitoring Unit
CDD	Client Due Diligence
SDD	Simplified Due Diligence
EDD	Enhanced Due Diligence
PEP	Politically Exposed Person
FATF	Financial Action Task Force

PREAMBLE:

The policy provides the guidelines to establish implement and monitor the controls developed against risk of Money Laundering (ML) and Terrorist Financing (TF). It also includes procedures required for client risk profiling and Know Your Customer (KYC) requirements.

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

Optimus Capital Management (Pvt) Ltd (OCM) is bound by Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018, Anti-Terrorism Act, 1997 and directives of KYC/CDD/AML/Terrorism Financing Issued by the Federal Government, SECP and other regulatory bodies from time to time. This policy helps us to understand our obligation of establishing an effective AML/CFT regime to deter criminals from using financial system for ML or TF purposes and to develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations.

Revision Procedure and Control Techniques

The following Policy revision control techniques will be used;

1. Ensure that the written procedures are followed without exception. The Policy holders would be requested to suggest revision, if the current policies seem impractical due to changing environment or new regulatory requirements are introduced.
2. Issue revised contents and index pages frequently with a request that Policy holders replace the old pages with the revised pages and check their policy for completeness.
3. The Board of Directors will be responsible for ensuring that the procedures for revision laid down in this Policy are followed.
4. The policy holders are responsible for updating their copies for all revisions made from time to time and ensuring that these revisions take effect as prescribed in the revision document.

Prior Approval for Changes

No changes will be made in the Policy unless duly approved and authorized by the Board of Directors. In case of any proposed revision in policies/controls and procedures, the details of proposed revision would be sent to every policy holder for their comments/suggestion. In case of no response from the Manual holder within a period of 15 days from sending of proposed revision details, the approval from the policy holder would be assumed and changes would be subsequently made in the policy.

A copy of the approved amendments will be sent to each of the policy holders by the Compliance Department to allow them to update their copy of the policy.

Manual Holders

- Chief Executive
- Board Of Directors
- Head of Compliance
- Head of Settlement
- Head of Sales

Property Rights

The Policy holders will be responsible for updating their copies for all revisions made from time to time and ensuring that these take effect as prescribed in the revision document.

This policy is the property of OCM. It is understood that the policy will be treated as a confidential document and access to which is to be limited to staff of OCM who need to refer to it during the course of their duties. No part of this policy may be photocopied or taken out of the Company's premises.

Effective date

The manual is effective from October 2018.

Responsibility for implementation

The Board of Directors will be responsible for implementation of this policy.

POLICY

Client Risk Assessment - Risk Based Approach

Risk associated with each individual client is a major area of concern for any organisation. Before establishing relationship with any client, assessment of his risk profile is essential. Client's risk will be assessed by following Risk Based Approach (RBA).

Before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied, CD will take into account all the relevant risk factors, such as geography, products and services, delivery channels, types of customers, or jurisdictions within which it or its customers do business.

In order to identify client's risk profile, CD shall take in to account the following factors:

1) Identification of ML/TF risks relevant to client;
2) Assessment of ML/TF risks in relation to-
    a. The Client (including beneficial owners);
    b. Country or geographic area in which customer resides or operate
    c. Delivery channels.

CD shall also take in to account OCM's internal risk factors such as Country or geographic area where the OCM operates, Services and transactions that OCM offers; and its delivery channels. CD shall Monitor and evaluate the implementation of mitigating controls and improve systems where necessary to keep their risk assessments up to date through ongoing reviews and, when necessary, updates. CD shall keep the risk assessment information up to date to provide it to Commission whenever required.

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

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

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

a) Identification of the area of the business operations susceptible to ML/TF
b) Analysis to assess the likelihood and impact of ML/TF;
c) Risk Management
d) Monitoring and review of those risks.

a) Identification, Assessment and Understanding Risks

Risk of ML/TF risk shall be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk for determining the overall risk classification (e.g. high, medium or low).

The ML/TF risks need to be assessed analyzed as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss from the crime, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself.

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

Potential ways to assess risk include but are not limited to:

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

Risk may be assessed through the likelihood of ML/TF activity. This assessment should involve considering each risk factor that have been identified, combined with business experience and information published by the Regulators and international organizations such as the FATF. The likelihood rating could correspond to:

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

When determining risk impact, number of factors can be considered, including:

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

On the basis of risk assessment, CD shall decide to submit an STR to the FMU. CD shall submit an STR to the FMU if it think activities or transactions are suspicious. The risk assessment will help target and prioritize the resources needed for ongoing CDD.

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

An effective risk assessment is an ongoing process. Risk levels may change as new products are offered, as new markets are entered, as high-risk customers open or close accounts, or as the products, services, policies, and procedures change. Risk assessment shall be

updated in every 12 to 18 months by CD to take account of these changes. Risk assessment information will be provided to the SECP, if required.

b) Analysis to assess the likelihood and impact of ML/TF

High-Risk Classification Factors

(1) ***Customer risk factors***: 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 OCM and the customer).
(b) Non-resident customers.
(c) Legal persons or arrangements
(d) Companies that have nominee shareholders.
(e) Business that is cash-intensive.
(f) The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons;
(g) Politically exposed persons
(h) Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
(i) Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
(j) Requested/Applied quantum of business does not match with the profile/particulars of client

OPTIMUS

(2) ***Country or geographic risk factors***: Country or geographical risk may not only arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of OCM itself, its location and the location of its geographical units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to ML/TF. The factors that may indicate a high risk are as follow:

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

(3) ***Product, service, transaction or delivery channel risk factors***: In identifying the risks of products, services, and transactions, the following factors should be considered:

(a) Anonymous transactions (which may include cash).
(b) Non-face-to-face business relationships or transactions.
(c) Payments received from unknown or un-associated third parties.

(d) The surrender of single premium life products or other investment-linked insurance products with a surrender value.
(e) International transactions, or involve high volumes of currency (or currency equivalent) transactions
(f) New or innovative products or services that are not provided directly by OCM, but are provided through channels of the institution;
(g) Products that involve large payment or receipt in cash; and
(h) One-off transactions.

Low Risk Classification Factors

(1) Customer risk factors:

Regulated Person and Banks provided that they are subject to requirements to combat AML and CFT, Public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership.

(2) Product, service, transaction or delivery channel risk factors:

Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(3) Country risk factors:

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

Risk Assessment

Risk assessment (Annex 1) shall be used 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.

c) Risk Management

Risk Tolerance

i. Risk tolerance is the amount of risk that OCM is willing and able to accept. OCM's risk tolerance impacts its decisions about risk mitigation measures and controls. For example, if it is determined that the risks associated with a particular type of customer exceed its risk tolerance, it may be decided not to accept or maintain that particular type of customer(s). Conversely, if the risks associated with a particular type of customer are within the bounds of risk tolerance, ESD shall ensure that the risk mitigation measures applied are commensurate with the risks associated with that type of customer(s).

ii. OCM may establish their risk tolerance. Such establishment shall be done by senior management and the Board. In establishing the risk tolerance, it shall be considered whether OCM has sufficient capacity and expertise to effectively manage the risks that it decides to accept and the consequences such as legal, regulatory, financial and reputational, of an AML/CFT compliance failure.

iii. If OCM decides to establish a high-risk tolerance and accept high risks then it should have mitigation measures and controls in place commensurate with those high risks.

Risk Mitigation

ESD shall monitor and mitigate the risks by considering number of aspects, which include:
1) OCM's customer, product and activity profile
2) Volume and size of transactions
3) Extent of reliance or dealing through third parties or intermediaries.

Risk mitigation measures may include:

1) Determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;
2) Setting transaction limits for higher-risk customers or products;
3) Requiring senior management intimation or approval for higher-risk transactions, including those involving PEPs;
4) CD may refuse to take on or terminate/cease high risk customers/products or services when there is any hint of money laundering;
5) Intimation or approval of CEO for high risk or large transactions when establishing relationship with high risk customers such as PEPs.

Evaluating Residual Risk and Comparing with the Risk Tolerance

Subsequent to establishing the risk mitigation measures, ESD shall 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 overall risk tolerance.

When the level of residual risk exceeds the risk tolerance, or risk mitigation measures do not adequately mitigate high-risks, risk mitigation measures shall be enhances accordingly.

d) Monitoring AML/CFT Systems and Controls

CD shall monitor the risks identified and assessed on periodic basis as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions.

In order to ensure effectiveness of risk mitigation procedures, CD will monitor certain aspects which include:

1) Changes in customer profile or transaction activity/behaviour, which comes to light in the normal course of business;
2) Abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;
3) Employee training and awareness;
4) Internal coordination mechanisms i.e., between AML/CFT compliance and other functions/areas;
5) The compliance arrangements (such as internal audit);
6) The performance of third parties who were relied on for CDD purposes (if any);

7) Changes in relevant laws or regulatory requirements; and
8) Changes in the risk profile of countries to which the OCM or its customers are exposed to.

Documentation and Reporting

OCM may adopt RBA as explained in this document. CD shall ensure that ML/TF risk management processes are kept under regular review which is at least annually. Management should review the program's adequacy when new products or services are introduced, opens or closes accounts with high-risk customers, or expands through mergers or acquisitions (if any). CD shall ensure that the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance criteria, its procedures concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT, are as per this policy and guidelines of regulators, required in case of SECP's on-site inspection. CD shall maintain Control Assessment Template (Annex 2) within the period as required by the SECP from time to time.

New Products and Technologies

CD shall ensure that senior management/ relevant departments have identified and assessed ML/TF risks that may arise in relation to the development/introduction/adoption of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:

1) Electronic verification of documentation;
2) Data and transaction screening systems.

Senior officials of relevant departments shall undertake a risk assessment prior to the launch or use of such practices and technologies; and take appropriate measures to manage and mitigate the risks.

OCM shall follow all the regulatory guidelines to prevent / mitigate risk of misuse of technological development in ML/TF schemes (such as online trading), particularly those technologies that favour anonymity

Initial application forms could be completed on-line and then followed up with all identification checks.

CD shall ensure that its systems and procedures are kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by them.

Cross-border Correspondent Relationship

Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's) customers may present high ML/TF risk and as such may require EDD.

In order to manage OCM's risks effectively, CD shall ensure to entering into a written agreement with the respondent institution before entering into the correspondent relationship including details of correspondent institution regarding AML /CFT controls.

Customer Due Diligence

CD shall take steps to know who their customers are. OCM shall not keep anonymous accounts or accounts in fictitious names. CD shall take steps to ensure that their customers are who they purport themselves to be. CD 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.

CD shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with their knowledge of the customer, its business and risk profile (Annex 3), including, where necessary, the source of funds. CD shall conduct CDD when establishing a business relationship if:

(1) There is a suspicion of ML/TF, Annex 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF. Although these may not be exhaustive in nature, it may help OCM to recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose; or

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

(3) In case of suspicion of ML/TF, CD shall:

(a) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and

(b) File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law. (Within seven days of forming that suspicion)

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

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

The Companies Act 2017 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."

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

CD/ESD shall identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person"). CD/ESD shall also verify whether that authorized person is properly authorized to act on behalf of the customer. CD shall conduct CDD on the authorized person(s) using the same standards that are applicable to a customer. Additionally, CD shall ascertain the reason for such authorization and obtain a copy of the authorization document.

Extent of CDD measures may vary, depending on the type and level of risk for the various risk factors. For example, normal CDD may be applied for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

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

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

Timing of Verification

Verification will be performed prior to entry into the business relationship or conducting a transaction. However, as provided in the Regulations verification may be completed after the establishment of the business relationship.

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:

(1) Non face-to-face business.

(2) Securities transactions. In the securities industry intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

(3) In cases of telephone or electronic business where payment is or is expected to be made from a bank or other account, the person verifying identity should:

(a) satisfy himself/herself that such account is held in the name of the customer at or before the time of payment; and

(b) not remit the proceeds of any transaction to the customer or his/her order until verification of identity has been completed.

The above are only examples, there are conditions under which an applicant may utilize the business relationship prior to verification. Such conditions may include restricting the funds received from being passed to third parties, imposing a limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. However where the ML/TF risks are high and enhanced due diligence measures are required to be performed, the verification shall not be postponed. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If the client does not pursue verification, it could be considered that this in itself is suspicious, and management shall evaluate whether a STR to FMU is required or not.

Where CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/TF, OCM shall not agree to open accounts with such customers. In such situations, CD shall file an STR with the FMU and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

Existing Customers

CD shall 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.

The CDD requirements entails that, if there is a suspicion of ML/TF or entity 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.

OCM shall be entitled to rely on the identification and verification steps that CD has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead 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.

Where CD 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, CD shall request with CEO to terminate the relationship. Additionally, CD shall consider making a STR to the FMU.

Tipping-off & Reporting

The Law prohibits tipping-off. However, a risk exists that customers could be unintentionally tipped off when CD is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible

STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

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

No Simplified Due Diligence for Higher-Risk Scenarios

CD shall not perform simplified due diligence measures where the ML/TF risks are high. CD shall identify risks and consider the relevant risk analysis in determining the level of due diligence.

On-going Monitoring of Business Relationships

Once the identification procedures have been completed and the business relationship is established, CD shall monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened. Ongoing monitoring helps to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

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

CD shall consider to update CDD records as a part its periodic reviews or on the occurrence of a triggering event, whichever is earlier.

*CDD of clients categorized as high risk shall be performed at least once in a year and CDD of Low/Medium risk clients shall be performed once in 3 years.

Examples of triggering events include:

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

Examples of the above circumstances include:

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

**Added through board resolution dated 18/04/2019*

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

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

If there is a suspicion of ML/TF or there is a lack of sufficient information about an existing customer, CD shall take steps to ensure that all relevant information is obtained as quickly as possible

Simplified Due Diligence Measures ("SDD")

CD shall conduct SDD in case of lower risks identified. However, CD shall ensure that the low risks it identifies are commensurate with the low risks identified by the country or the SECP. While determining whether to apply SDD, CD shall pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity.

The simplified measures should be commensurate with the low risk factors. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.

Where the risks are low and where there is no suspicion of ML/TF, the law allow relying upon third parties for verifying the identity of the applicants and beneficial owners.

Where it is decided to take SDD measures on an applicant/customer, CD should document the full rationale behind such decision (such as client risk profiling) and make available that documentation to the SECP on request.

Enhanced CDD Measures ("EDD")

CD shall 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.

Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, CD shall conduct enhanced CDD measures, consistent with the risks identified. In particular, CD shall

increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

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

(1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).

(2) Updating more regularly the identification data of applicant/customer and beneficial owner.

(3) Obtaining additional information on the intended nature of the business relationship.

(4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.

(5) Obtaining additional information on the reasons for intended or performed transactions.

(6) Obtaining the approval of senior management to commence or continue the business relationship.

(7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

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

High-Risk Countries

Countries associated with crimes such as drug trafficking, fraud and corruption poses a higher potential risk. Conducting a business relationship with an applicant/customer from such a country exposes to reputational risk and legal risk.

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

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

Publicly available information may be used to aware of the high-risk countries/territories. While assessing risk of a country, it is encouraged to consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF

and its regional style bodies (FSRBs) and Transparency international corruption perception index.

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

Politically Exposed Persons (PEPs)

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

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

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

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

(1) Confirm and verify during CDD process that customer does not fall in the definition of PEP. Information from independent / 3rd party resources and undertaking from customer in this regard may be obtained.

(2) obtain senior management approval for establishing business relationships with such customers;

(3) take reasonable measures to establish the source of wealth and source of funds; and

(4) conduct enhanced ongoing monitoring of the business relationship.

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

CD shall determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, CD shall consider factors such as whether the customer who is a PEP:

(1) Is from a high risk country;

(2) Has prominent public functions in sectors known to be exposed to corruption;

(3) Has business interests that can cause conflict of interests (with the position held).

The other red flags that shall be considered includes (in addition to the above and the red flags that they consider for other applicants):

(1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;

(2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties

(3) A PEP uses multiple bank accounts for no apparent commercial or other reason;

(4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

CD shall determine whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:

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

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

Record-Keeping Procedures

CD shall ensure that all information obtained in the context of CDD is recorded. This includes both;

a. recording the documents OCM is provided with when verifying the identity of the customer or the beneficial owner, and

b. transcription of client's risk profile into the back office system

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

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

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

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

Records relating to verification of identity will generally comprise:

1) a description of the nature of all the evidence received relating to the identity of the verification subject; and

2) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

Records relating to transactions will generally comprise:

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

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

Reporting of Suspicious Transactions / Currency Transaction Report

Special attention shall be paid to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. For all these type of transactions, inquiry shall be conducted by CD.

Where the enquiries conducted do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the AML/CFT Compliance Officer (CD).

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

(1) any unusual financial activity of the customer in the context of the customer's own usual activities;
(2) any unusual transaction in the course of some usual financial activity;

(3) any unusually-linked transactions;
(4) any unusual method of settlement;
(5) any unusual or disadvantageous early redemption of an investment product;
(6) any unwillingness to provide the information requested.

Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, CD will approach such situations with caution and make further relevant enquiries.

Where after due enquiry, it is difficult to judge that any cash transaction is reasonable, it should be considered as suspicious. CD shall file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

When it is necessary to file STR, the law require to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2015. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.

CD is required to report total number of STRs filed to the Commission on bi-annual basis within seven days of close of each half year.

CD shall maintain a register of all reports made to the FMU. Such registers should contain details of:

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

Where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF, that attempted transaction should be reported to the FMU.

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

Sanctions Compliance

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

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

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

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

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

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

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

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

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

CD shall screen customers, beneficial owners, transactions, and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to

the relevant sanctions lists, CD may discover that certain sanctions are applicable to one or more of their customers, existing or new.

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

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

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

Where the sanction lists are updated, CD/ESD shall ensure that existing customers are not listed.

In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, CD may consider raising an STR to FMU.

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

CD is required to consistently applied and supervised AML/CFT policy across the group. AML/CFT policy shall be appropriate to all branches (if any) and majority owned subsidiaries (if any) of OCM, even reflecting host jurisdiction [i.e., countries in which a branch (if any) or a subsidiary (if any) of OCM is located] requirements.

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

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

Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global AML/CFT policies and procedures is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements.

Internal Controls (Audit Function, Outsourcing, Employee Screening and Training)

OCM shall ensure that relevant departments shall monitor the following controls in relation to:

(1) Testing of the AML/CFT systems, policies and procedures by Internal Audit;

(2) Outsourcing arrangements;
(3) Employee screening procedures to ensure high standards when hiring employees; and
(4) An appropriate employee training program.

Audit Function

OCM shall on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The AML/CFT audits should be conducted to assess the AML/CFT systems which include:

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

(2) assess the adequacy of internal policies and procedures in addressing identified risks, including;
(a) CDD measures;
(b) Record keeping and retention;
(c) Third party reliance; and
(d) Transaction monitoring;

(3) assess compliance with the relevant laws and regulations;

(4) test transactions in all areas, with emphasis on high–risk areas,

(5) assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;

(6) assess the adequacy, accuracy and completeness of training programs;

(7) assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and

(8) assess the adequacy of the process of identifying suspicious activity including screening sanctions lists.

Outsourcing

OCM shall conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the service provider ("OSP") is fit and proper to perform the activity that is being outsourced.

Where the OCM decides to enter into an outsourcing arrangement, it shall be ensured that the outsourcing agreement clearly sets out the obligations of both parties. Senior management shall develop a contingency plan and a strategy to exit the arrangement in the event that the OSP fails to perform the outsourced activity as agreed.

The OSP shall report regularly to OCM within the timeframes as agreed upon with OCM. OCM shall have access to all the information or documents relevant to the outsourced activity maintained by the OSP. OCM shall not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

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

Employee Screening

CD in collaboration with HR/Admin shall screen prospective and existing employees to ensure high ethical and professional standards when hiring. The extent of employee screening should be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the particular risks associated with the individual positions.

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

CEO 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 HR/Admin may:

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

Employee Training

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

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

Training should be structured to ensure compliance with all of the requirements of the applicable legislation.

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

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

CD shall obtain an undertaking from their staff members (both new and existing) confirming that they have attended/received the training/updates on AML/CFT matters, read the AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.

CD/ESD/SD shall ensure that staff responsible for opening new accounts or dealing with new customers shall be aware of the need to verify the customer's identity, for new and existing customers. Staff shall be keep updated on the factors which may give rise to suspicions about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.

Staff involved in the processing of transactions shall be kept aware about the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances.

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

***Assessment of Money Laundering and Terrorist Financing Threats according to National Risk Assessment (NRA) 2019:**

The update NRA provides an overview of the inherent ML/TF risks in Pakistan i.e., before the application of any mitigation measures. These measures include a range of legal, regulatory, supervisory, and operational and enforcement measures to combat ML and TF activities in Pakistan. The inherent ML/TF risk assessment considers the ML/TF threats and inherent vulnerabilities of Pakistan as a whole. NRA provides assessment of transnational risks of ML / TF associated with our industry. Transnational risk relates to threat and vulnerabilities relating to customer, product, delivery channels and geographical location which are not confined to any single country. It includes crimes, their supportive infrastructure, sources of funding and their utilization for illegal acts, terrorism and corruption.

The assessment of ML threats included a review of all crimes based on the seriousness and magnitude of the crimes both domestically and internationally, the amount of potential proceeds generated, and the capacity of the criminal actors to launder proceeds (including third party launderers) and the sectors used to launder proceeds, according to information and data including Intelligence.

Following ML threats are highlighted in NRA with their risk categories:

Risk Category	ML Threats
High	Illicit Trafficking in Narcotic Drugs, Corruption and Bribery, Smuggling, Cash Smuggling, Tax Crimes, Illegal MVTS, Terrorism/TF.
Medium High	Organized Crime, Human Trafficking, Arm Trafficking, Robbery, Market Manipulation, Cybercrime, Fraud and forgery, Kidnapping, Extortion.
Medium	Sexual Exploitation, Trafficking of Good, Counterfeiting Currency, Piracy of Products, Murder.
Medium Low	Environmental Crime and Marine Piracy.

The assessment of the TF threats looked primarily at two main factors: the threat based on terrorism, and the threat based on the direction of financial flows, sources, and channels.

Following terrorist organisations are highlighted in NRA with their respected risk categories based on their TF threats:

No. of TOs	Risk	Names of Terrorist Organizations (TOs)
2	High	Daesh and TTP.
10	Medium High	AQ, JeM, JuD/ FIF, TTA, LeT, HQN, JuA, BLA, LeJ and BLF.
8	Medium	SSP, LeJ-Al-Almi, UBA, BRA, BLT, BRAS, HuA and Unknown.

21	Medium Low and Low	Jesh-ul-Islam, Lashkar-i-Islam, SMP, Lashkar-e-Balochistan, Balochistan Republican Guards, Self-radicalized (lone wolf) terrorists, Hazb-ul–Tehrir, Ahl-e-Sunnat Wal Jamat, Tehreek-e-Jafaria Pakistan, Jeay Sindh Mottahida Mahaz, Harkat-ul-Mujahideen, Tehreek - e- Taliban Swat, Al-Badar Mujahideen, Ansar-ul-Shariya, Balochistan Waja Liberation Army, Baloch Republican Party Azad, Balochistan United Army, Balochistan National Liberation Army, Balochistan , Liberation United Front, Baloch Student Organization Azad, Balochistan Muslla Defa Tanzeem.

Following terrorist financing (TF) threats are exists which becomes source of TF to terrorist organisations:

TF Threats
Afghan refugees/ diaspora
Narcotics/drugs trafficking
Kidnapping for ransom
Extortion
Cash smuggling
Collection and provision of funds, including from legitimate sources like NPO
Donations
Virtual Currencies (VCs)
Designated Non-Financial Businesses and Professions (DNFBPs) like real estate dealers, dealers in precious metals and stones (mostly jewelers), auditors and accountants, tax advisors, lawyers and notaries
Branchless bankings
Use of Internet and social media for electronic payments and crowd funding.

In NRA following geographical locations are considered as high risk based on their vulnerabilities to ML /FT threat. Accordingly clients, their nominees, authorized person and for legal person, their BOD. Trustee, office bearers are considered as high risk. For all high risk clients, enhance due diligence is required:

- Porous borders (Indian, Afghani and Iranian)
- Regions of Pakistan where most of the afghan diaspora / refugees are settled (like Khyber Pakhtunkhwa and Balochistan).
- Regions of Pakistan where most of the terroist, ethnic, separatist and sectarian groups operates and perform terrorist activities in country. (like Balochistan, southern Punjab, FATA).
- High risk countries identified by FATF (like Iran, Korea)

*__Assessment of inherent vulnerabilities of legal persons:__

Legal persons may carry inherent ML/TF vulnerabilities. The separation of ownership and control of assets from the ownership and control of the legal person/arrangement allows ultimate beneficial owners (UBO)/ and controllers of the assets to hide their identity, as well as to transfer ownership and control with relative ease. Following is the vulnerability rating scale ranging as Low, Medium and High:

Type of Legal Persons	Vulnerability Characteristics from UBO concealment	Assessed Ratings
Private companies	More vulnerability when: 1) complex structure with chains of ownership including trusts across multiple countries; 2) use formal (contractual) or informal nominee shareholders or directors where nominator identity undisclosed; 3) use of intermediaries (also vulnerable) in company formation; 4) shelf (dormant), shell (no activity) or front companies (often in customer service sector)	High
Public companies (including listed and unlisted Companies)	Stock exchange rules require high degree of transparency	Low
Public interest companies	Public Interest companies have the following sub categories; Listed Company Non-listed Company which is: (i) a public sector company as defined in the Act; or (ii) a public utility or similar company carrying on the business of essential public service; or (iii) holding assets in a fiduciary capacity for a broad group of outsiders, such as a bank, insurance company, securities broker/dealer, pension fund, mutual fund or investment banking entity. (iv) having such number of members holding ordinary shares as may be notified; or (v) holding assets exceeding such value as may be notified.	Low
Public sector companies	Ownership and control exercised by government. This can be in either the form of Private, Public Listed, and Unlisted company. The numbers are clubbed at the respective type of company.	Low
Companies limited by guarantee (s 2 (19))	Trade organizations licensed by Commerce Ministry, Director General of Trade Organizations. Also registered by SECP. Ownership is umbrella corporation with trade orgs under. Funds from govt. (not a norm) and members	Medium

	which may be orgs.	
Foreign companies	More vulnerability when: 1) complex structure with chains of ownership including trusts across multiple countries; 2) use formal (contractual) or informal nominee shareholders or directors where nominator identity undisclosed; 3) use of intermediaries (also vulnerable) in company formation; 4) could be shelf (dormant), shell (no activity) or front companies (often in customer service sector)	High
Domestic limited liability partnerships	Hybrid construct. Governing rules determined by contract with high degree of freedom in determining ownership and control among members, and exploiting nominees.	High
Foreign limited liability partnerships	Hybrid construct. Governing rules determined by contract with high degree of freedom in determining ownership and control among members including foreigners, and exploiting nominees.	High
Cooperatives	No UBO. Owned by 'members'	Low

*__Preventive controls:__

Based on the above mentioned domestic and transnational ML / TF threats and vulnerabilities; clients, products, delivery channels and jurisdictions are rated. All the high risk categories as per NRA 2019 should be reviewed more closely and regularly. EDD should be performed for all these high risk parameters. STR / CTR should be filed as per guidelines in AML Act and justifiable reasons for filling or non-filling of STR should be documented. Ultimate beneficial owners should be identified.

**Added through board resolution dated 07/11/2019*

Sectoral Risk Assessment of Legal Person and Legal Arrangements (LPLA)

The Sectoral Risk Assessment is a comprehensive process to help a country identify, assess, and understand the risks that arise from vulnerabilities of a particular sector that may facilitate money laundering or terrorist financing. The sectoral inherent vulnerability assessment consisted of an assessment of inherent ML/TF vulnerabilities of Legal Person and Legal Arrangements as a whole sector.

The following characteristics pertains to high-risk LP/LAs:

Type of LP/LA	Vulnerability characteristics of high-risk LP/LA
Private companies	– Multi-layered (having more than two layers) ownership or control structures; – Having foreign companies/ entities/trusts(whether registered in Pakistan or not) as member/shareholder; – Referred in financial intelligence received from FMU or LEAs; – Having Proscribed/designated persons as members, partners, directors or officers; – Inactive companies; – Having PEPs as members, partners, directors or officers; – Operating or registered in areas witnessing terrorist activities; – Large sized Companies having higher paid up capital, turnover, etc.; – Involved in deposit taking from the public, multi-level marketing, Ponzi schemes or other fraudulent or unauthorized business activities;
Public companies	Companies involved in insider trading and market manipulation.
Foreign companies	– International operations in countries rated as high risk; – Having shareholders or directors from high risk and monitored jurisdictions.
Domestic LLPs	– Partners with foreign nationality – Partners who are politically exposed persons; – Multiple layers of ownership.
Foreign LLPs	– International operations in countries rated as high risk; – Having partners from high-risk and monitored jurisdictions.
Cooperatives	– Societies having high working capital; – Higher number of members; – Geographical position of the society is in border areas; – Business of the society is in multiple districts; – Members are from multiple districts.
Trusts	– The trusts operating in border areas or in merged districts; – Trusts with off-land (foreign countries, inter-provincial) bank accounts; – trusts having multiple bank accounts; – If foreigner is trust member; – Trust sponsored from abroad; – Trusts having multiple layers of ownerships or the funding not directly provided by the Trust Author(s) or is routed through multiple channels; – The details of beneficiaries of the Trusts are not up to date or their documentation is incomplete. – The Trust not functioning as per their mandate or found violative of their purpose; – The Trust reports not timely complied/submitted.
Waqfs	– Geographical location of waqf property; – Shrines, especially those shrines where number of Zaeerin / visitors is greater as well as Cash Boxes are installed; – private waqf properties especially shrines and Masajid who are recipient of any foreign charity or donor agencies.

REPORTING:

1. Due Diligence shall be performed for clients having net investment above the threshold on monthly basis as prescribed by SECP from time to time. In case any suspicious transaction found, it will be reported to regulator.

2. Fortnightly reporting regarding any Al-Quaida member or clients whose funds are freezed as per UNSC resolution and SECP. Report will be send to SECP, CDC and PSX. Online reporting will be made on NCHS.

3. Suspicious Transaction Reporting (STR) without delay after forming suspicion.

4. Currency Transaction Reporting (CTR) within 7 days of all cash base transactions of 2 Million and above.

~~5. Bi annual reporting for number of STR files during the half year within 7 days of close of each half year.*****~~

6. **Annual risk assessment and control/compliance assessment framework reporting to SECP by ~~July 31~~ ******March 31 of each financial year.

7. **Quarterly submission of information to SECP as on 30th of subsequent month of every quarter.

8. ***Compliance report on statutory regulatory orders issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions and intimation from National Counter Terrorism Authority/Ministry of Interior regarding updates in list of proscribed persons under the Anti-Terrorism Act, 1997, to SECP within Forty Eight Hours of receiving the same.

9. ****Filling of Form 45, within fifteen days from the receipt of declaration received from members (Form 43 or Form 44), and thereafter along with its annual return to the registrar concerned.

** *Through SRO 55(I)/2020 dated 28th January, 2020*
*** *Through SRO 920(I)/2020 dated 28th September, 2020*
****Through SRO 928(I)/2020 dated 28th September, 2020*
***** *vide new AML/CFT Regulations 2020 dated September 28, 2020*
****** *Through SRO 197 (1)/2021 dated 12th February 2021*

Annex 1

AML/CFT Risk Assessment

Step 1 – Identify Customer Risk

Customer Risk Type						
Customer Type	Number of Customers (having active UIN) as on XXXX	Asset under custody as on XXXXX		Internal Risk Rating by RP		
		Securities	Cash at Bank	Total Number Classified as Low Risk	Total Number Classified as Medium Risk	Total Number Classified as High Risk
A	B=D+E+F			D	E	F
1. Natural Persons						
Resident						
Non-Resident (including Foreign)						
Total Natural Persons	0			0	0	0
2. Legal Persons						
Resident						
Non-Resident (including Foreign)						
Total Legal Persons	0			0	0	0
Total	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 of Products	Total Number as on XXXX		Total Number as on XXXX	
	Domestic PEP	Foreign PEP	Domestic	Foreign
Trading of Eligible Listed Securities in ready market				
Trading of Eligible Listed Securities in future market				
Underwriter				
Consultants to the Issue				
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 (including non-resident)					
Type	Total number of customers	Total Purchase/Financing extended from XXXX to XXXX		Total Sale/Financing availed/income ffrom XXXX to XXXX		Total Value of securities/finaincing /income and bank balances on cutoff date	Total number of customers	Total Purchase/Financing extended ffrom XXXX to XXXX		Total Sale/Financing availed/income ffrom XXXX to XXXX		Total Value of securities/finaincing /income and bank balances on cutoff date
		Number	Value in Rupees	Number	Value in Rupees			Number	Value in Rupees	Number	Value in Rupees	
Products and Services													
Trading of Eligible Listed Securities in ready market													
Trading of Eligible Listed Securities in future market													
Underwriter													
Consultants to the Issue													
Other (specify)													
Transactions													
PEP-local													
PEP-foreign													
High Networth Individuals (as per internal policy)													
Private Limited Companies and public unlisted companies													
Listed Companies													
Financial institutions													
NGO/NPO/ Charities/ Trust/ legal arrangements that receive donations													
Govt institutions/ departments													
Sole Proprietor Business													
Students													
House Wives													
Retired Persons													
Individuals-Service /Profession													
Other (specify)													
Total			0.00		0.00	0.00							0.00

Step 4- Identify Wire Transfer Activity

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

Step 5- IIdentify Customer Type by Geographic Location

Types of Customers	Number of Customers	Total asset under custody and bank balance as on XXXX
Natural Persons		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the FATF		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions		
Legal Persons		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the FATF		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions		
Total	0.00	0.00

Step 6 - Develop Risk Likelihood Table

Risk Likelihood Table			
Type of Customer	Customer	Transaction	Geography
PEP-local			
PEP-foreign			
High Networth Individuals (as per internal policy)			
Private Limited Companies and public unlisted companies			
Listed Companies			
Financial institutions			
NGO/NPO/ Charities/ Trust/ legal arrangements that receive donations			
Retirement Funds (Provident Funds, Gratuity Funds etc)			
Govt institutions/ departments			
Sole Proprietor Business			
Students			
House Wives			
Retired Persons			
Individuals-Service /Profession			
Total			

Risk Likelihood Table			
Product Type wherever applicable	**Customers**	**Transactions**	**Geography**
Trading of Eligible Listed Securities in ready market			
Trading of Eligible Listed Securities in future market			
Underwriter			
Consultants to the Issue			
Other (specify)			

Risk Likelihood Table			
Delivery Channels	**Customer**	**Transactions**	**Geography**
Third Party payments			
cash based			
Internet/online trading			
Amount received through Domestic Banks			
Remittance received from aborad			
Remittance received in foreign currency			
Online fund transfer where trail of transferror is not traceable			

Internal AML/CFT Entity Level Risk Assessment Likelihood Results	
	Low / Moderate / High
Customer Type	
Product Type	
Delivery Channels	
Geography	
Overall Risk Rating	

Annex 2

Controls Assessment Template

SECP AML/CFT Compliance Assessment Checklist		
Name of the Financial Institution		
Checklist completed by (Name)		
(Designation)		
Date		
The AML / CFT Self-Assessment Checklist has been designed to provide a structured and comprehensive framework for RFIs and their associated entities to assess compliance with key AML / CFT requirements. RFIs are advised to use this as part of their regular review to monitor their AML/CFT compliance. The frequency and extent of such review should be commensurate with the risks of ML/TF and the size of the firm's business. Note: *This AML / CFT Self-Assessment Checklist is neither intended to, nor should be construed as, an exhaustive list of all AML/CFT requirements.*		

Sr No.	***Question***	***Yes /No (N/ A)***	***If No, provide explanation and plan of action for remediation.***
(A) AML/CFT Systems			
1	RPs are required to assess their ML / TF risk and then implement appropriate internal policies, procedures and controls to mitigate risks of ML/TF.		
	Have you taken into account the following risk factors when assessing your own ML / TF risk?		
	(a) Product / service risk		
	(b) Delivery / distribution channel risk		

	(c) Customer risk		
	(d) Country risk		
2	RPs are required to have effective controls to ensure proper implementation of AML/CFT policies and procedures.		
	Does your AML/CFT systems cover the following controls?		
	(a) Board of Director and Senior management oversight		
	(ii) Have you appointed an appropriate staff as a Compliance Officer ('CO') ?		
	(iii) Do you ensure that CO is:		
	1. the focal point for the oversight of all activities relating to the prevention and detection of ML/TF		
	2. independent of all operational and business functions as far as practicable within any constraint of size of your institution		
	3. of a sufficient level of seniority and authority within your institution		
	4. provided with regular contact with and direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and the measures against the risks of ML/TF is sufficient and robust		
	5. fully conversant in the statutory and regulatory requirements and ML/TF risks arising from your business		
	6. capable of accessing on a timely basis all required available information to undertake its role		
	7. equipped with sufficient resources, including staff		
	8. overseeing your firm's compliance with the relevant AML requirements in Pakistan and overseas branches and subsidiaries		
	(b) Audit function		
	(i) Have you established an independent audit function?		

	(ii) If yes, does the function regularly review the AML/CFT systems to ensure effectiveness?		
	(iii) If appropriate, have you sought review assistance from external sources regarding your AML/CFT systems?		
	(c) Staff screening		
	(i) Do you establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees?		
3	RP with overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure an overall compliance with the CDD and record-keeping requirements.		
	Does your firm have overseas branches and subsidiary undertakings?		
	Do you have a group AML/CFT policy to ensure that all overseas branches and subsidiary undertakings have procedures in place to comply with the CDD and record-keeping requirements similar to those set under the AML Regulations?		
	If yes, is such policy well communicated within your group?		
	In the case where your overseas branches or subsidiary undertakings are unable to comply with the above mentioned policy due to local laws' restrictions, have you done the following?		
	(a) inform the SECP of such failure		
	(b) take additional measures to effectively mitigate ML/TF risks faced by them		
(B) Risk-Based Approach ('RBA')			
4	RPs are required to determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction or service used by that customer.		
	Does your RBA identify and categorize ML/TF risks at the customer level and establish reasonable measures based on risks identified?		
	Do you consider the following risk factors when determining the ML/TF risk rating of customers?		
	(a) Country risk - customers with residence in or connection with the below high-risk jurisdictions		

	(i) countries identified by the FATF as jurisdictions with strategic AML/CFT deficiencies		
	(ii) countries subject to sanctions, embargoes or similar measures issued by international authorities		
	(iii) countries which are vulnerable to corruption		
	(iv) countries that are believed to have strong links to terrorist activities		
	(b) Customer risk - customers with the below nature or behaviour might present a higher ML/TF risk		
	(i) the public profile of the customer indicating involvement with, or connection to, politically exposed persons ('PEPs')		
	(ii) complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial rationale		
	(iii) request to use numbered accounts or undue levels of secrecy with a transaction		
	(iv) involvement in cash-intensive businesses		
	(v) nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities		
	(vi) the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified		
	(c) Product/service risk - product/service with the below factors might present a higher risk		
	(i) services that inherently have provided more anonymity		
	(ii) ability to pool underlying customers/funds		
	(d) Distribution/delivery channels		
	(i) a non-face-to-face account opening approach is used		
	(ii) Business sold through third party agencies or intermediaries		
	Do you adjust your risk assessment of customers from time to time or based upon information received from a competent authority, and review the extent of the CDD and ongoing monitoring to be applied?		

	Do you maintain all records and relevant documents of the above risk assessment?		
	If yes, are they able to demonstrate to the SECP the following?		
	(a) how you assess the customer		
	(b) the extent of CDD and ongoing monitoring is appropriate based on that customer's ML/TF risk		
(C) - Customer Due Diligence ('CDD')			
5	RPs are required to carry out CDD, which is a vital tool for recognizing whether there are grounds for knowledge or suspicion of ML/TF.		
	Do you conduct the following CDD measures?		
	(a) identify the customer and verify the customer's identity using reliable, independent source documents, data or information		
	(b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity, including in the case of a legal person or trust, measures to enable you to understand the ownership and control structure of the legal person or trust		
	(c) obtain information on the purpose and intended nature of the business relationship established with you unless the purpose and intended nature are obvious		
	(d) if a person purports to act on behalf of the customer:		
	(i) identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information		
	(ii) verify the person's authority to act on behalf of the customer (e.g. written authority, board resolution)		
	Do you apply CDD requirements in the following conditions?		
	(a) at the outset of a business relationship		
	(b) when you suspect that a customer or a customer's account is involved in ML/TF		
	(c) when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity		
6	RPs are required to identify and take reasonable measures to verify the identity of a beneficial owner.		

	When an individual is identified as a beneficial owner, do you obtain the following identification information?		
	(a) Full name		
	(b) Date of birth		
	(c) Nationality		
	(d) Identity document type and number		
	Do you verify the identity of beneficial owner(s) with reasonable measures, based on its assessment of the ML/TF risks, so that you know who the beneficial owner(s) is?		
7	RPs are required to identify and take reasonable measures to verify the identity of a person who purports to act on behalf of the customer and is authorized to give instructions for the movement of funds or assets.		
	When a person purports to act on behalf of a customer and is authorized to give instructions for the movement of funds or assets, do you obtain the identification information and take reasonable measures to verify the information obtained?		
	Do you obtain the written authorization to verify that the individual purporting to represent the customer is authorized to do so?		
	Do you use a streamlined approach on occasions where difficulties have been encountered in identifying and verifying signatories of individuals being represented to comply with the CDD requirements?		
	If yes, do you perform the following:		
	(a) adopt an RBA to assess whether the customer is a low risk customer and that the streamlined approach is only applicable to these low risk customers		
	(b) obtain a signatory list, recording the names of the account signatories, whose identities and authority to act have been confirmed by a department or person within that customer which is independent to the persons whose identities are being verified		

8	RPs are required to take appropriate steps to verify the genuineness of identification provided if suspicions are raised.		
	In case of suspicions raised in relation to any document in performing CDD, have you taken practical and proportionate steps to establish whether the document offered is genuine, or has been reported as lost or stolen? (e.g. search publicly available information, approach relevant authorities)		
	Have you rejected any documents provided during CDD and considered making a report to the authorities (e.g. FMU, police) where suspicion on the genuineness of the information cannot be eliminated?		
9	RPs are required to understand the purpose and intended nature of the business relationship established.		
	Unless the purpose and intended nature are obvious, have you obtained satisfactory information from all new customers (including non-residents) as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the relevant account opening documentation?		
10	RPs are required to complete the CDD before establishing business relationships.		
	Do you always complete the CDD process before establishing business relationships? If you always complete CDD process before establishing a business relationship		
	If you are unable to complete the CDD process, do you ensure that the relevant business relationships must not be established and assess whether this failure provides grounds for knowledge or suspicion of ML/TF to submit a report to the FMU as appropriate?		
	If the CDD process is not completed before establishing a business relationship, would these be on an exception basis only and with consideration of the following:		

	(a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed.		
	(b) it is necessary not to interrupt the normal course of business with the customer (e.g. securities 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 that it is carried out as soon as reasonably practicable		
	(b) placing appropriate limits on the number of transactions and type of transactions that can be undertaken pending verification		
	(c) ensuring that funds are not paid out to any third party		
	(d) other relevant policies and procedures		
	When terminating a business relationship where funds or other assets have been received, have you returned the funds or assets to the source (where possible) from which they were received?		
11	RPs are required to keep the customer information up-to-date and relevant.		
	Do you undertake reviews of existing records of customers to ensure that the information obtained for the purposes of complying with the AML requirements are up-to-date and relevant when one of the following trigger events happen?		
	(a) when a significant transaction is to take place		
	(b) when a material change occurs in the way the customer's account is operated		
	(c) when your customer documentation standards change substantially		

	(d) when you are aware that you lack sufficient information about the customer concerned		
	(e) if there are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box		
	Are all high-risk customers subject to a review of their profile?		
12	RPs are required to identify and verify the true and full identity of each natural person by using reliable and independent sources of information.		
	Do you have customers which are natural persons?		
	Do you collect the identification information for customers:		
	(i) Residents		
	(ii) Non-residents		
	(iii) Non-residents who are not physically present		
	Do you document the information?		
	If yes, please provide a list of acceptable documents that you obtain for verifying residential address (e.g. utility bills or bank statements). For the avoidance of doubt, please note according to the Guideline on AML and CFT that certain types of address verification should not be considered sufficient, e.g. a post office box address, for persons residing in Pakistan or corporate customers registered and/or operating in Pakistan.		
	In cases where customers may not be able to produce verified evidence of residential address have you adopted alternative methods and applied these on a risk sensitive basis?		
	Do you require additional identity information to be provided or verify additional aspects of identity if the customer, or the product or service, is assessed to present a higher ML/TF risk?		

13	RPs are required to identify and verify the true and full identity of each legal person and trust and its beneficial owners by using reliable and independent sources of information.		
	Do you have measures to look behind each legal person or trust to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets?		
	Do you fully understand the customer's legal form, structure and ownership, and obtain information on the nature of its business, and reasons for seeking the product or service when the reasons are not obvious?		
14	Corporation		
	Do you have customers which are corporations?		
	Do you obtain the following information and verification documents in relation to a customer which is a corporation?		
	For companies with multiple layers in their ownership structures, do you have an understanding of the ownership and control structure of the company and fully identify the intermediate layers of the company?		
	Do you take further measures, when the ownership structure of the company is dispersed/complex/multi-layered without an obvious commercial purpose, to verify the identity of the ultimate beneficial owners?		
15	Partnerships and unincorporated bodies		
	Do you have customers which are partnerships or unincorporated bodies?		
	Do you take reasonable measures to verify the identity of the beneficial owners of the partnerships or unincorporated bodies?		

	Do you obtain the information and verification documents in relation to the partnership or unincorporated body?		
	Do you have customers which are in the form of trusts?		
	Do you obtain the information and verification documents to verify the existence, legal form and parties to a trust?		
	Have you taken particular care in relation to trusts created in jurisdictions where there is no or weak money laundering legislation?		
16	RPs may conduct simplified 'Know Your Customer' due diligence ('SDD') process instead of full CDD measures given reasonable grounds to support it. Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing. SDD is a condition where the timing of the actual verification of a particular customer is deferred until such time the entire CDD process is completed, rather than reducing what needs to be obtained, under a risk-based approach.		
	Have you conducted SDD instead of full CDD measures for your customers?		
	Do you refrain from applying SDD when you suspect that the customer, the customer's account or the transaction is involved in ML/TF, or when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying or verifying the customer?		
	Before the application of SDD on any of the customer categories, have you performed checking on whether they meet the criteria of the respective category?		
17	RPs are required, in any situation that by its nature presents a higher risk of ML/TF, to take additional measures to mitigate the risk of ML/TF.		

	Do you take additional measures or enhanced due diligence ('EDD') when the customer presents a higher risk of ML/TF?		
	If yes, do they include the following?		
	(a) obtaining additional information on the customer and updating more regularly the customer profile including the identification data		
	(b) obtaining additional information on the intended nature of the business relationship, the source of wealth and source of funds		
	(c) obtaining the approval of senior management to commence or continue the relationship		
	(d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.		
18	RPs are required to apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview.		
	Do you accept customers that are not physically present for identification purposes to open an account?		
	If yes, have you taken additional measures to compensate for any risk associated with customers not physically present (i.e. face to face) for identification purposes?		
	If yes, do you document such information?		
19	RPs are required to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person ('PEP') and to adopt EDD on PEPs.		
	Do you define what a PEP (foreign and domestic) is in your AML/CFT policies and procedures?		
	Have you established and maintained effective procedures for determining whether a customer or a beneficial owner of a customer is a PEP (foreign and domestic)?		

	If yes, is screening and searches performed to determine if a customer or a beneficial owner of a customer is a PEP? (e.g. through commercially available databases, publicly available sources and internet / media searches etc)		
20	Foreign PEPs		
	Do you conduct EDD at the outset of the business relationship and ongoing monitoring when a foreign PEP is identified or suspected?		
	Have you applied the following EDD measures when you know that a particular customer or beneficial owner is a foreign PEP (for both existing and new business relationships)?		
	(a) obtaining approval from your senior management		
	(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds		
	(c) applying enhanced monitoring to the relationship in accordance with the assessed risks		
21	Domestic PEPs		
	Have you performed a risk assessment for an individual known to be a domestic PEP to determine whether the individual poses a higher risk of ML/TF?		
	If yes and the domestic PEP poses a higher ML/TF risk, have you applied EDD and monitoring specified in question C.40 above?		
	If yes, have you retained a copy of the assessment for related authorities, other authorities and auditors and reviewed the assessment whenever concerns as to the activities of the individual arise?		
	For foreign and domestic PEPs assessed to present a higher risk, are they subject to a minimum of an annual review and ensure the CDD information remains up-to-date and relevant?		
22	RPs have the ultimate responsibility for ensuring CDD requirements are met, even intermediaries were used to perform any part of the CDD measures.		

	Have you used any intermediaries to perform any part of your CDD measures?		
	When intermediaries (not including those in contractual arrangements with the RFI to carry out its CDD function or business relationships, accounts or transactions between RFI for their clients) are relied on to perform any part of the CDD measures, do you obtain written confirmation from the intermediaries that:		
	(a) they agree to perform the role		
	(b) they will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of you upon request.		
	When you use an intermediary, are you satisfied that it has adequate procedures in place to prevent ML/TF?		
	When you use overseas intermediaries, are you satisfied that it:		
	(a) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction		
	(b) has measures in place to ensure compliance with requirements		
	(c) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities in PK		
	In order to ensure the compliance with the requirements set out above for both domestic or overseas intermediaries, do you take the following measures?		
	(a) review the intermediary's AML/CFT policies and procedures		
	(b) make enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited		
	Do you immediately (with no delay) obtain from intermediaries the data or information that the intermediaries obtained in the course of carrying out the CDD measures?		

	Do you conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay?		
	Have you taken reasonable steps to review intermediaries' ability to perform its CDD whenever you have doubts as to the reliability of intermediaries?		
23	RPs are required to perform CDD measures on pre-existing customers when trigger events occur.		
	Have you performed CDD measures on your pre-existing customers when one of the following trigger events happens?		
	(a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is inconsistent with your knowledge of the customer or the customer's business or risk profile, or with your knowledge of the source of the customer's funds		
	(b) a material change occurs in the way in which the customer's account is operated		
	(c) you suspect that the customer or the customer's account is involved in ML/TF		
	(d) you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying and verifying the customer's identity		
	(e) Are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box		
24	RPs are not allowed to maintain anonymous accounts or accounts in fictitious names for any new or existing customers.		
	Do you refrain from maintaining (for any customer) anonymous accounts or accounts in fictitious names?		
25	RPs are required to assess and determine jurisdictional equivalence as this is an important aspect in the application of CDD measures.		
	When you do your documentation for assessment or determination of jurisdictional equivalence, do you take the following measures?		
	(a) make reference to up-to-date and relevant information		

	(b) retain such record for regulatory scrutiny		
	(c) periodically review to ensure it remains up-to-date and valid		
	(D) - Ongoing monitoring		
26	RPs are required to perform effective ongoing monitoring for understanding customer's activities and it helps the firm to know the customers and to detect unusual or suspicious activities.		
	Do you continuously monitor your business relationship with a customer by:		
	(a) monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds.		
	(b) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF		
	Do you monitor the following characteristics relating to your customer's activities and transactions?		
	(a) the nature and type of transaction (e.g. abnormal size of frequency)		
	(b) the nature of a series of transactions (e.g. a number of cash deposits)		
	(c) the amount of any transactions, paying particular attention to substantial transactions		
	(d) the geographical origin/destination of a payment or receipt		
	(e) the customer's normal activity or turnover		
	Do you regularly identify if the basis of the business relationship changes for customers when the following occur?		
	(a) new products or services that pose higher risk are entered into		
	(b) new corporate or trust structures are created		
	(c) the stated activity or turnover of a customer changes or increases		
	(d) the nature of transactions change or the volume or size increases		
	(e) if there are other situations, please specify and further elaborate in the text box		

	In the case where the basis of a business relationship changes significantly, do you carry out further CDD procedures to ensure that the ML/TF risk and basis of the relationship are fully understood?		
	Have you established procedures to conduct a review of a business relationship upon the filing of a report to the FMU and do you update the CDD information thereafter?		
27	RPs are required to link the extent of ongoing monitoring to the risk profile of the customer determined through RBA.		
	Have you taken additional measures with identified high risk business relationships (including PEPs) in the form of more intensive and frequent monitoring?		
	If yes, have you considered the following:		
	(a) whether adequate procedures or management information systems are in place to provide relevant staff with timely information that might include any information on any connected accounts or relationships		
	(b) how to monitor the sources of funds, wealth and income for higher risk customers and how any 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 risks arising from its business		
	(c) the nature of its systems and controls		
	(d) the monitoring procedures that already exist to satisfy other business needs		
	(e) the nature of the products and services (including the means of delivery or communication)		
	In the case where transactions are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, do you examine the background and purpose, including where appropriate the circumstances of the transactions?		

	If yes, are the findings and outcomes of these examinations properly documented in writing and readily available for the SECP, competent authorities and auditors?		
	In the case where you have been unable to satisfy that any cash transaction or third party transfer proposed by customers is reasonable and therefore consider it suspicious, do you make a suspicious transaction report to the FMU?		
(E) - Financial sanctions and terrorist financing			
28	RPs have to be aware of the scope and focus of relevant financial/trade sanctions regimes.		
	Do you have procedures and controls in place to:		
	(a) ensure that no payments to or from a person on a sanctions list that may affect your operations is made		
	(b) screen payment instructions to ensure that proposed payments to designated parties under applicable laws and regulations are not made		
	If yes, does this include:		
	(a) drawing reference from a number of sources to ensure that you have appropriate systems to conduct checks against relevant lists for screening purposes		
	(b) procedures to ensure that the sanctions list used for screening are up to date		
	Do you take the following measures to ensure compliance with relevant regulations and legislation on TF?		
	(a) understand the legal obligations of your institution and establish relevant policies and procedures		
	(b) ensure relevant legal obligations are well understood by staff and adequate guidance and training are provided		
	(c) ensure the systems and mechanisms for identification of suspicious transactions cover TF as well as ML		
	Do you maintain a database (internal or through a third party service provider) of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have been made known to it?		

	If yes, have you also taken the following measures in maintaining the database?		
	(a) ensure that the relevant designations are included in the database.		
	(b) the database is subject to timely update whenever there are changes		
	(c) the database is made easily accessible by staff for the purpose of identifying suspicious transactions		
	Do you perform comprehensive screening of your complete customer base to prevent TF and sanction violations?		
	If yes, does it include the following?		
	(a) screening customers against current terrorist and sanction designations at the establishment of the relationship		
	(b) screening against your entire client base, as soon as practicable after new terrorist and sanction designation are published by the SECP		
	Do you conduct enhanced checks before establishing a business relationship or processing a transaction if there are circumstances giving rise to a TF suspicion?		
	Do you document or record electronically the results related to the comprehensive ongoing screening, payment screening and enhanced checks if performed?		
	Do you have procedures to file reports to the FMU if you suspect that a transaction is terrorist-related, even if there is no evidence of a direct terrorist connection?		
(F) - Suspicious Transaction reports			
29	RPs are required to adopt on-going monitoring procedures to identify suspicious transactions for the reporting of funds or property known or suspected to be proceeds of crime or terrorist activity to the Joint Financial Intelligence Unit ('FMU').		
	Do you have policy or system in place to make disclosures/suspicious transaction reports with the FMU?		

	Do you apply the following principles once knowledge or suspicion has been formed?		
	(a) in the event of suspicion of ML/TF, a disclosure is made even where no transaction has been conducted by or through your institution		
	(b) internal controls and systems are in place to prevent any directors, officers and employees, especially those making enquiry with customers or performing additional or enhanced CDD process,committing the offence of tipping off the customer or any other person who is the subject of the disclosure		
	Do you provide sufficient guidance to your staff to enable them to form a suspicion or to recognise when ML/TF is taking place?		
	If yes, do you provide guidance to staff on identifying suspicious activity taking into account the following:		
	(a) the nature of the transactions and instructions that staff is likely to encounter		
	(b) the type of product or service		
	(c) the means of delivery		
	Do you ensure your staff are aware and alert with the SECP's guidelines with relation to:		
	(a) potential ML scenarios using Red Flag Indicators		
	(b) potential ML involving employees of RPs.		
	Subsequent to a customer suspicion being identified, have you made prompt disclosures to the FMU if the following additional requests are made by the customer: Note: RPs are required to make prompt disclosure to FMU in any event, but the following requests are considered to be more urgent.		
	(a) instructed you to move funds		
	(b) close the account		
	(c) make cash available for collection		
	(d) carry out significant changes to the business relationship		

(G) - Record Keeping and Retention of Records			
30	RPs are required to maintain customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements.		
	Do you keep the documents/ records relating to customer identity?		
	If yes to the above documents/ records, are they kept throughout the business relationship with the customer and for a period of six years after the end of the business relationship? Note: While the AMLO identifies relevant documents to be retained for 6 years, the RFI should consider other SECP requirements when determining the record keeping and retention period of each document.		
	Do you keep the following documents/ records relating to transactions?		
	(a) the identity of the parties to the transaction		
	(b) the nature and date of the transaction		
	(c) the type and amount of currency involved		
	(d) the origin of the funds		
	(e) the form in which the funds were offered or withdrawn		
	(f) the destination of the funds		
	(g) the form of instruction and authority		
	(h) the type and identifying number of any account involved in the transaction		
	Are the documents/ records, they kept for a period of five years after the completion of a transaction, regardless of whether the business relationship ends during the period as required under the AML/CFT Regulations?		
	In the case where customer identification and verification documents are held by intermediaries, do you ensure that the intermediaries have systems in place to comply with all the record-keeping requirements?		
(H) - Staff Training			

31	RPs are required to provide adequate ongoing training for staff in what they need to do to carry out their particular roles with respect to AML/CFT.		
	Have you implemented a clear and well articulated policy to ensure that relevant staff receive adequate AML/CFT training?		
	Do you provide AML/CFT training to your staff to maintain their AML/CFT knowledge and competence?		
	If yes, does the training program cover the following topics?		
	(a) your institution's and the staff's own personal statutory obligations and the possible consequences for failure to report suspicious transactions under relevant laws and regulations		
	(b) any other statutory and regulatory obligations that concern your institution and the staff under the relevant laws and regulations, and the possible consequences of breaches of these obligations		
	(c) your own policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting		
	(d) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by your staff to carry out their particular roles in your institution with respect to AML/CFT		
	Do you provide AML/CFT training for all your new staff, irrespective of their seniority and before work commencement?		
	If yes, does the training program cover the following topics?		
	(a) an introduction to the background to ML/TF and the importance placed on ML/TF by your institution		
	(b) the need for identifying and reporting of any suspicious transactions to the Compliance Officer, and the offence of 'tipping-off'		
	Do you provide AML/CFT training for your members of staff who are dealing directly with the public?		
	If yes, does the training program cover the following topics?		

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

Annex 3

RISK PROFILING OF CUSTOMER

For Internal Use

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

6	Intermediaries' e.g. Third parties acting on behalf of customers (Lawyers, Accountants etc.).		
7	Performed further screening of details of customer, beneficial owner of the customer, person acting on behalf of the customer, or connected party of the customer against other information sources, for example, google, the sanctions lists published and/or other third party screening database. Are there adverse news or information arising?		
8	Customer's source of wealth/ income is high risk/ cash intensive		
9	Does the customer have nominee shareholder(s) in the ownership chain where there is no legitimate rationale?		
10	Is the customer a shell company?		
11	Does the customer have unusual or complex shareholding structure (e.g. involving layers of ownership structure, different jurisdictions)?		
12	Does the stated source of wealth / source of funds and the amount of money involved correspond with what you know of your customer?		
Section C: Country / Geographic Risk Factors			
1	Is the customer, beneficial owner of the customer or person acting on behalf of the customer from or based in a country or jurisdiction: a. Identified as High-risk jurisdiction by the FATF and for which financial institutions should give special attention to business relationships and transactions. (Countries having weak governance, law enforcement, and regulatory regimes). b. Countries subject to sanctions, embargos or similar measures issued by international authorities (E.G. UN, WB, IMF) c. Countries where protection for customer's privacy prevents effective implementation of AML/CFT requirements and/or facilitates the framework for establishment of shell-companies. d. Countries/ Geographies identified by recognized sources as having significant levels of organized crime, corruption or criminal activity. e. Countries/ Geographies identified by recognized sources as providing funding or support for terrorist activities or have terrorist organizations operating within them.		
Section D: Services / Transactions Risk Factors			
1	Is the business relationship with the customer established through non face-to-face channel?		
2	Has the customer given any instruction to perform a transaction (which may include cash) anonymously?		
3	Has the customer transferred any funds without the provision of underlying services or transactions?		
4	Are there unusual patterns of transactions that have no apparent		

	economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)?		
5	Are there unaccounted payments received from unknown or un-associated third parties for services and/or transactions provided by the customer?		
6	Does the value of the transaction appear to fall within the financial means of your customer, given their income and savings?		
7	Is there any divergence in the type, volume or frequency of services and/or transactions expected in the course of the business relationship with the customer?		
8	Significant and unexplained geographic distance between residence or business location of the customer and the location where the product sale took place.		
9	Customers seek or accept very unfavorable account/policy/contract provisions or riders and rely on free look up provisions		
10	Customers transfer the benefit of a product to an apparently unrelated third party		
11	Customer uses brokerage accounts as long term depository accounts for funds		
12	Customer is conducting transactions that do not have apparent economic rationale		
13	Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting Thresholds		
14	Transactions involve penny/microcap stocks		
15	Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation		
16	Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology		
17	Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason		
18	Customer trades frequently, selling at a loss		
19	Customer invests in securities suddenly in large volumes, deviating from previous transactional activity		
20	Cross border correspondent financial institutions relationships		
21	Products/ Services		
22	Transaction Amount		

Section E: Customer Risk Assessment

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

Document reasons for customer risk rating:	
Section F: Recommendation	
☐ Accept Customer	☐ Reject Customer
Assessed By: Designation: Signature: Date:	Approved By: Designation: Signature: Date:

Annex 4

ML/TF Warning Signs/ Red Flags

The following are some of the warning signs or "red flags". The list is not exhaustive, but includes the following:

(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.

(24) Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

(25) Customer, Products, delivery channels and jurisdictions vulnerable to domestic and transnational ML/TF threats as identified in NRA 2019.

Suspected Person:

The following actions and factors will help in identifying suspected persons:

a) A customer is an office bearer (trustee/ member/ director/ authorized signatory etc.) of a designated/ proscribed entity.

b) A customer is a business partner of an office bearer (trustee/ member/ director etc.) of a designated/ proscribed entity.

c) A customer is a close family member of a designated/ proscribed individual who is also suspected to be associated with the business of the designated/ proscribed individual by way of financial or other assistance.

d) An entity has a designated/ proscribed individual on its board or management.

e) Unilateral sanctions listing (i.e. NACTA Database for Proscribed individuals & entities) identify linkage/ association of a customer with a designated/ proscribed individual or entity.

f) Media (Broadcast/ Print/ Social) news highlights customer's involvement in providing financial or other assistance to designated/ proscribed individual or entity.

g) A customer has provided the same residential/ office address that matches the known residential/ office address of a designated/ proscribed individual or entity.

h) A customer has provided the same personal contact number that matches the contact number provided earlier by a proscribed/ designated customer.

i) A customer depositing funds in the account of a person or entity listed in an international or foreign jurisdiction's sanctions lists maintained in accordance with UNSC resolution 1373.

j) A customer listed in an international or foreign jurisdiction's sanctions list maintained in accordance with UNSC resolution 1373, is depositing funds in another customer's account.

k) Inquiry from law enforcement agency/ intelligence agency indicating linkage of a customer with designated/ proscribed individual or entity.

l) A customer appears to have conducted transactions on behalf of or at the direction of a designated/ proscribed individual during the process of due diligence.

Annex 5

DOCUMENTS /INFORMATION REQUIRED TO OBTAIN FROM CLIENTS

S No.	Type of Customer	Information/Documents to be Obtained
1.	Individuals	A photocopy of any one of the following valid identity documents; (i) Computerized National Identity Card (CNIC) issued by NADRA. (ii) National Identity Card for Overseas Pakistani (NICOP) issued by NADRA. (iii) Pakistan Origin Card (POC) issued by NADRA. (iv) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (v) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2.	Sole proprietorship	(i) Photocopy of identity document as per Sr. No. 1 above of the proprietor. (ii) Copy of registration certificate for registered concerns. (iii) Copy of certificate or proof of membership of trade bodies etc, wherever applicable. (iv) Declaration of sole proprietorship on business letter head. (v) Account opening requisition on business letter head. (vi) Registered/ Business address.
3.	Partnership	(i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed'. (iii) Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. (iv) Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. (v) Registered/ Business address.
4.	Limited Companies/ Corporations	(i) Certified copies of: (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; (b) Memorandum and Articles of Association; (c) Certificate of Incorporation;

		(d) Certificate of Commencement of Business, wherever applicable; (e) List of Directors on 'Form-A/Form-B' issued under Companies Act, 2017, as applicable; and (f) Form-29, wherever applicable. (ii) Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account;
5.	Branch Office or Liaison Office of Foreign Companies	(i) A copy of permission letter from relevant authority i-e Board of Investment. (ii) Photocopies of valid passports of all the signatories of account. (iii) List of directors on company letter head or prescribed format under relevant laws/regulations. (iv) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account. (v) Branch/Liaison office address.
6.	Trust, Clubs, Societies and Associations etc.	(i) Certified copies of: (a) Certificate of Registration/Instrument of Trust (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. (iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (iv) Registered address/ Business address where applicable.
7.	NGOs/NPOs/Charities	(i) Certified copies of: (a) Registration documents/certificate (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. (iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (iv) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain

		the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer. (v) Registered address/ Business address.
8.	Agents	(i) Certified copy of 'Power of Attorney' or 'Agency Agreement'. (ii) Photocopy of identity document as per Sr. No. 1 above of the agent and principal. (iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person. (iv) Registered/ Business address.
9.	Executors and Administrators	(i) Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator. (ii) A certified copy of Letter of Administration or Probate. (iii) Registered address/ Business address.
10.	Minor Accounts	(i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate). (ii) Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.

Note:

(i) The photocopies of identity documents shall be validated through NADRA verisys.

(ii) In case of a salaried person, in addition to CNIC, an attested copy of his service card or certificate or letter on letter head of the employer will be obtained.

(iii) In case of an individual with shaky/immature signatures, in addition to CNIC, a passport size photograph of the new account holder will be obtained.

(iv) In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that regulated person shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account. For CNICs which expire during the course of the customer's relationship, regulated person shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, regulated person are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.

(v) In case the CNIC does not contain a photograph, regulated person shall obtain following-

(a) a duly attested copy of either driving license, service card, nikkah nama, birth certificate, educational degree/certificate, pension book, insurance certificate.

(b) a photograph duly attested by gazetted officer/Administrator/ officer of the regulated person.

(c) a copy of CNIC without photograph duly attested by the same person who attested the photograph.

(vi) The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the regulated person.

(vii) The condition of obtaining photocopies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where regulated person should obtain photocopies of identity documents of only those directors and persons who are authorized to establish and maintain Business Relationship. However, regulated person shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and 'Form 29' and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.

Explanation:- For the purpose of this Annexure I the expression "NADRA" means National Database and Registration Authority established under NADRA Act, (VIII of 2000).

OPTIMUS

Annex 6

Proliferation Financing Warning Signs/Red Alerts

OCM shall 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.

OCM shall remain alert about 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.