



Your X factor to Investments

Know Your Customer (KYC), Customer Due Diligence
(CDD), Anti Money Laundering (AML), Combating
Financing Of Terrorism (CFT)



Your X factor to Investments

June 2023

1. INTRODUCTION

- 1.1 This document covers StocXinvest Securities (Private) Limited (**the Company or StocXinvest**) policies, procedures and practices in relation to Know Your Customer (KYC), Customer Due Diligence (CDD), Anti-Money Laundering (AML) & Combating Financing of Terrorism (CFT).

2. OBJECTIVE

- 2.1 To protect itself from the increasing risk of organized criminal activity, money laundering, and terrorist financing. Further,
- 2.2 To perform overall risk assessment of the Company in relation to the Money Laundering (ML)/ Terrorist Financing (TF).
- 2.3 To streamline the company procedures and practices in line with
- Securities Act, 2015 and related regulations issued thereunder,
 - PSX Rule Book,
 - Anti-Money Laundering Act, 2010, and
 - Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations 2018
 - International best practices recommended from Financial Action Task Force (FATF) published in February 2012.
http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
 - Guidelines on SECP (AML & CFT) Regulations, 2018 issued by SECP in September 2018.
- 2.4 To develop and implement policies and procedures that will help discourage money laundering and to monitor and remain alert regarding suspicious transactions and /or parties who may be attempting to launder money.

3. SCOPE

- 3.1 This policy is applicable to all operations of the Company including business of other Financial Institutions routed through the Company in order to ensure compliance with the Regulations of the country on KYC, CDD AML/CFT or that of the SECP, and recommendations of FATF whichever is more exhaustive.

4. DEFINITIONS

4.1 **Know your customer (KYC)** is the process of a business identifying and verifying the identity of its customers and ascertain relevant information required for doing business with them. KYC involves:

- Seeking evidence of identity and address from the customer and independently confirming that evidence at the start of a relationship with the Company; and
- Seeking information regarding the sources of income and nature of business etc. of the customer.

4.2 **Customer Due Diligence (CDD)** information comprises the facts about a customer that should enable an organization to assess the extent to which the customer exposes it to a range of risks. These risks include money laundering and terrorist financing.

4.3 **Customer** is defined as a person or an entity that applies for or maintains a trading account with the Company.

4.4 All specific terms used in this policy will have the same meaning as defined in Anti-Money Laundering Act, 2010, and Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations 2018.

5. ELEMENTS OF THE POLICY

The following elements have been incorporated in the KYC / CDD Policy:

A. Entity Risk Assessment in relation to ML/TF

B. Customer Risk

B1. Customer identification

B2. Risk Assessment of Customer

B3. High Risk Classification Factors

B4. Low Risk Classification Factors

C. On-going Diligence

D. Compliance function

E. Monitoring and Reporting

F. Data Retention

G. Training and employee screening

H. Audit Function

A. ENTITY RISK ASSESSMENT IN RELATION TO ML/ TF

A1 On annual basis, the Company shall undertake a risk assessment exercise to identify, assess and understand its money laundering and terrorism financing risk in relation to

- Its customers
- The jurisdictions or countries its customer are from or in
- The jurisdictions or countries the Company has operations or dealings in
- The product, services, transactions and delivery channels of the Company

A2 Following steps will be undertaken in the process of the entity risk assessment:

- Documentation of the areas and factors which may create related risk
- Considering all the relevant risk factors before determining the level of overall risk and the appropriate type and extent if mitigation to be applied
- Defining the company's risk tolerance and capacity to effectively manage the risks taken
- Identifying the likelihood of occurring (high, medium, low) of the risks highlighted
- Keeping the risk assessment up-to-date and be alert to any event / changes in regulatory framework and other factors.
- Categorizing the overall entity level risk as high, medium or low based on the result of risk assessment
- Having appropriate mechanisms to provide its risk assessment information to the Commission

A3 In view of the fact that the nature of the TF differs from that of ML, the risk assessment must also include an analysis of the vulnerabilities of TF. Since the funds used for TF may emanate from legal sources, the nature of the sources may vary when the source of the TF originate from criminal activities, the risk assessment related to ML is also applicable to TF.

A4 The document depicting the overall entity level risk will be prepared by Compliance Department and will be reviewed by COO and CEO. The same document will also be sent to Board of Directors along with Monthly Compliance Report at year end.

A5 Matters to consider in Identification, Assessment and Understanding Risks

A5.1 The Company s should understand, identify and assess the inherent ML/TF risks posed by its customer base, products and services offered, delivery channels and the jurisdictions within which it or its customers do business, and any other relevant risk category. The risk

assessment policies and procedures adopted by the Company should be appropriate to their size, nature and complexity.

A5.2 ML/TF risks may be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk for determining the overall risk classification (e.g. high, medium or low). The Company should make their own determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, The Company should take into consideration the relevance of different risk factors in the context of a particular customer relationship.

A5.3 In the second stage, the ML/TF risks that can be encountered by the Company's need to be assessed analyzed as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the Company from the crime, monetary penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself. The analysis of certain risk categories and their combination is specific for each business segment so that the conclusion on the total risk level must be based on the relevant information available.

A5.4 For the analysis, the Company should identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but not possible. In assessing the impact, the Company can, for instance, look at the financial damage by the crime itself or from regulatory sanctions or reputational damages that can be caused. The impact can vary from minor if they is an only short -term or there are low-cost consequences, to very major, when they are found to be very costly inducing long-term consequences that affect the proper functioning of the securities broker business.

A5.5 Risk mitigation and applying Risk based Approach:

The risk mitigation tools to be deployed by the Company shall include, but not limited to:

- Development and implementation of policies, procedures and controls which are approved by its Board of directors, which enable effective management and

mitigation of risk that are identified in the risk assessment of ML/TF or notified to commission

- Monitoring of its implementation phase.
- Enhanced measures for higher risk
- Independent audit function to test the system.
- MIS to be built for enhancement of compliance of AML.
- Regulations and AML policy to be incorporated in Internal Audit Plan.

A6 New Products, Practices and Technologies:

A6.1 Identify and assess the money laundering and terrorism financing risks that may arise in relation to-

- the development of new products and new business practices, including new delivery mechanisms; and
- the use of new or developing technologies for both new and pre- existing products;

A6.2 Undertake the risk assessments, prior to the launch or use of such products, practices and technologies, and shall take appropriate measures to manage and mitigate the risks.

A6.3 In complying with the requirements of clauses A6.1 and A6.2, the special attention is needed to pay over any new products and new business practices, including new delivery mechanisms; and new or developing technologies that favor anonymity.

A7 **Format for Company's risk assessment** as provided in SECP AML/CFT Guidelines detailed in **Annexure – I** will be followed.

A8 The management should **assess the adequacy of systems, controls, policies and procedures** relating to AML / CFT through a Compliance Assessment Checklist detailed in **Annexure – II**.

A9 Some of the risk mitigation measures that Company may consider include:

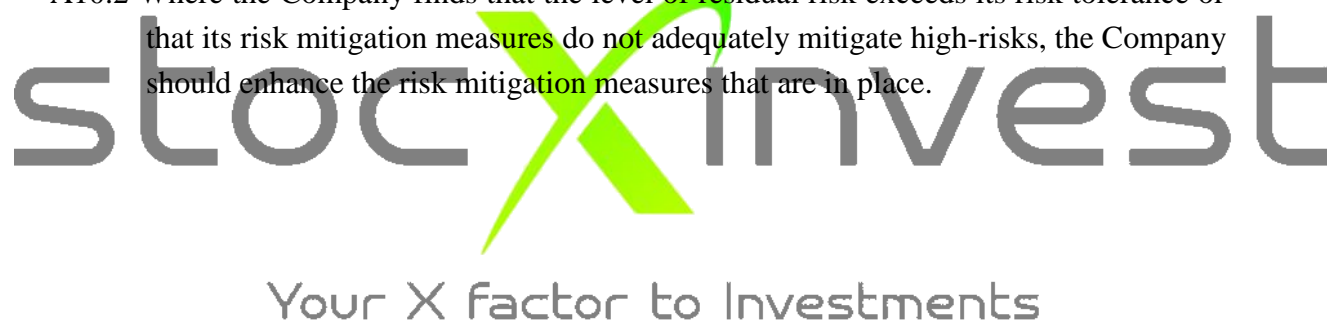
- Determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;
- Setting transaction limits for higher-risk customers or products;

- Requiring senior management approval for higher-risk transactions, including those involving PEPs;
- Determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;
- Determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

A10 Evaluating Residual Risk and Comparing with the Risk Tolerance

A10.1 Subsequent to establishing the risk mitigation measures, the Company should evaluate their residual risk, the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the Company's overall risk tolerance.

A10.2 Where the Company finds that the level of residual risk exceeds its risk tolerance or that its risk mitigation measures do not adequately mitigate high-risks, the Company should enhance the risk mitigation measures that are in place.



B. MANAGING CUSTOMER RISK

B1 Customer Identification:

B1.1 No account shall be opened in the name of person who fails to disclose his/her true identity or fails to provide valid identity document. To authenticate identity of new customer, following steps are and should be taken:

- Legible attested copy of CNIC / NICOP / Passport shall be obtained before account opening. In case of person other than individual, the same will be obtained of Directors / Trustees / Authorized Person / Partners in addition to incorporation document.
- Identity of above CNIC should be cross verified with NADRA Verisys.
- Account opening form should be signed in physical presence (including video chat through Skype and other social media platforms).
- The signature should match with the signature as per CNIC. In case of different signature, an indemnity bond will be provided by client of stamp duty of Rs. 250
- Source of income shall be essentially disclosed by the customer. In case source of customer's income is business / employment, name of the business / employer shall also be disclosed.
- All prospective customers must be seen either face to face by ----- Securities representative or on video call through social media like Skype, WhatsApp etc. and details verified over a recorded call on registered phone number.
- If a customer is acting on behalf of another person than the identity of that person should be ascertained and relevant documents of that person should also be obtained.

B1.2 For non-individual customers (e.g. companies, pension funds, government owned entities, non-profit organizations, foreign companies/ organizations) additional care has to be taken to establish the ownership and control structure of such an organization and who (i.e. person(s)) actually owns the organization and who manages it. It should be ensured that the person who represents himself as authorized signatory with powers to open and operate the brokerage account is actually authorized by the organization.

B1.3 Accounts of Institutions/ organizations / corporate bodies shall not be opened in the name of employee(s)/official(s). Because of sensitive nature of public sector (government) entities and risk of potential conflict of interest, it is critical for the Company and its representatives to ensure that accounts of Govt. Institutions are not opened in the individual name of any employee/official. Any such account, which is to be operated by an officer of a govt. owned

entity, is to be operated by an officer of the Federal/Provincial/Local Government in his/her official capacity, shall be opened only on production of a special resolution/authority from the concerned administrative department, duly endorsed by the Ministry of Finance or Finance Department of the concerned Provincial or Local Government.

B1.4 Purpose of investment and Risk appetite

B1.4.1 When an individual or an organization/institution opens brokerage account with the Company, it is important to find out and document in broad terms what does the customer intend to do. For example, are there any specific sectors or stocks that the customer does not wish to participate in; is the customer intending to invest for short-term only or is the customer intending to invest for longer term; will investment be only in liquid scrips or any scrip; or any other special needs or requirements of the customer. This, along with customer's other information such as age, gender, occupation, knowledge of market, etc. will help the Company develop a sense of the risk taking capacity and profile of the customer and thus guide the customer in more effective manner. At the same time, it will also help the Company understand whether the customer should be classified as a low risk or a high risk customer from the KYC/CDD perspective. For example, a domestic customer working in a company with regular income would be low risk category; on the other hand, a government employee may be in a higher risk category because of the potential for conflict of interest; or a foreign organization having foreign currency sources would be in high risk category requiring more careful identification procedure and close monitoring of account operations.

B1.4.2 In the above context, Company has to carefully determine the source of funding especially if the customer is expected to receive/send funds in foreign currency.

B1.5 All receipts/payments above Rs 25,000/- are made through cross-cheques, bank drafts, pay orders or other crossed banking instruments. Where any cash is accepted from a customer in an exceptional circumstance only, it has to be immediately reported to the Exchange with clear reasons as to why the cash receipt was accepted by the Company. A written request shall be obtained from customers highlighting the reason for cash deposits above the prescribed limit.

B1.6 In general, physical presence of the account opener/authorized representative is necessary at the time of opening a brokerage account. In the case of non-resident/overseas customers or customers in other cities where the Company does not have a branch/office, the Company shall ensure that identity verification process is completed through alternative means.

Alternative means include communicating video chat via Skype etc. with instruction to client to show original CNIC.

B1.7 The Company shall obtain such documents from different types of customers as provided in **Annexure-III**.

B1.8 The list refused customer must be maintained and apply CDD requirement to existing customer on the basis of trading volume. The materiality must be based on the trading volume.

B1.9 Sanctions Compliance

B1.9.1 The Regulations require the securities broker not to form business relationship with the individuals/entities and their associates that are either, sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

B1.9.2 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.

B1.9.3 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 are 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>

B1.9.4 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/>

Your X factor to Investments

B1.9.5 The Company shall make its sanctions compliance program an integral part of their overall AML/CFT compliance program and accordingly should have procedures and systems and controls in relation to sanctions compliance. The Company shall provide adequate sanctions related training to their staff.

B1.9.6 When conducting risk assessments, the Company shall take into account any sanctions that may apply (to customers or countries).

B1.9.7 The Company 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, the Company may discover that certain sanctions are applicable to one or more of their customers, existing or new.

B1.9.8 Where there is a true match or suspicion, the Company shall take steps that are required to comply with the sanctions obligations including freeze without delay and without prior notice, the funds or other assets of designated persons and entities and reporting to the Commission, if they discover a relationship that contravenes the UNSCR sanction or a proscription.

B1.9.9 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.

B1.9.10 The Company shall document and record all the actions that have been taken to comply with the sanctions regime, and the rationale for each such action.

B1.9.11 The Company is expected to keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed.

B1.9.12 In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, the Company may consider raising an STR to FMU.

Your X Factor to Investments

B2 Risk Assessment of Customer

B2.1 The assessment and categorization of customers as low, medium or high risk profile shall be done by the Company on the basis of information obtained at the time of brokerage account opening and on the basis of duly filled KYC/CDD Checklist (**Annexure – IV**). The Risk profile shall be updated on the basis of information obtained during the relationship and doing business with the customer. It should be based on customer's identity, nature of income, source of funding, location/domicile of customer, etc.

B2.2 The Company should verify the identity of the customer and beneficial owner before or during the course of account opening or may complete further documentation after the opening of account provided that:

- The completion of documentation occurs as soon as reasonably practicable as but not later than 10 working days.
- the ML/TF risks are effectively managed

B3 High-Risk Classification Factors

B3.1 Customer risk factors:

B3.1.1 The Company will describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the Company for ML or TF, and the consequent impact if indeed that occurs. Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

- a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the Company 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; (as per available information)
- g) Politically Exposed Persons (PEPs)
- 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

B3.2 Country or geographic risk factors:

B3.2.1 Country or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of the Company itself, its location and the location of its branches. 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.

B3.3 Product, service, transaction or delivery channel risk factors:

B3.3.1 A comprehensive ML/TF risk assessment must take into account the potential risks arising from the products, services, and transactions that the Company offers to its customers and the way these products and services are delivered. In identifying the risks of products, services, and transactions, the following factors should be considered:

- a) Anonymous transactions (which may include cash and accordingly reported to PSX as per PSX Rule Book).
- b) Non-face-to-face business relationships or transactions.
- c) Payments received from unknown or un-associated third parties. (and accordingly returned back to the original payer)
- d) Net investment of client in a month exceeds the threshold prescribed in Circular 17 of 2017 of SECP which does not match the customer profile and requires further questioning and EDD from client.
- e) International transactions, or involve high trading volumes of currency (or currency equivalent) transactions with individual customer / legal arrangements not subject to regulatory requirement relating to AML / CFT.

- f) One-off transactions with a new client exceeding the threshold prescribed in Circular 17 of 2017 of SECP.

B4 Low Risk Classification Factors

B4.1 Customer risk factors:

B4.1.1 A customer that satisfies the requirements under regulation 11 (2) (a) and (b) of the SECP AML/CFT Regulations which are:

- Securities Broker, Commodities Broker, Insurers, Takaful Operators, NBFC, Modarabas and Banks provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements.
- Public listed companies

B4.2 Product, service, transaction or delivery channel risk factors:

B4.2.1 The product, service, transaction or delivery channel that satisfy the requirement under regulation 11(2) (c) to (g) of the SECP AML/CFT Regulations including pension schemes and financial product or services that provide appropriately defined and limited service to certain type of customers, so as to increase access for financial inclusion purpose.

B4.3 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.

B4.4 Company shall consider updating customer CDD records as a part its periodic reviews (within the timeframes set by the Company based on the level of risk posed by the customer) or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:

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

B4.4.1 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.

B4.5 The Company should be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

- 1) Transaction type
- 2) Frequency
- 3) Amount
- 4) Geographical origin/destination
- 5) Account signatories

C. ON-GOING DUE DILIGENCE:

C1 It is important for the Company and its agents to realize that Customer Due Diligence (CDD) is not a one-time exercise at the time of account opening only. In order to guard against misuse of its good offices against criminal transactions, the Company need to be vigilant at all the times, and keep monitoring transactions of their customers to ensure that the transactions executed in any particular account are within the understanding of the Company in terms of the customer's profile, risk profile, source of funds, and historical pattern of the transactions and their historic funding source. On-going Due Diligence can be classified into Simplified Due Diligence and Enhanced Due Diligence on the basis of risk categorization assigned at time of KYC.

C2 In the above context, the Company should keep all customer records updated and should have a practice of assessing any change in customer profile on regular basis, which change should be documented and sufficient information should be obtained regarding such change.

C3 Monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, the customer's business and risk profile, including, the source of funds *and*, updating records and data/information to take prompt action when there is material departure from usual and expected activity through regular matching with information

C4 It should be noted that this exercise of categorizing customers in LOW, MEDIUM, HIGH RISK category applies to all customers, including existing customers on the basis of materiality of trading volume, Thus, once the broker has carried out the above exercise, if an existing customer falls into the HIGH RISK CATEGORY, the above requirements for monitoring and reporting suspicious transactions and senior management approval for continuing with the customer will also apply to such customer(s).

C5 SIMPLIFIED DUE DILIGENCE

C5.1 The decision to categorize the client as low risk should be justified through KYC Checklist.

In addition to cases previously discussed in A3 above, low risk cases may include but are not limited to the following:

- Securities Broker, Commodities Broker, Insurers, Takaful Operators, NBFC, Modarabas and Banks provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements.
- Public listed companies
- Financial product or services that provide appropriately defined and limited service to certain type of customers, so as to increase access for financial inclusion purpose

C5.2 Simplified CDD should not be followed when there is an identified risk of money laundering or terrorist financing.

C5.3 Simplified Due Diligence measures are limited to the following-

- reducing the frequency of customer identification updates;
- reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable monetary threshold; and
- not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature & from the type of transaction or business relationship established:

C5.4 Provided that Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

C6 ENHANCED DUE DILIGENCE (EDD)

C6.1 Once a customer has been categorized as HIGH RISK, it is necessary for the Company to have EDD when dealing with such a customer. Policies and procedures should be put in place by Risk Department so that activities and transactions of HIGH RISK customers are monitored and any unusual transactions are reported in a SUSPICIOUS TRANSACTION REPORT (STR).

C6.2 The activities / customer which creates 'red flag' on customer are attached as **Annexure – V**.

C6.3 EDD measures include but are not limited to the following:

- obtain approval from senior management (CEO / COO) to open / continue account with high risk customers
- Ascertain the source of wealth and / or fund through appropriate means including initial documentation for source of income, publicly available information such as companies' website, professional websites, inquiry and subsequent documentation.
- Conduct enhanced monitoring of trading and fund movement through a properly designed MIS enabling reporting of STR and maintenance of report as required under Circular 10 of 2017 of SECP
- Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
- Updating more regularly the identification data of applicant/customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining additional information on the source of funds or source of wealth of the applicant/customer.
- Obtaining additional information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.

- 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.

C6.4 “Politically Exposed Persons” (PEPs’)

C6.4.1 PEP’s also fall under HIGH RISK CATEGORY. These include individuals in prominent positions such as senior politicians, senior government, judicial or military officials; senior executives of State Corporations and their family members and close associates. These individuals present reputational risk and potential conflict of interest and extra caution is required when opening their brokerage account and monitoring their account activity. The Enhanced Due Diligence must be performed to mitigate such risks. The controls in relation to PEP include

- Training of front office staff to remain alert on knowledge which may lead to believe the client as PEP while opening a new account as well as working with existing client
- Continuous monitoring of current occupation of clients by traders and other staff
- Appropriate risk management systems to determine whether the customer is a politically exposed person;
- Senior management approval for establishing business relationships with such customers;
- Reasonable measures to establish the source of wealth and source of funds; and
- Enhanced ongoing monitoring of the business relationship.

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

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

D. COMPLIANCE FUNCTION

D1 To achieve KYC/CDD, two key elements have to be instituted at the Company's end;

- a) Compliance Function with suitable human resource
- b) Information system capable of effective and robust Reporting capability

D2 The person responsible for overseeing compliance should be a management level officer and should have sufficient skills and experience to effectively perform the compliance function. The Head of Compliance should report to the Board of Directors / Audit Committee of the Company.

D3 It is the responsibility of the compliance function to ensure that KYC/CDD policy is being complied with as well as with other regulatory requirements. This includes maintaining record of violations / non-compliance identified which has to be reported to the Board of Directors. Any such record has to be available for inspection by Securities and Exchange Commission of Pakistan (SECP) and Pakistan Stock Exchange (PSX) as and when required. The Compliance function should ensure:

- The Company's effective compliance with the relevant provisions of these Regulations, the AML Act, the Anti-Money Laundering Rules, 2008, the Anti-Money Laundering Regulations, 2015 and other directions and guidelines issued under the aforementioned regulations and laws by SECP, PSX & FATF, as amended from time to time;
- ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the Company and are effectively implemented;
- monitoring, reviewing and updating AML/CFT policies and procedures, of the Company;
- providing assistance in compliance to other departments and branches of the Company;
- Timely submission of accurate data/ returns as required under the applicable laws
- Monitoring and timely reporting of Suspicious and Currency Transactions to FMU.

E. MONITORING AND REPORTING

- E1 All business relationship with customer shall be monitored on an ongoing basis to ensure that the transactions are consistent with the Company's knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.
- E2 The Company shall obtain information and examine, as far as possible the background and purpose of all complex and unusual transactions, which have no apparent economic or visible lawful purpose and the background and purpose of these transactions, shall be documented with a view of making this information available to relevant competent authorities when required.
- E3 The Company shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for high risk categories of customers. The review period should be on half yearly basis and procedures should include review of expiry of identity, client communication with the sales person, being alert for any information related to change in source of income and / or funds.
- E4 As per Anti-Money Laundering Act, 2010, **Suspicious Transaction Reporting (STR)** is required to be filed for transactions when the Company knows, suspects, or has reason to suspect that the transaction or a pattern of transaction of which the transaction is a part:
- Involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime;
 - Is designed to evade any requirements of the Act;
 - Has no apparent lawful purpose after examining the available fact, including the background and possible purpose of the transaction; and
 - Involves financing of terrorism.

- E5 The Company shall pay attention to all complex and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transaction shall, as far as possible, be examined, the findings established in writing, and be available to assist the relevant authorities in inspection and investigation.
- E6 As per Circular 10 of 2017, the Company shall maintain monthly report (in format as per **Annexure – VI**) of investor whose net traded amount (i.e. value brought – value sold) in a month exceeds the following threshold:

Investor Class	Investment Amount (Rs. in million)
Corporate	25.00
Proprietary- Broker	20.00
Individual	5.00

- E7 The transactions, which are out of character, are inconsistent with the history, pattern, or normal operation of the account or are not commensurate with the level of income of customer shall be viewed with suspicion, be properly investigated and referred to Compliance Officer for possible reporting to FMU under the AML Act.
- E8 Provided that Suspicious Transaction Report shall be filed by the Company with the Financial Monitoring Unit (FMU) immediately but not later than seven working days after forming that suspicion.
- E9 CTRs should be reported for the transaction of rupees two million and above by the Company with the FMU immediately, but not later than seven working days, after the respective currency transaction.
- E10 The Company shall keep and maintain all records related to STR and CTR filed by the Company for a period of at least five years after reporting of transaction.
- E11 The company shall report total number of STRs, if any, filed to the Commission on bi-annual basis within seven days of close of each half year.
- E12 Further, the company shall also maintain a register of all reports made to the FMU, containing 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. The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.

E13 All the employees are strictly prohibited to disclose the fact to the customer or any other quarter that a STR or related information is being or has been reported to any authority, except if required by law.

E14 The Company, without disclosing the contents of STRs, shall intimate to the SECP on bi-annual basis the number of STRs reported to FMU and the Company shall ensure that status report (including no. of STRs only) shall reach the AML Department within seven days of close of each half year.



F. DATA RETENTION

F1 The Company shall maintain all necessary records of transactions, both domestic and international, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of five years from completion of the transaction. Provided that the Company will retain those records for longer period where transactions, customer or accounts involve litigation or it is required by court or other competent authority.

F2 In relation to closed account, the record, including identification documents, account opening forms, KYC Forms, verification documents and other documents along with record of account files and correspondence, shall be maintained for a minimum period of ten years after the date of close of account.

F3 In case change in any of the particulars is requested by the customer, the Company shall update the record on customer's written request or request received through his/ her registered email address.

F4 In the case of customers who cease to be a customer of the company, information regarding the beneficial ownership of the customer (legal entity) shall be maintained for at least 5 years.

G. TRAINING AND EMPLOYEE SCREENING

- G1 Training shall be provided on KYC/CDD policy by HR/Compliance Department. There has to be on-going training of the employees and agents to ensure that they understand their duties under KYC/CDD and are able to perform those duties satisfactorily.
- G2 The Company should have appropriate screening procedures when hiring and also on an ongoing basis to ensure high standards of staff in terms of honesty, integrity, ethics and professionalism. This is important not just for the sake of Company's own safety and reputation but the reputation of the Capital Market. For this purpose:
- Company's HR Manual should include a comprehensive employee due diligence policy and procedure to be carried out at the time of hiring all employees permanent, contractual, or through outsourcing. This shall include but not limited to verification of antecedents and screening procedures to verify that person being inducted/ hired has a clean history; Further, the company shall, periodically thereafter conduct employee screening at least annually.
 - Suitable training program will be arranged in relation to KYC formalities, awareness of KYC/AML/CFT policies and relevant rules, regulations and guidelines for relevant employees on half yearly basis, in order to effectively implement the regulatory requirements and Company's own policies and procedures relating to AML/ CFT. The employees training shall enable them to understand new developments, money laundering and financing of terrorism techniques, methods and trends. The training should also include their responsibilities of employee relating to AML/ CFT.

H. AUDIT FUCTION

- H1 For the purpose of Company-wide monitoring and review, the company's Internal audit function shall conduct, periodically, AML/CFT audits on a regular basis. The frequency of the audit should be commensurate with the company's nature, size, complexity, and risks identified during the risk assessments. The main areas of the audit shall include but not limited to:
- H2 The overall integrity and effectiveness of the AML/CFT systems and controls and compliance with relevant laws and regulations;
- 1) 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;
 - 2) Employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
 - 3) Completeness and adequacy of training programs
 - 4) Emphasis on testing high risk areas identified in the organization
 - 5) Adequacy of the process of identifying suspicious activities by employees and general controls to identify any ML/TF activities such as screening sanction lists.

ANNEXURE - I

COMPANY'S OVERALL RISK ASSESSMENT IN RELATION TO ML/TF

Likelihood Scale			
Consequence Scale	Low	Moderate	High

Name of Reporting Entity _____
 Reporting Date 30-Sep-18
 Reporting Period From October 1, 2017 to September 30, 2018

Step 1 – Identify Customer Risk

Customer Risk Type						
Customer Type	Number of Customers (having active UIN) as on September 30, 2018	Asset under custody as on September 30, 2018		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

M/S
30-Sep-18
From October 1, 2017 to September 30, 2018

[illegible]

Name of Reporting Entity	M/S
Reporting Date	30-Sep-18
Reporting Period	From October 1, 2017 to September 30, 2018

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 September 30, 2018		Total Number as on September 30, 2018	
	Domestic PEP	Foreign PEP	Domestic	Foreign
Product 1				
Product 2				
sample category of products for reference:				
Trading of Eligible Listed Securities in ready market				
Trading of Eligible Listed Securities in future market				
Trading of Mutual Funds				
Trading of Corporate Bonds/Debt Instruments Term Finance Certificates, Sukuk Etc.				
Trading of Government Securities in GDS Market				
Margin Financing Availed				
Margin Financing Provided				
Margin Trading as Financer				
Margin Trading as Finantee				
Physical Securities				
Securities Adviser				
Securities Manager				
Underwriter				
Consultants to the Issue				
Book Runner				
Trading of Commodities Futures at PMEX				
Other (specify)				
Total	0.00	0.00	0.00	0.00

Business Risk	Type	Total number of customers	Products and Services					Foreign (including non-resident)				
			Domestic					Foreign (including non-resident)				
			Total Purchase/Financing extended from October 1, 2017 to September 30, 2018		Total Sale/Financing availed/Income from October 1, 2017 to September 30, 2018		Total Value of securities/financing/income and bank balances on cutoff date	Total Purchase/Financing extended from October 1, 2017 to September 30, 2018		Total Sale/Financing availed/Income from October 1, 2017 to September 30, 2018		Total Value of securities/financing/income and bank balances on cutoff date
			Number	Value in Rupees	Number	Value in Rupees		Number	Value in Rupees	Number	Value in Rupees	
	NGO/NPO/ Charities/ Trust/ legal arrangements that receive donations											
	Retirement Funds (Provident Funds, Gratuity Funds etc)											
	Shell Companies											
	Govt Institutions/ departments											
	Partnership Company (specify nature of business)											
	Individuals other than High Net Worth which may be broken down into following categories											
	Sole Proprietor Business											
	Students											
	House Wives											
	Retired Persons											
	Individuals-Service /Profession											
	real estate dealers											
	dealers in precious stones											
	lawyers/ notaries											
	Individual-Agriculturist											
	Total			0.00		0.00	0.00					0

Name of Reporting Entity _____
Reporting Date 30-Sep-18
Reporting Period From October 1, 2017 to September 30, 2018

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
1 Wire Transfers (SWIFT)				
2 Domestic Payments				
3 Total	0.00	0.00	0.00	0.00

Signature _____
Name _____
Designation _____
Date _____

Name of Reporting Entity M/S
Reporting Date 30-Sep-18
Reporting Period From October 1, 2017 to September 30, 2018

Step 5- Identify Customer Type by Geographic Location

Types of Customers	Number of Customers	Total asset under custody and bank balance as on September 30, 2018
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

Name of Reporting Entity
Reporting Date
Reporting Period

30-Sep-18

From October 1, 2017 to September 30, 2018

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

Risk Likelihood Table			
Type of Customer	Customer	Transaction	Geography
Customer Type 1 Customer Type 2 Examples of customer type			
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)			
Shell Companies			
Govt institutions/ departments			
Partnership Company (specify nature of business)			
Individuals other than High Net Worth which may be broken down into following categories			
Sole Proprietor Business			
Students			
House Wives			
Retired Persons			
Individuals-Service /Profession			
real estate dealers			
dealers in precious stones			
lawyers/ notaries			
Individual-Agriculturist			
Total			

Note: regulated person must provide information in respect of **all customers** divided into different customer types as per its internal policies and procedures. The above examples can be used as reference

Signature _____

Name _____

Designation _____

Date _____

Name of Reporting Entity

Reporting Date

Reporting Period

30-Sep-18

From October 1, 2017 to September 30, 20

Step 6 - Develop Risk Likelihood Table

Product Wise

Risk Likelihood Table			
Product Type wherever applicable	Customers	Transactions	Geography
Product Type 1			
Product Type 2			
Product Type 3			
Product Type 4			
sample category of products:			
Trading of Eligible Listed Securities in ready market			
Trading of Eligible Listed Securities in future market			
Trading of Mutual Funds (open-end and closed-end) units			
Trading of Corporate Bonds/Debt Instruments Term Finance Certificates, Sukkuk Etc.			
Trading of Government Securities in GDS Market			
Margin Financing Availed			
Margin Financing Provided			
Margin Trading as Financer			
Margin Trading as Financee			
Physical Securities			
Securities Adviser			
Securities Manager			
Underwriter			
Consultants to the Issue			
Book Runner			
Trading of Commodities Futures at PMEX			
Other (specify)			

Note: reporting entity may provide further breakdown of each product.

Signature

Name

Designation

Name of Reporting Entity

Reporting Date

Reporting Period

30-Sep-18

From October 1, 2017 to September 30, 2018

Step 6 - Develop Risk Likelihood Table

Delivery Channels Wise

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

Annexure II


S No.	Type of Customer	Information/Documents to be Obtained
1.	Individuals	<p>A photocopy of any one of the following valid identity documents;</p> <ul style="list-style-type: none"> (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	<ul style="list-style-type: none"> (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	<ul style="list-style-type: none"> (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	<ul style="list-style-type: none"> (i) Certified copies of: <ul style="list-style-type: none"> (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;

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

		the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.
8.	Agents	(v) Registered address/ Business address. (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).



Your X Factor to Investments