AKD Securities Limited

AKD Securities Limited
(formerly 'BIPL Securities Limited')

Policy Name:	Know Your Customer (KYC), Customer Due Diligence (CDD), Anti Money Laundering (AML), Combating Financing Of Terrorism (CFT) Policies and Procedures
Approval Authority:	Board of Directors

1. INTRODUCTION

1.1 This document covers AKD Securities Limited, (formerly 'BIPL Securities Limited') policies, procedures and practices in relation to Know Your Customer (KYC), Customer Due Diligence (CDD), Anti-Money Laundering (AML) & Combating Financing of Terrorism (CFT).

1.2 This document supersedes KYC Policy of AKD Securities Limited, (formerly 'BIPL Securities Limited') approved in 2010 and KYC/CDD, AML/CFT policy created on January 2, 2018.

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 AKD Securities Limited, (formerly 'BIPL Securities Limited') 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, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself. The analysis of certain risk categories and their combination is specific for each 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 A6.3, 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 AKD Securities Limited, (formerly 'BIPL Securities Limited') 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 through video chat via Skype with instructions 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/
https://nfs.punjab.gov.pk/
http://www.fia.gov.pk/ur/redbooktriff.pdf

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 shall conduct forthnightly screening of all existing customers as part of on-going monitoring from the lists of UNSC/NACTA/FIA Redbook.

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.

B1.9.13 The Company shall scan its customer data bases and their Beneficial Owners /associates for any matches with the stated designated/proscribed person(s)/entity(ies) on the receipt of notifications issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/ Home Departments of Provinces/Ministry of Interior regarding updates in list of proscribed persons under the Anti- Terrorism Act, 1997. Compliance report on statutory regulatory orders shall be submitted to the Commission within three day of receiving the same through the SECP E-services portal.

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.
e) Jurisdictions identified by SECP in the National Risk Assessment 2019 as high risk jurisdictions with respect to the threat of Money Laundering and Terrorist Financing subject to the judgment of the Company and validity of the documents obtained for the purpose of the client's profile and source of income.

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 as per the internal assessment of the Company which does not match the customer profile and requires further questioning and EDD from the 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.

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, transection 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.

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 a 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.

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

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 functions 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
Almost Certain	Moderate	Moderate	High
Possible	Moderate	Moderate	High
Unlikely	Low	Moderate	Moderate

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***

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 P ersons ('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 Septembe r 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 Coporate 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				
Tradin g of Commodities Futures at PMEX				
Other (specify)				
Total	0.00	0.00	0.00	0.00

Note: regulated person must provide information for all products. Further, it may choose to provide further breakdown of each product.

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

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 October 1, 2017 to September 30, 2018		Total Sale/Financing availed/income from October 1, 2017 to September 30, 2018		Total Value of securities/finainci ng/inc ome and bank balances on cutoff date	Total number of customers	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/finai ncing/income and bank balances on cutoff date
		Number	Value in Rupees	Number	Value in Rupees			Number	Value in Rupee s	Number	Value in Rupees	
Products and Services													
Product 1													
Product 2													
Product 3													
example 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 Coporate 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 Financ ee													
Physical Securities													
Securities Adviser													
Securities Manager													
Underwriter													
Consultants to the Issue													
Book Runner													
Trading of Commodities Futures at PMEX													
Other (specify)													
Transactions													
Customer Type 1													
Customer Type 2													
Customer Type 3													
Customer Tyoe 4													
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													

Products and Services												
Business Risk		Do mestic					Foreign (including non - resident)					
Type	Total number of customers	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/finainci ng/income and bank balances on cutoff date	Total number of customers	Total Purchase/Financing ex tended from October 1, 2017 to Sept ember 30, 2018		Total Sale/Financing availed/income from October 1, 2017 to September 30, 2018		Total Value of securities/finai ncing/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												
Stude nts												
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						0.00

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 - IIdentify Customer Type by Geographic Location

Types of Customers	Number of Customers	Total asset under custody and bank b alance 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 Jurisdict ions' 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' a s identified by the financial institutions		
Total	0.00	0.00

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

Step 6 - Develop Risk Likelihood Table

Customer wise

R isk 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 co mpanies			
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 s tones			
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 30-Sep-18
Reporting Period From October 1, 2017 to September 30, 20

Step 6 - Develop Risk Likelihood Table

Product Wise

Risk Likelihood Table			
Pro duct 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 fu ture market			
Trading of Mutual Funds (open - end and closed - end) units			
Trading of Coporate 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 _____

Date _____

Name of Reporting Entity	
Reporting Date	30-Sep-18
Reporting Period	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 aborad			
Remittance received in foreign currency			
Online fund transfer where trail of transferror is not traceable			

BIPL SECURITIES LIMITED

ASSESSMENT AS AT SEPTEMBER 30, 2018

Internal AML/CFT Risk Assessment Likelihood Results

		Low / Modera te / High
1	Customer Type	
2	Product Type	
3	Delivery Channels	
4	Geography	
5	Over All Risk Rating	

ANNEXURE II

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 ('RB A')		
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 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		
(l) 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?		

Annexure - III

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).

Annexure - IV

RISK PROFILING CHECKLIST - INDIVIDUAL

Date:	Account Title:	Account / UIN #:

S.No.	Description	Yes / No
SECTION A: MINIMUM DOCUMENTATION (KYC)		
If the response to any of the statements in Section A is "No", the entity shall NOT establish business relationship with the client		
1.	CNIC / NICOP / POC of Main Applicant and Joint Applicant(s) / Passport for Foreign Nationals	
2.	Proof of Employment/Business Copy of service card or any other acceptable evidence of service, such as certificate from the employer including pay slip, experience letter as evidence of income. Proof of business for self-employed persons (such as Income Tax Returns, Business Cards, Invoice of Shop, Letterhead etc., Financial Statements (audited /un-audited)	
3.	Proof of mailing/ permanent address (if applicable) In case the address provided is same as in CNIC, no additional document is mandatory. In other cases, any of the following documents shall be obtained: Utility bills; rental agreement; driving license, etc.	
4.	Applicant, Beneficial Owner of the applicant, person acting on behalf of the applicant, or connected party of the applicant does not match the details in the following lists: a. Prescribed under the United Nations Security Council b. NACTA - Schedule IV (Proscribed Person) data c. FIA Red Book(s)	
5.	Information required to be verified as per the regulations, can be verified to independent and reliable documents	
6.	There is no apparent suspicion of money laundering and/or terrorist financing.	
7.	Is the applicant (investor) also the ultimate beneficiary of the funds to be invested?	

SECTION B : CUSTOMER RISK FACTOR (CDD)		Yes / No	Suggested Risk (Low / Medium / High)
8.	Is the applicant, any of the beneficial owners of the applicant or person acting on behalf of the applicant a Politically Exposed Person (PEP), family member of a PEP or close associate (social /professional) of PEP?		High (if Yes)
9.	Is the applicant non-resident Pakistani? (i.e. holds NICOP/ Pakistan Origin Card / Foreign service / Foreign Residential address) a) Professional / Service b) Others		 Low High
10.	Is the applicant foreign national?		High (if Yes)
11.	Applicant's source of wealth/ income is high risk/ cash intensive? (Real estate business, Agriculture, Lawyer, etc.)		High (if Yes)
12.	Is the business relationship with the applicant established through face-to-face channel? (i.e. Account is opened through in-person visit by client i.e. meeting of client with BIPLS staff either in-person or through video call.)		High (if No)
13.	Is there any reason to believe that the applicant has been refused account opening by another Financial Institution / Brokerage House ?		
14.	Does the stated source of wealth / source of funds and the amount of money involved corresponds with what you know of the applicant?		

SECTION C : COUNTRY / GEOGRAPHIC RISK FACTORS (CDD)		Yes / No
15.	The applicant, beneficial owner of the applicant or person acting on behalf of the applicant is not from or based in a country or jurisdiction: a. Identified as High-risk jurisdiction by the FATF and for which financial institutions should give special attention to business relationships and transactions. (Countries having weak governance, law enforcement, and regulatory regimes). b. Countries subject to sanctions, embargos or similar measures issued by international authorities (E.G. UN, WB, IMF) c. Countries where protection for customers' privacy prevents effective implementation of AML/CFT requirements and/or facilitates the framework for establishment of shell companies. d. Countries/ Geographies identified by recognized sources as having significant levels of organized crime, corrup-	

I hereby declare that I have met the Applicant, Mr./Mrs./Ms. _____ at;

☐ BIPL Securities Branch Office
☐ Applicant's Office / Business address
☐ Applicant's House address, as mentioned in his account opening form / supporting documents.
☐ Other; please specify _____

I have also seen the original CNIC/SNIC/NICOP/ARC/POC/Passport (as applicable) of Applicant.

Purpose and intended nature of the business relationship? ☐ Equity Trading ☐ Commodities Trading

Applicant's Expected level of Investment will be Rs._____.

Intention of Trading
☐ Long Term ☐ Short Term ☐ Both

Section E: Applicant Risk Assessment

☐ Low Risk ☐ Medium Risk ☐ High Risk

Comments: _____

_____

_____

Section F: Recommendation

☐ Accept applicant ☐ Reject applicant

(High Risk applicant should be approved by Senior Management (CEO / CFO and HOO jointly)

Completed by:	**Checked by:**
Name of Sales Person: _____	Name of Compliance Person: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

Annexure - V

Brokerage Houses

(1) Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
(2) Customers who wish to deal on a large scale but are completely unknown to the broker;
(3) Customers who wish to invest or settle using cash;
(4) Customers who use a cheque that has been drawn on an account other than their own;
(5) Customers who change the settlement details at the last moment;
(6) Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
(7) Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
(8) Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
(9) Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
(10) Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
(11) Customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
(12) Customer trades frequently, selling at a loss
(13) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
(14) Customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
(15) Any transaction involving an undisclosed party;
(16) Transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
(17) Significant variation in the pattern of investment without reasonable or acceptable explanation
(18) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
(19) Transactions involve penny/microcap stocks.
(20) Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
(21) Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
(22) Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
(23) Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
(24) Customer conducts mirror trades.
(25) Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reas