ANTI-MONEY LAUNDERING, COUNTERING FINANCING OF TERRORISM, AND PROLIFERATION FINANCING POLICY

April 10, 2025

Pine Capital Management (Private) Limited

Updated: April 10, 2025

Contents

Document Review and Approval

Revision History:

Sr.	Version	Author	Date	Revision
1	1.1	Zahoor Ahmad	April 10, 2025	-
2				
3				
4				
5				

Reviewed By:

Sr.	Reviewer	Signature	Date Reviewed
1	Adil Khan Swati		April 10, 2025
2			
3			
4			
5			

Approved By:

Sr.	Name	Signature	Date Approved
1	Adil Khan Swati		April 10, 2025
2			
3			
4			
5			

Policy No.: 001
Effective Date: 10 April, 2025
Updated: 10 April, 2025

COMPANY'S POLICY

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will be used later for criminal purposes. All employees are required to receive a copy of the Company's AML policy and are required to follow such policy and procedures. If an employee is caught violating any portion of the Company's AML policies and procedures, a meeting with the Compliance Officer will occur, with the employee given written warning of such violation. If the employee violates the AML policies and procedures for the second time, immediate termination will occur.

PURPOSE

The objective of this policy is to ensure that the products and services of the Pine Capital Management (Private) Limited (**Pine**) are not used to launder the proceeds of crime and that all of the **Pine's** staff is aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing. The document also provides a framework to comply with applicable laws, Regulatory guidelines specially related with detection and reporting of suspicious activities.
Other objectives pursued by this policy are as follows:

- Promote a "Know Your Customer" policy as a cornerstone principle for the Brokerage firm's ethics and practices;
- Introduce a controlled environment where no business with a Customer is transacted until all essential information concerning the Customer has been obtained;
- Conduct self-assessments of compliance with AML policy and procedures;
- Introducing to the employees the stages of money laundering process and their individual duties;
- Establishing a review process which will be used to identify opportunities that might be used to launder money;
- Providing instructions regarding taking appropriate action once a suspicious activity or a money laundering activity is detected or suspected.

Adherence to this policy is absolutely fundamental for ensuring that the Pine fully complies with applicable anti-money laundering rules and regulations.
The Pine is committed to examining its anti-money laundering strategies, goals and objectives on an ongoing basis and maintaining an effective AML Policy for its business.

SCOPE

This policy is applicable to the **Pine's** local as well as overseas operations (if any) including business of other Financial Institutions routed through Pine.
In overseas offices (if any), Pine shall ensure compliance with the Regulations of the host country on KYC, CDD AML/CFT or that of the SECP whichever are more exhaustive.

Our coverage will include:

- Compliance of AML Act 2010.
- Compliance of SECP requirements on KYC, CDD AML/CFT.
- Compliance of local country legislations/ regulations on KYC, CDD AML/CFT& subsequent updates.
- FATF Recommendations
- International Standards and guidelines, including Regulatory sanctions as applicable.
- Pakistan National Risk Assessment on Money Laundering and Terrorism Financing. (2019 –update)

RESPONSIBLE PARTY:

Compliance Officer

REGULATORY OVERSIGHT & COMPLIANCE RISK

Pine is bound to use SECP, PSX guidelines and International Regulatory guidelines/standards as applicable to formulate its own KYC, CDD AML/CFT Policy. The consequence of contravening the Regulations or failing to comply can be significant and include disciplinary measures, imprisonment or fine or both under local laws as well as the loss of reputation for Pine.
Notwithstanding the statutory and regulatory penalties, increased vigilance by Management and staff will protect Pine from the following risks:

- Reputational
- Operational
- Legal
- Financial

Reputational risk: The reputation of a business is usually at the core of its success. The ability to attract good employees, customers and business is dependent on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong KYC, CDD AML/CFT policy helps to prevent a business from being used as a vehicle for illegal activities.

Operational risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If KYC, CDD AML/CFT policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

Legal risk: If a business is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations.

Financial risk: If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching. If a business does not know the true identity of its customers, it will also be difficult to retrieve money that the customer owes.

CUSTOMER DUE DILIGENCE & KNOW YOUR CUSTOMER

CDD is closely associated with the fight against money-laundering. Supervisors around the world are increasingly recognizing the importance of ensuring that their financial institutions have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, financial institutions can be exposed to reputational, operational, legal and financial risks.

It is policy of Pine that:

- Prior to establishing a relationship with a new customer, basic background information about the customer should be obtained, in particular, information related with customer's business and source/utilization of funds.
- Prior to establishing relationships with financial institutions or agents, appropriate steps must be taken to confirm the identity, integrity and due diligence procedures of those representatives or agents and, where necessary, the identities of underlying clients.
- The underlying beneficial ownership of all companies and other legal entities with which Pine conduct business must be established, including the beneficial ownership of all funds or other properties that are handled by the Pine.
- All new relationships should be filtered through automated solution for possible name matching with individuals / entities appearing on various negative lists maintained by Pine. In case of exact match, relationship should be discontinued.
- Pine shall reject the account opening application in case the applicants name is found in OFAC's (Office of Foreign Asset Control) specially designated persons or blocked person list maintained by the U.S department of the Treasury (www.treasury.gov)

Know Your Customer

The inadequacy or absence of KYC standards can subject Pine's to serious customer and counterparty risks, especially reputational, operational, Legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to Pine, along with considerable management time and energy to resolving problems that arise.
Effectively devised KYC policy is the most important defense against the money launderers. While fulfilling legal requirements, the contents of regulatory requirements should be kept in view before establishing a customer/account opening relationship.

Procedures

The knowledge of the customer base and business operations will also help Pine as under:

a) Detect suspicious activity in a timely manner.
b) Promote compliance with all brokerage laws.
c) Promote safe and sound brokerage practices.
d) Minimize the risk of brokerage channels being used for illicit activities.
e) Protect Pine reputation & image.
f) Bolster confidence among its customers, other brokerage houses, and brokerage regulators.
g) Protect Pine against negative legal consequences related to cooperating with entities supporting terrorism.

Pine would not do business with;

- Individuals / entities subject to UN sanctions
- Individuals / entities under OFAC or local country sanctions as applicable
- Unauthorized money changers/prize bond dealers
- Anonymous customers
- Customers hiding beneficial ownership of the account
- Client or business segment black listed by brokerage house, Pine or by the Regulators.
- Shell Banks & off shore corporate clients.
- Fund, investment manager, fund custodian or institution that operates omnibus accounts.
- Government officials willing to open government's accounts in their personal names.

Pine shall conduct enhanced due diligence procedures before establishing relationships with the following High Risks Customers;

- Trusts, NGOs, NPOs, Foundations, Welfare Association, Religious Entities, Club, Societies,
- Authorized Money Exchange Cos., Controversial entity, Jewelers, Arms Dealers.
- Politically Exposed Persons (PEPs)

- Any individual or entity that has caused or has been related to a credit, operational or reputational loss to Pine
- Accounts of foreign nationals belonging to sanctioned countries
- Walk in customers
- Non- resident customers

Any customer relationship where the customer's conduct gives the Pine reasonable cause to believe or suspect involvement with illegal activities is required to be reported to the Regulators or relevant authorities.

PROCEDURES FOR DOCUMENTATION & VERIFICATION OF LOW RISK CUSTOMER

Documentation

Type of Customer	Information/Documents
Individual/Sole Proprietorship	**Name**
	Father Name
	Address
	Telephone Number
	Copy of CNIC or Passport
	Source of income
	Business/Employment proof
Partnership Account	**Name of partnership and Partners**
	Father's name of partners
	Address
	Telephone No.
	Copies of CNIC of all the partners
	Copies of latest financials of partnership
Joint Stock Companies	**Name of Companies and its Directors**
	Registered Address
	Telephone number
	Copies of CNIC of all Directors
	Audited Accounts of the company
	Memorandum and Articles of Association
	Board Resolution
Trust	**Copy of CNIC of all the Trustees**
	Certified Copy of Trust Deeds
	Trustee/ Governing Body Resolution
	Copy of Latest Financials of the Trust

Documentation for Investors who can't sign or have unsuitable signatures

Investors who cannot sign or have unstable signatures shall be required to submit two recent passport size photographs and Thumb impression on the Account Opening form attested by the Branch Manager of the Bank where the investor maintains an account.

Sending Account Statement

After opening of a new account, the Transfer Agent sends an Account Statement to the investor through a registered post/ courier on his/her postal address in order to notify the investor of their account status and to confirm the address of the investor.

Steps for Enhanced Due Diligence

Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions and implementing suspicious activity monitoring system that reduces the Pine reputation, compliance, and transaction risks.
Pine determines if a customer possess a higher risk because of the customer's business activity, ownership structure, anticipated or actual volume and types of transactions, including those transactions involving higher risk jurisdictions.

I. Request for further documentation/ Information
II. Review of the documents/ Information
III. Approval for Account opening of the higher risk customers.

When the Pine is not able to satisfactorily complete required CDD/KYC measures, account opening applications are rejected; business relationships are not established/ terminated and business transaction are not carried out.

MONITORING AND REPORTING OF SUSPICIOUS TRANSACTION/ACTIVITY

In case where the Pine is not able to satisfactorily complete required CDD/KYC measures, accounts are not opened; business relationships are not established/ terminated and business transaction are not carried out. Instead reporting of suspicious transaction may be considered as outlined later in this document.

All personnel are diligent in monitoring for any unusual or suspicious transactions/activity based on the relevant criteria applicable.

Suspicious Transactions

The following are examples of potential suspicious transactions for both money laundering and terrorist financing. The lists of situations given below are intended mainly as a means of highlighting the basic ways in which money may be laundered. These lists are not all-inclusive

While each situation may not be sufficient to suggest that money laundering or a criminal activity is taking place, a combination of such situations may be indicative of such a transaction. A customer's declaration regarding the background of such transaction shall be checked for plausibility. Closer scrutiny shall help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

It is justifiable to suspect any customer who is reluctant to provide normal information and documents required routinely by the financial institutions in the course of the business relationship. The Pine will pay attention to customers who provide minimal, false or misleading information or, when applying to open an account, provide information that is difficult or expensive to verify.

I. Transaction which do not make economical sense
II. Transaction inconsistent with the customer's business
III. Transactions involving transfers to and from abroad
IV. Transactions involving structuring to avoid reporting or identification requirement

Potential Indicators of Money Laundering/Terrorist Financing

The following examples of potentially suspicious activity that may involve money laundering or terrorist financing threat are primarily based on guidance note provided by the FATF in the name of "Guidance for Financial Institutions in Detecting Terrorist Financing". FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

I. Activities inconsistent with the customer business
II. Fund Transfers
III. Other transactions that appears unusual or suspicious

Reporting of Suspicious Transaction

It is a Policy of Pine:

- To remain vigilant on unusual or suspicious transactions or other activities that appear not to make good business or economic sense, or activities that appear to be inconsistent with the given profile of the customer, including activities that may be indicative of criminal conduct, terrorism or corruption.
- To act competently and honestly when assessing information and circumstances that might give reasonable grounds to suspect Money Laundering (ML) or Terror Financing(TF).
- To co-operate with law enforcement authorities in investigations concerning possible ML or TF within the confines of applicable laws.
- Not to alert or provide any information to any person regarding suspicion or inquiry on his or her account or transactional activities or any indication of being reported to the Regulators.

Training

Training on anti-money laundering is provided to those new employees who work directly with customers and to those employees who work in other areas that may be exposed to money laundering and terrorist financing threats. Follow-up trainings also take place once a year.

Non Compliance with PINE'S AML/CDD/CFT Policy

Failure to abide by the Policy set by Pine to prevent money laundering and terrorist financing will be treated as a disciplinary issue. Any deliberate breach will be viewed as severe misconduct. Such cases will be referred to HR for onward initiation of disciplinary action that could lead to termination of employment and could also result in criminal prosecution and imprisonment for the concerned staff member

RECORD RETENTION

It is policy of Pine:

- To retain identification and transaction documentation for the minimum period as required by applicable Laws and Regulations.
- To retain records of all suspicious activity reports made by Compliance department to Regulators for an indefinite period unless advised by the Regulator otherwise.
- To be in a position to retrieve, in a timely fashion, records that are required by law enforcement agencies as part of their investigations.

To keep records of KYC, CDD, AML/CFT training provided to the employees, nature of the training and the names of staff who received such training.

ACCOUNTABILITIES AND RESPONSIBILITIES

The Board is Responsible for:

- Ensuring that adequate systems and controls are in place to deter and recognize criminal activity, money laundering and terrorist financing.
- Seeking compliance reports including coverage of AML/CFT issues) on quarterly basis and taking necessary decisions required to protect Pine from use by criminals for ML & TF activities.
- The Oversight of the adequacy of systems and controls that are in place to deter and recognize criminal activity, money laundering and terrorist financing.

Management is Responsible for:

- Ensuring that AML/CDD/CFT policy is implemented in letter and spirit.

All Employees Are Responsible for:

- Remaining vigilant to the possibility of money laundering / terrorist financing through use of Pine's products and services.
- Complying with all AML/CFT policies and procedures in respect of customer identification, account monitoring, record keeping and reporting.
- Promptly reporting to CO where they have knowledge or grounds to suspect a criminal activity or where they have suspicion of money laundering or terrorist financing whether or not they are engaged in AML / CFT monitoring activities.
- Understanding Pine's Policy and Procedures on AML/CDD/CFT and to sign-off on the require Form.
- Employees who violate any of the Regulations or the Pine's AML/CDD/CFT policies and procedures will be subject to disciplinary action.

Risk Assessment and Applying a Risk Based Approach

(Please refer to Annex 1 for Risk Assessment Tables)

Risk Assessment and Applying a Risk Based Approach

- **Pine** will develop an appropriate Risk Based Approach ('RBA') and apply the RBA on a group-wide basis, where appropriate. As a part of the RBA, Pine shall:
    - Identify ML/TF risks relevant to them;
    - Assess ML/TF risks in relation to-
        - Customers (including beneficial owners);
        - Country or geographic area in which its customers reside or operate and where the Pine operates;
        - Products, services and transactions that Pine offers; and
        - Delivery channels.
    - Design and implement policies, controls and procedures approved by its Board of Directors;
    - Monitor and evaluate the implementation of mitigating controls;
    - Keep their risk assessments current through ongoing reviews;
    - Document the RBA including implementation and monitoring procedures and updates to the RBA; and
    - Have appropriate mechanisms to provide risk assessment information to the Commission.

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

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

- The process of ML/TF risk assessment has four stages:
    - Identifying the area of the business operations susceptible to ML/TF;
    - Conducting an analysis in order to assess the likelihood and impact of ML/TF;
    - Managing the risks; and
    - Regular monitoring and review of those risks.

Identification, Assessment and Understanding Risks

- The first step in assessing ML/TF risk is to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels. Depending on the specificity of the operations, other categories could be considered to identify all segments for which ML/TF risk may emerge. The significance of different risk categories may vary from institution to institution, i.e. Pine may decide that some risk categories are more important to it than others.
- In the second stage, the ML/TF risks that can be encountered by Pine 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 Pine 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 client so that the conclusion on the total risk level must be based on the relevant information available.
- For the analysis, Pine will 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, moderate if it can occur two to three per year and low if it is unlikely, but not possible. In assessing the impact, Pine will, 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 low if there is only short-term or there are low-cost consequences, to high when there is cost inducing long-term consequences, affecting the proper functioning of the institution.
- The following is an example of a likelihood scale with 3 risk ratings as an example.

Likelihood Scale			
Consequence Scale	***Low***	***Moderate***	***High***
Almost Certain	Moderate	Moderate	High
Possible	Moderate	Moderate	High
Unlikely	Low	Moderate	Moderate

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

    - How likely an event is;
    - Consequence of that event;
    - Vulnerability, threat and impact;

- The effect of uncertainty on an event;

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

Risk Assessment (lower complexity)

In line with this guidance, Pine may assess risk by only considering the likelihood of ML/TF activity. This assessment will involve considering each risk factor that have been identified, combined with business experience and information published by the Commission and international organizations such as the FATF. The likelihood rating could correspond to:

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

Risk Assessment (moderate complexity)

If Pine has identified that one of its products is vulnerable to ML/TF and Pine assesses that the likelihood of this product being used in ML/TF activity is probable and Pine judge the impact of the identified risk happening in terms of financial loss then the consequence is assessed as moderate.

Cross-referencing possible with moderate risk results in a final inherent risk rating of moderate. The program should then address this moderate risk with appropriate control measures. Pine will undertake this exercise with each of the identified risks.

Risk Assessment (higher complexity)

Pine could assess risk likelihood in terms of threat and vulnerability. If Pine consider domestic tax evasion criminals as the threat, and accounts dealing with cash payments as the vulnerability, then depending on the risk assessment method this could result in an inherent risk rating of almost certain. Pine may then assess the impact of this event on the business and the wider environment.
Determining the impact of ML/TF activity can be challenging but can also help focus AML/CFT resources in a more effective and targeted manner. When determining impact, Pine may consider a number of factors, including:

- Nature and size of business (domestic and international);
- Economic impact and financial repercussions;
- Potential financial and reputational consequences;
- Terrorism-related impacts;
- Wider criminal activity and social harm;
- Political impact;
- Negative media.

Applying the Risk Assessment

The risk assessment should help rank and prioritize risks and provide a framework to manage those risks.
The assessment should help in determining suspicion and consequently assist in the decision to submit an STR to the FMU. Pine will submit an STR to the FMU if it thinks activities or transactions are suspicious. For instance, RPs may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and submit an STR.

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

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

New and Developing Technologies and Products

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

Material Changes and Risk Assessment

The risk assessment should adapt when there is a material change in the nature and purpose of the business or relationship with a customer. A material change could present an increase, or decrease, in ML/TF risk.
Material change could include circumstances where Pine introduce new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when Pine start using new methods of delivering services or have new corporate or organizational structures. It could result from deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, Pine may refresh the risk assessment.

Pine will document their risk assessment in order to be able to demonstrate their allocation of compliance resources. An effective risk assessment is an ongoing process. Risk levels may change as new products are offered, as new markets are entered, as high-risk customers open or close accounts, or as the products, services, policies, and procedures change. Pine will therefore update its risk assessment every 12 to 18 months to take account of these changes. Pine will also have appropriate mechanisms to provide risk assessment information to the Commission, if required.

Risk Classification Factors

Below are some examples that can be helpful indicators of risk factors/indicators that may be considered while assessing the ML/TF risks for different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

High-Risk Classification Factors

Customer risk factors:

Pine 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 Pine 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:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the RP and the customer).
- Non-resident customers.
- Legal persons or arrangements
- Companies that have nominee shareholders.
- Business that is cash-intensive.
- 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;
- Politically exposed persons
- shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
- trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
- Requested/Applied quantum of business does not match with the profile/particulars of client

- real estate dealers,
- dealers in precious metal and stones, and
- lawyers/notaries

Scenarios of Customer Types

Small and Medium Sized Enterprises:

Small and medium business enterprise customers usually entail domestic companies with simple ownership structures. Most of these businesses deal with cash and multiple persons that can act on its behalf. The likelihood that funds deposited are from an illegitimate source is HIGH, since it can't be easily be identified and can have a major impact on a large number of SME customers. Thus, the risk assessment and risk rating result is HIGH.

International corporations:

International corporate customers have complex ownership structures with foreign beneficial ownership (often). Although there are only a few of those customers, it is often the case that most are located in offshore locations. The likelihood of Money Laundering is High because of the limited number of customers of this type and the beneficial ownership could be questionable, with two criteria that in this scenario result in a possible risk impact of moderate and a moderate risk assessment.

These descriptions will be analyzed as per bellow table:

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

Note: The above risk analysis is a general one for types or categories of customers. It is the starting point for the risk classification of an individual customer. Based on the circumstances of an individual customer, such as its background or information provided, the risk classification of an individual customer can be adjusted. Based on that individual risk classification, customer due diligence measures would be applied.

Country or geographic risk factors:

Country or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer.

The factors that may indicate a high risk are as follow:

- 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.
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- 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.
- Jurisdictions in which the customer and beneficial owner are based;
- Jurisdictions that are the customer's and beneficial owner's main places of business.

Product, service, transaction or delivery channel risk factors:

A comprehensive ML/TF risk assessment must take into account the potential risks arising from the products, services, and transactions that the Pine 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:

- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payments received from unknown or un-associated third parties.
- The surrender of single premium life products or other investment-linked insurance products with a surrender value.
- International transactions, or involve high volumes of currency (or currency equivalent) transactions
- New or innovative products or services that are not provided directly by the Pine, but are provided through channels of the institution;
- Products that involve large payment or receipt in cash; and
- One-off transactions.
- To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions.
- Any introducers or intermediaries the firm might use and the nature of their relationship with the RP.
- Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?
- Has the customer been introduced by another part of the same financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk? What has the firm done to satisfy itself that the group entity applies CDD measures?
- Has the customer been introduced by a third party, for example, a Financial Institution that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision? What has the firm done to be satisfied that:
- The third party applies CDD measures and keeps records to standards and that it is supervised for compliance with comparable AML/CFT obligations;

Low Risk Classification Factors

Customer risk factors:

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

Product, service, transaction or delivery channel risk factors:

The product, service, transaction or delivery channel that satisfy the requirement under regulation 11(2) (c) to (g) of the SECP AML/CFT Regulations

Country risk factors:

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

In making a risk assessment, Pine will, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

These descriptions will be analyzed as per below table:

Transaction Type	***Likelihood***	***Impact***	***Risk Analysis***
Intermediaries	High	Moderate	Moderate
Online Transaction	High	High	High

Bank Transfer	Moderate	Moderate	Moderate

Risk Matrix

In assessing the risk of money laundering and terrorism financing, Pine will establish whether all identified categories of risks pose a low, moderate, high or unacceptable risk to the business operations. Pine will review different factors, e.g., number and scope of transactions, geographical location, and nature of the business relationship. In doing so, the Pine will also review the differences in the manner in which the Pine establishes and maintains a business relationship with a customer (e.g., direct contact or non-face-to-face). The geographical risk will be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk.

Pine will use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing. In classifying the risk, the RPs take into account its specificities, may also define additional levels of ML/TF risk.

The development of a risk matrix may include the consideration of a wide range of risk categories, such as the products and services offered by the Pine, the customers to whom the products and services are offered, the Pine's size and organizational structure, etc.

Pine has developed their own risk matrix based on their own risk analysis as per following table:

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

Risk Management

Risk Mitigation

- Pine keep appropriate policies, procedures and controls that enable it to manage and mitigate effectively the inherent risks that they have identified, including the national risks. It will monitor the implementation of those controls and enhance those, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) must be consistent with legal and regulatory requirements.
- The nature and extent of AML/CFT controls will depend on a number of aspects, which include:
    - The nature, scale and complexity of the Pine's business
    - Diversity, including geographical diversity of the Pine's operations
    - Pine's customer, product and activity profile
    - Volume and size of transactions
    - Extent of reliance or dealing through third parties or intermediaries.
- Some of the risk mitigation measures that Pine will 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 Pine 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).

Evaluating Residual Risk and Comparing with the Risk Tolerance

- Subsequent to establishing the risk mitigation measures, Pine will 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 Pine's overall risk tolerance.
- Where the Pine finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high-risks, Pine will enhance the risk mitigation measures that are in place.

NATIONAL RISK ASSESSMENT REPORT ON MONEY LAUNDERING AND TERRORIST FINANCING – 2019

Security Exchange commission of Pakistan has prepared the " Updated National Risk Assessment Report on Money Laundering and Terrorist Financing - 2019", the concerned portion related to Security Brokers is attached as Annexure 5 for reference and record. Complete details about the brokers, clients and matters pertaining to ML & TF are provided in the document.

As directed by SECP, Schedule Reporting on " Updated Internal Risk Assessment" in light of 'National Risk Assessment 2019' and as per attached ' Guidance Note Annexure 6' covering all aspects including transnational TF risk to be submitted as and when require by SECP (Security Market Division).

Complete data would be prepared and updated on schedule basis as per following annexure and forwarded to PSX and SECP as per requirement.

Annexure 1

Preparing AML/CFT Risk Assessment

"Establish KYC-CDD and customer risk profiling prior to Risk Assessment process"

Step 1 – Identify Customer Risk

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

Step 2- Politically Exposed Persons and High Net worth Individuals

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

Step 3 - Identify Risk by Product, Services and Transactions

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

Step 4- Identify Wire Transfer Activity

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

Step 5 – Identify Customer Type by Geographic Location

Types of Customers	Number of Customers	Total Deposits/Value of Trade/Gross Premium
Natural Persons		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the FATF		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions		
Legal Persons		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the FATF		
Of which, non-resident customers from 'High risk Jurisdictions' as identified by the financial institutions		
Total 0.00		0.00

Step 6 - Develop Risk Likelihood Table

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

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

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

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

Annexure 2

AML/CFT Compliance Assessment Checklist

Anti-Money Laundering Compliance Assessment			
Name of the Financial Institution			
Checklist completed by (Name)			
	(Designation)		
Date			
The AML / CFT Self-Assessment Checklist has been designed to provide a structured and comprehensive framework for RFIs and their associated entities to assess compliance with key AML / CFT requirements. RFIs are advised to use this as part of their regular review to monitor their AML/CFT compliance. The frequency and extent of such review should be commensurate with the risks of ML/TF and the size of the firm's business. **Note: *This AML / CFT Self-Assessment Checklist is neither intended to, nor should be construed as, an exhaustive list of all AML/CFT requirements.***			
Sr No.	***Question***	***Yes/No (N/A)***	***If No, provide explanation and plan of action for remediation.***
	(A) AML/CFT Systems		
1	RPs are required to assess their ML / TF risk and then implement appropriate internal policies, procedures and controls to mitigate risks of ML/TF.		
	Have you taken into account the following risk factors when assessing your own ML / TF risk?		
	(a) Product / service risk		
	(b) Delivery / distribution channel risk		
	(c) Customer risk		
	(d) Country risk		
2	RPs are required to have effective controls to ensure proper implementation of AML/CFT policies and procedures		
	Does your AML/CFT systems cover the following controls?		
	(a) Board of Director and Senior management oversight		
	(II) Have you appointed an appropriate staff as a Compliance Officer ('CO') ?		
	(III) Do you ensure that CO is:		
	1. the focal point for the oversight of all activities relating to the prevention and detection of ML/TF		
	2. independent of all operational and business functions as far as practicable within any constraint of size of your institution		
	3. of a sufficient level of seniority and authority within your institution		
	4. provided with regular contact with and direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and the measures against the risks of ML/TF is sufficient and robust		
	5. fully conversant in the statutory and regulatory requirements and ML/TF risks arising from your business		
	6. capable of accessing on a timely basis all required available information to undertake its role		

	7. equipped with sufficient resources, including staff		
	8. overseeing your firm's compliance with the relevant AML requirements in Pakistan and overseas branches and subsidiaries		
	(b) Audit function		
	(I) Have you established an independent audit function?		
	(II) If yes, does the function regularly review the AML/CFT systems to ensure effectiveness?		
	(III) If appropriate, have you sought review assistance from external sources regarding your AML/CFT systems?		
	(c) Staff screening		
	(I) Do you establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees?		
3	RP with overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure an overall compliance with the CDD and record-keeping requirements.		
	Does your firm have overseas branches and subsidiary undertakings?		
	Do you have a group AML/CFT policy to ensure that all overseas branches and subsidiary undertakings have procedures in place to comply with the CDD and record-keeping requirements similar to those set under the AML Regulations?		
	If yes, is such policy well communicated within your group?		
	In the case where your overseas branches or subsidiary undertakings are unable to comply with the above mentioned policy due to local laws' restrictions, have you done the following?		
	(a) inform the SECP of such failure		
	(b) take additional measures to effectively mitigate ML/TF risks faced by them		
	(B) Risk-Based Approach ('RBA')		
4	RPs are required to determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction or service used by that customer.		
	Does your RBA identify and categorize ML/TF risks at the customer level and establish reasonable measures based on risks identified?		
	Do you consider the following risk factors when determining the ML/TF risk rating of customers?		
	(a) Country risk - customers with residence in or connection with the below high-risk jurisdictions		
	(I) countries identified by the FATF as jurisdictions with strategic AML/CFT deficiencies		
	(II) countries subject to sanctions, embargoes or similar measures issued by international authorities		
	(III) countries which are vulnerable to corruption		
	(Iv) countries that are believed to have strong links to terrorist activities		
	(b) Customer risk - customers with the below nature or behaviour might present a higher ML/TF risk		
	(I) the public profile of the customer indicating involvement with, or connection to, politically exposed persons ('PEPs')		
	(II) complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial rationale		

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

	When an individual is identified as a beneficial owner, do you obtain the following identification information?		
	(a) Full name		
	(b) Date of birth		
	(c) Nationality		
	(d) Identity document type and number		
	Do you verify the identity of beneficial owner(s) with reasonable measures, based on its assessment of the ML/TF risks, so that you know who the beneficial owner(s) is?		
7	RPs are required to identify and take reasonable measures to verify the identity of a person who purports to act on behalf of the customer and is authorized to give instructions for the movement of funds or assets.		
	When a person purports to act on behalf of a customer and is authorized to give instructions for the movement of funds or assets, do you obtain the identification information and take reasonable measures to verify the information obtained?		
	Do you obtain the written authorization to verify that the individual purporting to represent the customer is authorized to do so?		
	Do you use a streamlined approach on occasions where difficulties have been encountered in identifying and verifying signatories of individuals being represented to comply with the CDD requirements?		
	If yes, do you perform the following:		
	(a) adopt an RBA to assess whether the customer is a low risk customer and that the streamlined approach is only applicable to these low risk customers		
	(b) obtain a signatory list, recording the names of the account signatories, whose identities and authority to act have been confirmed by a department or person within that customer which is independent to the persons whose identities are being verified		
8	RPs are required to take appropriate steps to verify the genuineness of identification provided if suspicions are raised.		
	In case of suspicions raised in relation to any document in performing CDD, have you taken practical and proportionate steps to establish whether the document offered is genuine, or has been reported as lost or stolen? (e.g. search publicly available information, approach relevant authorities)		
	Have you rejected any documents provided during CDD and considered making a report to the authorities (e.g. FIU, 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 [illegible])		
	(c) verification is completed as soon as reasonably practicable.		
	(d) the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable.		
	Have you adopted appropriate risk management policies and procedures when a customer is permitted to enter into a business relationship prior to verification?		
	If yes, do they include the following?		
	(a) establishing timeframes for the completion of the identity verification measures and that it is carried out as soon as reasonably practicable		
	(b) placing appropriate limits on the number of transactions and type of transactions that can be undertaken pending verification		
	(c) ensuring that funds are not paid out to any third party		
	(d) other relevant policies and procedures		
	When terminating a business relationship where funds or other assets have been received, have you returned the funds or assets to the source (where possible) from which they were received?		
11	RPs are required to keep the customer information up-to-date and relevant.		
	Do you undertake reviews of existing records of customers to ensure that the information obtained for the purposes of complying with the AML requirements are up-to-date and relevant when one of the following trigger events happen?		
	(a) when a significant transaction is to take place		
	(b) when a material change occurs in the way the customer's account is operated		
	(c) when your customer documentation standards change substantially		
	(d) when you are aware that you lack sufficient information about the customer concerned		
	(e) if there are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box		
	Are all high-risk customers subject to a review of their profile?		
12	RPs are required to identify and verify the true and full identity of each natural person by using reliable and independent sources of information.		
	Do you have customers which are natural persons?		
	Do you collect the identification information for customers:		
	(I) Residents		
	(II) Non-residents		
	(III) Non-residents who are not physically present		

	Do you document the information?		
	If yes, please provide a list of acceptable documents that you obtain for verifying residential address (e.g. utility bills or bank statements). For the avoidance of doubt, please note according to the Guideline on AML and CFT that certain types of address verification should not be considered sufficient, e.g. a post office box address, for persons residing in Pakistan or corporate customers registered and/or operating in Pakistan.		
	In cases where customers may not be able to produce verified evidence of residential address have you adopted alternative methods and applied these on a risk sensitive basis?		
	Do you require additional identity information to be provided or verify additional aspects of identity if the customer, or the product or service, is assessed to present a higher ML/TF risk?		
13	**RPs are required to identify and verify the true and full identity of each legal person and trust and its beneficial owners by using reliable and independent sources of information.**		
	Do you have measures to look behind each legal person or trust to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets?		
	Do you fully understand the customer's legal form, structure and ownership, and obtain information on the nature of its business, and reasons for seeking the product or service when the reasons are not obvious?		
14	Corporation		
	Do you have customers which are corporations?		
	Do you obtain the following information and verification documents in relation to a customer which is a corporation?		
	For companies with multiple layers in their ownership structures, do you have an understanding of the ownership and control structure of the company and fully identify the intermediate layers of the company?		
	Do you take further measures, when the ownership structure of the company is dispersed/ complex/multi-layered without an obvious commercial purpose, to verify the identity of the ultimate beneficial owners?		
15	Partnerships and unincorporated bodies		
	Do you have customers which are partnerships or unincorporated bodies?		
	Do you take reasonable measures to verify the identity of the beneficial owners of the partnerships or unincorporated bodies?		
	Do you obtain the information and verification documents in relation to the partnership or unincorporated body?		
	Do you have customers which are in the form of trusts?		

	Do you obtain the information and verification documents to verify the existence, legal form and parties to a trust?		
	Have you taken particular care in relation to trusts created in jurisdictions where there is no or weak money laundering legislation?		
16	RPs may conduct simplified 'Know Your Customer' due diligence ('SDD') process instead of full CDD measures given reasonable grounds to support it. Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing. SDD is a condition where the timing of the actual verification of a particular customer is deferred until such time the entire CDD process is completed, rather than reducing what needs to be obtained, under a risk-based approach.		
	Have you conducted SDD instead of full CDD measures for your customers?		
	Do you refrain from applying SDD when you suspect that the customer, the customer's account or the transaction is involved in ML/TF, or when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying or verifying the customer?		
	Before the application of SDD on any of the customer categories, have you performed checking on whether they meet the criteria of the respective category?		
17	RPs are required, in any situation that by its nature presents a higher risk of ML/TF, to take additional measures to mitigate the risk of ML/TF.		
	Do you take additional measures or enhanced due diligence ('EDD') when the customer presents a higher risk of ML/TF?		
	If yes, do they include the following?		
	(a) obtaining additional information on the customer and updating more regularly the customer profile including the identification data		
	(b) obtaining additional information on the intended nature of the business relationship, the source of wealth and source of funds		
	(c) obtaining the approval of senior management to commence or continue the relationship		
	(d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.		
18	RPs are required to apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview.		
	Do you accept customers that are not physically present for identification purposes to open an account?		
	If yes, have you taken additional measures to compensate for any risk associated with customers not physically present (i.e. face to face) for identification purposes?		
	If yes, do you document such information?		
19	RPs are required to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person ('PEP') and to adopt EDD on PEPs.		

	Do you define what a PEP (foreign and domestic) is in your AML/CFT policies and procedures?		
	Have you established and maintained effective procedures for determining whether a customer or a beneficial owner of a customer is a PEP (foreign and domestic)?		
	If yes, is screening and searches performed to determine if a customer or a beneficial owner of a customer is a PEP? (e.g. through commercially available databases, publicly available sources and internet / media searches etc)		
20	Foreign PEPs		
	Do you conduct EDD at the outset of the business relationship and ongoing monitoring when a foreign PEP is identified or suspected?		
	Have you applied the following EDD measures when you know that a particular customer or beneficial owner is a foreign PEP (for both existing and new business relationships)?		
	(a) obtaining approval from your senior management		
	(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds		
	(c) applying enhanced monitoring to the relationship in accordance with the assessed risks		
21	Domestic PEPs		
	Have you performed a risk assessment for an individual known to be a domestic PEP to determine whether the individual poses a higher risk of ML/TF?		
	If yes and the domestic PEP poses a higher ML/TF risk, have you applied EDD and monitoring specified in question C.40 above?		
	If yes, have you retained a copy of the assessment for related authorities, other authorities and auditors and reviewed the assessment whenever concerns as to the activities of the individual arise?		
	For foreign and domestic PEPs assessed to present a higher risk, are they subject to a minimum of an annual review and ensure the CDD information remains up-to-date and relevant?		
22	RPs have the ultimate responsibility for ensuring CDD requirements are met, even intermediaries were used to perform any part of the CDD measures.		
	Have you used any intermediaries to perform any part of your CDD measures?		
	When intermediaries (not including those in contractual arrangements with the RFI to carry out its CDD function or business relationships, accounts or transactions between RFI for their clients) are relied on to perform any part of the CDD measures, do you obtain written confirmation from the intermediaries that:		
	(a) they agree to perform the role		
	(b) they will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of you upon request.		
	When you use an intermediary, are you satisfied that it has adequate procedures in place to prevent ML/TF?		
	When you use overseas intermediaries, are you satisfied that it:		
	(a) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction		
	(b) has measures in place to ensure compliance with requirements		

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

	(b) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF		
	Do you monitor the following characteristics relating to your customer's activities and transactions?		
	(a) the nature and type of transaction (e.g. abnormal size of frequency)		
	(b) the nature of a series of transactions (e.g. a number of cash deposits)		
	(c) the amount of any transactions, paying particular attention to substantial transactions		
	(d) the geographical origin/destination of a payment or receipt		
	(e) the customer's normal activity or turnover		
	Do you regularly identify if the basis of the business relationship changes for customers when the following occur?		
	(a) new products or services that pose higher risk are entered into		
	(b) new corporate or trust structures are created		
	(c) the stated activity or turnover of a customer changes or increases		
	(d) the nature of transactions change or the volume or size increases		
	(e) if there are other situations, please specify and further elaborate in the text box		
	In the case where the basis of a business relationship changes significantly, do you carry out further CDD procedures to ensure that the ML/TF risk and basis of the relationship are fully understood?		
	Have you established procedures to conduct a review of a business relationship upon the filing of a report to the FMU and do you update the CDD information thereafter?		
27	REs 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 change 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	REs 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 MLRO, 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 MLROs?		
	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		
	(J) 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 3

ML/TF Warning Signs/ Red Flags

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

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 reason.

Annexure 4

Proliferation Financing Warning Signs/Red Alerts

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

(a) customers and transactions associated with countries subject to sanctions;
(b) instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;
(c) customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;
(d) reasonableness of invoiced goods against market value, inconsistency or discrepancies in trade-related documentation.

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

(a) significant withdrawals or deposits of bulk cash that could potentially be used to evade targeted financial sanctions and activity-based financial prohibitions;
(b) opening of banking accounts by DPRK diplomatic personnel, who have been limited to one account each under relevant UNSCRs (including number of bank accounts being held, holding of joint accounts with their family members);
(c) clearing of funds, granting of export credits or guarantees to persons or entities that are associated with trading transactions relating to the DPRK;
(d) providing insurance or re-insurance services to maritime vessels owned, controlled or operated, including through illicit means, by the DPRK or classification services to vessels which there are reasonable grounds to believe were involved in activities, or the transport of items, prohibited by UNSCRs concerning the DPRK, unless the Security Council 1718 Committee determines otherwise on a case-by-case basis;
(e) direct or indirect supply, sale or transfer to the DPRK of any new or used vessels or providing insurance or re-insurance services to vessels owned, controlled, or operated, including through illicit means, by the DPRK, except as approved in advance by the Security Council 1718 Committee on a case-by-case basis; or
(f) the leasing, chartering or provision of crew services to the DPRK without exception, unless the Security Council 1718 Committee approves on a case-by-case basis in advance;38 or
(g) using real property that DPRK owns or leases in Pakistan for any purpose other than diplomatic or consular activities

Annexure 5

Updated National Risk Assessment Report 2019

Securities Market (Medium High Vulnerability).

As of May 31, 2019, the securities sector had a total of 217 active Pakistan Stock Exchange brokers with Rs. 273.198 billion of assets and a total of 66 Active PMEX Pakistan Mercantile Exchange brokers with Rs. 2.243 billion of assets under their custody, as of May 31, 2019. There were 202 CIS with assets under management of Rs. 621.396 billion, 19 Pension Schemes with assets under management of Rs. 26.059 billion, three Private Equity Funds with assets under management of Rs. 6.568 billion and 25 AMCs, investment advisors & private equity companies with assets under management of Rs. 37.166 billion. Thus, the securities market sector holds about 1.48% of the total assets held by financial market sector in Pakistan.

Category	No.
Independent securities broker-dealer (independent brokerage firms) – large	4
Independent securities broker-dealer (independent brokerage firms) – medium/small	192

Securities brokerage subsidiary of large commercial banks	4
Securities brokerage subsidiary of medium/small commercial banks	4
Securities brokerage subsidiary of subsidiary of medium/small Financial Groups other than Banks	13
Large registered investment companies (mutual funds, closed-end funds, unit investment trusts, and private investment funds) (Mutual Funds, Plans and VPS of value Rs. 50 million and above)	313
Medium/small registered investment companies (mutual funds, closed-end funds, unit investment, trusts, and private investment funds) (Mutual Funds, Plans and VPS of value Below 50 million)	20
Large investment/financial advisors (Investment Advisors managing portfolios above Rs. 50 million)	19
Medium/small investment/financial advisors (Investment Advisors managing portfolios below Rs. 50 million)	1
Commodities futures and option broker – dealers, commodity trading advisors, futures commission merchant, futures pool operator – large	12
Commodities futures and option broker – dealers, commodity trading advisors, futures commission merchant, futures pool operator – medium/small	54

Products and Services

There are only four active products currently offered in the Securities Market sector, such as Ready Market, Deliverable Futures Contract, Margin Trading System and Margin Financing. However, that does not prevent it from being used for potential ML/TF purposes. Equity market products could be used to layer or integrate the proceeds of crime, or to transfer value to terrorists, and are therefore vulnerable for ML/TF activities. Currently, there are 558 companies listed on the Pakistan Stock Exchange with a Market Capitalization of Rs. 9,386 billion. Products and services may be categorized based on general characteristics and the degree of ML/TF risk associated with utilization of new payment methods, delivery channels and jurisdiction/geographic locations of customers.

Case studies of product of Securities Market Sector- Ready Market Trade

Individuals, both local and foreign investors, corporate and other entities, including government-owned entities generally trade in the ready market of securities market. For this purpose investors/clients placed their funds with the brokers. The investors can transfer their funds by using online banking and transfer of funds through ATMs. The brokers generate their commission income based on the number of trades executed by them and commission is one source of income of the brokerage house. High net worth individuals (HNWI) and corporate entities normally trade in large volume in bulk quantity and most frequent trading. Major trades are executed through online trading. 72% of total market trades (ready and future) consist of ready market out of which about 53% pertains to online trading. It has been observed that investors specially HNWI are reluctant in providing evidence regarding source of their income relating to funds deposited by them with the brokers. Most of the corporate entities. including private limited companies, partnership companies and sole proprietorship entities, normally do not prepare accounts and financial statements.

Large amounts of money collected from investors in the securities market cannot be completely verified due to constraints in the system.

Customers

PEPs

The securities sector is inherently vulnerable to ML/TF from the 1,562 identified PEPs. Since almost all the payments/receipts in this sector are routed through the banking channels, the proceeds of corruption can be routed through banking channels for investment/placement in the securities sector. Securities brokers not allowed to accept cash of more than Rs 25,000 from any customer, and cash accepted by the securities brokers constitutes less

than 0.05% of total market settlement.

High Net-worth Individuals

There are 5134 High Net Worth customers investing in the securities sector out of around 154,000 customers. These customers may have generated their wealth from multiple sources and regulated persons may not have enough information to identify and verify all sources of funds. The possibility of source of fund resulting from any predicate offence of ML is very likely making the securities sector inherently vulnerable for ML/TF.

Foreign Clients

There are 7,320 non-resident individual customers in Securities out of around 154,000 customers. It is unknown how much money is invested in Pakistani capital markets by these non-residents. However, due to the significant possibility that large amounts of Pakistani criminal proceeds are laundered abroad, it also seems likely that final integration could occur by bringing back such proceeds and investing them in Pakistani assets, including through capital markets. The capital market has a significant portion of foreign investments also due to its high volatility and large returns. The regulator as well as broker have a difficult task to ensure legitimacy of the sources. In view of this, the inherent vulnerability to ML/TF in the securities sector from the foreign clients is assessed as Medium-High.

Geography

99% of branches of securities brokers are centered in Karachi, Islamabad and Lahore. Further, no broker has any branch out of Pakistan. Out of total active and inactive customers following is the region wise distribution of customers i.e. 7199 in KPK, 209 in FATA, 75,649 in Punjab, 109,320 in Sindh, 1454 in Balochistan, 7554 in Islamabad, 112 in Gilgit/Baltistan and 823 in Azad Jammu & Kashmir. Branches alongside porous borders/in different provinces or business through agents/distributors belonging to porous borders pose high vulnerability for ML/TF. The border of Balochistan and KPK has porous borders with Afghanistan and Iran, therefore are highly exposed to geographical vulnerability. These borders are used for smuggling, cash movement, illegal business and border crossing. Customers from high-risk jurisdictions may seek a business relationship with any security broker to potentially use the sector for facilitation in their motives of ML/TF. Customers from jurisdictions identified as high risk by FATF or securities brokers pose higher ML/TF risk for the sector.

Delivery channels

As in any country, delivery channels can increase ML risk in the securities market based on the use of wire transfers, online payment transaction, payment through debit/credit cards, and Internet-based payment systems. There were 432,531 wire transfers amounting to Rs. 356 billion, equal to 9% of the total market settlement, from June 01, 2018 to May 31, 2019, whereas, cash accepted by the securities brokers are less than 0.05% of the total market settlement. The remaining settlement was performed through other **banking channels.**

Annexure 6

Guidance Note

1. Latest data or data as at June 30, 2019 may be used for the assessment.
2. Analysis of ML/TF Threat and vulnerability should be done specifically mentioning Transnational Risk in light of NRA 2019.
3. Data to be considered only in respect of incremental aspects e.g.
    a. Customers categories (e.g. Afghans diaspora) located in High Risk Areas/Jurisdiction (e-g porous borders) identified in NRA 2019

    b. Branches/Agents located in High Risk Jurisdiction and areas as identified in NRA 2019
4. How various types of crimes and their ML ratings will change your existing ratings assigned to various customer types such as;
    a. importer/exporters in view of high risk rating for the smuggling crime,
    b. legal persons, NPOs and DNFBPs etc. in light of the updated risk rating assigned to these in NRA etc.
5. Share the narrative on various threats and vulnerabilities in light of NRA 2019 that impact your Entity and assign risk rating with respect to following parameters;
    a. Customers
    b. Products
    c. Delivery Channels
    d. Geography
6. The subjective analysis must reflect the statistical data.
7. What remedial measures/controls are in place to mitigate the risks with respect to various types of customers and their nature of business.
8. Following minimum contents may be covered in the Internal Risk Assessment Report:
    a. Introduction of the Entity
    b. Methodology for conducting Risk Assessment
    c. Assessment of Crimes mentioned in NRA 2019 with relevance to the customers of the entities
    d. Assessment of TF Threat including;
        i. Entities of Concern and
        ii. Transnational Risk
    e. Assessment of Sectoral Vulnerabilities
        i. Customers
        ii. Products
        iii. Delivery Channel
        iv. Geography
    f. Controls Measures specifically mentioning incremental controls put in place to address the enhanced risks.
    g. Any other matter as may be considered relevant
    h. Conclusion on Overall Risk rating of the Entity