
**ANTI-MONEY LAUNDERING (AML),
COMBATING THE FINANCING OF TERRORISM (CFT), and
COUNTERING PROLIFERATION FINANCING AML (CPF) POLICY
(AML Policy)**

Nael Capital (Pvt) Limited

Effective Date: January 2025

Document Metadata and Version Control	
Effective Date	January 20, 2025
Approval Date	January 20, 2025
Document Type	Policy
Version Number	3.0
Review Frequency	Annual
Status	Adhoc
Applicable Entities	All departments of Nael Capital (Pvt) Limited (NCPL)
Document Sponsor	Compliance Manager
Document Owner	Chief Executive
Key Changes	<p>Key Changes include:</p> <ul style="list-style-type: none">• Inclusion of Clause 30 of AML / CFT Regulations, 2020 issued by SECP on 28th September 2020 in Section: Compliance Program• Renumbering of the sections

Table of Contents

Definition Of Money Laundering and Terrorist Financing	4
Purpose And Scope of AML and CFT Regime	5
Compliance Program.....	5
Duties Of Compliance Officer	5
Correspondent Relationship	7
Customer Due Diligence (CDD)	8
For Natural Persons	8
Beneficial Ownership of Legal Persons and Legal Arrangements.....	9
Identification of Customers that are not physically present	10
Existing Customer	10
If Customer Due Diligence Measures are Not Completed.....	10
On-Going Monitoring	11
Enhanced Customer Due Diligence Measures	12
High Risk Business Relationship	12
High Risk Countries and Territories	12
Complex and Unusual Transactions.....	13
Suspicious Accounts.....	13
Simplified Due Diligence Measures (SDD)	14
General Principles of SDD	14
Category of Low-Risk Customers	14
SDD Measures	14
Politically Exposed Persons (PEP).....	14
Definition Of PEP.....	14
Seeking approval from senior management.....	16
Taking adequate measures to establish source of wealth and source of funds.....	16
Targeted Financial Sanctions	16
Suspicious Transaction Reporting	18
Defining what is a suspicious transaction?	18
How you and your employees/agents will identify suspicious transactions	18

Reporting to Compliance Officer	19
Ongoing Due Diligence and Reporting to Relevant Authority	19
Reporting to Commission and FMU	20
Tipping-off & Reporting	21
Risk Based Assessment (RBA)	21
Record Keeping	23
Internal Controls	24
Compliance Officer and Compliance Function.....	24
Internal Audit Function	24
Employee Screening.....	25
Employee Training	25
Monitoring AML/CFT/CPF Systems and Controls	26

Definition Of Money Laundering and Terrorist Financing

Money Laundering (“**ML**”) and Terrorist Financing (**TF**) are economic crimes that threaten a country’s overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF.

Purpose And Scope of AML and CFT Regime

An effective Anti-Money Laundering and Countering the Financing of Terrorism (**AML/CFT**) regime requires financial institutions to adopt and effectively implement appropriate ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF. AML and CFT Regime is governed under Anti-Money Laundering Act, 2010 (**AML Act**), Anti-Money Laundering Rules, 2008 (**AML Rules**) made under the Anti-Money Laundering Ordinance, 2007 (**AML Ordinance**), Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018 (**SECP AML/CFT Regulations**) made under the Securities and Exchange Commission of Pakistan Act, 1997 (**SECP Act**), upon recommendation of Financial Monitoring Unit (**FMU**) established under AML Act and Guidelines on SECP AML/CFT Regulations issued by SECP in September 2018 and Pakistan National Risk Assessment (**PNRA 2019**) Report on Money Laundering and Terrorist Financing issued in September 2019

Compliance Program

- a) NCPL shall implement the following internal policies, procedures and controls for an effective compliance program.
 - i) compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the Company’s compliance with these Regulations, the AML Act and other directions and guidelines issued under the aforementioned regulations and laws;
 - ii) screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively;
 - iii) an ongoing employee training program; and
 - iv) an independent audit function to test the system

Duties Of Compliance Officer

- a) NCPL shall ensure that the compliance officer:
 - (1) reports directly to the board of directors or chief executive officer or committee
 - (2) has timely access to all customer records and other relevant information which they may require to discharge their functions, as well as any other persons appointed to assist the compliance officer;

- (3) has sufficient resources, including time and support staff
- (4) be responsible for the areas including, but not limited to
 - (a) ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the Company and are effectively implemented;
 - (b) monitoring, reviewing and updating AML/CFT/CPF policies and procedures, of the Company
 - (c) providing assistance in compliance to other departments and branches of the Company
 - (d) timely submission of accurate data/ returns as required under the applicable laws; v. monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
 - (e) ensures regular audits of the AML/CFT/CPF program; vii. maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person (“PEPs”), and requests from Commission, FMU and Law Enforcement Agencies (“LEAs”) particularly in relation to investigations; and
 - (f) responds promptly to requests for information by the SECP/Law enforcement agency. ix. Provides guidance in day-to-day operations of the AML/CFT/CPF policies and procedures
 - (g) Is entrusted with other responsibilities as the company may deem necessary in order to ensure compliance with the regulatory requirements.
- (5) The compliance officer shall also refer all the Rules, Regulations, notices and directives issued by the competent authority along with the policy and procedures and maintain a checklist example of which is given in **Annexure 2 (AML/CFT/CPF Compliance Assessment Checklist)** which can be updated from time to time to ensure effective compliance with the applicable regulatory requirements

Correspondent Relationship

- i) NCPL shall perform the following measures, in addition to other measures prescribed in these regulations, when forming a correspondent relationship
- ii) assess the suitability of the respondent financial institution by taking the following steps
 - (1) gather adequate information about the respondent financial institution to understand fully the nature of the respondent financial institution's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;
 - (2) determine from any available sources the reputation of the respondent financial institution and the quality of supervision over the respondent financial institution, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and
 - (3) assess the respondent financial institution's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent financial institution operates.
- iii) clearly understand and document the respective AML/CFT responsibilities of the financial institution and the respondent financial institution;
- iv) assess the respondent financial institution in the context of sanctions/embargoes and Advisories about risks; and
- v) obtain approval from the financial institutions' senior management before providing correspondent services to a new financial institution.
- b) NCPL shall document the basis for its satisfaction that the requirements of this regulations are met
- c) NCPL shall pay special attention when establishing or continuing correspondent relationship with financial institutions which are located in jurisdictions that have been identified or called for by FATF for inadequate and poor AML/CFT standards in the fight against money laundering and financing of terrorism.
- d) NCPL shall not enter into or continue correspondent relationship with another financial institution that does not have adequate controls against money laundering or terrorism financing activities, is not effectively supervised by the relevant authorities or is a shell financial institution.

Explanation: For the purposes of this regulation the expression "**shell financial institution**" means a financial institution incorporated, formed or established in a country or jurisdiction where the financial institution has no physical presence and which is unaffiliated with a financial group that is subject to effective consolidated supervision.

- e) NCPL shall also take appropriate measures when establishing a Correspondent Relationship, to satisfy itself that its respondent financial institutions do not permit their accounts to be used by shell financial institutions.

Customer Due Diligence (CDD)

- a) The Company shall ensure it take steps to know its customers. No anonymous accounts or accounts in fictitious names shall be kept and or operated. The company shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer. The identity of the customer, beneficial owner /or legal person shall be verified using reliable and independent documents, data and information as set out in **Annexure 5**.

For Natural Persons

- i) The Nael Capital (Pvt.) Limited ("**House**") is required to carry out KYC and anonymous accounts or accounts in fictitious names are, as a policy, not allowed. The House takes the following steps to ensure that its customers are who they purport themselves to be:
 - (1) identify and verify the customers including their beneficial owners;
 - (2) understand the intended nature and purpose of the relationship;
 - (3) know actual ownership; and
 - (4) know control structure of the customer.
- ii) The House conducts ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that transactions being conducted are consistent with:
 - (1) Knowledge of the customer;
 - (2) Assessment of Business and Risk Profiles;
 - (3) Where necessary, the source of funds.
- iii) The House conducts CDD when establishing a business relationship if:
 - (1) There is a suspicion of ML/TF; or
 - (2) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.
- iv) In case of suspicion of ML/TF, the House:
 - (1) Seeks to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and

- (2) File a Suspicious Transaction Reporting (“STR”) with the FMU, in accordance with the requirements under the Law.
- v) The House monitors transactions to determine whether they are linked and restructured into two or more transactions of smaller values to circumvent the applicable threshold.
- vi) The House verifies the identification of a customer using reliable independent source documents, data or information including verification of CNICs from NADRA Verisys/Biometric.
- vii) The House ensures that they understand the purpose and intended nature of the proposed business relationship or transaction.
- viii) The house also verifies whether that authorized person is properly authorized to act on behalf of the customer while conducting CDD on the authorized person(s) using the same standards that are applicable to a customer and ascertaining the reason for such authorization and obtain a copy of the authorization document.
- ix) Assign Risk Rating (risk categorization) as
 - (1) High
 - (2) Medium
 - (3) Low

Beneficial Ownership of Legal Persons and Legal Arrangements

- i) The House identifies and verifies the identity of the customer, and understands the nature of its business, and its ownership and control structure.
- ii) The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold:
 - (1) First, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and
 - (2) Second, to take appropriate steps to mitigate the risks.
- iii) If the House has any reason to believe that an applicant has been refused facilities by another House due to concerns over illicit activities of the customer, it should consider classifying that applicant:
 - (1) as higher-risk and apply enhanced due diligence procedures to the customer and the relationship;
 - (2) filing a STR; and/or
 - (3) not accepting the customer in accordance with its own risk assessments and procedures.
- b) The House accepts copies of the documents for identifying a customer verified by seeing originals during establishing business relationship.

Identification of Customers that are not physically present

- i) The House applies equally effective Customers identification procedures and ongoing monitoring standards for Customers not physically present for identification purposes as for those where the client is available for interview.
- ii) Consequently, there are increased risks and practices must carry out at least one of the following measures to mitigate the risks posed:
 - (1) further verifying the Customer's identity on the basis of documents, data or information referred in Annexure-1 to AML/CFT Regulations, but not previously used for the purposes of verifying the client's identity; and
 - (2) taking supplementary measures to verify the information relating to the client that has been obtained by the practice.

Existing Customer

- i) The Company shall apply CDD requirement to its existing customers on the basis of materiality and risk and should conduct due diligence on existing relations at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.
- ii) For existing customers who opened accounts with old NICs, the company shall ensure that attested copies of identity documents shall be present in the company's record. The Company shall block accounts without identity document (after serving one-month prior notice) for all withdrawals, until the subject regulatory requirement is fulfilled. However, upon submission of attested copy of identity document and verification of the same from NADRA or biometric verification, the block from the accounts shall be removed
- iii) For customers whose accounts are dormant or in-operative, withdrawals shall not be allowed until the account is activated on the request of the customer. For activation, the Company shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfill the regulatory requirements. **Dormant or in-operative account** means the account in which no transaction or activity or financial service has been extended by the regulated person from last three (3) years

If Customer Due Diligence Measures are Not Completed

Where the House is unable to complete and comply with CDD requirements as specified in the Regulations:

- i) **For New Customers:**
 - (1) it shall not open the account
 - (2) commence a business relationship; or

- (3) perform the transactions

ii) For Existing Customers:

- (1) the house shall terminate the relationship
- (2) additionally, the house shall consider making a STR to the FMU

On-Going Monitoring

- a) Once the identification procedures have been completed and the business relationship is established, the company shall monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was operated. The company shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps to keep the due diligence information up-to-date and reviewing/adjusting the risk profiles of the customers, where necessary
- b) Company shall conduct ongoing due diligence on the business relationship, including:
 - i) scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, their business and risk profile, including where necessary, the source of funds. For this purpose, the company shall ensure that client's deposit and net investment may be gauged against their profile (such monitoring serves as enhanced due diligence on pre transaction basis).
 - ii) Obtaining information and examining, as far as possible, the background and purpose of all complex and unusual transactions which have no apparent economic or visible lawful purpose. The background and purpose of these transactions shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required. In addition to the above, customers' profiles should be revised keeping in view the CDD and basis of revision shall be documented.
 - iii) Undertaking reviews of existing records and ensuring that documents, data or information collected for the CDD purposes is kept up-to-date and relevant, particularly for higher risk categories of customers.
 - iv) In addition to the above on-going monitoring measures, the company shall consider updating customer CDD records as a part its periodic reviews (i.e. annually) or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:
 - Material changes to the customer risk profile or changes to the way that the account usually operates;
 - Where it comes to the attention of the company that it lacks sufficient or significant information on that particular customer
 - Where a significant transaction takes place
 - Where there is a significant change in customer documentation standards
 - significant changes in the business relationship.
 - there is a suspicion of ML/T, **Annexure 4** gives some examples of potentially suspicious activities or "red flags" for ML/TF, that will help recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered.
 - New products or services being entered into

- A significant increase in a customer's deposit
- A person has just been designated as a PEP
- The nature, volume or size of transactions changes.

Enhanced Customer Due Diligence Measures

- a) The Company shall apply EDD where a customer presents high risk of ML/TF including but not limited to the following circumstances:
 - i) a. business relationships and transactions with natural and legal persons when the ML/TF risks are higher;
 - ii) business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF;
 - iii) PEPs and their close associates and family members.

High Risk Persons or Transactions

- i) The House performs Enhanced Due Diligence on the following:
 - (1) Persons or transactions involving a country identified as higher risk by FATF;
 - (2) Persons or transactions involving higher risk countries for ML, TF and corruption or subject to international sanctions; and
 - (3) Any other situation representing a higher risk of ML/TF including those that you have identified in your Risk Assessment

High Risk Business Relationship

- i) The House applies enhanced CDD measures for high-risk business relationships include:
 - (1) Obtaining additional information on the applicant/customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.);
 - (2) Updating more regularly the identification data of applicant/customer and beneficial owner;
 - (3) Obtaining additional information on the intended nature of the business relationship;
 - (4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer;
 - (5) Obtaining additional information on the reasons for intended or performed transactions;
 - (6) Obtaining the approval of CEO, Compliance Officer and Head of Sales to commence or continue the business relationship; and
 - (7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

High Risk Countries and Territories

- i) Company should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries. The company shall consult publicly available information to ensure that they are aware of the high-risk countries/territories

including sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions (www.fatf-gafi.org), and Transparency international corruption perception index (www.transparency.org). NCPL consults the following sources but not limited to identify above persons or transactions to be aware of the high-risk countries/territories

- Sanctions list issued by the UN
- National Risk Assessment Report 2019;
- FATF high risk and non-cooperative jurisdictions; and
- FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index.

Complex and Unusual Transactions

- i) The House examines the background and purpose of all complex, unusual large transaction, and all unusual patterns of transactions, that have no apparent economic or lawful purpose and conduct enhanced CDD Measures consistent with the risk identified.

Suspicious Accounts

- i) The house applies enhanced CDD measures on the following accounts:
 - (1) Customers who instruct not to issue any correspondence to the account holder's address;
 - (2) Customers who have 'Hold mail' accounts; and
 - (3) Where the evidence of identity of the account holder is not already in the file.
- ii) Enhanced CDD Measures that could be applied for high-risk business relationships include but are not limited to
 - 1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
 - 2) Updating more regularly the identification data of applicant/customer and beneficial owner
 - 3) Obtaining additional information on the intended nature of the business relationship
 - 4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer
 - 5) Obtaining additional information on the reasons for intended or performed transactions
 - 6) Obtaining the approval of senior management to commence or continue the business relationship as per the format enclosed as **Addendum 3**
 - 7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
 - 8) Monitoring of the net investment of the clients as per **Addendum 4** on monthly basis to also help in identifying any STR

Simplified Due Diligence Measures (SDD)

General Principles of SDD

- i) NCPL conducts SDD in case of lower risks identified by it. However, the House ensures that the low risks it identifies are commensurate with the low risks identified by the country or the Commission. While determining whether to apply SDD, the House will pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity.
- ii) SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.
- iii) Where the risks are low and where there is no suspicion of ML/TF, the law allows the House to rely on third parties for verifying the identity of the applicants and beneficial owners.
- iv) Where House decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

Category of Low-Risk Customers

- i) The House rates a customer as low risk justifying it in writing and low risk Customers may include the following:
 - (1) regulated persons and banks provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements;
 - (2) public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership; and
 - (3) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

SDD Measures

- i) The House applies following Simplified Due Diligence measures on Low-risk Customer:
 - (1) reducing the frequency of customer identification updates;
 - (2) reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold; and
 - (3) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established

Politically Exposed Persons (PEP)

Definition Of PEP

- i) A Politically Exposed Person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is, or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be

abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption, bribery, and conducting activity related to terrorist financing (TF). The potential risks associated with PEPs justify the application of additional anti-money laundering/counter-terrorist financing (AML/CFT) preventative measures with respect to business relationships with PEPs.

- ii) Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose the company to significant reputational and/or legal risk. Such persons, commonly referred to as 'politically exposed persons' (PEPs) includes heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates

Politically Exposed Persons Categories

- i) The difference between foreign and domestic PEPs may be relevant for making specific risk assessments to help gain a holistic view of potential risk. In the first instance PEPs are classified at a high level in the following categories:

Foreign PEPs

Individuals who are, or have been entrusted with prominent public functions by a foreign country, for example heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Domestic PEPs

Individuals who are, or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, and senior executives of state-owned corporations, important political party officials.

International Organization PEPs

A person who is, or has been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions i.e., directors, deputy directors, and members of the board.

Family Members

Individuals who are related to a PEP, either directly (consanguinity) or through marriage.

Close Associates

- (a) Individuals who are closely connected to a PEP, either socially or professionally or have joint beneficial ownership of a legal person or
- (b) legal arrangement or any other close business relations with a PEP;
- (c) any individual(s) who have beneficial ownership of a legal person or a legal arrangement which is known to have been set up for the benefit of a PEP

- (d) an individual who is reasonably known to be closely connected with the PEP for any other reason, including socially or professionally

Seeking approval from senior management

- i) The House shall obtain CEO, CO and/or Head of Sales' approval (refer **Addendum 3**) to determine the nature and extend of EDD where the ML/TF risks are high. In assessing the ML/TF risk of a PEP, the Houses shall consider factors such as whether the Customer who is a PEP:
 - (1) is from a high-risk country;
 - (2) has prominent public function in sectors know to be exposed to corruption;
 - (3) has business interests that can cause conflict of interests (with the position held)

Taking adequate measures to establish source of wealth and source of funds

- i) The House consider following red flags (in addition to the Red Flags considered for other applicants):
 - (1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
 - (2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
 - (3) A PEP uses multiple bank accounts for no apparent commercial or other reason;
 - (4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.
- ii) The House shall take a risk-based approach in determining whether to continue to consider a customer as PEP who is no longer a PEP. The factors that they should consider include:
 - (1) the level of (informal) influence that the individual could still exercise; and
 - (2) Whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).
- iii) Additionally, where appropriate, House shall consider filing a STR.

Targeted Financial Sanctions

- a) The company shall undertake TFS obligations under the United Nations (Security Council) Act 1948 and/or Anti-Terrorism Act 1997 and any other relevant regulations prescribed the Government of Pakistan or its designated functions thereafter.
- b) The company shall have mechanisms, processes and procedures in an automated manner for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with the stated designated/proscribed persons in the SROs and notifications issued by MoFA, under United Nations (Security Council) Act 1948 or intimation from NACTA/ Law Enforcement Agencies/ Home Departments of Provinces/Ministry of Interior regarding additions, deletions and updates in list/SRO under the Anti- Terrorism Act, 1997.

- c) If during the process of screening or monitoring of customers or potential customers the company finds a positive or potential match, it shall immediately
 - i) Freeze the relevant funds and assets without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer in accordance with the respective SRO
 - ii) Lodge a STR with the FMU, and simultaneously
 - iii) Prohibit from making any funds or other assets, economic resources, or financial or other related services and funds in accordance with the respective SRO
 - iv) Reject the transaction or attempted transaction or the customer, if the relationship has not commenced. e. Notify SECP and the Ministry of Foreign Affairs in case that person is designated under United Nations Security Council Resolutions or the National Counter Terrorism Authority ("NACTA") in case that person is Proscribed under the Anti-Terrorism Act, 1997.
- d) The Company is also required to screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list
- e) The House must make their Targeted Financial Sanctions (TFS) compliance program an integral part of their overall AML/CFT compliance program, and accordingly should have policies, procedures, systems and controls in place with respect to sanctions compliance.
- f) The House must track all the applicable sanctions and where the sanction lists are updated, shall ensure that existing customers are not listed. The Consolidated lists available at NACTA, MoFA and the UNSC Sanctions Committees' websites.
- g) The company shall implement any other obligation under the AML Act 2010, United Nations (Security Council) Act 1948 and Anti-Terrorism Act 1997 and any regulations made there under
- h) Compliance report on Statutory Regulatory Orders issued by the Ministry of Foreign Affairs under United Nations (Security Council) Act, 1948 or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/Home Departments of Provinces/Ministry of Interior regarding updates in the list of proscribed person(s)/entity(ies) under the Anti-Terrorism Act, 1997, shall be submitted to the Commission within forty eight (48) hours of receiving the same in the manner as may be instructed from time to time by the Commission
- i) The Company shall comply with the requirements of Red Flags/ indicators for identification of persons or entities suspected to be acting on behalf of or at the direction of designated/proscribed individuals or entities as detailed in **Annexure 4**
- j) The Company is prohibited, on an ongoing basis, from providing any financial services to proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed designated name or with a different name. The company shall monitor its business relationships with the entities and individuals on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the Company shall take immediate action as per law, including reporting to the FMU.

Explanation: Associates means persons and entities acting on behalf of, or at the direction, or for the benefit, of proscribed/ designated entities and individuals that may be determined on the basis of appropriate screening of sanctions lists, disclosed nominee/beneficiary information,

publicly known information, Government or regulatory sources or reliable media information, etc.

- k) the sanctions compliance program shall be an integral part of the overall AML/CFT/CPF compliance program
- l) NCPL shall document and record all the actions that have been taken to comply with the sanctions regime, and the rationale for each such action
- m) NCPL shall keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed. The Company shall maintain list of all SROs as per format given in **Addendum 5**
- n) Results of the screening (manual and or system based) shall be maintained which shall depict the results of the screening. The same shall be reviewed by the compliance officer and reported to the CEO and BODs on immediate basis and monthly basis, respectively. The compliance office shall document the results of the screening with regard to screening performed against - “Al-Qaida and Taliban related entities/individuals mentioned in the UNSC Consolidated List” as per **Addendum 6** and - “proscribed persons/organizations list of UN /NACTA” **Addendum 7**.
- o) The House shall not provide any services to proscribed/ designated entities and individuals or their associated persons as required under the Regulations.
- p) The company shall ensure that while screening the list of clients against the sanctioned list, the client list shall include details including but not to be limited to main account holder, all joint account holders, nominees, majority shareholders of legal clients (excluding listed companies), board of Directors, trustees, authorized signatories, office bearers, etc.

Suspicious Transaction Reporting (STR)

Defining what is a suspicious transaction?

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence.

A suspicious transaction can include one that was attempted.

How you and your employees/agents will identify suspicious transactions

- i) The House may assess the following transactions as suspicious where a transaction is inconsistent in amount, origin, destination, or type with a customer’s know, legitimate business or personal activities;
- ii) The House shall put on enquiry if transaction is considered unusual.
- iii) The House shall pay special attention to the following transactions:
 - (1) All complex transactions;
 - (2) Unusual large transactions; and
 - (3) Unusual pattern of transactions.
 - (4) Which have no apparent economic or visible lawful purpose.
- iv) NCPL should deploy an automated system for transaction monitoring

Reporting to Compliance Officer

Where the enquiries conducted by the House do not provide a satisfactory explanation of the transactions, respective sales agent may consider that there are grounds for suspicion requiring disclosure and escalating the matter to the Compliance Officer.

Ongoing Due Diligence and Reporting to Relevant Authority

- i) NCPL shall conduct enquiries regarding complex, unusual large transaction, and unusual patterns of transactions, their background and document their results properly. He may make such transaction available to relevant authorities upon their request.
- ii) NCPL shall conduct CDD and ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds. The company shall enhance its scrutiny level in the following instances as they may prompt filing of STR
 - (1) There is a suspicion of ML/TF. **Annexure 4** gives some examples of potentially suspicious activities or "red flags" for ML/TF, that will help recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose; or
 - (2) There are doubts as to the veracity or adequacy of the previously obtained customer identification information. The Company shall take steps to ensure that all relevant information is obtained as quickly as possible
 - (3) CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of offences and crimes related to ML/TF, the company should not voluntarily agree to open accounts with such customers. In such situations, the company should file an STR with the FMU and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.
 - (4) there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile
 - (5) NCPL is unable to complete and comply with CDD requirements as specified in this policy. NCPL shall not operate the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the company shall terminate the relationship. Additionally, the company shall consider making a STR to the FMU.
- iii) Activities which should require further enquiry may be recognizable as falling into one or more of the following categories:
 - (1) any unusual financial activity of the Customer in the context of the Customer's own usual activities;
 - (2) any unusual transaction in the course of some usual financial activity;

- (3) any unusually-linked transactions;
 - (4) any unusual method of settlement;
 - (5) any unusual or disadvantageous early redemption of an investment product;
 - (6) any unwillingness to provide the information requested.
- iv) In case of suspicion of ML/TF
- (1) The Company should seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold; and
 - (2) Where the enquiries conducted by the company do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate the matter to the AML/CFT CO and
 - (3) Where a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF that attempted transaction should be reported to the FMU, in accordance with this policy
- v) The basis of deciding whether an STR is being filed or not, shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not
- vi) In addition to reporting the suspicious activity, the company shall ensure that appropriate action is taken to adequately mitigate the risk of the company being used for criminal activities. This may include a review of either the risk classification of the customer or account or of the entire relationship itself. Appropriate action shall be to escalate the matter to CEO to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.
- vii) Where the company files STR with respect to a customer with whom it has an existing business relationship, and if the company considers it appropriate to retain the customer, then the company shall
- (1) substantiate and document the reasons for retaining the customer; and
 - (2) subject the business relationship to proportionate risk mitigation measures, including enhanced ongoing monitoring.

Reporting to Commission and FMU

- (1) NCPL is required to report total number of STRs filed to the Commission on bi-annual basis within seven days of close of each half year.
- (2) Vigilance systems should require the maintenance of a register of all reports made to the FMU. Such registers should contain details of:
 - (a) the date of the report;
 - (b) the person who made the report;
 - (c) the person(s) to whom the report was forwarded; and
 - (d) reference by which supporting evidence is identifiable.

- (3) Where an applicant or a Customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), the House shall consider filing a STR.
- (4) Where an attempted transaction gives rise to knowledge or suspicion of ML/TF, the Securities Broker shall report attempted transaction to the FMU.
- (5) Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity The Securities Broker shall ensure that appropriate action is taken to adequately mitigate its risk being used for criminal activities.
- (6) The House may include a review of either the risk classification of the Customer or account or of the entire relationship itself.
- (7) Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU

Tipping-off & Reporting

- i) The Law prohibits tipping-off
- ii) A risk exists that Customers could be unintentionally tipped off when the House is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF
- iii) The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation
- iv) If the House forms a suspicion of ML/TF while conducting CDD or ongoing CDD, it will take into account the risk of tipping-off when performing the CDD process.
- v) The House reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR.
- vi) The House ensures that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD
 - (1) Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented, and made available to the relevant authorities upon request.
- vii) The company is also obligated to file **Currency Transaction Report (CTR)**, for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above. However, for the sake of clarity, the company shall not accept any cash-based transaction and or any transaction involving wire transfer/fund transfer to and from a foreign jurisdiction.
- viii) If the company decides that a disclosure should be made, the law require the company to report STR promptly (without delay) to the FMU, in standard form as prescribed under AML Regulations 2008. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AML_Regulations-2008.pdf

Risk Based Assessment (RBA)

- a) The House must consider the following guidance material to determine the level of risk involved in relation to customers, products/services, delivery channels and countries/regions:
 - i) Latest National Risk Assessment;

- ii) Sector Risk Assessment guidance by the SECP;
- iii) Any applicable guidance by relevant authorities (such as FMU, SBP, MoFA, NACTA etc.);
- iv) Information and guidance published by international organizations such as the FATF, APG;
- v) Personal business experience in relation to certain risks.
- b) Establish risk categories as high, medium or low based on the result of risk assessment
- c) As part of assessing risk, the House must do risk analysis
- d) Capture any material change in risk as part of ongoing monitoring
- e) Deploy appropriate software which can help identify and mitigate the risk effectively
- f) Complete and Report Enterprise Risk Report to the regulator as and when required by law
- g) The Company should have an adequate Risk Assessment Program.
- h) The company shall maintain **Risk Assessment Tables** (see **Annexure 1**) and AML/CFT/CPF Compliance Assessment Template (see **Annexure 2**) within the period as required by the Commission from time to time. At present the Company shall ensure meticulous compliance with the Commission's S.R.O. 920 (I)/2020 dated; 28 September, 2020
- i) The Company must conduct and document its **RBA**. Conduct and documentation of the assessment results should enable the company to demonstrate
 - i) Risk assessment process including how the Company assesses ML/TF risks
 - ii) Details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment
 - iii) How it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
 - iv) The arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk mitigation systems and control processes.
- j) The Company on the basis of the assessment should be able to provide information to the Commission
- k) The company shall take enhanced measures to manage and mitigate the risks where higher risks are identified. The company may take simplified measures to manage and mitigate risks, if lower risks have been identified. Simplified measures should not be permitted whenever there is a suspicion of ML/TF
- l) It shall be noted that the ML/TF risk assessment is not a one-time exercise and therefore, the company must ensure that ML/TF risk management processes are kept under regular review which is at least annually
- m) The management should identify and assess the ML and TF risk (also review the program's adequacy) that may arise in the development of new products, businesses and practices, including new delivery mechanism, and the use of new and pre-existent technology. Prior to the launch or use of product, practice or technology, shall undertake the risk assessment and take appropriate measures to manage and mitigate the risks
- n) The Company should categorize its own overall entity level risk as high, medium or low based on the result of risk assessment and any other risk assessment publicly available or provided by the Commission
- o) Detailed guidance and requirements of Risk based Assessment is enclosed as **Annexure 3** to this policy

Record Keeping

- a) The House should ensure that all information obtained in the context of CDD is recorded. This includes:
 - i) Documents provided by the client when verifying the identity of the customer or Beneficial Owner
 - ii) Verification of CNIC through NADRA Verisys/ Biometric
 - iii) Transcription into the House's own IT systems of the relevant CDD information
- b) The House should maintain a comprehensive record of AML/CFT reports with respect to internal enquiries and reporting to FMU. Such documentation may include:
 - i) the report itself and all its attached information / documents in copy;
 - ii) the date of the report;
 - iii) the person who made the report and the recipient;
 - iv) any decision based on the STR for the specific customer or a group of customers;
 - v) any updating or additional documentation taken based on the report; and
 - vi) the reasoning underlying the decisions taken
- c) Where transactions, customers or instruments are involved in litigation or where relevant records are required by a court of law or other competent authority, the House will retain such records until such time as the litigation is resolved or until the court of law or competent authority indicates that the records no longer need to be retained.
- d) The House will maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification
- e) The company should ensure that all information obtained in the context of CDD is recorded. This includes both;
 - i) recording the documents the company is provided with when verifying the identity of the customer or the beneficial owner, and
 - ii) Transcription into the company's own IT systems of the relevant CDD information contained in such documents or obtained by other means.
- f) The company shall maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification (refer Addendum 1)
- g) The company shall keep and maintain all record related to STRs and CTRs filed by it for a period of at least 10 years after reporting of transaction.
- h) The company shall maintain, for at least 5 years after termination, all necessary records on transactions (obtained through CDD process including copies of identification documents, account opening forms, Know Your Customer forms, verification documents, other documents and result of any analysis along with records of account files and business correspondence) to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity

Internal Controls

Compliance Officer and Compliance Function

- i) The Compliance Officer must have the authority and ability to oversee the effectiveness of AML/CFT systems. His responsibilities include compliance with applicable AML/CFT legislation, reporting of suspicious and currency transactions, and providing guidance in day-to-day operations of the AML/CFT policies and procedures, including freezing of accounts/funds if subsequently identified on proscribed lists. CO must be a person who is fit and proper to assume the role and who:
 - (1) has sufficient skills and experience to develop and maintain systems and controls (including submitting written policies and procedures for management's approval);
 - (2) reports directly and periodically to the Board of Directors and/or Chief Executive on AML/CFT systems and controls;
 - (3) has sufficient resources and access to all information and data
 - (4) maintains various logs, as necessary, with respect to declined business/rejected transactions, internal investigations, suspicious transaction reports, and freezing or blocking of payments under Sanction Regime;
 - (5) responds promptly to requests for information by the SECP/Law Enforcement Agencies (LEAs)

Internal Audit Function

- i) Have an effective internal audit function to evaluate the effectiveness of compliance with various policies including AML/CFT policies and procedures.
- ii) The frequency of the audit should be at least annual for high-risk activities and every 2 years for low-risk activities.
- iii) The AML/CFT audits should assess:
 - (1) Overall governance structure, including the role, duties and responsibilities of the Compliance Officer/function;
 - (2) Ownership taken by management and board of directors (where applicable), in particular Risk Assessment, Risk Based Approach, AML/CFT related internal enquiries, suspicious transaction reports and regulatory compliance;
 - (3) Integrity and effectiveness of the AML/CFT systems and controls and the adequacy of internal policies and procedures in addressing identified risks, including:
 - (4) CDD measures, monitoring and updating of customer data;
 - (5) Screening process for TFS
 - (6) Testing transactions with emphasis on high-risk customers, geographies, products and services;
 - (7) Record keeping and documentation.
 - (8) The effectiveness and the adequacy of identifying suspicious activity, internal investigations and reporting;
 - (9) The adequacy and effectiveness of training programs and employees' knowledge of the laws, regulations, and policies & procedures.

Employee Screening

- i) NCPL shall should maintain adequate procedures to screen prospective and existing employees to ensure high ethical and professional standards when hiring. The extent of employee screening should be proportionate to the particular risks associated with the individual positions. NCPL shall screen prospective and existing employees to ensure high ethical and professional standards.
- ii) Employee screening should be conducted at the time of recruitment and where a suspicion has arisen as to the conduct of the employee
- iii) Employee screening should be conducted periodically where a suspicion has arisen as to the conduct of the employee. NCPL shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, NCPL should verify:
 - (1) references provided by the prospective employee at the time of recruitment;
 - (2) employee's qualifications, employment history, and professional memberships;
 - (3) details of any regulatory actions or actions taken by a professional body and the existence of any relevant criminal convictions.
 - (4) Periodic screening against Proscribed and Targeted Financial Sanctions or any connections with the sanctioned countries or parties should be done

Employee Training

- i) All concerned staff receive training on ML/TF/PF prevention on a regular basis, at least annually or more frequently where there are changes to the regulatory requirements or where there are significant changes to the RP's business operations or customer base. RP must ensure that all staff fully understand the procedures and need for compliance with the regulations.
- ii) The company shall ensure that all appropriate staff, receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation
- iii) Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes in the company's business operations or customer base.
- iv) The company should provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of the company's risk assessments. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.
- v) Staff should be aware on the AML/CFT/CPF legislation and regulatory requirements, systems and policies. They should know their obligations and liability under the legislation should they fail to report information in accordance with internal procedures and legislation. All staff should be encouraged to provide a prompt and adequate report of any suspicious activities.
- vi) All new employees should be trained on ML/TF and should know the requirement to report, and of their legal obligations in this regard.

- vii) The company shall obtain an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT/CPF matters, read the company's AML/CFT/CPF manuals, policies and procedures, and understand the AML/CFT/CPF obligations under the relevant legislation. Undertaking with regard to the reading and understanding of the company's AML/CFT/CPF manuals, policies and procedures, and understand the AML/CFT/CPF obligations under the relevant legislation shall be obtained as per **Addendum 8**.
- viii) Staff members who deal with the public such as sales persons are the first point of contact with potential money launderers, and their efforts are vital to an organization's effectiveness in combating ML/TF. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers. Training should be given on the factors which may give rise to suspicious about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.
- ix) Staff involved in the processing of transactions should receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances
- x) The Compliance Officer (CO) should receive in-depth training on all aspects of the primary legislation, the Regulations, regulatory guidance and relevant internal policies. They should also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.
 - (1) Record with regard to training obtained from outside the company shall be maintained as per the format given in **Addendum 9**, whereas, record of all internal trainings shall be maintained as per the format given in **Addendum 10**.

Monitoring AML/CFT/CPF Systems and Controls

- a) The Company shall ensure that it maintains programs and systems to prevent, detect and report ML/TF. It shall be the responsibility of the senior management to ensure that appropriate systems are in place to prevent and report ML/TF and that the company is in compliance with the applicable legislative and regulatory obligations and this policy. The management shall utilize Backoffice software as well, to ensure to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. The management shall update the back office as appropriate to suit the change in risks.
- b) The systems should be commensurate to the size of the business and nature of the company and the ML/TF risks to which it is exposed and should include
 - i) Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists
 - ii) procedures to undertake a **Risk Based Approach (RBA)**;

- iii) procedures and controls to combat ML/TF, including appropriate risk management arrangement

ANNEXURES

ANTI-MONEY LAUNDERING (AML), COMBATING THE FINANCING OF TERRORISM (CFT) and COUNTERING PROLIFERATION FINANCING AML (CPF) POLICY


NAEL CAPITAL (PVT) LIMITED (NCPL)

TABLE OF CONTENTS.....	1
A. LIST OF ANNEXURES.....	2
B. ANNEXURE 1: AML/CFT/CPF Risk Assessment.....	2
C. ANNEXURE 2: AML/CFT/CPF Compliance Assessment	2
D. ANNEXURE 3: Risk Based Assessment	3
E. ANNEXURE 4: ML/TF Warning Signs/ Red Flags	18
F. ANNEXURE 5: Identification and Verification of Customer	20

A. LIST OF ANNEXURES

No.	Related Annexures
1	AML/ CFT/CPF Risk Assessment
2	AML/ CFT/CPF Compliance Assessment
3	Risk Based Assessment
4	ML/TF Warning Signs/ Red Flags
5	Identification and Verification of Customer

B. ANNEXURE 1: AML/CFT/CPF RISK ASSESSMENT

S. No	Work Paper	Attachment
1	AML/CFT/CPF Risk Assessment	 ANX 1 - AML CFT RISK ASSESSMENT.xls

C. ANNEXURE 2: AML/CFT/CPF COMPLIANCE ASSESSMENT

S. No	Work Paper	Attachment
1	AML/CFT/CPF Compliance Assessment	 ANX 2 - AML CFT Compliance Assessm

D. ANNEXURE 3: RISK BASED ASSESSMENT

The Company has updated its Risk Based Assessment (“RBA”) document in light of the AML Act, AML Regulations 2020, Notices and Directives of SECP and PSX, the awareness sessions organized and conducted by the frontline Regulator and Apex Regulator and in particular the National Risk Assessment 2023 (“NRA 2023”).

This document addresses the national assessment and overview of the national setting for ML/TF threats and vulnerabilities 2) ML threats 3) TF threats 4) and the Securities Sector vulnerabilities.

Accordingly, the document in turn allows the Company to gauge the risks of ML/TF associated with Securities Sector and its aspects covering geography, delivery channels, customers and product & Services. This further allows the Company to have risk mitigating controls in place.

1. NATIONAL ASSESSMENT AND OVERVIEW OF THE NATIONAL SETTING FOR ML/TF THREATS AND VULNERABILITIES

The inherent vulnerability assessment at national level consisted of an assessment of inherent ML/TF vulnerabilities of Pakistan as a whole (e.g., economy, geography, demographics, social and religious) and its key economic sectors and financial and non-financial products. The porous border, hostile neighborhood, high number of Afghan migrants, the long coastal line, the level of poverty etc. has exposed the country to significant risk of money laundering and terrorist financing.

The inherent ML/TF vulnerabilities were evaluated for various sectors, both financial and non-financial. The inherent ML/TF vulnerabilities were identified for sectors taking into consideration their customers, products and geographical locations. The analysis of the inherent vulnerability specifically looked at the inherent risks associated to legal entities and arrangements and their formation.

The consequences of ML and TF in Pakistan are both evident and serious. The High ML and TF risks in Pakistan can adversely affect the financial and non-financial sectors and the society as a whole. Self-assessment by the private sector entities such as our company will help country in strengthening its AML/CFT/CPF Regime. The Company has therefore updated its AML policy and RBA in light of the findings of the NRA 2023 and has adopted mitigating steps in accordance with the identified ML/TF risks.

Those national characteristics that can be exploited or abused for ML/TF purposes are identified and understood in NRA 2023 with a view to enable and apply effective AML/CFT/CPF measures. In the context of Pakistan, it is important to consider the following when assessing ML/TF risks.

Geography

Pakistan’s geographical landscape and porous borders increase its vulnerability to both ML and TF, heightening in particular Pakistan’s TF risks associated to cash smuggling.

Pakistan’s geographic location emanates some specific money laundering risks that the country is exposed to. Longest borders with arch-rival India to the East (3171 km), Afghanistan to the West (2600 km) and Iran to the Southeast (909km) make Pakistan vulnerable to both ML and TF, as it increases the risks of predicate crimes such as drug and human trafficking, cash couriers and illegal trade/smuggling. Pakistan is a transit country for drugs and precursor chemicals, whereby

originating and destination countries are different, and funds are not necessarily required to be routed through transit routes. Additionally, the 1001 km long coastline remains vulnerable to smuggling and illicit trafficking as scores of trespassers are frequently apprehended.

Afghan Diaspora

As per UNHCR published statistics, Pakistan hosts approximately 1.3 million registered Afghan refugees as of 30th June 2022, of which about 20% fall in the age bracket of 18-59 years. KPK and Balochistan host most refugees (i.e. 52.2% and 24.5% respectively), thus increasing these provinces' ML/TF vulnerability. The erstwhile Federally Administered Tribal Area (FATA) became host to domestic and foreign terrorist organisations that would execute politically motivated terrorist attacks on the general public, the military and paramilitary forces.

Conflict and Terror

Countering Terrorism and Terrorism Financing continues to be the highest priority for Pakistan, and the same has been reflected by way of CTF-centric policies and controls put in place. Pakistan remained the second most impacted country in the region in 2022. The risk of Terrorism and Terrorism financing continues to be of prime importance, considering that the impact of terrorism in the years 2021 and 2022 has increased due to the unstable political situation in Afghanistan.

Demography

There are a large number of Afghan refugees and internally displaced people (IDPs). UNDP ranks Pakistan 150th out of 189 countries in its 2018 Human Development Index. The Multidimensional Poverty Index (MPI) classified nearly 39% of Pakistanis as living in multidimensional poverty. The overall figure masks significant regional variation in poverty incidence, ranging from over 70% in former FATA and Balochistan, to around 30% in Punjab and Azad Jammu and Kashmir. Pakistan has a significant poverty gap between urban (9.3%) and rural (54.6%). There are instances where the same low level of social indicators is exploited by money launderers for identity theft issues.

The population of the border areas of Khyber Pakhtunkhwa and parts of Balochistan are highly mobile, with people moving across borders because of a common history, cultural features, and blood ties. It also creates opportunities for sub-nationalists, hostile agencies, and other problem groups.

Social and Religious Norms

The concept of person to person charity, khairat, sadqa, zakat or helping orphans / widows or religious organization serving Islam stems from Pakistan socio-economic and religious culture. Donations are a principle source of funding for nearly all assessed NPOs in Pakistan create a significant risk including channels for transfer of funds particularly in the transnational context. International reports and open source information suggests that many terrorist organizations derive their funding from licit sources such as donations through fund-raising.

Education

According to the Pakistan Demographics Survey 2020¹, the literacy rate of the population is around 61.38 %. High poverty and low literacy rate make the youth vulnerable to illegal activities, including falling prey to criminal and terrorist groups/organizations.

Economy

The per capita income of Pakistan is around USD 1,660 as of 2022; on that basis, the World Bank classifies Pakistan as a lower-middle-income country. A slow real GDP growth rate impacts employment opportunity for Pakistan's growing young population, making them vulnerable to exploitation for criminal activities. The World Bank estimated that as of 2021, the unemployment rate stood at 4.4% in Pakistan.

Social Media

During the year 2022, the use of the Internet penetrated approximately 51% of Pakistan's total population jumping from 133,900 users in 2000 to 116 million users by July 2022. With increased social media exposure came, the risk of being exploited by fraudsters and propagation of extremist ideologies, including crowdfunding. Further, the enforcement data validates using encrypted Person-to-Person communication apps for illegal MVTs. Due to the excessive use of ghost/fake accounts and virtual private networks (VPNs), it remains challenging for the LEAs to monitor such activities.

Therefore, social media and special applications remain highly vulnerable to both ML/TF risks.

2. ASSESSMENT OF ML THREATS

The assessment of ML threats (As per NRA 2023) included a review of all crimes based on the seriousness and magnitude of the crimes both domestically and internationally, the amount of potential proceeds generated, and the capacity of the criminal actors to launder proceeds (including third party launderers) and the sectors used to launder proceeds, according to ML Threat Intelligence. All the 21 offences designated predicate offences under the FATF Standards were included. The most significant ML threats identified in Pakistan are as follows;

S #	Type of Crime in Pakistan	ML Threat Rating		Domestic or Foreign ML
		2019	2023	
1	Illicit Trafficking in Narcotic Drugs and Psychotropic Substances;	H	H	Foreign
2	Corruption and Bribery (transnational risk)	H	VH	Foreign
3	Smuggling; (Including in Relation to Customs and Excise Duties and Taxes);	H	VH	Both

4	Tax Crimes (Related to Direct Taxes and Indirect Taxes);	H	VH	Both
5	Illegal MVTs/Hawala/Hundi	H	VH	Both
6	Cash Smuggling	H	VH	Both
7	Trafficking in Human Beings and Migrant Smuggling;	MH	H	Both
8	Illicit Arms Trafficking;	MH	M	Domestic
9	Fraud and forgery;	MH	H	Domestic
10	Kidnapping, Illegal Restraint and Hostage-Taking;	MH	M	Foreign
11	Robbery or Theft;	MH	M	Domestic
12	Extortion;	MH	M	Domestic
13	Insider Trading and Market Manipulation	MH	M	Both
14	Cyber Crime	MH	H	Both
15	Sexual Exploitation, Including Sexual Exploitation of Children;	M	L	Both
16	Illicit Trafficking in Stolen and Other Goods	M	L	Both
17	Counterfeiting Currency;	M	L	Domestic
18	Counterfeiting and Piracy of Products;	M	M	Both
19	Murder, Grievous Bodily Injury;	M	L	Domestic
20	Environmental Crime;	ML	M	Both
21	Maritime Piracy;	ML	L	Both

In all cases, proceeds laundered through third countries may round-trip back to Pakistan for integration. The channels through which laundered proceeds are routed are considered to be mostly unauthorized and illegal, namely hawala/hundi and cash couriers. Being criminal activities,

these have also been rated as High threat for ML. Legal channels have also been exploited through Benami Accounts, Trade Based Money Laundering, investments in products which are vulnerable to ML like prize bonds and un-regulated sectors like Real Estate. Proceeds of crimes may take various routes in and/or out of Pakistan.

The above crimes while assessed in the context of Securities Sector helps in identifying the risk rating of the products, geography, delivery channels and customers of the sector. One such analysis is detailed below, which includes the impact of all the Risks rates as high;

S #	Type of Crime in Pakistan	ML Threat Rating	impact on sectoral assessment	
1	Illicit Trafficking in Narcotic Drugs and Psychotropic Substances;	H	Geography	foreign clients, clients from porous border/remote areas of KP and Baluchistan
2	Corruption and Bribery (transnational risk)	VH	customers	PEP /HNWI
3	Smuggling; (Including in Relation to Customs and Excise Duties and Taxes);	VH	customers	importers and exporters (sole proprietorship /companies) / clients from porous border and remote areas of KP & Baluchistan
4	Tax Crimes (Related to Direct Taxes and Indirect Taxes);	VH	customers	Lawyers and notaries
5	Illegal MVTs/Hawala/Hundi	VH	Geography/customers	clients from porous border and remote areas of KP & Baluchistan /importers and exporters (sole proprietorship /companies), PEP
6	Cash Smuggling	H	Geography	clients from porous border and remote areas of KP & Baluchistan
7	Terrorism, Including Terrorist Financing;	VH	customers / Geography	NPOs/NGOs/unregistered charities/ clients from porous border and remote areas of KP & Baluchistan

8	Trafficking in Human Beings and Migrant Smuggling;	H	Geography	clients from porous border/remote areas of KP and Baluchistan
9	Illicit Arms Trafficking;	M	Geography	clients from porous border/remote areas of KP and Baluchistan
10	Kidnapping, Illegal Restraint and Hostage-Taking;	M	Geography	clients from porous border/remote areas of KP and Baluchistan
11	Insider Trading and Market Manipulation	M	Geography /Customers	foreign clients/HNWIs

3. ASSESSMENT OF TF THREATS

Under the WB methodology, the assessment of the TF threats looks primarily at two main factors: the threat based on terrorism, and the threat based on the direction of financial flows, sources, and channels.

Direction of financial flows

The assessment looked at the possible directions of TF flows to determine to what extent the TF threat is primarily internal (generated domestically and used to finance domestic terrorism), external (either generated domestically and used to finance foreign terrorism, or vice versa) or a combination of both. In some instances, the TF may simply pass through Pakistan moving from one foreign jurisdiction to another. It is essential to establish the direction of the flows as this information is needed to determine which CFT controls need to be adopted or strengthened.

Sources

The assessment also aimed at determining the source of TF. It may come from legitimate sources or from the commission of predicate offences.

Channels

In order to assess the level and magnitude of threat that certain sectors, products, or services can be exposed to, the assessment examined which channels are being used, or are suspected of being used, for TF.

Despite some improvements in recent years, Pakistan continues to face significant terrorism and TF threats. Thousands of Pakistani civilians, law enforcement and security forces personnel, and religious minorities have been targeted by various factions of TOs. The sectarian violent extremism and terrorism have also been observed at the national level.

Pakistan also faces significant external security threat since its inception, Pakistan has faced hostility on its eastern border. This phenomenon was aggravated after the War against Terrorism when the western border also got hostile. Pakistan has a highly active western border with fast moving populations across the border because of common history, cultures and blood ties. Demography, sectarian lines and presence of Afghan refugees also aggravated the situation and have given space to terrorist organizations, Hostile Intelligence Agencies (HIAs) and other anti-

State elements in furtherance of their nefarious motives. This resulted in significant drug trafficking, smuggling in all kind and illegal border crossing in particular.

Owing to this geographic situation, Pakistan is facing terrorism and TF threat, emanating from terrorist organizations having footprints in Afghanistan, terrorist organizations having presence in Pakistan like TTP and operating mainly in areas adjacent to Pak-Afghan border areas. Long porous border with Iran and Afghanistan is a major cause of illegal border crossing, cash smuggling, illegal trade, drug trafficking, kidnapping for ransom, extortion and hawala business.

As for the terrorism threat, the TF threat is also domestic and external, as funds are generated both at home and in foreign jurisdictions for funding or otherwise support TOs and terrorist operations within the country.

The presence of **Afghan refugees/ diaspora** in Pakistan also poses a threat from TF perspective. Afghan refugees are perfect vulnerability to exploitation, and thus a risk to serve as conduit of Transnational TF (structured Hawala, P2P Hawala and cash mules).

Collection of funds, as well as the provision of funds (through both formal and informal channels), including through the NPO sector, continue to present a threat for TF.

Based on this information, the TF threat assessment analyses and rates the TF threats from 87 TOs including lone wolf terrorists.

Given below is the summary position of ratings assigned to the TOs posing significant and lower TF threats:

No. of TOs	Risk	Names of Terrorist Organizations (TOs)
4	Very High	TTP, Daesh/ISKP, BLA and MB
8	High	BLF, AQIS, JeM, JuD/FiF, TTA, HQN, JuA and LeT
7	Medium	BRA, UBA, HuA, BNA, SRA, BRAS and BRG
68	Low	68 others

Overall assessment

The overall TF threat was assessed as High when the TF Risk Assessment was completed in 2019. Based on the analysis and assessment of the data during NRA 2023 and the information provided, understanding is developed that the overall TF threat at the country level remains persistent and very significant.

4. ASSESSMENT OF SECURITIES SECTOR VULNERABILITIES

Data analyzed through NRA 2019 confirms no TFS violations have been observed in the securities market sector. The TF screening mechanism in the brokerage industry is based on three tiers. Firstly, all brokers promptly screen their customer database. Secondly, NCCPL, has a database of every market participant, also conducts immediate independent screening of the customer database of all the securities brokers. Thirdly, CDC, which maintains a separate database of all shareholders, also promptly conducts screening against the database of shareholders. Considering that all transactions coming in the securities markets derive from the

banking channel and the primary focus of investors in these markets is an investment in securities of the companies, the securities markets are exposed to a lower TF risk. Further, LEAs and FMU have not found any incident or suspicion of TF being linked with the securities or commodities markets. Therefore, the TF risk for this channel is rated as Low.

To assess the vulnerability of the sector, following aspects of the sector have been taken into account;

- a) Products
- b) Geography
- c) Delivery channel
- d) Customers – Legal
- e) Customers – Natural

a) PRODUCTS

There are only four active products currently offered in the Securities Market sector, such as;

- Ready Market,
- Deliverable Futures Contract,
- Margin Trading System / MFS and
- Securities Lending and Borrowing Products.

Products of the equity market can be 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.

However, the following factors make the products less vulnerable for potential ML/TF purposes;

- Regulatory requirements of conducting CDD (at the time of the account opening and on an ongoing basis)
- Frequent inspections, audits and reviews by the front line Regulator and the apex Regulator
- All the transactions coming to the securities markets is through banking channel (with third party payments restricted) and Securities brokers are not allowed to accept cash of more than Rs 25,000 from any customer.
- Withdrawals from the trading account cannot be made in favor of third party or directly to any foreign jurisdiction.
- The securities markets as per NRA 2023 are exposed to a lower TF threat abuse. Further, LEAs and FMU have so far not found any incident of TF having a link with the securities or commodities markets.

The risks of potential ML/TF associated with the products and services is more reasonably analyzed through other factors such as utilization of new payment methods, delivery channels and jurisdiction/geographic locations of customers.

Taking into account the above factors, the aforementioned products of the securities market pose low ML/TF risk for the sector.

b) GEOGRAPHY

To assess the sector with regard to geography, assessment of the following categories are taken into account;

- Non-resident customers from 'High risk Jurisdictions' as identified by the FATF
- Non-resident customers from 'High risk Jurisdictions' as identified by FI
- Resident customers from 'High risk Jurisdictions' of Pakistan (porous border and remote areas of KP and Baluchistan)

- Non-resident customers from FATF compliant countries

The Securities sector largely has a local footprint. 80% of branches of securities brokers are centred in Karachi, Islamabad and Lahore. Further, no broker has any branch outside Pakistan. Region-wise distribution of total customers comprises 12,596 in KPK, 389 in FATA, 114,440 in Punjab, 141,898 in Sindh, 2,480 in Baluchistan, 11,189 in Islamabad, 309 in Gilgit/Baltistan and 1,636 in Azad Jammu & Kashmir.

Branches alongside porous borders in different provinces or businesses through agents/distributors in such areas constitute a high vulnerability for ML/TF. Approximately 15,465 customers from high-risk jurisdictions pose higher ML/TF risk for the sector.

The total number of non-resident individual investors investing through Roshan Digital Accounts in the market is around 10,000, mostly from the Middle East, the USA and Europe. Foreign corporate clients also invest in Pakistan. The ownership structure of such foreign corporate clients poses a risk to ML in the sector.

In view of the above, following risk categorization has been carried out along with risk mitigation;

GEOGRAPHY	ML/TF Risk	Risk Mitigation
non-resident customers from 'High risk Jurisdictions' as identified by the FATF	High	Client shall not be accepted by the Company
non-resident customers from 'High risk Jurisdictions' as identified by FI	High	
resident customers from 'High risk Jurisdictions' of pakistan (porous border area and remote areas of KP and balochistan)	High	Client shall be accepted only after proper enhanced CDD and approval of the higher management. If the company cannot obtain the requisite documents with regard to CDD, the customer shall not be accepted.
non-resident customers from FATF compliant countries	High	

c) DELIVERY CHANNELS

All customers' on-boarding is carried out face to face, and there is no incidence of anonymity. All the transactions (deposits and withdrawals) with customers' brokerage accounts must be made through banking channels. Securities purchased and sold in the market are kept electronically in the central depository and settled through the NCCPL. All securities being traded in the capital market are kept in the name of the shareholder, and no bearer securities exist. Only a small amount of cash transactions to the extent of PKR 25,000 can be conducted.

Following factors are worth noting during assessment of the delivery channels in securities market;

- Regulatory requirements of conducting CDD (at the time of the account opening and on an ongoing basis)
- All the transactions coming to the securities markets is through banking channel (with third party payments restricted) and Securities brokers are not allowed to accept cash of more than Rs. 25,000 from any customer.
- Withdrawals from the trading account cannot be made in favor of third party or directly to any foreign jurisdiction.
- No remittance is accepted from abroad neither in foreign currency.
- The securities markets as per NRA 2023 are exposed to a lower TF threat abuse. Further, LEAs and FMU have so far not found any incident of TF having a link with the securities or commodities markets.

In view of the above, following risk categorization has been carried out along with its risk mitigation;

DELIVERY CHANNELS	ML/TF Risk	Risk Mitigation
cash based	High	Not accepted by the Company
Remittance received from abroad	High	
Remittance received in foreign currency	High	
Amount received through Domestic Banks	Low	CDD as per policy of the Company

d) CUSTOMERS - LEGAL

The total number of legal persons registered in Pakistan stand at 198,738. Overall, the corporate sector primarily comprises small size, domestic, private limited companies as far as the numbers are concerned. Most of the corporate sector is therefore seen as having in practice a relatively low level of inherent vulnerability – given its small size and a large domestic focus. The ML/TF threats however are very significant in Pakistan overall and there are cases when legal persons have been used for ML/TF.

It is internationally recognized that legal arrangements are inherently vulnerable to ML/TF. Pakistan has a system of trust law and also Waqf both of which can be abused for ML/TF.

ML/TF inherent vulnerability characteristics and assessed inherent vulnerability levels by type of legal persons is given in the below table:

Type of Legal Persons	Vulnerability Characteristics from UBO Concealment	Assessed Ratings
Public companies (including listed and unlisted Companies)	Stock exchange rules require high degree of transparency	Low

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

	activity) or front companies (often in customer service sector)	
Domestic limited liability partnerships	Hybrid construct. Governing rules determined by contract with high degree of freedom in determining ownership and control among members, and exploiting nominees	Medium
Foreign limited liability partnerships	Hybrid construct. Governing rules determined by contract with high degree of freedom in determining ownership and control among members including foreigners, and exploiting Nominees	High
NPOs/NGOs	Explained below	High
Charities	Explained below	High
Waqf	Explained below	Medium
Trust	Explained below	Medium

NPOs

The abuse of NPOs for TF purposes continue to pose a significant threat, both domestically and externally.

Several cases analyzed, confirmed that the sector poses a significant threat of TF abuse.

NPOs can also be misused by TOs: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for TF, including for the purpose of evading asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes.

Overall, a large segment of the NPO sector in Pakistan is seen as having a significant inherent vulnerability for TF. Given the significant TF threats in Pakistan, the overall TF risk is also very significant.

Charities

There are unregistered charities operating without opting for registration or licensing under any of the prevalent regulatory framework. Such customers shall not be accepted by the Company.

Waqf

Waqfs, which are a form of Islamic charitable trusts also operate in Pakistan.

e) CUSTOMERS – NATURAL

PEPs

The securities sector is inherently vulnerable to ML/TF from the 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. PEPs therefore poses higher risk for the sector.

High Net worth Individuals

HNWI 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. Further, 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.

HNWIs therefore poses higher risk for the sector.

Online clients

Online clients are those clients of the company who trade on their behalf themselves and have no interaction with the traders/KAT operators of the Company. Because of no frequent interaction and coordination with the company representatives these clients may anonymous with regard to their trading pattern. Hence risk of these clients is rated High.

Designated Non-Financial Businesses and Professions (DNFBPs)

The DNFBP sector comprises real estate dealers, dealers in precious metals and stones (mostly jewelers), auditors and accountants, lawyers and notaries.

Although the DNFBP sector is largely unregulated and without any formal supervision, the TF threat of the sector appears to be, overall, relatively low.

1. Real estate dealers

Buying property is considered the safest form of investment in Pakistan, and the real estate sector remains one of the most attractive investment hotspots for both resident and non-resident Pakistanis. In the past, the real estate sector has served as a safe way to launder untaxed wealth, and as a major vehicle for laundering criminal proceeds. However, since 2014, considerable efforts have been made to determine fair market valuations for properties located in major cities across Pakistan, and the Finance Act of 2019 requires marking real estate to market for tax purposes. These actions may make the real estate sector a less attractive way to integrate untaxed wealth. The Finance Act of 2019 also prohibits cash transactions of Rupees five million or above, which may make it harder to disguise the amount of funds invested in real estate, or to disguise its origins. Also, the Benami Transactions (prohibition) Act was passed also by Parliament in 2017 to take action against the assets/properties acquired in the name of benamidars (third parties).

Real estate dealers/sector still remain outside the effective oversight of the governmental authorities, whether federal, provincial or local. Even though the attractiveness of using real estate

for ML purposes may have declined due to the aforementioned changes, the lack of any regulation of real estate agents provides space for the inherent risks in that sector.

Real estate dealers pose high inherent vulnerability due to their limited regulatory regime. Bank accounts of these DNFBPs may also serve as an avenue to hide funds of money launderers. The funds in their accounts may possibly come from some of their customers involved in criminal activities.

Accordingly, the inherent ML/TF vulnerability has been assessed as Very High.

2. Dealers in Precious Metals and Stones

Gold is used as investment product for long-term savings. At the same time, gold and jewelry may be used to convert, store and transfer tainted funds. In particular, high monetary value helps move large value with significantly smaller quantity of precious metals and stones compared with cash. Most of the trade of gold, precious stones and other jewelry is conducted on cash basis, which makes this sector more vulnerable to ML/TF. Large transactions are carried out on a cash basis mostly with walk-in customers.

Jewelers pose high inherent vulnerability due to their limited regulatory regime. Bank accounts of these DNFBPs may also serve as an avenue to hide funds of money launderers. The funds in their accounts may possibly come from some of their customers involved in criminal activities.

Overall, the inherent ML/TF vulnerability has been assessed as high.

3. Accountants, Auditors and Tax Advisors

The accountancy, audit and tax advisory professions comprise both regulated and unregulated professionals.

Auditors in Pakistan do not generally provide these services, which are most relevant as DNFBP:

- manage client money, securities or other assets;
- manage bank, savings or securities accounts;
- organize contributions for the creation, operation, or management of companies;
- create, operate, or manage of legal persons or arrangements, and buying and selling of business entities

ICAP is a statutory body for the regulation of the profession of accountancy in Pakistan and is primarily responsible for maintaining professional standards of excellence amongst chartered accountants.

The inherent ML/TF vulnerability for this sector is medium as the members of ICAP, ICMAP, CIMA, ACCA and ICAEW are required to comply with the code of ethics.

Overall, the inherent ML/TF vulnerability has been assessed as Low.

4. Lawyers and notaries

The involvement of lawyers in the incidences of ML/TF in Pakistan have remained insignificant. Based on the contextual factors, significance of their role in providing advice to the other sectors and issuances of Government stamp papers the inherent ML/TF vulnerability of lawyers and notaries is Low.

Summary of ML/TF vulnerability of DNFBP is given below;

DNFBP	ML/TF Risk
Real Estate Dealers	Very High
Lawyers & Notaries	Low
Dealers in precious metals and stones (n.a)	High
Auditors and accountants (591)	Low

Other Natural customers

Summary of ML/TF vulnerability of other natural persons is given below;

Other Natural customers	ML/TF Risk
Individuals-Service /Profession	Low
Sole Proprietor Business (NW above 500k)	High
Sole Proprietor Business (NW below 500k)	Medium
Sole Proprietor Business (dormant)	Low
employees	Low
Students (Net worth Above Rs. 50k)	High
Students (Net worth Below Rs. 200k)	Low
House Hold/House wives (Net worth Above Rs. 500k)	High
House Hold/House wives (Net worth Below Rs. 500k)	Low
Retired Persons	Low
Individual-Agriculturist	Medium

5. ASSESSMENT OF SECURITIES SECTOR VULNERABILITIES

The sector only offers four types of products. More than 80% of branches of securities brokers are centred in big cities (Karachi, Lahore and Islamabad), while no broker has any branch outside

Pakistan. Foreigners and non-resident Pakistanis are allowed to invest in the stocks through a defined mechanism. There is no element of anonymity, and transactions are made through bank accounts. The total number of customers in the sector is 0.16% of the country's total population, with around 1% foreigners and about 7% nonresident Pakistanis. Since the overall clientele base is low, interactions with PEPs and high-risk occupations is also mild. The maximum limit to deal in cash is PKR 25,000 only. Given the inherent characteristics of this sector, along with an individual assessment of the various risk factors in the sector, as described above, the sector's vulnerability to ML/TF risks is assessed as a "Medium".

Moving forward, NRA will be regularly updated every 2 years by the government and it will continue to monitor emerging threats and vulnerabilities in the interim period. The Company will accordingly adjust its RBA, policies and activities as needed to effectively mitigate ML/TF risks. The Company will also ensure that any updates and findings from the NRA shall be incorporated in its RBA so as to ensure it reflects the risks of the sector in an adequate manner and in line with the updated information and to support its ongoing understanding of ML/TF methods.

Furthermore, the Company will ensure that such an assessment shall not be a static exercise, but should rather be on-going in light of the evolving nature of risks due to newly emerging threats and vulnerabilities. In addition, strategies to mitigate will be adjusted to meet evolving risks.

IMPORTANT NOTES AND GUIDANCE TO RBA

- a. Afghan refugees/nationals (even if have obtained Pakistani nationality) shall not be accepted by the company.
- b. The company may maintain centralized database of its RBA as per **Addendum 11**.
- c. The company shall ensure that the risks category assigned to the client in KYC/CDD, **Addendum 11** and the backoffice system match. In case of any discrepancy, the same shall be reported to the compliance officer.
- d. maintain record of transferring clients from one risk category to another risk category
- e. Client from porous border and southern Punjab includes;
 - Porous border of KP; includes all areas of KP except Peshawar city
 - Porous border of Baluchistan; includes all areas of Baluchistan except Quetta city
 - Cities of Southern Punjab; Burewala, Bhakkar, Bahawalnagar, Bahawalpur, Khanewal , Dera Ghazi Khan, Hasilpur, Layyah, Lodhran, Multan, Muzaffargarh, Rahimyar Khan, Rajanpur, Vehari, Ahmed Pur East and Mailsi, etc.

E. ANNEXURE 4: ML/TF WARNING SIGNS/ RED FLAGS

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

1. Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
2. Customers who wish to deal on a large scale but are completely unknown to the broker;
3. Customers who wish to invest or settle using cash;
4. Customers who use a cheque that has been drawn on an account other than their own;
5. Customers who change the settlement details at the last moment;
6. Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
7. Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;

-
8. Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
 9. Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
 10. Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
 11. 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.
 26. Customers who are unknown to the broker and verification of identity / incorporation

The following are some of Red Flags/ indicators for identification of persons or entities suspected to be acting on behalf of or at the direction of designated/proscribed individuals or entities:-

I. The following indicators should be used to identify suspected persons:

- a. A customer appears to have conducted transactions on behalf of or at the direction of a designated/ proscribed individual.
- b. A customer is an office bearer (trustee/ member/ director/ authorized signatory etc.) of a designated/ proscribed entity.
- c. A customer is a business partner of an office bearer (trustee/ member/ director etc.) of a designated/ proscribed entity.

- d. A customer is a close family member of a designated/ proscribed individual who is also suspected to be associated with the business of the designated/ proscribed individual by way of financial or other assistance.
- e. An entity has a designated/ proscribed individual on its board or management.
- f. Unilateral sanctions listing identifies linkage/ association of a customer with a designated/ proscribed individual or entity.
- g. Media (Broadcast/ Print/ Social) news highlights customer's involvement in providing financial or other assistance to designated/ proscribed individual or entity.
- h. Inquiry from law enforcement agency/ intelligence agency indicating linkage of a customer with designated/ proscribed individual or entity.

II. Red Flags based on behavior of an Account Holder associated with proscribed individuals or entities:

- a. A customer has provided the same residential/ office address that matches the known residential/ office address of a designated/ proscribed individual or entity
- b. A customer has provided the same personal contact number that matches the contact number provided earlier by a proscribed/ designated customer
- c. A customer depositing funds in the account of a person or entity listed in an international or foreign jurisdiction's sanctions lists maintained in accordance with UNSC resolution 1373
- d. A customer listed in an international or foreign jurisdiction's sanctions list maintained in accordance with UNSC resolution 1373, is depositing funds in another customer's account.

F. ANNEXURE 5: IDENTIFICATION AND VERIFICATION OF CUSTOMER

S No.	Type of Customer	Information/Documents to be Obtained
1.	Individuals	<p>A copy of any one of the following valid identity documents;</p> <ul style="list-style-type: none"> (i) Computerized National Identity Card (CNIC) issued by NADRA. (ii) National Identity Card for Overseas Pakistani (NICOP/SNICOP) issued by NADRA. (iii) Form-B/Juvenile card/ Child Registration Certificate (CRC) issued by NADRA to children under the age of 18 years. (iv) Pakistan Origin Card (POC) issued by NADRA. (v) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (vi) Proof of Registration (POR) Card issued by NADRA (vii) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only). <p>Detailed Guidance on the type of customers and required documents is detailed in Addendum 12</p>

1(a)	Joint Account	<ul style="list-style-type: none"> (i) Copy of any one of the documents mentioned at Serial No. I; (ii) In the case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them is individual customers of the RP.
2.	Sole proprietorship	<ul style="list-style-type: none"> (i) Copy of identity document as per Sr. No. 1 above of the proprietor. (ii) Attested Copy of registration certificate for registered concerns. (iii) Copy of certificate or proof of membership of trade bodies etc, wherever applicable. (iv) Sales tax registration or NTN, wherever applicable (v) . (vi) Account opening requisition on business letter head. (vii) Registered/ Business address. <p>Detailed Guidance on the type of customers and required documents is detailed in Addendum 12</p>
3.	Partnership	<ul style="list-style-type: none"> (i) Copies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed'. (iii) Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. (iv) Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. (v) Registered/ Business address. (vi) Certificate or proof of membership of trade bodies etc., (if any)
4.	Limited Companies/ Corporations	<ul style="list-style-type: none"> (i) Certified copies of: <ul style="list-style-type: none"> (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; (b) Memorandum and Articles of Association; (c) Certificate of Incorporation; (d) Certificate of Commencement of Business, wherever applicable; Certified copy of Latest 'Form-A/Form-B'. (e) Incorporate Form II in case of newly incorporated company and Form A / Form C whichever is applicable; and Form 29 in already incorporated companies

7.	NGOs/NPOs/Charities	<p>(i) Certified copies of:</p> <p>(a) Registration documents/certificate</p> <p>(b) By-laws/Rules & Regulations</p> <p>(ii) Resolution Governing Body/Board of Trustees/Executive, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account.</p> <p>(iii) Copy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.</p> <p>(iv) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.</p> <p>(v) Registered address/ Business address.</p>
8.	Agents	<p>(i) Certified copy of 'Power of Attorney' or 'Agency Agreement'.</p> <p>(ii) Copy of identity document as per Sr. No. 1 above of the agent and principal.</p> <p>(iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person.</p> <p>(iv) Registered/ Business address.</p>
9.	Executors and Administrators	<p>(i) Copy of identity document as per Sr. No. 1 above of the Executor/Administrator.</p> <p>(ii) A certified copy of Letter of Administration or Probate.</p> <p>(iii) Registered address/ Business address.</p>
10.	Minor Accounts	<p>(i) Copy of Form-B, Birth Certificate or Student ID card (as appropriate).</p> <p>(ii) Copy of identity document as per Sr. No. 1 above of the guardian of the minor.</p>

Notes:

- i. For due diligence purposes, at the minimum following information shall also be obtained and recorded on KYC (Know Your Customer)/CDD form or account opening form:
- Full name as per identity document;
 - Father/Spouse Name as per identity document;
 - Mother Maiden Name;
 - Identity document number along with date of issuance and expiry;
 - Existing residential address (if different from CNIC);

-
- f. Contact telephone number(s) and e-mail (as applicable);
 - g. Nationality-Resident/Non-Resident Status
 - h. FATCA/CRS Declaration wherever required;
 - i. Date of birth, place of birth;
 - j. Incorporation or registration number (as applicable);
 - k. Date of incorporation or registration of Legal Person/ Arrangement;
 - l. Registered or business address (as necessary);
 - m. Nature of business, geographies involved and expected type of counter-parties (as applicable);
 - n. Type of account/financial transaction/financial service;
 - o. Profession / Source of Earnings/ Income: Salary, Business, investment income;
 - p. Purpose and intended nature of business relationship;
 - q. Expected monthly turnover (amount and No. of transactions); and
 - r. Normal or expected modes of transactions/ Delivery Channels.
- ii. The Copies of identity documents shall be validated through NADRA verisys or Biometric Verification. The regulated person shall retain copy of NADRA Verisys or Biometric Verification (hard or digitally) as a proof of obtaining identity from customer.
 - iii. In case of a salaried person, in addition to CNIC, a copy of his salary slip or service card or certificate or letter on letter head of the employer will be obtained.
 - iv. In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that regulated person shall obtain copy of obtain copy of renewed CNIC of such customer within 03 months of the opening of account.
 - v. For CNICs which expire during the course of the customer's relationship, regulated person shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, regulated person are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.
 - vi. The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the regulated person.
 - vii. The condition of obtaining Copies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where regulated person should obtain copies of identity documents of only those directors and persons who are authorized to establish and maintain Business Relationship. However, regulated person shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and 'Form 29' and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of copies of identity documents.
 - viii. Government entities accounts shall not be opened in the personal names of a government official. Any account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government.

Explanation: For the purposes of this regulation the expression "Government entities" includes a legal person owned or controlled by a Provincial or Federal Government under Federal, Provincial or local law.