Riaz Ahmed Securities (Pvt) Limited

ANTI MONEY LAUNDERING/TERRORIST FINANCING/ PROLIFERATION FINANCING & KNOW YOUR CUSTOMER INTERNAL CONTROL POLICIES AND PROCEDURES

The KYC & AML/CFT Policy of "RASL' is issued with the aim to ensure the carrying out of activities in compliance with the national legal requirements and the legislation regarding Anti Money Laundering and Terrorism financing, to ensure the observance of the prudential, sound Brokerage House practices and in order to promote high ethical and professional standards and prevent the Brokerage House from being used intentionally or unintentionally in illegal or criminal activities performed by its customers.

Updated & Approved By the Board

27-Oct-23

Table Of Contents

1. Introduction Purpose Goal and Objective

Introduction:

A robust Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime ensures that financial systems and the broader economy are protected from the threats of Money Laundering ("ML"), Terrorist Financing ("TF") and Proliferation Financing ("PF"), thereby strengthening financial sector integrity and contributing to safety and security.

Anti-Money Laundering (AML) policies are essential components of financial institutions and other businesses operating in sectors susceptible to money laundering and financial crimes. The introduction section of an AML policy provides a brief overview of the purpose and significance of the policy. It may highlight the global and national efforts to combat money laundering, emphasizing the organization's commitment to integrity, transparency, and regulatory compliance.

Purpose:

The purpose section outlines the primary objectives and goals of the AML policy. This typically includes:

1. **Prevention of Money Laundering:** The primary goal is to prevent the organization from being used as a vehicle for money laundering activities.
2. **Compliance with Regulatory Requirements:** Ensuring adherence to national and international laws and regulations related to anti-money laundering is a crucial purpose. This includes compliance with standards set by regulatory bodies like the Financial Action Task Force (FATF).
3. **Risk Mitigation:** AML policies aim to identify and mitigate the risks associated with money laundering and terrorist financing. This involves assessing and managing risks related to customers, products, and geographic locations.
4. **Protection of Reputation:** Implementing robust AML measures helps protect the organization's reputation by demonstrating a commitment to ethical business practices and compliance with legal requirements.
5. **Enhanced Due Diligence:** The policy may include provisions for conducting thorough due diligence on customers, especially those deemed to be of higher risk.
6. **Scope:** The scope of the AML policy delineates the range of activities and areas to which the policy applies. It typically includes:

   Applicability to all Business Units: The policy usually applies to all departments. This ensures consistency in implementing AML measures across the entire business.

   Covered Products and Services: The scope identifies the specific products and services that fall under the purview of the AML policy. This may include banking services, insurance, investment products, etc.

   Geographical Coverage: Specifies the geographic locations where the policy is applicable. This is particularly important for organizations with a global presence.

   Customer Categories: Identifies the types of customers covered by the policy. This may include

individual customers, corporate entities, politically exposed persons (PEPs), or other categories.
Employee Coverage: Outlines the extent to which the policy applies to employees, including training requirements and reporting responsibilities.

A well-defined introduction, purpose, and scope set the foundation for an effective AML policy, the organization in its efforts guiding to combat money laundering and fulfil regulatory obligations.

Goal of AML Policy:

The overarching goal of an Anti-Money Laundering (AML) policy is to prevent and detect activities related to money laundering and terrorist financing within an organization. Money laundering involves the process of making illegally-gained proceeds (such as criminal activities or corruption) appear legal by passing them through a complex sequence of banking transfers or commercial transactions. The goal of the AML policy is to safeguard the integrity of the organization, financial system, and broader economy by creating a robust framework that actively combats these illicit activities.

Objectives of AML Policy:

1. **Legal Compliance:** Ensure full compliance with local and international laws and regulations related to anti-money laundering and countering the financing of terrorism. This includes adherence to guidelines set by regulatory bodies such as the Financial Action Task Force (FATF).
2. **Risk Identification and Assessment:** Systematically identify, assess, and understand the risks associated with money laundering and terrorist financing. This involves evaluating risks related to customers, products, services, and geographic locations.
3. **Customer Due Diligence (CDD):** Implement thorough due diligence procedures to understand and verify the identity of customers. This includes assessing the nature of the customer's business, the source of their funds, and monitoring transactions for unusual or suspicious activities.
4. **Transaction Monitoring:** Establish mechanisms for real-time monitoring of transactions to detect patterns or anomalies that may indicate potential money laundering or terrorist financing activities.
5. **Reporting and Record Keeping:** Develop and maintain robust reporting mechanisms for suspicious activities. This involves reporting to relevant authorities when necessary and keeping records of transactions and customer information in accordance with regulatory requirements.
6. **Employee Training and Awareness:** Ensure that all employees are well-trained and aware of the policies and procedures in place to combat money laundering. This includes ongoing training programs to keep staff informed about emerging threats and regulatory changes.
7. **Internal Controls and Processes:** Establish internal controls and processes to mitigate the risk of money laundering effectively. This may involve the use of technology, regular audits, and periodic reviews of AML policies and procedures.
8. **Sanctions Screening:** Implement processes to screen customers against national and international sanctions lists to prevent the provision of services to individuals or entities involved in illegal or sanctioned activities.

9. **Enhanced Due Diligence (EDD):** Apply enhanced due diligence measures for high-risk customers, such as politically exposed persons (PEPs), to obtain a deeper understanding of their financial activities and sources of wealth.
10. **Continuous Improvement:** Regularly review and update the AML policy to reflect changes in the regulatory environment, emerging risks, and advancements in technology. Continuous improvement ensures that the organization's AML framework remains effective and up-to-date.

Adherence to this policy is absolutely fundamental for ensuring that the RASL is fully complied with applicable Money Laundering ("ML"),Terrorist Financing ("TF") and Proliferation Financing ("PF") rules and regulations under the amended (Anti-Money Laundering) Act, 2020.

The RASL is committed to examining its anti-money laundering strategies, goals and objectives on an ongoing basis and maintaining an effective AML Policy for its business.

In case of any clarification contact Compliance Department of RASL at junaidriaz@riazahmedsecurities.com.pk

2. Background-

Financial Action Task Force (FATF)

The FATF is an international task force established in 1989 to develop international standards to combat ML, TF and PF. The FATF published a revised set of 40 Recommendations on AML/CFT measures in 2012, which are being continuously updated. Further information on the FATF is available at http://www.fatf-gafi.org

Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is a FATF Style Regional Body. The APG is an associate member of FATF. It is an international organisation, consisting of 41 member jurisdictions. The APG is focused on ensuring that its members effectively implement the FATF Recommendations against ML, TF and PF. (For further information on the APG, visit: http://www.apgml.org Page 2 of 63 Pakistan is not a member of the FATF, but is a member of the APG. The APG undertook a mutual evaluation of Pakistan in 2019. A copy of the Mutual Evaluation Report of Pakistan 2019 is available at http://www.apgml.org/documents

3. Money Laundering, ML Stages, Terrorist Financing and Proliferation Financing ("PF)

Money laundering

ML is the method by which criminals disguise or attempt to disguise the illegal origins of their wealth and protect their asset bases, so as to avoid the suspicion of law enforcement agencies and prevent leaving a trail of incriminating evidence.

Money is the foremost reason for engaging in any type of criminal activity that generates funds. A predicate offence is the underlying crime that generates the funds to be laundered. The examples of predicate offences include inter-alia corruption, bribery, fraud, forgery, counter feiting, kidnapping and corporate and fiscal offences.

Stages of Money Laundering

Money Laundering Stage 1: Placement in the financial system

Placement is when "dirty money" is introduced into the financial system. This is often done by breaking up large amounts of cash into less conspicuous smaller sums to deposit directly into a bank account or by purchasing monetary instruments such as checks or money orders that are collected and deposited into accounts at other locations.

Other placement methods include:

- Adding illicit cash from a crime to the legitimate takings of a business, particularly those with little or no variable costs
- False invoicing
- Smurfing, where small amounts of money below the AML reporting threshold are inserted into bank accounts or credit cards and used to pay expenses, etc
- Hiding the beneficial owner's identity through trusts and offshore companies
- Taking small amounts of cash below the customs declaration threshold abroad and lodging it in foreign bank accounts before being re-sent

Money Laundering Stage 2: Layering the funds

The **layering stage** is when the launderer moves the money through a series of financial transactions with the goal of making it difficult to trace the original source.

The funds could be channelled through the purchase and sales of investments, a holding company, or simply moved through a series of accounts at banks around the globe. Widely scattered accounts are most likely to be found in jurisdictions that do not cooperate with AML investigations. In some instances, the launderer could disguise the transfers as payments for goods or services or as a private loan to another company, giving them a legitimate appearance.

While the three stages of money laundering also apply to crypto currencies, layering is the **most common entry point for crypto**, as criminals use it alongside the traditional financial system to disguise the origins of their funds.

Layering tactics to look out for:

- Chain-hopping — converting one crypto currency into another and moving from one block chain to another
- Mixing or tumbling — the blending of various transactions across several exchanges, making transactions harder to trace back to a specific exchange, account, or owner

- Cycling —making deposits of fiat currency from one bank, purchasing and selling crypto currency, and then depositing the proceeds into a different bank or account

Money Laundering Stage 3: Integration into the legitimate financial system

The integration stage of money laundering is the final step in the laundering process. This is when the launderer attempts to integrate illicitly obtained funds into the legitimate financial system. To use the funds to buy goods and services without attracting attention from law enforcement or the tax authorities, the criminal may invest in real estate, luxury assets, or business ventures.

They are often content to use payroll and other taxes to make the "washing" more legitimate, accepting a 50% "shrinkage" in the wash as the cost of doing business.

Common Integration tactics include:

- Fake employees – a way of getting the money back out. Usually paid in cash and collected
- Loans – to directors or shareholders, which will never be repaid
- Dividends – paid to shareholders of companies controlled by criminals

Terrorist Financing ("TF")

Terrorist financing refers to the processing of funds to sponsors involved in or those who facilitate terrorist activity. Terrorist individuals/ groups/ organization derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents involved do not always know the illegitimate end of that income.

Proliferation Financing ("PF")

Proliferation Financing (PF) refers to the financial support provided to entities or activities involved in the proliferation of weapons of mass destruction (WMD) and their delivery systems. Unlike traditional forms of financing that may support criminal enterprises or terrorism, proliferation financing specifically targets the funding of activities related to the development, acquisition, or use of WMDs.
The primary concern with proliferation financing is its contribution to the proliferation of weapons that pose a significant threat to global peace and security. The term is often associated with the efforts to curb the spread of nuclear, chemical, and biological weapons, as well as the means to deliver them, such as ballistic missiles.

4.Obligation of the Company in Establishing an Effective AML/CFT Governance and Compliance Regime

It is the obligation of the RASL to establish an effective AML/CFT regime to deter criminals from using the Company as a platform for Money Laundering ("ML"),Terrorist Financing ("TF") and Proliferation Financing ("PF") purposes, and to develop a comprehensive AML, CFT and PF compliance program to comply under the following laws and regulations:

- Anti-Money Laundering Act, 2020 (AMLA);
- SECP AML/CFT Regulations, 2020;
- The United Nations (Security Council) Act 1948 (UNSC Act);
- The Anti-Terrorism Act 1997 (ATA);
- United Nations Security Council (Freezing and Seizure) Order, 2019;
- UNSC Act Statutory Regulatory Orders (UN SROs) by the Ministry of Foreign Affairs;
- Ministry of Interior/National Counter Terrorism Authority (NACTA) Proscribed Organizations under Schedule-1 and Proscribed individuals under Schedule-4 of ATA;
- AML/CFT Sanction Rules 2020;
- Counter Measures for High Risk Jurisdiction Rules, 2020.

5. Internal Controls (Compliance Function, Audit Function, Employee Screening, Ongoing Training Program and Outsourcing

Internal Controls

RASL are expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF/PF risks identified. RASL should establish and maintain internal controls in relation to:

- compliance management arrangements;
- screening procedures to ensure high standards when hiring employees;
- an ongoing employee training program me; and
- an independent audit function to test the system.

Riaz Ahmed Securities should establish the following three lines of defence to combat ML/TF/PF:

First line of defence:

RASL directs the sales force (e.g. front office, customer-facing activity, front-line and mid-line managers, who have day-to-day ownership of management of risks and controls) is the first line of defence. For each decision or approval, they need to determine and ensure that sufficient resources are provided for carrying out policies and procedures related to AML/CFT due diligence.

Second line of defence:

Compliance Officer and Compliance Function 1) Compliance Officer, back office, internal control and risk management functions, the compliance function and human resources or technology are the second line of defence.

As part of second line of defence, the Compliance Officer must have the authority and ability to oversee the effectiveness of RP's 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.

Compliance Officer

To ensure that the RASL's policies and procedures are adhered to, RASL shall designate Compliance Officer.

The RASL is required to appoint a management level officer as compliance officer ("CO"), who shall report directly, and periodically to the Board of Directors ("Board") or to another equivalent executive position or committee. The CO must be a person who is fit and proper to assume the role and who:

- has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
- has sufficient resources, including time and support staff;
- has access to all information necessary to perform the AML/CFT compliance function;
- ensure regular audit of the AML/CFT program;
- maintain various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and request from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigation ; and
- respond promptly to requests for information by the SECP/LEAs or regulator^

Third line of defense:

Internal Audit Function

- On a regular basis the RASL, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit should be commensurate with the RASL's nature, size, complexity, and risks identified during the risk assessments. The AML/CFT audits should assess:
- overall governance structure of the RASL for AML/CFT, including the role, duties and responsibilities of the Compliance Officer/function;
- 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; Page 24 of 63 integrity and effectiveness of the AML/CFT systems and controls and the adequacy of internal policies and procedures in addressing identified risks, including:
- CDD measures, monitoring and updating of customer data;
- Screening process for TFS, and test its functionality;
- testing transactions with emphasis on high–risk customers, geographies, products and services;
- Record keeping and documentation.
- the effectiveness of parameters for automatic alerts and the adequacy of RASL's process of identifying suspicious activity, internal investigations and reporting;
- the adequacy and effectiveness of training programs and employees' knowledge of the laws, regulations, and policies & procedures.

All compliances are checked by the internal auditor on a monthly basis and issue a report. In case of discrepancies/non-compliances observed during audit process, the findings and along with recommendations shall be communicated to the Audit Committee including Compliance Officer;

Internal Auditor shall follow-up their findings and recommendation until their complete rectifications.

Employee Screening

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

Employee screening should be conducted periodically where a suspicion has arisen as to the conduct of the employee. RASL shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, the RP should verify:

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

Employee Training

- RASLs should ensure that all appropriate staff, receive training on ML/TF prevention on a regular basis, ensure that all staff fully understand the procedures and their importance, that they will be committing criminal offences if they contravene the provisions of the legislation.
- Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements
- RASL provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of the RASL's risk assessments. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.
- Staff should be aware on the AML / CFT legislation and regulatory requirements, systems and policies.
- All staff should be encouraged to provide a prompt and adequate report of any suspicious activities.
- All new employees should be trained on ML/TF know the legal requirement to report, and of their legal obligations in this regard.
- RASLs shall consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML / CFT matters, read the RASL's AML / CFT manuals, policies and procedures, and understand the AML / CFT obligations under the relevant legislation.

- 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.
- 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.
- All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a customer with a personal account opening a business account
- Although Directors and Senior Managers may not be involved in the handling ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML / CFT policies and procedures.
- Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML / CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.
- The 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.

OUTSOURCING:

- Company will maintain policies and procedures in relation to outsourcing where it intends to outsource some of its functions. The Company will conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the outsourced service provider ("OSP") is fit and proper to perform the activity that is being outsourced. Where the Company decides to enter into an outsourcing arrangement, the Company will ensure that the outsourcing agreement clearly sets out the obligations of both parties.
- The Company while entering into an outsourcing arrangement will develop a contingency plan and a strategy to exit the arrangement in the event that the OSP fails to perform the outsourced activity as agreed. The OSP will report regularly to the Company within the timeframes as agreed upon with the Company.
- The Company will have access to all the information or documents relevant to the outsourced activity maintained by the OSP. The Company as a matter of policy will not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.
- Further, Company will ensure that the outsourcing agreement require OSPs to file a STR with the FMU in case of suspicions arising in the course of performing the outsourced activity.

6. Customer Due Diligence (CDD), Customer Enhance Diligence (EDD), Simplified Due Diligence Measures.

Customer Due Diligence (CDD)

RASL 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.

Conducting CDD

- RASL shall take steps to know who all their customers are. RASL shall not keep anonymous accounts or accounts in fictitious names. RASL shall take steps to ensure that their customers are who they purport themselves to be.
- RASL shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from NADRA Verisys/Biometric. Similarly, RASL shall identify and verify the customer's beneficial owner(s) to ensure that the RP understands who the ultimate beneficial owner is.
- RP must assess each customer's risk to allow for correct application of enhanced due diligence, standard, simplified or special measures for PEPs and other designated categories as per the Regulations. Necessary minimum customer risk rating categories are: (a) High (b) Standard (c) Low
- Standard CDD is likely to apply to most of the customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer. It also includes the verification of that information. For beneficial owners the verification is according to the level of risk involved. Page 8 of 63
- Simplified CDD can only be conducted on a specified set of circumstances such as government departments, local authorities and certain listed companies.
- EDD must be conducted when RP considers that the level of risk involved is such that EDD should apply. EDD requires the collection and verification of the same information as standard CDD as well as, according to the level of risk involved, the collection and verification of information relating to the source of wealth (SoW) and source of funds (SoF) of the customer.
- RASL are entitled to ask customers all relevant CDD questions and may refuse business if the necessary questions are not answered, or the necessary data and documents are not provided.
- If an RP has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report (STR).
- RASL should assess different levels of money laundering/terrorism financing risks posed by their customers' beneficial owners. For example, RASL should consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.
- For complex structures, foreign entities or foreign owned entities, RASL are required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet.

- If RASL form a suspicion of ML/TF/PF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If the RP reasonably believes that performing the CDD or on-going process will tip-off the customer, it may choose not to pursue that process and should file a STR. RASL should ensure that their employees are aware of these issues when conducting CDD or ongoing CDD.

Risk-based implementation of Beneficial Ownership (BO) obligations

- The Beneficial Owner is the natural person at the end of the chain who ultimately owns or controls the customer. BO as per AMLA means:

A. *natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted; or*
B. *natural person who exercises ultimate effective control over a legal person or legal arrangement*

- For the beneficial ownership in the context of natural person, where a natural person seeks to open an account in his/her own name, the RASL should inquire whether such person is acting on his own behalf. However, in relation to student, senior citizens and housewife accounts (where doubt exists that the apparent account holder is acting on his own behalf) the RASL may obtain a self-declaration for source and beneficial ownership of funds from the customer and perform further due diligence measures accordingly.
- For legal persons or arrangements, it is essential to understand the ownership and control structure of the customer. This may be done based on plausibility and records. In any case of lack of transparency or doubt, or higher risk, verification is needed. For legal persons, the primary source for verification of ultimate beneficial ownership is the Register of Ultimate Beneficial Ownership.
- For complex structures, foreign entities or foreign owned entities, RASLs are required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet.
- RASLs may adopt a risk-based approach to the verification of beneficial ownership of a customer. Identifying beneficial ownership of a customer is an obligation that must be satisfied, regardless of the level of risk associated with that Page 9 of 63 customer. However, the reasonable steps to take to verify the identity and information depends upon on the risk assessment of the customer.
- RASLs should assess different levels of money laundering/terrorism financing risks posed by their customers' beneficial owners. For example, RASLs should consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.
- If an RASL has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report to FMU.

Enhanced Due Diligence

- In some higher ML/TF/PF risk or in cases of unusual or suspicious activity an increased level of CDD is required. This includes situations where the RASL consider (based on risk assessment) that the level of risk involved is such that enhanced CDD should apply. In such situations the RASL need to use

increased or more sophisticated measures to obtain and verify customer's details, their beneficial ownership structure and take reasonable steps to do this according to the level of risk involved

- RASL should usually obtain and verify information relating to the source of wealth (SoW) or source of funds (SoF) of your customer. In particular, RASLs should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.
- In case of low risk customer, the regulated person should obtain information of source of income however, no specific evidence is required. In case of high-risk customers, where EDD is required, evidence of source of income may be requested from the customer.
- List of examples of appropriate information and/or supporting documentation required to establish source of wealth and funds is as follows (any one of the documents may be obtained):
- When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations.
- Examples of enhanced CDD measures that could be applied for high-risk business relationships include:
  1. Obtaining additional information, for example, about the volume of assets and information available through public databases, internet, etc. and more regularly updating the identification data of customer and beneficial owner;
  2. Obtaining additional information on the intended nature of the business relationship;
  3. Obtaining information about source of funds or source of wealth of the customer;
  4. Obtaining information on the reasons for intended or performed transactions;
  5. Obtaining approval of senior management to commence or continue the business relationship;
  6. 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.
- However, enhanced CDD could be required again as a result of any material changes in your business relationship with your customer or due to ongoing CDD and account monitoring.
- An insurer/ takaful operator will include the beneficiary of a life insurance policy as a relevant risk factor in determining whether EDD measures are applicable

Simplified Due Diligence Measures

- Under Regulation 23(1), RASL may conduct SDD in case of lower risks identified through adequate analysis and assessment and in line with the latest National Risk Assessment. While determining whether to apply SDD, RPs should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity as mentioned in the latest National Risk Assessment.
- In addition, under Regulation 23(2) the decision to rate a customer as low risk will be justified in writing by the regulated person.
- Simplified measures may include the following measures:
  (a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
  (b) Reducing the degree of on-going monitoring and scrutinizing of transactions;

(c) 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 transactions or business relationship established.

SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF/PF, or the applicant is acting on behalf of a person that is engaged in ML/TF/PF.

Special Cases of Higher Risk and Enhanced Due Diligence

Politically Exposed Persons (PEPs)

- PEPs hold positions of power and influence, thus potentially making them and their close associates more susceptible to corruption. The proceeds of corruption could be routed through the financial sector for the purpose of ML.
- Under Regulation 3(q) of the Regulations 2020 PEPs means an individual who is or has been entrusted with a prominent public function either domestically or by a foreign country, or in an international organization.
- Business relationships with PEPs holding important public positions may expose RP to significant reputational and/or legal risk. In addition, PEPs because of their position, may expose RASL and their business partners to a high degree of public expectation and scrutiny.
- Family members of a PEP spouse of the PEP and lineal descendants and ascendants and siblings of the PEP. Close associates have in many cases been used to provide a cover for the financial activities of a PEP, and may not be in any way connected to the PEP in an official capacity. The CDD done by RASL on the source of funds or source of wealth of a customer may be the first clear documentation of a close association.
- The AML/CFT National Risk Assessment of Pakistan has determined the risk of corruption and therefore the risk of providing financial services to PEPs is high. This means that all domestic PEPs must be scrutinized, particularly for their source of funds wealth and assets.
- In assessing the ML/TF risks of a PEP, the RP shall consider factors such as whether the customer who is a PEP: (a) Has prominent public functions in sectors known to be exposed to corruption; (b) Has business interests that can cause conflict of interests (with the position held); (c) Has been mentioned in media related to illicit financial behaviour; and (d) Is from a high risk country.
- The PEP red flags that the RASL shall consider include: The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
  (a) A family member of a PEP without own financial means is transacting with the RP without declaring the relationship to a PEP, or the origin of the funds transacted;
  (b) The PEP is associated with, or owns, or signs for, complex legal structures that are commonly used to hide Beneficial Ownership;
  (c) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
  (d) A PEP uses multiple bank accounts for no apparent commercial or other reason;

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

- RASL shall take a risk-based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that RASL should consider include:
  (a) the level of (informal) influence that the individual could still exercise; and
  (b) 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, or through continued strong ties within a party, family or institution).
- RASL are encouraged to be vigilant in relation to domestic and foreign PEPs who are seeking to establish business relationships. RASL, in addition to performing standard due diligence measures should also:
  (a) have appropriate risk management systems to determine whether the customer a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
  (b) obtain approval from senior management to establish or continue a business relationship where the customer or a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
  (c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP; and
  (d) conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as a PEP, close associate and family member of a PEP.
  (e) An insurer/ takaful operator will take reasonable measures at the time of payout of a life insurance policy to determine whether the beneficiaries and/or, where applicable, the beneficial owner of the beneficiary are politically exposed persons.
  (f) Where higher risks are identified at payout to a PEP, the insurer or takaful operator must inform senior management before the payout of the policy proceeds, conduct enhanced scrutiny and also consider making a suspicious transaction report.
- The RP should undertake an independent check which may include an internet search of the customer's or beneficial owner's background and databases and reports from commercial service providers. Commercial screening service providers do provide databases of PEPs. They may be good for foreign PEPs, but may not be as good for Pakistani PEPs and their family and close associates.
- In low risk scenarios declaration may be sufficient. This should be in a signed declaration as part of the customer acceptance/application form. In higher risk scenario, a search of publicly available information, such as internet public sources or commercial databases is necessary.
- During ongoing monitoring RP should later identify the customer and/or the beneficial owner as a PEP. This may occur if the individual customer is promoted into a more senior role, or a ownership of a company changes and an individual acquires 25% or more, or some other controlling interest, or for some other reasons.

Non-Profit Organizations

- Both by international standards and in Pakistan's National Risk Assessment, NPOs are classified as a High Risk Sector for TF.
- The objective of Enhanced Customer Due Diligence for NPOs is to ensure that NPOs are not misused by terrorist organizations:
  (a) by posing as legitimate entities;
  (b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
  (c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, for terrorist purposes.
- RASL who transact with NPOs should understand:
  (a) Beneficiaries and Beneficial Owners including certain donors that maintain decision rights;
  (b) Flow of funds, in particular the use of funds by an NPO

High Net worth Individuals (HNWIs)

High net worth individuals while an attractive customer for RASLs, can expose the RASL to higher risk of financial transactions that may be illicit. There is no standard size of HNWI. RASL knows to whom it is offering its products and services, and can establish criterion for HNWI applicable to their particular business.

RASL should scrutinize HNWI customers to determine, whether they carry a higher risk of ML/FT and require additional due diligence measures. Such scrutiny must be documented and updated as part of the Risk Assessment of the RASL.

High-risk Countries and Higher Risk Regions within country

- Pursuant to recommendations by the National Executive Committee, when called upon to do so by FATF and as indicated by the Federal Government, regulated persons will apply appropriate counter measures and EDD against high risk countries that is proportionate to the risk indicated.
- Certain countries, or regions within countries have a specific higher AML/CFT risk profile. Examples are border regions, large goods transit points such as ports, or regions experiencing social unrest, that can be associated with specific crime patterns such as cash or people smuggling, drug trafficking, violent crimes, fraud and corruption, and consequently pose a higher potential risk to the RP. Conducting a business relationship with a customer from such a country/region exposes the RP to risk of channeling illicit money flows.
- RASL should exercise additional caution, and conduct enhanced due diligence on individuals and/or entities based in high-risk countries / regions. RASL are advised to consult publicly available information to ensure that they are aware of the high-risk countries/territories. RASL should consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs).
- Complex legal structures may be created in jurisdictions specializing in obscuring the trail to Beneficial Owners and allowing easy creation of complex corporate vehicles, so called offshore jurisdictions. RASL

engaging with foreign complex legal structures, or with local companies owned by such foreign legal structures, need to educate themselves on offshore financial centres and acquire adequate expertise to understand their customers' ownership structure up to the Beneficial Owner and be able to assess documents presented to them.

Timing of Due Diligence

- Customer Due Diligence and verification measures should be undertaken when establishing the business relationship and before any financial service or transaction occurs (Regulation 8).
- However, as provided in the Regulations RASL may complete verification after the establishment of the business relationship as soon as is practicable where the risks of ML/TF/PF are low (Regulation 16). Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:
  (a) Non face-to-face business;
  (b) Securities transactions. In the securities industry, intermediaries may be required to perform transactions very
- rapidly according to the market conditions at the time the customer is contacting them and the performance of the transaction may be required before verification of identity is completed.
- RASL need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.
- Where an RASL is unable to complete and comply with CDD requirements as specified in the Regulations, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the RASL shall terminate the relationship. Additionally, the RASL shall consider making a STR to the FMU.

Due Diligence of Existing Customers

i. Existing customers must be assigned a risk rating based on the Risk Matrix which RASL has created together with RASL Risk Assessment in its Risk based Approach.
ii. RASL are required to apply CDD measures to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken, and the adequacy of data obtained.
iii. The CDD requirements entails that if an RASL has a suspicion of ML/TF/PF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.
iv. An RASL is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an

institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

v. Finally, RASL should entertain filing a suspicious transaction report if there are any indicators that support such an action.

vi. For existing customers who opened accounts with old NICs, the RASL will ensure that attested copies of identity documents are present in the RASL records. The RASL will 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.

vii. For customers whose accounts are dormant or in-operative, withdrawals will not be allowed until the account is activated on the request of the customer. For activation, the regulated person 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 fulfil the regulatory requirements. viii. If an RASL has a suspicion of ML/TF/PF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

7. Record Keeping Procedures

Record Keeping Procedures

1. RASL will ensure that all information obtained in the context of CDD is recorded. This includes:

- Documents provided to the RASL when verifying the identity of the customer or BO;
- Verification of CNIC through NADRA Verisys / Biometric;
- Transcription into the RASL own IT systems of the relevant CDD information.

2. The RASL 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.

3. The RASL should maintain a comprehensive record of AML/CFT reports with respect to internal enquiries and reporting to FMU. Such documentation may include:

- the report itself and all its attached information / documents in copy;
- the date of the report;
- the person who made the report and the recipient;
- any decision based on the STR for the specific customer or a group of customers;
- any updating or additional documentation taken based on the report; and
- the reasoning underlying the decisions taken

4. 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 RASL 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.

5. The RASL 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.

6. The regulated person will provide, when requested by the Commission, investigating or prosecuting agency and FMU, any record promptly after the request has been made or such time as may be instructed by the relevant authority.

7. Also RASL will maintain the entire record regarding customer relationship, trading and source of order I.e. telephone recording, voucher signing, email, trade log and confirmation, receiving, payments etc.

8. The entire record for the past five years will be retained by RASL.

8. Client Identification Procedures for Individual, Joint and Corporate Accounts, Beneficial ownership

CDD is the process through which an RASL develops an understanding regarding customers and the ML/TF/PF risks they pose to the business. RASL 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.

Client Identification Procedures for Individual Persons

For Identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on KYC/CDD form or account opening form:

- Full name as per Identity document of the Applicant
- Date of Birth, Gender, Marital status, Religion, Occupation, and Qualification
- Residential Status, Nationality, Country of Residence
- Details of Employer/Business
- CNIC/NICOP/SNIC/POC/Passport Number
- Existing Mailing and Permanent address
- Residential Telephone Number, Office Telephone Number, Fax Number, Mobile Number and Email address
- NTN and STN number
- Nature and Type of Account
- Details of Bank Account
- Details of Investor Account maintaining with CDC and Details of Sub Account maintaining with other Broker(s)
- Source of Income, Gross Annual Income, Sources of Fund for Stock Market, Expected value of Investment

- Knowledge of stock Market and Investment experience
- Normal or expected mode of transaction

Client Identification Procedures for Joint Accounts:

In case of Joint account, the customer due diligence measures on all of the joint account holders shall be performed as if each of them were individual customers of the RASL. In order to confirm the identity of the Client, copies of the following documents will be obtained and retained for RASL's record:

- Duly filled and signed Account Opening Form (AOF) by Title and Joint Account Holder(s).
- Bank Verification on AOF from the bank where Title Account Holder is maintaining a bank account.
- Physical presence of Title and Joint Account Holder(s) at any of the RASL Office along with valid original ID document.
- Attested Copies of valid ID document of Title and Joint Account Holder(s).
- Attested Copies of valid ID document of witnesses.
- Local Mobile Number and/or email address.
- Copy of Zakat Declaration (CZ-50) duly attested by notary public as per the prescribed format for Zakat exemption (Optional).
- For Non-Muslims RASL, written request for Zakat non-applicability.
- Power of Attorney duly attested by Notary Public on prescribed format duly signed by all Account Holders (optional).
- Copy of NTN certificate, if NTN is provided in AOF.
- Copy of NICOP for non-resident Pakistanis, Passport for foreigners duly attested by Consulate office of Pakistan or Notary Public of respective country.
- Bank statement or utility bill; or other residential identifying information;
- Bank references.
- Proof of Employment/ Business
- If the account is opened by the officer of government, Special resolution/Authority from the Federal/Provincial/Local Government department duly authorized by the Ministry of Finance or Finance department of the concerned provincial or Local Government.

Client Identification Procedures for Corporations, Partnerships, Trusts and Other Legal Entities:

RASL shall take reasonable steps to ascertain satisfactory evidence of an entity Client's name and address, its authority to make the contemplated investment. For Identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on KYC/CDD form or account opening form:

- Full name as per Identity document
- Company registration /Incorporation number
- Date and country of Incorporation
- Date of Business Commenced

- Residential Status
- Type of Business
- Name of parent Company
- Email, website and contact number
- Registered and mailing address
- NTN number and Sales Tax number
- Details of Contact Person and authorized person to operate the account
- Nature and Type of Account
- Details of Bank Account
- Details of Investor Account maintaining with CDC and Details of Sub Account maintaining with other Broker(s)
- Financial and General Information including Investment experience, Expected value of investment, recent change in ownership of the company, customer type,
- Normal or expected mode of transaction RASL will obtain the following documents, as appropriate under the circumstances
- Certified true copy of Board Resolution. (Specimen provided as per Annexure "A") / Power of Attorney*
- Certified true copies of Constitutive Documents of the Applicant (Memorandum & Articles of Association, Act / Charter / Statute / By-laws / Rules & Regulations, Certificate of Incorporation, Certificate of Commencement of Business, Prospectus for Madaraba, Relevant licenses and registration issued by Regulatory Bodies etc.)
- Certified copy of list of Directors / Trustee (if applicable)*
- List of authorized signatories.
- List of Nominated persons allowed placing orders.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Authorized Signatories.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Contact Person.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Witnesses.
- Certified copy of N.T.N. Certificate. (If exempted please provide Exemption Certificate).
- Latest Audited Accounts of the Company.

Beneficial ownership

If a customer has authorized another person, than the additional documentation are required. These include:

- Attested copies of ID document of Authorized person
- Power of Attorney duly attested by Notary Public on prescribed format duly signed by all Account Holders with the following minimum information:
- Name of Authorized person and his/her Relationship
- CNIC/NICOP/Passport number
- Contact Details and email address

- Specimen Signature of the person authorized.
- Nature of business of beneficial owner

The authorized person is only allow to issue instruction for buy or sale of securities on behalf of client and all payments or receipt of funds must be made to or from the client own accounts and must include CNIC number clearly marked on all payment cheques.

Client Identification Procedures

RASL's AML / CFT policy and procedures are intended to ensure that, prior to accepting funds from Clients, all reasonable and practical measures are taken to confirm the Clients' identities.

RASL may take assistance from the bank or other financial institutions for completing client identification process. The assistance shall not relieve the RASL for identification process to be conducted by the company. These Client Identification Procedures are based on the premise that the RASL will accept funds from a new and existing Client only after:

- RASL has confirmed the Client's identity and that the Client is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made; or
- If the Client is acting on behalf of others, RASL has confirmed the identities of the underlying third parties.

Customer acceptance policies

At first the transaction from a customer is accepted, as per policy criteria set under the heading of Restricted Personal List.

After this the understanding of the customer’s business and its activities help a lot to contribute to the company’s overall reputational, concentration, operational and legal risk management through the detection of potentially harmful activities.

Conducting CDD, EDD

- RASL shall take steps to know who all their customers are.
- RASL shall not keep anonymous accounts or accounts in fictitious names. RASL shall take steps to ensure that their customers are who they purport themselves to be.
- RASL shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from NADRA Verisys/Biometric. Similarly, RASL shall identify and verify the customer’s beneficial owner(s) to ensure that the RP understands who the ultimate beneficial owner is.
- RASL must assess each customer’s risk to allow for correct application of enhanced due diligence, standard, simplified or special measures for PEPs and other designated categories as per the Regulations. Necessary minimum customer risk rating categories are:
    - High
    - Standard
    - Low

- Standard CDD is likely to apply to most of the customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer. It also includes the verification of that information. For beneficial owners the verification is according to the level of risk involved.
- Simplified CDD can only be conducted on a specified set of circumstances such as government departments, local authorities and certain listed companies.
- EDD must be conducted when RP considers that the level of risk involved is such that EDD should apply. EDD requires the collection and verification of the same information as standard CDD as well as, according to the level of risk involved, the collection and verification of information relating to the source of wealth (SoW) and source of funds (SoF) of the customer.
- RASL are entitled to ask customers all relevant CDD questions and may refuse business if the necessary questions are not answered, or the necessary data and documents are not provided.
- If RASL has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report (STR).
- RASL shall assess different levels of money laundering/terrorism financing risks posed by their customers' beneficial owners. For example, RPs should consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.
- For complex structures, foreign entities or foreign owned entities, RASL are required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet.
- If RASL form a suspicion of ML/TF/PF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If the RASL reasonably believes that performing the CDD or on-going process will tip-off the customer, it may choose not to pursue that process and should file a STR. RASL shall ensure that their employees are aware of these issues when conducting CDD or ongoing CDD.

RASL shall conduct CDD of the entire customers (New, Existing etc.) at least on annual basis, or when raise any suspicious in the existing clients.

Sahulat Accounts

As per new amendment by the AML/CFT/PF regulation 2020, all resident Pakistani individual customers can open a Sahulat Account in a single capacity. RASL are encouraged to provide digital /online account opening facilities to their customers.

The Sahulat Account enables investors to trade freely up to

- Purchase positions up to PKR 1,000,000/-
- Net trades of up to PKR 1,000,000/- per day.
- Sell securities up to their full value.

Key Features of Sahulat Trading Account

- Sahulat Account can be opened for each investor as a single individual without any joint account holder
- Sahulat Account Holders can convert their account to normal trading account anytime they want
- Investors can trade freely in the Regular Delivery Contract Market also known as Ready Market.
- Online Trading Facility available with RASL.
- Computerized/Smart National Identity Card (CNIC/SNIC may be used as a proof of identity for opening of Sahulat Account
- No additional document is required from customer for establishing his /her source of income where customer is identified as a low risk customer
- In case of minor accounts, the security broker shall obtain photocopy of Form-B, Birth Certificate or Student ID card (as appropriate) from the minor
- photocopy of identity document of the guardian shall be obtained.
- Any person that already has a normal trading account with a Securities Broker cannot open a Sahulat Account with any Securities Broker.
- normal trading account cannot be converted into a Sahulat Account.
- The existing system has checks in place to restrict any securities broker from opening Sahulat Account of a customer who already has a normal trading account
- To perform risk assessment for a Sahulat Account;
- RASL ask for additional documents from the customer Based on the characteristics of Sahulat Account, the account can be marked as low risk. However,
- to ensure compliance with FATF standards and AML/CFT regulatory framework for SECP

The following link regarding the said account can be used for guidance.
https://www.psx.com.pk/psx/resources-and-tools/investors/sahulat-account

9. Ongoing Monitoring of Customers, Systems and Controls, Restricted Personal List

Ongoing Monitoring of Customers, Systems and Controls

i. Once the identification procedures have been completed and the business relationship is established, the RASL is required to monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated, when the relationship/account was opened.

ii. The regulated person should conduct ongoing due diligence on the business relationship by

a) Scrutinizing transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the regulated person's knowledge of the customer, their business and risk profile, including where necessary, the source of funds;
b) Examining the background and purpose of all complex and unusual transactions that have no apparent economic or visible lawful purpose. The background and purpose of these transactions will be inquired

and findings documented with a view to making this information available to the relevant competent authorities, when required.

c) Carrying out reviews of existing records and ensuring that documents, data or information collected for CDD purposes is kept up-to-date and relevant, particularly for higher risk categories of customers.

d) It is important to review and revise the profiles of customers identified in (b) that are involved in complex and unusual transactions that have no apparent economic or visible lawful purpose.

iii. Additionally, RASL will assess the effectiveness of their risk mitigation procedures and controls, identify areas for improvement and update their systems as appropriate to suit the change in risks. This allows them to manage their AML/CFT risk effectively. For this purpose, RASL monitors:

- changes in customer profile or transaction activity/behaviour in the normal course of business including incidents related to suspicious transactions and terrorist financing sanctions (TFS);
- changes in risk relative to countries and regions to which the RASL or its customers are exposed;
- the potential for abuse of products and services because of their size, unusual patterns, ambiguity and complexity;
- deficiencies in internal cooperation and coordination mechanisms, and employee awareness of their roles in AML/CFT compliance and other functions/areas; and e) selection, training and performance of agents, intermediaries and third parties who are in any way involved in the AML/CFT processes of the PASL.

IV. RASL should ensure that CDD data or information is kept up-to-date by undertaking routine reviews of existing records. RASL shall consider updating customer CDD records within the time frames set by the RP based on the level of risk posed by the customer or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:

- Material changes to the customer risk profile or the way that account usually operates;
- RASL lacks sufficient or significant information on a particular customer;
- Where a significant transaction takes place;
- Where there is a significant change in customer documentation standards;
- Significant changes in the business relationship;
- Transaction restructuring to circumvent the applicable threshold

V. Annexure 4 and 5 gives some examples of potentially suspicious activities or “red flags” for ML/TF/PF, enabling RPs to recognize possible ML/TF/PF schemes. 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.

vi. In case a customer has no active business with the RASL, and cannot be reached, or refuses to engage in updating because there is no active business, account should be marked inactive with the instruction that relationship cannot be re-activated without full CDD.

vii. In case due diligence cannot be updated, a formal ending of the relationship should be done by following the legal process for ending a customer relationship under the applicable laws.

viii. RASL encourage to invest in computer systems for transactions monitoring specifically designed to assist the detection of ML/TF/PF. It is recognized that this may not be necessary in a risk-based approach. In such circumstances, RPs will need to ensure they have alternative systems in place for conducting on-going monitoring.

ix. Alternate or manual systems of ongoing monitoring may rely on Compliance Officer generated lists or instructions and regular lists generated from IT system such as:

- High transaction list for each day;
- Periodic list of transactions over determined thresholds;
- Periodic list of new clients and relations closings;

Monthly or yearly lists of inactive clients;

Monitoring of Business Relationships

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

The Company will conduct an on-going due diligence which will include scrutinizing the transactions undertaken throughout the course of the business relationship with a customer. Further, the Company' risk department has put in place a weekly review mechanism which includes comparison of client deposits and available KYC/CDD clients' information to confirm that the clients have disclosed adequate income sources to justify the value of deposits. Where inadequacy is identified additional documents/information is obtained from the clients by sending emails and making follow-up calls. Where clients provides the required document, their profile is updated. In cases where clients do not provide the requisite information, the same is discussed with Head of Risk on a client to client basis and recommendation is made to CO for necessary course of action including re-categorization of client's risk category and/or filing STR with FMU.

Company will stay vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts and the customer updated KYC profile. Possible areas to monitor could be:

(1) transaction type

(2) frequency

(3) amount

(4) geographical origin/destination

(5) account signatories

(6) mandate

It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring mechanism. Hence, Company take support of the technology to the extent possible while use manual procedures where current technology does not support certain report types and analysis. For example, screening against UNSC consolidate sanctions list is performed daily through an internally developed matching and alerts-based solution while individual transactions of customers are matched against customer profiles using Microsoft Excel spreadsheet analytical tool. Along with that our Back Office Software allows us to screen all Account holders, Joint Account holders, Nominees, through UN/NACTA Proscribed persons list, screening is performed whenever its required.

Restricted Personal List

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

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

www.un.org/sc/committees/1267/aq_sanctions_list.shtml

https://www.un.org/sc/suborg/en/sanctions/1988/materialss

https://www.un.org/sc/suborg/en/sanctions/1718/materialss

http://www.un.org/en/sc/2231/list.shtmll

https://www.un.org/sc/suborg/en/sanctions/1718/prohibited-itemss

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

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

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

10. ML/TF Warning Signs/ Red Flag, Responding to Red Flag, Targeted Financial Sanctions (TFS)

Red Flags

The following are some of the warning signs or "red flags" to which RASL should be alerted.Red flags that signal possible money laundering or terrorist financing may include, but are not limited to:

- Customers who are unknown to the Company and verification of identity / incorporation proves difficult;
- Customers who wish to deal on a large scale but are completely unknown to RASL;
- Customers who wish to invest or settle using cash;
- Customers who use a cheque that has been drawn on an account other than their own;
- Customers who change the settlement details at the last moment;
- Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
- Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
- Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution.
- 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;
- Customer trades frequently, selling at a loss
- Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
- 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;
- Any transaction involving an undisclosed party;
- transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
- Significant variation in the pattern of investment without reasonable or acceptable explanation
- Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
- Transactions involve penny/microcap stocks.
- 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.

- Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
- Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
- Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
- Customer conducts mirror trades.
- Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

Responding to Red Flags and Suspicious Activity

Conducting comprehensive KYC/CDD of the customer at the time of opening of account and tagging all red flags customers as "High risk customers" and make enhanced due diligence of these red flag customers at the time of account opening.

Receiving cash and cash equivalents at Company's premises will be strictly prohibited;

Payments from any customer are only acceptable through proper banking channel, from customers' own account, third party cheques are not acceptable.

Funds shall not be transferred from one account to any other customers' accounts in any case;

In case of withdrawals cheque must be issued in customer's name and no payments shall be made to any third party on behalf of the customers in any case. However, funds can be transferred in the name of the company issuing right shares, in order to purchase right shares, on instructions of the customer.

Targeted Financial Sanctions (TFS) under UNSC Resolutions

TFS obligations are provided under the following legal instruments: a) United Nations (Security Council) Act, 1948 (UNSC Act) b) United Nations Security Council (Freezing and Seizure) Order, 2019 c) Statutory Regulatory Orders (SROs) issued under UNSC Act d) Anti-Terrorism Act, 1997 (ATA) e) Notifications issued under ATA f) AML Act, 2010 and rules, regulations and directives issued thereunder. 2. What are the UNSC and Domestic Sanctions Regimes in Pakistan? The Government of Pakistan under the UNSC Act gives effect to the decisions of United Nations Security Council (UNSC) whenever the Consolidated List is updated maintained by the relevant Sanctions Committee. The details of sanctions imposed by the UNSC along with the Consolidated Lists are available on the UNSC Sanctions Committees' websites at the following links:

a) https://www.un.org/securitycouncil/content/un-sc-consolidated-list

b) https://scsanctions.un.org/search/

c) https://www.un.org/securitycouncil/sanctions/1267

d) https://www.un.org/securitycouncil/sanctions/1988

e)https://www.un.org/securitycouncil/sanctions/1718

f) https://www.un.org/securitycouncil/content/2231/background

3. Where can I find notifications issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions? MOFA issues SROs to provide legal cover for implementing sanction measures under UNSC resolutions. These SROs in respect of designated individuals/ entities require assets freeze, travel ban and arms embargo in addition to other measures in accordance with the UNSC resolutions, and are available publicly at the following links:

a) http://mofa.gov.pk/unsc-sanctions/

b) http://www.secdiv.gov.pk/page/sro-unscr-sanctions

a) https://nacta.gov.pk/proscribed-organizations-3/

b) https://nacta.gov.pk/pp/

c) https://nfs.punjab.gov.pk/

11 Customer risk factors, LPLA, Risk Profiling Of Customers, geographic risk factors, Afghan National.

Customer risk factors:

The RASL must list and describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the RP for ML/TF/PF and the consequent impact, if indeed that occurs.

Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

(a) The business relationship is conducted in unusual circumstances
(b) Non-resident customers.
(c) Legal persons or arrangements
(d) Companies that have nominee shareholders
(e) Business that is cash-intensive.
(f) Politically exposed persons.

(g) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
(h) Requested/Applied amount of business does not match the profile/particulars of client
(i) Designated Non-Financial Business and Professions:
(j) real estate dealers, dealers in precious metal and stones,
(k) accountants and lawyers/ notaries

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

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

The LPLA risk assessment provide the following factors in this regard:

• Entities possessing following inherent characteristics are more likely to be abused for ML/TF purposes having foreign companies/entities/trusts (whether registered in Pakistan or not) as member/ shareholder/investor/partner/trustee;

- Trust sponsored from abroad; o those waqf properties who are recipient of any foreign charity or donor agencies. o having foreign bank accounts; •

Moreover, the use of foreign trusts might convey risks of unlawful practices owing to criminals making the most of the differing treatment of these legal arrangements by tax authorities and of the potential lack of coordination between them

Account Shall Not Open

Where CDD Measures are not completed, In case the RASL is not been able to satisfactorily completed required CDD measures, account shall not be opened or any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR.

Anonymous or Fictitious Account: RASL shall not open or maintain anonymous account or accounts in the name of factitious persons.

Government Accounts: Government Account shall not be opened in the personal names of the government officials.

Proscribed Individuals/Entities:RASL shall not provide services to Proscribed Individuals, Groups and Entities declared/ listed by UNSC (United Nations Security Council) and/ or by OFAC (Office of Foreign Asset Control –

USA) OR those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

Risk Profiling Of Customers

All relationships shall be categorized with respect to their risk levels i.e. High, Medium and Low based on the risk profiling of customer (through KYC/CDD application and as guided in the operational Manual for making effective decision whether to perform Simplified Due Diligence (SDD) or Enhanced Due Diligence (EDD) both at the time of opening and ongoing monitoring of business relationship.

Risk profiling of the customers shall conducted when raise any suspicious during the business. Normally RASL shall review the entire clients risk profiling annually.

Cross-border Correspondent Relationship:

Cross-border correspondent relationships are the provision of services by one institution to another institution (the respondent institution). Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's) customers may present high ML/TF risk and as such may require Enhanced Due Diligence ("EDD").

Risk Assessment and Applying a Risk Based Approach ("RBA")

i. The RBA enables the Company to ensure that AML, CFT AND PF measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. RBA is applied keeping into consideration the Company's size, geographical coverage, structure and business activities and applied the RBA on RASL (group-wide) basis, where appropriate e.g. daily system-based sanction screening. As a part of the RBA, The Company:
   1) Identify ML/TF risks relevant to it;
   2) Assess ML/TF risks in relation to-
      a. Its customers (including beneficial owners);
      b. Country or geographic area in which its customers reside or operate and where the Company operates;
      c. Products, services and transactions that the Company offers; and d. Their delivery channels.

3) Design and implement policies, controls and procedures that are approved by its Board to manage and mitigate the ML/TF risks identified and assessed;

4) Monitor and evaluate the implementation of mitigating controls and improve systems where necessary;

5) keep its risk assessments current through ongoing reviews and, when necessary, updates;

6) Implement and monitor procedures and updates to the RBA; and

7) Have appropriate mechanisms to provide risk assessment information to the Commission.

iii. Under the RBA, where there are higher risks, the Company takes enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures are permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF. In the case of some very high-risk situations or situations which are outside the Company's risk tolerance, the Company may decide not to take or accept the customer, or to exit from the relationship. CO in such cases will consider need to raise an STR to FMU.

iv. In view of the fact that the nature of the TF differs from that of ML, the risk assessment must also include an analysis of the vulnerabilities of TF. Many of the CFT measures the Company has in place will overlap with its AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, and escalation of suspicions and liaison relationships with the authorities.

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

1) Identifying the area of the business operations susceptible to ML/TF

2) Conducting an analysis in order to assess the likelihood and impact of ML/TF;

3) Managing the risks; and

4) Regular monitoring and review of those risks.

a) Identification, Assessment and Understanding Risks

i. The first step in assessing ML/TF risk is to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels that are specific to the Company.

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

iii. For the analysis, the Company will identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but possible. In assessing the impact, the Company will, for

instance, look at the financial damage by the crime itself or from regulatory sanctions or reputational damages that can be caused. The **impact can vary from minor if that are only in short-term or there are low-cost consequences, to very major, when they** are found to be very costly inducing long-term consequences that affect the proper functioning of the institution.

iv. The following is an example of a likelihood scale with 3 risk ratings as an example.

LIKELIHOOD SCALE

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

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

1) How likely an event is;

2) Consequence of that event;

3) Vulnerability, threat and impact;

4) The effect of uncertainty on an event;

vi. The assessment of risk will be informed, logical and clearly recorded. Further, the risk assessment should indicate how the Company arrived at this rating.

Risk Assessment (lower complexity)

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

1) Unlikely - There is a small chance of ML/TF occurring in this area of the business;

2) Possible - There is a moderate chance of ML/TF occurring in this area of the business;
3) Almost Certain - There is a high chance of ML/TF occurring in this area of the business.

Risk Assessment (moderate complexity)

Another way to determine the level of risk is to work out how likely the risk is going to happen and cross-reference that with the consequence of that risk. Using likelihood ratings and consequence ratings can provide the Company with a more comprehensive understanding of the risk and a robust framework to help arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist the Company in applying the appropriate risk management measures as detailed in the program.

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

Risk Assessment (higher complexity)

Company will further assess risk likelihood in terms of threat and vulnerability. Determining the impact of ML/TF activity can be challenging but to focus AML, CFT AND PF resources in a more effective and targeted manner. When determining impact, Company can consider a number of factors, including:

1) Nature and size of your business (domestic and international);

2) Economic impact and financial repercussions;

3) Potential financial and reputational consequences;

4) Terrorism-related impacts;

5) Wider criminal activity and social harm;

6) Political impact;

7) Negative media.

Company will more weight to certain factors to provide a more nuanced understanding of your ML/TF risk. In addition, Company may consider how its risks can compound across the various risk factors.

Applying the Risk Assessment

The risk assessment will assist in ranking and prioritizing risks and providing a framework to manage those risks. The risk assessment will enable the Company to prepare a comprehensive program. It will enable to meet relevant obligations under the regulations, including obligations to conduct CDD, monitor accounts and activities and report suspicious activity. The assessment will help in determining suspicion and consequently assist in the decision to submit an STR to the FMU. The Company will submit an STR to the FMU if it thinks that activities or

transactions are suspicious. The Company will conduct ongoing CDD. The risk assessment will help target and prioritize the resources needed for ongoing CDD. The Company will undertake account monitoring. The risk assessment will help to design the triggers, red flags and scenarios that can form part of account monitoring.

New and Developing Technologies and Products

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

Material Changes and Risk Assessment

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

Material change could include circumstances where the Company introduces new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when the Company starts using new methods of delivering services or have new corporate or organizational structures. It could result from deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, the Company will need to refresh its risk assessment.

vi. Compliance resources are accordingly allocated to the areas with higher Inherent Risk to bring the Residual Risk within tolerable band. This risk assessment is an ongoing process and is reviewed on an annual basis to factor in new and emerging risks due to business dynamics and changes in regulatory framework. This include changes in risk levels as new products are offered, as new markets are entered, as high-risk customers open or close accounts, or as the products, services, policies, and procedures change. The Company also have appropriate mechanisms to provide risk assessment information to the Commission, if required. This is done through a specially designed document which is provided as Annexure 1 to these policy and procedures.

Examples of Risk Classification Factors

Below are some examples that can be helpful indicators of risk factors / indicators that may be considered while assessing the ML/TF risks for different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels. However, this list is not exhaustive and staff should use critical thinking in determining risk of ML/TF.

High-Risk Clients The Compliance Officer will provide and will continuously update a list of the types of Clients that RASL considers to be of 'high risk,' such that enhanced due diligence procedures are warranted compared to the routine Client Identification Procedures. Following are the examples of Clients who pose a high money laundering risk:

- Non-resident customers;
- Legal persons or arrangements including non-governmental organizations; (NGOs)/ notfor-profit organizations (NPOs) and trusts / charities;
- Customers belonging to countries where CDD/KYC and antimony laundering regulations are lax or if funds originate or go to those countries;
- Customers whose business or activities present a higher risk of money laundering such as cash based business;
- Customers with links to offshore tax havens;
- High net worth customers with no clearly identifiable source of income;
- There is reason to believe that the customer has been refused brokerage services by another brokerage house;
- Non-face-to face / on-line customers;
- Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations; and
- Politically Exposed Persons (PEPs) or customers holding public or high profile positions. Politically Exposed Persons (PEPs) these generally include individuals in prominent positions such as senior politicians, senior government, judicial or military officials; senior executives of State Corporations and their family members and close associates. These individuals present reputational risk and potential conflict of interest and extra caution is required when opening their brokerage account and monitoring their account activity. The above definition is not intended to cover middle ranking / junior officials in above noted categories. However, prudence requires brokers to be careful while dealing with such customers

Enhanced Client Identification Procedures for 'High Risk' Natural Persons Enhanced Client Identification

Procedures for 'high risk' natural persons as Clients include, but are not limited to, the following:

- Assessing the Client's business reputation through review of financial or professional references, generally available media reports or by other means;
- Considering the source of the Client's wealth: including the economic activities that generated the Client's wealth, and the source of the particular funds intended to be used to make the investment;
- Reviewing generally available public information, such as media reports, to determine whether the Client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists;
- Conducting a face-to-face meeting with the Client to discuss/confirm the account opening documents.

The enhanced due diligence procedures undertaken with respect to 'high risk' Clients must be thoroughly documented in writing, and any questions or concerns with regard to a 'high risk' Clients should be directed to the Compliance Officer.

Enhanced Client Identification Procedures for 'High Risk' Corporations, Partnerships, Trusts and Other legal Entities Enhanced Client Identification

Procedures for 'high risk' Corporations, partnerships and other legal entities include, but are not limited to, the following:

- Assessing the Client's business reputation through review of financial or professional references, generally available media reports or by other means;
- Reviewing recent changes in the ownership or senior management of the Client;
- Conducting a visit to the Client's place of business and conducting a face-to-face meeting with the Client to discuss/confirm the account application, the purpose of the account and the source of assets;
- Reviewing generally available public information to determine whether the Client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any criminal investigation, indictment, conviction or civil enforcement action relating to financing of terrorists.

As an example, these descriptions can result in a table as depicted below:

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

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

Country or geographic risk factors, Porous Border, Afghan National.

Country or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of the Company itself, its location and the location of its geographical units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to ML/TF. The factors that may indicate a high risk are as follow:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML, CFT AND PF systems

(b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations

(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity

(d) Countries or geographic areas identified by credible sources as providing funds or support for terrorist activities, or that have designated terrorist organizations operating within their country

(e) Entities and individuals from jurisdictions which are known tax heavens

RASL staff shall vigilantly obtain required documents when establish business relationship with any customer from porous border area, nonresident or Afghan national. If any suspicious raise during the period than file STR to the relevant authority on prompt basis.

Countries which are hostile to national interest of Pakistan or with which diplomatic relations are suspended

Product, service, transaction or delivery channel risk factors:

Company, while doing its ML/TF risk assessment, takes into account the potential risks arising from the products, services, and transactions that the Company offers to its customers and the way these products and services are delivered. In identifying the risks of products, services, and transactions, the following factors are considered:

(a) Anonymous transactions (which may include cash)
(b) Non-face-to-face business relationships or transactions
(c) Payments received from unknown or un-associated third parties
(d) International transactions, or involve high volumes of currency (or currency equivalent) transactions
(e) One-off transactions
(f) Transaction for which payments are made from more than two bank accounts of a customer
(g) Products that involve large payment or receipt in cash; and
(h) One-off transactions.

(i) Is the customer physically present for identification purposes? If they are not, has the Company used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?

Low Risk Classification Factors

(1) Customer risk factors: The customer is a regulated person or bank and is subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements, or

Public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership;

(2) Product, service, transaction or delivery channel risk factors: Financial products or services that provide appropriately defined and limited services to certain types of customers.

(3) Country risk factors:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML, CFT AND PF systems.

(b) Countries identified by credible sources as having a low level of corruption or other criminal activity.

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

Risk Matrix

In assessing the risk of money laundering and terrorism financing, the Company will establish whether all identified categories of risks pose a low, moderate, high or unacceptable risk to the business operations. The Company will review different factors, e.g., number and scope of transactions, geographical location, and nature of the business relationship. In doing so, it must also review the differences in the manner in which it establishes and maintains a business relationship with a customer (e.g., direct contact or non-face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from institution to institution. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk.

The Company will use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing.

The development of a risk matrix can include the consideration of a wide range of risk categories, such as the products and services offered by the Company, the customers to whom the products and services are offered, the size and organizational structure, etc. A risk matrix is not static: it changes as the circumstances of the Company change. A risk analysis will assist the Company to recognize that ML/TF risks may vary across customers, products, and geographic areas and thereby focus its efforts on high-risk areas in its business

The following is an example of a risk matrix of client product combination:

Customer Transaction [redacted]	Online [redacted] Transactions	Domestic [redacted] Transfers	Deposit or [redacted] Investment	Securities [redacted] Account
Domestic Retail Customer	Moderate	Moderate	Moderate	Low
High Net Worth Customers	High	Moderate	High	Moderate
SME Business Customer	High	Moderate	High	Moderate
International Corporation	High	Moderate	High	Moderate
Company Listed on Stock Exchange	Moderate	Low	Moderate	Low
PEP	High	Moderate	High	Moderate
Mutual Fund Transactions	High	Moderate	High	N/A

Risk Mitigation

i. Company will develop appropriate policies, procedures and controls that will enable it to manage and mitigate effectively the inherent risks that it has identified, including the national risks. Company will monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures will be approved by the senior management of the Company, and the measures will be taken to manage and mitigate the risks (whether higher or lower) to ensure that measures are consistent with legal and regulatory requirements.

ii. The nature and extent of AML, CFT AND PF controls the Company puts in place depends on a number of aspects, which include:

1) The nature, scale and complexity of the Company's business
2) Diversity, including geographical diversity of the Company's operations

3) Company's customer, product and activity profile
4) Volume and size of transactions

5) Extent of reliance or dealing through third parties or intermediaries, which is minimal in case of Company and restricted to Administration department related services

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

1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers

2) setting transaction limits for higher-risk customers or products

3) requiring senior management approval for higher-risk transactions, including those involving PEPs

4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services

5) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs)

Evaluating Residual Risk and Comparing with the Risk Tolerance

Subsequent to establishing the risk mitigation measures, the Company will evaluate its residual risk, which is the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks are kept in line with the Company's overall risk tolerance and this sets the cornerstone of accepting and continuing business relations.

New Products and Technologies

The Company will design a special template to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:

1) Electronic verification of documentation;

2) Data and transaction screening systems; or

3) The use of virtual or digital currencies

Company will undertake a risk assessment prior to the launch or use of such products, practices and technologies; and take appropriate measures to manage and mitigate the risks. These policy and procedures provides governance framework to prevent the misuse of technological development in ML/TF schemes,

particularly those technologies that favour anonymity. For example, securities trading and investment business on the Internet, add a new dimension to the Company's activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF, and fraud.

To insulate itself against risk of anonymity of customer, Company will offer an on-line account opening only after appropriate identification checks and fulfilment of its all applicable KYC requirements.

To maintain adequate systems, the Company will ensure that its systems and procedures will be kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by the Company. Risks identified must be fed into the Company business risk assessment.

Payment Mechanism

For amounts greater than PKR 25,000

The RASL shall accept from/ pay to the Account Holder(s) through "A/C Payee Only" crossed cheque, bank drafts, pay orders or other crossed banking instruments in case if amounts exceeds Rs. 25,000/=.

Electronic transfer of funds through banks would be regarded as good as cheque. The RASL shall be responsible to provide the receipt to the Account Holder(s) in the name of Account Holder(s) duly signed by authorized agents / employee of the Broker and the Account Holder(s) shall be responsible to obtain the receipt thereof.

For amounts less than or equivalent to PKR 25000.

In case of cash dealings, proper receipt will be taken and given to the Account Holder(s), specifically mentioning if payment is for margin or the purchase of securities. The RASL shall immediately deposit in its bank accounts all cash received in whole i.e. no payments shall be made from the cash received from clients.

Exceptional Circumstances

However, in exceptional Circumstances, where it becomes necessary for the RASL to accept cash in excess of Rs. 25,000/=, the RASL shall immediately report within one business day, such instances with justification thereof, to the Stock Exchange in accordance with the mechanism prescribed by the Exchange.

Copies of these payment instruments including cheques, pay orders, demand drafts and online instructions shall be kept in record for a minimum period of five years.

12 General Reporting Procedures, STR, CTR

General Reporting Procedures

- The Compliance Officer on behalf of the organization is nominated to receive disclosures under this regulation.
- Anyone in the organization, to whom information comes in the course of the relevant business as a result of which he suspects that a person is engaged in money laundering, must disclose it to the Compliance Officer;
- Where a disclosure is made to the Compliance Officer, the officer must consider it in the light of any relevant information which is available to RASL and determine whether it gives rise to suspicion:
- Where the Compliance Officer determines in consultation with the Senior Management, the information must be disclosed to the Regulatory Authority after obtaining an independent legal advice.

Reporting Suspicious Transactions

1.RASL should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose. Activities requiring further enquiry may fall into one or more of the following:

- any unusual financial activity of the customer not in line with the customer's profile;
- any unusual transaction in the course of some usual financial activity;
- any unusually-linked transactions;
- any unusual method of settlement;
- unusual or disadvantageous early redemption of an investment product;
- unexplained unwillingness to provide the information requested.

2. Where the enquiries conducted by the RASL do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalation of matters to the CO. Ultimately,

3. RASL must decide whether to file a suspicious transaction report based on the above. If it decides not to file, reasons must be documented for this decision.

4. RASL may refuse business that they suspect might be criminal in intent or origin. Where a customer is hesitant/fails to provide adequate documentation, consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF/PF, that attempted transaction should be reported to the FMU.

5. After concluding an internal enquiry, or making an STR, the RASL has to decide whether to close the enquiry, take additional steps such as higher risk rating of customer, or ending the business relationship. This decision must be documented with an explanation for the reasoning behind it.

6. If the RASL decides that a disclosure should be made, the law require the RASL to report STR without delay to the FMU. Under Section 7 (1) of the AMLA, the requirements is that the STR must be filed promptly by the RASL with the FMU. Page 21 of 63

As required by the FMU, all STR reporting is via the FMU's online goAML system. The RASLs are required to get themselves registered on the GoAML system of the FMU. The link to this system is as follows: www.fmu.gov.pk/goamL

7. In order to ensure quality reporting, the reason(s) for suspicion should be supported with proper analysis and should contain following elements:

- Information on the person/entity conducting the suspicious transaction/activity;
- Details of the transaction, such as the pattern of transactions, type of products or services and the amount involved;
- Description of the suspicious transaction or its circumstances
- Tax profile of person/entity (if available)
- If the reported subject (e.g. client/customer) has been the subject of a previous STR then the reference number with date should be provided.
- Information regarding the counterparties, etc.
- Any other relevant information that may assist the FMU in identifying potential offences and individuals or entities involved.

8. There are two types of suspicious reports which can be submitted by the RASL to FMU.

- **STR- A** is to be reported on parties (Person, Account or Entity) involved in any suspicious activity, which does not involve transaction (s) or transmission of funds, However,
- **STR-F** should be filed in case where the transactions have been conducted.
- STR-F is to be reported on parties (Person, Account or Entity) for reporting of transactions and/or financial activity in which funds are involved and appears to be suspicious. An activity/event in which funds transmitted from one party to another must be reported as STR-F.

The link of the goAML registration guide is provided as follows: http://www.fmu.gov.pk/docs/RegistrationGuideFMU.pdf. The link of the goAML reporting guide is provided as follows: http://www.fmu.gov.pk/docs/Financial-Monitoring-Unit-FMU-goAML-Web-Users-Guide Updated-2020.

Currency Transaction Report (CTR)

- The purpose of Currency Transaction Report (CTR) is to identify cash transactions with the financial system, either directly or via financial institution. The aim is to provide additional information to the FMU to develop financial intelligence for law enforcement agencies to investigate potential ML, TF or other offences.
- As per Gazette notification SRO 73 (I)/2015 dated 21-01-2015, the minimum amount for reporting a CTR to FMU is two million rupees. Accordingly, all cash-based transactions of two million rupees or

above involving payment, receipt, or transfer are to be reported to FMU as CTR. Aggregation of cash transactions during the day for the purpose of reporting a CTR is not required. However, if there is a suspicion that the customer is structuring the transaction into several broken cash transactions to evade reporting of CTR, the same may be reported in the form of an STR

- Section 5 of AML Regulations 2015 further explains that the CTR is filed on a prescribed format when a cashbased transaction involving payment, receipt, or transfer of an amount, as specified by the National Executive Committee, occurs.
- Under Section 7 (3) of the AMLA, the CTR must be filed by the RP with the FMU not later than seven working days, after the respective currency transaction.
- Similar to STR reporting to the FMU, all CTR reporting is via the FMU's online goAML system – refer: https://goamlweb.fmu.gov.pk/PRD/Home

13. Policy Review Period, Approval from Board of Directors

Policy Review Period:

The AML / CFT Policy & Procedures will be reviewed on annual basis and updated as and when required.

Approval from Board of Directors:

This policy has updated and approved by the Board of Directors on **October 27, 2023** and access has been provided to the relevant employees of RASL.

Annexure 1

S NO.	TYPE OF CUSTOMER	INFORMATION/DOCUMENTS TO BE OBTAINED
1	Individuals	A photocopy of any one of the following valid identity documents; (i) Computerized National Identity Card (CNIC) issued by NAD. (ii) National Identity Card for Overseas Pakistani (NICOP) issued by NAD. (iii) Pakistan Origin Card (POC) issued by NAD. (iv) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NA), Ministry of Interior (local currency account only). (v) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2	Sole proprietorship	(i) Photocopy of identity document as per Sr. No. 1 above of the proprietor. (ii) Copy of registration certificate for registered concerns. (iii) Copy of certificate or proof of membership of tde bodies etc, wherever applicable. (iv) Declation of sole proprietorship on business letter head. (v) Account opening requisition on business letter head. (vi) Registered/ Business address.

3	Partnership	(i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed'. (iii) Attested copy of Registtion Certificate with Registr 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 opete firm's account. (v) Registered/ Business address.
4	Limited Companies/ Corpotions	(i) Certified copies of: (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; (b) Memorandum and Articles of Association; (c) Certificate of Incorporation; (d) Certificate of Commencement of Business, wherever applicable; (e) List of Directors on 'Form-A/Form-B' issued under Companies Act, 2017, as applicable; and
		(f) Form-29, wherever applicable. (ii) Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and opete the account;

5	Bnch Office or Liaison Office of Foreign Companies	(i) A copy of permission letter from relevant authority i-e Board of Investment. (ii) Photocopies of valid passports of all the signatories of account. (iii) List of directors on company letter head or prescribed format under relevant laws/regulations. (iv) A Letter from Principal Office of the entity authorizing the person(s) to open and opete the account. (v) Bnch/Liaison office address.
6	Trust, Clubs, Societies and Associations etc.	(i) Certified copies of: (a) Certificate of Registtion/Instrument of Trust (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to opete the account. (iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (iv) Registered address/ Business address where applicable.

7	NGOs/ NPOs / Charities	(i) Certified copies of: (a) Registration documents/certificate (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to opete the account. (iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (iv) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer. (v) Registered address/ Business address.
8	Agents	(i) Certified copy of 'Power of Attorney' or 'Agency Agreement'. (ii) Photocopy of identity document as per Sr. No. 1 above of the agent and principal. (iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person. (iv) Registered/ Business address.

9	Executors and Administtors	(i) Photocopy of identity document as per Sr. No. 1 above of the Executor/Administtor. (ii) A certified copy of Letter of Administtion or Probate. (iii) Registered address/ Business address
10	Minor Accounts	(i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate). (ii) Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.

Note:

The photo copies of identity documents shall be validated through NADRA verisys.

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

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

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

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

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

a photograph duly attested by gazetted officer/Administrator/ officer of the regulated person

a copy of CNIC without photograph duly attested by the same person who attested the photograph. 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. The condition of obtaining photocopies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where regulated person should obtain photocopies of identity documents of only those directors and persons who are authorized to establish and maintain Business Relationship. However, regulated person shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and 'Form 29' and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.

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