SEPTEMBER 30, 2022

AML-CFT POLICY AND PROCEDURES

Aba Ali Habib Securities (Pvt.) Ltd

Approval & Amendments

Approvals	Title	Signature
Prepared By	Internal Audit	Afras & Company
Reviewed By	CEO	Zahid Ali Habib
Approved By	BOD	BOD Meeting

Version	Effective Date	Description of Change
1st	30 November, 2019	Updates in AML laws and regulations
2nd	31 May, 2020	Updates in Laws and regulation
3rd	10 August, 2020	Change in Laws and regulation
4th	5th October, 2020	Update in AML rules and regulations
5th	25th June, 2021	Update with respect to industry practices
6th	30 September, 2021	Updates as per changes and red flags by FMU

KNOW YOUR CUSTOMER / CUSTOMER DUE DILIGENCE, ANTI-MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND PROLIFERATION FINANCING POLICY AND PROCEDURES UPDATED UNDER NRA 2019

BACKGROUND:

Money Laundering ("ML") and Terrorist Financing ("TF") are economic crimes that threaten a country's overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF. An effective Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime requires financial institutions to adopt and effectively implement appropriate ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF.

Securities and Exchange Commission of Pakistan ("SECP"), in order to maintain the integrity of its regulated financial sector inter-alia; the brokers in respect of preventing and combating ML and TF, notified the Securities and Exchange Commission of Pakistan Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018 ("the SECP AML/CFT Regulations "or" the Regulations"). The SECP AML/CFT Regulations require relevant Regulated Persons (RPs) to establish systems to detect ML and TF, and therefore assist in the prevention of abuse of their financial products and services.

Additionally, SECP has issued detailed AML/CFT Guidelines ("the Guidelines"), which complements the SECP AML/CFT Regulations. These Guidelines are applicable to all Regulated Persons ("RPs") as defined under the Regulations conducting relevant financial business and designed to assist RPs in complying with the Regulations. These Guidelines clarify and explain the general requirements of the legislation to help RPs in applying national AML/CFT measures, developing an effective AML/CFT risk assessment and compliance framework suitable to their business, and in particular, in detecting and reporting suspicious activities.

These Guidelines are based on Pakistan AML/CFT legislation and reflect, so far as applicable, the 40 Recommendations and guidance papers issued by the Financial Action Task Force ("FATF").

The Policies and Procedures are updated in line with Pakistan's updated National Risk Assessment Conducted on Money Laundering and Terrorism Financing covering all aspects including transnational TF risks so as to introduce required controls including implementation of required systems for mitigation of ML/TF risks commensurate to the level of risk identified.

1. **Introduction, Purpose and Scope:**

These Policies and Procedures are in line with requirements of Anti Money Laundering and Countering Financing of Terrorism Regulations, 2020, the related Guidelines issued by the SECP and National Risk Assessment performed.

These Policies and related Procedures establish the standards to which **Aba Ali Habib Securities (Pvt.) Ltd** ("the Company") should adhere to. This document will be used to create an understanding amongst employees concerning the risks of Money Laundering and Terrorist Financing. Accordingly, the Company is required to adopt Risk-Based Approach (**"RBA"**) to prevent the Company as a conduit for Money Laundering or Terrorist Financing activities.

2. **Objectives:**

The followings are the main objectives of the Company's AML/CFT Policies and Procedures:

(i) Understand the obligation of establishing an effective AML/CFT regime to deter criminals from using financial system for ML or TF purposes.

(ii) Develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations.

(iii) Cater for the continuous Risk Assessments done at National level and develop internal mitigation measures to identify, analyze and assess the inherent threats and their vulnerabilities in light of such risk assessment of the country as a whole.

(iv) Company's Board of Directors and Senior Management are engaged in the decision making on AML/CFT policies, procedures and control and take ownership of the risk-based approach.

(v) Awareness of the level of ML/TF risk the Company is exposed to and takes a view on whether the Company is equipped to mitigate that risk effectively.

(vi) Establish and maintain an effective AML/CFT compliance culture and adequately train its staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with the Regulations.

(vii) Establish written internal procedures so that, in the event of a suspicious activity being discovered, employees are aware of the reporting chain and the procedures to be followed.

(viii) Appoint a Compliance Officer (**"CO"**) at the management level, who shall report directly to the Board of Directors ("Board") and shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit ("FMU").

(ix) Ensure that any suspicious transaction report must be made by employees to the CO, who is well versed in the different types of transactions which the Company handles and which may give rise to opportunities for ML/TF.

(x) Responsibility for ensuring that employees are aware of their reporting obligations and the procedure to follow when making a suspicious transaction report ("STR").

3. **Definitions:**

(i) **Know Your Customer ("KYC")** is the process of identifying and verifying the identity of its customers and ascertain relevant information required for doing business with them. KYC involves:

a. Seeking evidence of identity and address from the customer and independently confirming that evidence at the start of a relationship with the Company and periodically updating the information as per customer risk classification; and
b. Seeking information regarding the sources of income and nature of business etc. of the customer.

(ii) **Customer Due Diligence ("CDD")** information comprises the facts about a customer that should enable an organization to assess the extent to which the customer exposes it to a range of risks. These risks include money laundering, terrorist financing and having business relationship with sanctioned individuals/entities or designated terrorists under Pakistan's Anti-Terrorism law.

(iii) **Money Laundering ("ML")** is the involvement of any transaction or series of transactions seeking to conceal or disguise the nature or source of proceeds derived from illegal activities, including narcotics trade, human trafficking, terrorism, ransom, extortion money, organized crime, fraud, and other crimes.

(iv) **Financing Terrorism ("TF")** refers to activities that provide financing or financial support to individual terrorists or non-state actors.

(v) **Customer** means any natural person, legal person or legal arrangement to whom financial services have been extended by a regulated person.

(vi) **Beneficial Owner** in relation to a customer of the Company means, the natural person who ultimately owns or control a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement.

(vii) **Legal Persons** mean entities other than natural persons whether incorporated or not or a legal arrangement that can establish a permanent customer relationship with a regulated person or otherwise own property and include companies, bodies corporate, foundations, Limited Liability partnership (LLP), partnerships, or associations and other relevantly similar entities.

(viii) **FMU** means Financial Monitoring Unit established under section 6 of the AML Act, 2010.

(ix) **Regulated person** means securities brokers, commodities brokers, Insurers, Takaful Operators, NBFCs and Modaraba.

(x)

4. **Customer Identification:**

(i) No account shall be opened in the name of person who fails to disclose his/her true identity or fails to provide valid identity document. To authenticate identity of new customer:

(a) Legible and attested copy of Computerized National Identity Card (CNIC)/Smart National Identity Card (SNIC) issued by NADRA. /National Identity Card for Overseas Pakistani (NICOP/SNICOP) issued by NADRA/ Form-B/Juvenile card issued by NADRA to children under the age of 18 years/Pakistan Origin Card (POC) issued by NADRA/Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only)/ Valid Proof of Registration (POR) Card issued by NADRA/Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only)shall be obtained before account opening.

(b) For Joint Account documents specified in (a), and CDD measures on all of the joint account holders shall be performed as if each of them is individual customers of the RP.

(c) For Sole proprietorship documents specified in (a), attested copy of registration certificate for registered concerns, sales tax registration or NTN, wherever applicable, Account opening requisition on business letter head and registered/ Business address.

(b) The photocopies of identity documents shall be validated through NADRA Verisys, identifying presence of any adverse remarks in the comments.

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

(ii) Source of income shall be essentially disclosed by the customer.

(a) In case source of customer's income is business / employment, name of the business / employer shall also be disclosed.
(b) In case of a salaried person an attested copy of his service card or salary slip or certificate or letter on letter head of the employer will be obtained.

(iii) All prospective customers must be seen either face to face by the Company's customer service representative or trader or on video call through communication tool like Skype, WhatsApp etc. and details verified over a recorded call on registered phone number.

(iv) For any new account opening form, the Compliance Department shall match the particulars of the customer from the followings:

(a) UNSC Sanctions list obtained daily from UNSC website under consolidated sanction list (https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list);
(b) Notifications of proscribed individuals /entities pursuant to the Anti-Terrorism Act, 1997 issued by Ministry of Interior obtained daily from National Counter Terrorism Authority's website (http://nacta.gov.pk/proscribed-organizations); and

If any matching name is found the account is being declined and reported to FMU simultaneously in the form of STR.

(v) If a customer is acting on behalf of another person than the identity of that person will be ascertained and relevant documents of that person will also be obtained such as:

(a) CNIC / NICOP / Passport copy of person so acting on behalf of the original customer along with the signed authority letter of the customer and reason for appointment of such representative.

(b) CNIC/NICOP/Passport copy of the representative is also verified through NADRA Verisys portal and screened against UNSC and terrorists databases as mentioned above.

(vi) For non-individual customers (e.g. companies, association of persons, pension funds, government owned entities, non-profit organizations, foreign companies/ organizations) additional care must be taken to understand the customer's business, establish the ownership and control structure of such an organization and who (i.e. person(s)) actually owns the organization and who manages it. It should be ensured that the person who represents himself as authorized signatory with powers to open and operate the brokerage account is actually authorized by the organization and obtain relevant information from the customer as per **Annexure 6**.

(vii) Accounts of Institutions / organizations / corporate bodies shall not be opened in the name of employee(s)/official(s).

5. **Compliance Program and Systems to prevent ML and TF:**

(i) The Company will establish and maintain programs and systems to prevent, detect and report ML/TF. The systems will be appropriate to the size of the Company and the ML/TF risks to which it is exposed and will include:

(a) Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;
(b) Policies and procedures to undertake a Risk Based Approach **("RBA")**;
(c) Internal policies, procedures and controls to combat ML/TF, including appropriate risk management arrangements;
(d) Customer Due Diligence measures;
(e) Record keeping procedures under AML rules and regulation;
(f) Group-wide AML/CFT programs;
(g) An audit function to test the AML/CFT system;
(h) Screening procedures to ensure high standards when hiring employees; and
(i) An appropriate employee-training program.

ii. It will be the responsibility of the Senior Management to ensure that appropriate systems are in place to prevent, detect and report ML/TF and the Company is in compliance with the applicable legislative and regulatory obligations.

6. **The Three Lines of Defense:**

(i) The Company will promote self-assessment culture at every level, making each function primarily accountable for its domain of responsibilities rather than dwelling on Compliance, Risk Management and Internal Audit to identify non-compliances, including ML/TF related non-compliance, in their reviews. To promote this Company will enforce three lines of defense concept;

(a) **First Line:** Although each unit will act as first line of defense for its own activities, the business units (e.g. front office, customer-facing staff/traders) and Operations department in particular will ensure in-depth knowledge of AML/CFT related requirements and will carry out the AML/CFT due diligence policies and procedures and be allotted sufficient resources and training to do this effectively;

(b) **Second Line:** This includes Compliance Department, Risk Management Department, Finance Department, Human Resources Department and Information Technology. These support functions will provide support for AML/CFT related compliances in the capacity of Company's second line of defense whereby, Finance will screen payments and ensure that cheques are received and paid to the customer only within defined threshold, Human Resource will perform adequate screening of each employee and ensure their timely trainings as per training schedule, Compliance will review fulfillment of all KYC related requirements at the time of on-boarding of customers/employees, review account closing and fund transfer processes at specified intervals, review of ongoing monitoring activities, provide support for continuous staff trainings, raising STRs and coordinating with all departments and regulatory bodies.

(c) **Third Line**: The Internal Audit function along with Board Audit Committee will act as the Company's final line of defense, which will ensure that first two lines of defense are performing their duties, including AML/CFT related compliances, as per Company's established policies and procedures, and these policies and procedures are aligned with country's regulatory framework.

(ii) In order to enable all employees in discharging their duties as first line of defense, policies and procedures will be clearly specified in writing and communicated to all employees. These will contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activities of the Company in compliance with the

Regulations. These include internal procedures for detecting, monitoring and reporting suspicious transactions.

(iii) As part of second line of defense, the CO must have the authority and ability to oversee the effectiveness of the Company's AML/CFT systems, compliance with applicable AML/CFT legislation and provide guidance in day-to-day operations of the AML/CFT policies and procedures.

(iv) CO must be a person who is fit and proper to assume the role and who:

(a) has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
(b) reports directly and periodically to the Board on AML/CFT systems and controls;
(c) has sufficient resources, including time and support staff;
(d) has access to all information necessary to perform the AML/CFT compliance function;
(e) ensures regular audits of the AML/CFT program;
(f) maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and requests from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigations; and
(g) Responds promptly to requests for information by the SECP/LEAs.
(h) Maintains confidentiality of affairs unless under duty to disclose to competent authority by operation of any law.

(v) An independent Internal Audit function, the third line of defense, should periodically conduct AML/CFT audits on an Institution-wide basis and be proactive in following up their findings and recommendations. As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate as approved by the Board, subject to any prescribed auditing requirements applicable to AML/CFT measures.

7. **Assessment of TF Threat:**

The company assesses TF threats initially at the time of account opening of the clients. The assessment is based on data available at UN sanctions committee's website, National Counter Terrorism Authority's website and different SROs issued by the Federal Government.

The company also performs screening of its existing entire clientele from the data available at the above mentioned regulatory websites and SROs.

During this exercise, in case of true match or suspicion, the authorized officer of the company is responsible to comply all the sanctions obligations including:

- Freeze the customer fund or block the transaction (existing customer)

- Reject the customer (new client)
- Lodge STR with FMU
- Notify the SECP and MOFA

As per the updated NRA 2019, Pakistan is facing terrorism and TF threat from terrorist organizations in Afghanistan, Afghan Refugees in Pakistan and in areas adjacent to Pak-Afghan border areas. Further, long porous border with Iran and Afghanistan is a major cause of crimes and Terrorist Financing. Therefore, in view of this information, we have updated risk of all those clients who belongs to these high risk areas. Their transactions are being monitored regularly as part of our ongoing monitoring. Inflows and outflows of the funds are properly monitored and investigated. Different systematic reports have been designed to analyze their transactions with their sources of income.

Screening is also performed for entities of concern mentioned in updated NRA 2019. The policy of the company in case of true match or suspicion is same as explained above.

It is mentioned in policy that the Company should not provide services to proscribed individuals, groups and entities declared by UNSC (United Nations Security Council) or notified by NACTA and those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

8. **Risk Assessment and Applying a Risk Based Approach ("RBA"):**

(i) The RBA enables the Company to ensure that AML/CFT 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 e.g. daily system-based sanction screening. As a part of the RBA, The Company:

(a) Identify ML/TF risks relevant to it;
(b) Document risk assessment
(c) Assess ML/TF risks in relation to all the relevant risk factors-
    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.
(d) Design and implement Policies, Controls and Procedures that are approved by its Board to manage and mitigate the ML/TF risks identified and assessed;

(e) Monitor and evaluate the implementation of mitigating controls and improve systems where necessary;
(f) Keep its risk assessments current through ongoing reviews and, when necessary, updates;
(g) Mark house risk assessment overall
(h) Implement and monitor procedures and updates to the RBA; and
(i) Have appropriate mechanisms to provide risk assessment information to the Commission.

(ii) Under the RBA, the following mechanism will be applied:

(a) where there are higher risks, the Company takes enhanced measures to manage and mitigate those risks; and
(b) Correspondingly, where the risks are lower, simplified measures are permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF.
(c) 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.

(iii) 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:

(a) risk assessment based on; National ML threats, Sectoral ML and TF risks and vulnerabilities
(b) CDD checks;
(c) transaction monitoring;
(d) escalation of suspicions; and
(e) Liaison relationships with the authorities.

(iv) The process of ML/TF risk assessment has four stages:

(a) Identifying the area of the business operations susceptible to ML/TF;
(b) Conducting an analysis in order to assess the likelihood and impact of ML/TF;
(c) Managing the risks;
(d) Regular monitoring and review of those risks; and
(e) Identification, Assessment and Understanding Risks.

(v) **The first step** in assessing ML/TF risk is to identify the risk categories, i.e. Customers, Countries or Geographical locations, Products and Services, Transactions and Delivery Channels that are specific to the Company.

(vi) **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 the followings:

(a) Financial loss to the Company from the crime and monitory penalties from regulatory authorities or the process of enhanced mitigation measures.
(b) 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.

(vii) 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:

(a) High, if it can occur several times per year;
(b) Medium if it can occur once per year; and
(c) Low if it is unlikely, but possible.

(viii) 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.

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

(ix) 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, practices, 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:

(a) How likely an event is;
(b) Consequence of that event;

(c) Vulnerability, threat and impact;
(d) The effect of uncertainty on an event;

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

9. Risk Assessment Mechanism:

(i) Risk Assessment (lower complexity):

The 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:

(a) Unlikely - There is a small chance of ML/TF occurring in this area of the business;
(b) Possible - There is a moderate chance of ML/TF occurring in this area of the business;
(c) Almost Certain - There is a high chance of ML/TF occurring in this area of the business

(ii) Risk Assessment (moderate complexity):

(a) 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.
(b) 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.
(c) 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.

(iii) Risk Assessment (higher complexity)

(a) The Company will further assess risk likelihood in terms of threat and vulnerability.
(b) Determining the impact of ML/TF activity can be challenging but to focus AML/CFT resources in a more effective and targeted manner. When determining impact, Company can consider a number of factors, including:
    a. Nature and size of your business (domestic and international);
    b. Economic impact and financial repercussions;
    c. Potential financial and reputational consequences;
    d. Terrorism-related impacts;

e. Wider criminal activity and social harm; 6) Political impact;
f. Negative media.
g. Cross boarder fund transfer for non-resident and foreign clients

(c) The Company wills more weight to certain factors to provide a more enhanced understanding of your ML/TF risk.
(d) In addition, Company may consider how its risks can compound across the various risk factors.

(iv) **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.

(a) New and Developing Technologies and Products:

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

(b) 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.

(v) The 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.

(vi) 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.

(a) High-Risk Classification Factors:

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

   i. The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the Company and the customer):
   ii. Non-resident customers;
   iii. Politically Exposed Persons (PEPs);
   iv. Legal persons or arrangements;
   v. Companies that have nominee shareholders;
   vi. Business that is cash-intensive;
   vii. The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons;
   viii. shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions (i) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets;

ix. Requested/Applied quantum of business does not match with the profile/particulars of client;
x. Not-For-Profit organization ("NPOs") with association with political parties or religious groups;
xi. Real Estate Dealers;
xii. Dealers in precious metal and stones, and
xiii. Designated Non-Financial Business and Professionals (DNFBPs) such as Lawyers/notaries, accountants.

Scenarios of Customer Types

i. **Small and Medium Sized Enterprises:**

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

ii. **International Corporations:**

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

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.

b. Country or geographic risk factors:

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

i. Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems;

ii. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;

ii. 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;

iii. Entities and individuals from jurisdictions which are known tax heavens;

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

v. Clients belonging to southern Punjab, KPK, Baluchistan and cross border areas of Pakistan.

c. Product, service, transaction or delivery channel risk factors:

The 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:

i. Anonymous transactions (which may include cash);

ii. Non-face-to-face business relationships or transactions;

iii. Payments received from unknown or un-associated third parties;

iv. International transactions, or involve high volumes of currency (or currency equivalent) transactions (e) One-off transactions;

v. Transaction for which payments are made from more than two bank accounts of a customer;

vi. Products that involve large payment or receipt in cash; and (h) One-off transactions; and

vii. 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?

(b) **Low Risk Classification Factors:**

a. Customer risk factors:

i. 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

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

b. Product, service, transaction or delivery channel risk factors:

Financial products or services that provide appropriately defined and limited services to certain types of customers.

c. Country risk factors:

i. Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.

ii. 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.

(vii) 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	Online Transactions	Domestic Transfers	Deposit or Investment	Securities 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

Note: When conducting risk assessment, the Company does not have to follow the processes in this document. As long as it complies with the obligations under the Act and any other applicable laws or regulations, the Company has a choice to select the method of risk.

(a) Risk Management:

(i) **Risk Mitigation**

i. The 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. M nature and extent of AML/CFT controls the Company puts in place depends on a number of aspects, which include:

   a. The nature, scale and complexity of the Company's business;
   b. Diversity, including geographical diversity of the Company's operations;
   c. The Company's customer, product and activity profile;
   d. Volume and size of transactions;
   e. Extent of reliance or dealing through third parties or intermediaries, which is minimal in case of Company and restricted to Administration department related services;

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

i. determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;

ii. setting transaction limits for higher-risk customers or products;

iii. requiring senior management approval for higher-risk transactions, including those involving PEPs;

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

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

(ii) <u>Evaluating Residual Risk and Comparing with the Risk Tolerance</u>:

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.

10. **Monitoring AML/CFT Systems and Controls:**

(i) The Company will have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. The Company will update their systems as appropriate to suit the change in risks.

(ii) Additionally, the Company will assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed. For that purpose, the Company will need to consider monitoring certain aspects which include:

(a) the ability to identify changes in a customer profile or transaction activity/behaviour, which come to light in the normal course of business;
(b) the potential for abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;
(c) the adequacy of employee training and awareness;
(d) the adequacy of internal coordination mechanisms i.e., between AML/CFT compliance and other functions/areas;
(e) the compliance arrangements (such as internal audit);
(f) changes in relevant laws or regulatory requirements; and
(g) Changes in the risk profile of countries to which the Company or its customers are exposed to.

11. **Documentation and Reporting:**

(i) Documentation of relevant policies, procedures, review results and responses will enable the Company to demonstrate to the Commission:

(a) risk assessment systems including how the Company will assess ML/TF risks;
(b) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;

(c) how it will monitor and, as necessary, improves the effectiveness of its systems and procedures; and
(d) the arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

(ii) The Company will note that the ML/TF risk assessment is not a one-time exercise and therefore, they must ensure that their ML/TF risk management processes are kept under regular review which is at least annually. Further, the Company management should review the program's adequacy when the reporting entity adds new products or services, opens or closes accounts with high-risk customers, or expands through mergers or acquisitions.

(iii) The Company will demonstrate to the Commission, the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance policy; its procedures and policies concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT, during the SECP's on-site inspection. The Company will maintain Risk Assessment Tables (Annexure 1), AML/CFT Compliance Assessment Template (Annexure 2) and Control Assessment Template (Annexure 3) within the period as required by the Commission from time to time.

12. **New Products, Practices and Technologies:**

(i) 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:

(a) Electronic verification of documentation;
(b) Data and transaction screening systems; or
(c) The use of virtual or digital currencies

(ii) The 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.

(iii) 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.

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

(v) 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.

13. **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").

(a) CO shall assess the suitability of the respondent financial institution by taking the following steps

i. gather adequate information about the respondent financial institution to understand fully the nature of the respondent financial institution's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

ii. determine from any available sources the reputation of the respondent financial institution and the quality of supervision over the respondent financial institution, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and

iii. assess the respondent financial institution's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent financial institution operates.

(b) CO shall clearly understand and document the respective AML/CFT responsibilities of the financial institution and the respondent financial institution;

(c) CO assess the respondent financial institution in the context of sanctions/embargoes and Advisories about risks; and

(d) CO shall obtain approval from the senior management before providing correspondent services to a new financial institution

14. **Customer Due Diligence and Beneficial Ownership:**

(i) The Company will take steps to know who their customers are. The Company as a policy matter will not open anonymous accounts or accounts in fictitious names and alias. Hence, for customers which are natural person, names contained in their CNIC / NICOP / Passports will be used as title of account, and same is verified from NADRA Verisys record. For entities the title of account offered is same as the one contained in their establishing/incorporation document. The Company will conduct CDD, which will comprise 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.

(ii) Additionally, Company will conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, its business and risk profile (Annexure 4), including, where necessary, the source of funds. The Company will conduct CDD when establishing a business relationship if:

(a) There is a suspicion of ML/TF, Annexure 5 gives some examples of potentially suspicious activities or "red flags" for ML/TF. Although these may not be exhaustive in nature, it may help the Company to recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose; or

(b) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.

(iii) In case of suspicion of ML/TF, the Company will:

(a) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and

(b) File an STR with the FMU, in accordance with the requirements under the Law.

(iv) The Company will monitor transactions to determine whether they are linked. Transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold.

(v) The Company will verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys. Similarly, the Company will identify and verify the customer's beneficial owner(s) to ensure that the Company understands who the ultimate beneficial owner is.

(vi) The Company will ensure that it understands the purpose and intended nature of the proposed business relationship or transaction. The Company will assess and ensures that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

(vii) The Regulations require the Company to identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person"). In this regard Company will also verify whether that authorized person is properly authorized to act on behalf of the customer by demanding an authorization letter in Company's designed pro-forma (which requires reason for using third person) and matching customer signatures against those in Company's record. Customer Call Back confirmation will also performed where customer signatures would be doubtful. The Company will conduct CDD on the authorized person(s) using the same standards that are applicable to a customer.

(viii) The Company may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa.

(ix) When performing CDD measures in relation to customers that are legal persons or legal arrangements, the Company identifies and verifies the identity of the customer, and understands the nature of its business, and its ownership and control structure.

(x) The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and second, to take appropriate steps to mitigate the risks. In this context, the Company will identify the customer and will verify its identity. The type of information that will be needed to perform this function shall be as specified in **Annexure 6**.

(xi) If the Company will have any reason to believe that an applicant has been refused facilities by another Brokerage house due to concerns over illicit activities of the customer, it will consider classifying that applicant as higher-risk and will apply enhanced due diligence procedures to the customer and the relationship, filing an STR and/or not accepting the customer in accordance with its own risk assessments and procedures.

(a) Timing of Verification:

a. The Company will undertake verification prior to entry into the business relationship or conducting a transaction.
b. Where CDD checks will raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/TF, the Company will decline trading accounts to such customers. In such situations, the Company will consider filing an STR with the FMU and will ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

(b) Existing Customers:

a. The Company will apply CDD/EDD 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. For this purpose,

Company will perform CDD/EDD measures on its existing customers at the frequency as defined in the following section of Period Risk Reviews.

b. Further, if the Company will have suspicion of ML/TF or will become aware at any time that it lacks sufficient information about an existing customer, it will take steps to ensure that all relevant information is obtained as quickly as possible irrespective of CDD/EDD revised information collection frequency set as per risk classification of customer.
c. The Company will 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 Company to have doubt include significant change in the value of injections into his/her trading account, or change in correspondent address to an area / country with high susceptibility to money laundering, terrorist financing or other predicated offences.
d. In case of existing customers who opened accounts with old NICs, the compliance officer shall collect attested copies of identity documents shall be present in the regulated person record. The regulated person shall block accounts without identity document (after serving one-month prior notice) for all withdrawals, until the subject regulatory requirement is fulfilled. However, upon submission of attested copy of identity document and verification of the same from NADRA or biometric verification, the block from the accounts shall be removed.
e. The customers whose accounts are dormant or in-operative, withdrawals shall not be allowed until the account is activated on the request of the customer. For activation, the CO shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfill the regulatory requirements.
f. Where the Company will be unable to complete and comply with ongoing CDD/EDD requirements as specified above, the Company will terminate the relationship. Additionally, the Company will consider filing an STR to the FMU.

(c) Tipping-off & Reporting:

a. The Law prohibits tipping-off any information about the suspicious matter to the concerned customer or to a person not relevant in the process of filing an STR. However, a risk exists that customers could be unintentionally tipped-off when the Company is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.
b. Therefore, if the Company will form a suspicion of ML/TF while conducting ongoing CDD/EDD, it will take into account the risk of tipping-off when performing the CDD process. If the Company reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it might not pursue that process, and will

file an STR. For this Company will ensure that its employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD/EDD.

(xii) No Simplified Due Diligence for Higher-Risk Scenarios:

The Company will not adopt simplified due diligence measures where the ML/TF risks are high. The Company will identify risks and have regard to the risk analysis in determining the level of due diligence to be performed in each case.

15. **Period Risk Review ("PRR"):**

The Company will perform periodic customer profile updating exercise every two years for customers classified as high risk while perform this exercise every four years for Low risk classified customers.

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

(a) Material changes to the customer risk profile or changes to the way that the account usually operates;
(b) Where it comes to the attention of the Company that it lacks sufficient or significant information on that particular customer;
(c) Where a significant transaction takes place;
(d) Where there is a significant change in customer documentation standards;
(e) Significant changes in the business relationship.

Examples of the above circumstances include:

(a) A significant increase in a customer's deposits;
(b) The stated turnover or activity of a customer increases;
(c) A person has just been designated as a PEP;
(d) The nature, volume or size of transactions changes.

16. **On-going 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.

(i) 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. CO shall obtain information and examining, as far as possible, the background and purpose of all complex and unusual transactions which have no apparent economic or visible lawful purpose. The background and purpose of these transactions shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required. Co shall undertake to reviews of existing records and ensuring that documents, data or information collected for the CDD purposes is kept up-to-date and relevant, particularly for higher risk categories of customers. 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 provide 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.

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

(a) transaction type;
(b) frequency;
(c) amount;
(d) geographical origin/destination;
(e) account signatories;
(f) mandate

(iii) 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 uses 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.

(iv) The compliance staff shall monitor the existing records of the customer and evaluate the transaction whether to call/ follow-up for further documents to justify the transaction or transactions patterns. To keep the document up to date and correct risk categorization in higher risk factors.

(v) All assessment shall be recorded with updated records, recording the reason for the assessment and risk classification change if necessary and filing STR where suspicion on client activity and its profile monitoring.

17. Simplified Due Diligence Measures ("SDD")

The Company may conduct SDD in case of lower risks identified by it. However, the Company will ensure that the low risks it identified commensurate with the low risks identified by the country or the Commission. While determining whether to apply SDD, Company pays particular attention to the level of risk assigned to the relevant sector, type of customer or activity.

The simplified measures Company will apply shall be commensurate with the low risk factors.

The Company however will not use SDD procedures in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.

Where the Company to take SDD measures on an applicant/customer, it will document the full rationale behind such decision and maintain its record to make it available to the Commission on request.

18. **Enhanced CDD Measures ("EDD")**

The Company will examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF, PEPs and their close associates and family members that have no apparent economic or lawful purpose.

Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, the Company will conduct enhanced CDD measures, consistent with the risks identified. In particular, the Company will increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

(a) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
(b) Updating more regularly the identification data of applicant/customer and beneficial owner;
(c) Obtaining additional information on the intended nature of the business relationship.
(d) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.
(e) Obtaining additional information on the reasons for intended or performed transactions.
(f) Obtaining the approval of senior management to commence or continue the business relationship.
(g) 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.

(i) High-Risk Countries:

Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to the Company. Conducting a business relationship with an applicant/customer from such a country exposes the Company to reputational risk and legal risk.

The Company will exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

Caution will also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks will be undertaken on such individuals/entities to ensure their legitimacy and reliability.

The Company therefore will consult publicly available information to ensure that they are aware of the high-risk countries/territories. While assessing risk of a country, the Company will also 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) and Transparency international corruption perception index.

Useful websites include: FATF website at www.fatf-gafi.org and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

Information about these high-risk geographies will be provided to employees in on-going trainings and will be disseminated through pan-Company broadcast messages once every six months.

19. Politically Exposed Persons:

(i) Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose the Company to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes, grease money or commit fraud. Such persons, commonly referred to as PEPs and defined in the Regulations, an include inter-alia, heads of state, ministers, influential public officials, judges and senior military officials and includes their family members and close associates, hereinafter referred to as linked PEPs.

(ii) Family members of a PEP are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. Close associates to PEPs are individuals who are closely connected to PEP, either socially or professionally.

(iii) Provision of financial services to corrupt PEPs exposes the Company to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. Hence, Company will remain extra vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. The Company should, in relation to PEPs, in addition to performing normal due diligence measures will:

(a) have appropriate risk management systems to determine whether the customer is a PEP;
(b) obtain senior management approval for establishing business relationships with such customers; (3) take reasonable measures to establish the source of wealth and source of funds; and
(c) Conduct enhanced ongoing monitoring of the business relationship.

18. The Company will obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.
19. The Company will take a risk-based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, Company will consider factors such as whether the customer who is a PEP:
    (a) Is from a high-risk country;
    (b) Has prominent public functions in sectors known to be exposed to corruption;
    (c) Has business interests that can cause conflict of interests (with the position held).
20. The other red flags that the Company will consider include (in addition to the above and the red flags that they consider for other applicants):
    (a) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
    (b) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;

(c) A PEP uses multiple bank accounts for no apparent commercial or other reason;
(d) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

21. The Company will take a risk-based approach in determining whether to continue to consider a customer as PEP who is no longer PEP. The factors that they 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).

20. Reliance on Third Parties:

The Company may rely on a third party to conduct CDD on its behalf as set out in provisions 8-23 of these AMLA regulations 2020 whenever contracted with third party.

21. TFS Obligations:

(1) The CO shall undertake TFS obligations under the United Nations (Security Council) Act 1948,or Anti-Terrorism Act 1997, United Nations Security Council (Freezing and Seizure) Order, 2019, Statutory Regulatory Orders (SROs) issued under UNSC Act, Notifications issued under ATA, AML Act, 2010 and rules, regulations and directives issued thereunder, including:

(a) CO Shall develop mechanisms, processes and procedures for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with the stated designated/proscribed persons in the SROs and notifications issued by MoFA, NACTA and MoI.

(b) If during the process of screening or monitoring of customers or potential customers the CO finds a positive or potential match, it shall immediately:

i. freeze the relevant funds and assets without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer in accordance with the respective SRO. prohibit from making any funds or other assets, economic resources, or financial or other related services and funds in accordance with the respective SRO
ii. Reject the transaction or attempted transaction or the customer, if the relationship has not commenced.
iii. In all cases referred to in (b), the CO shall file a suspicious transaction report to the FMU in case that person is designated under United Nations Security Council Resolutions, or proscribed under the Anti-Terrorism Act, 1997 and simultaneously notify the Commission in the manner as may be instructed from time to time by the Commission.
iv. Implement any other obligation under the AML Act 2010, United Nations (Security Council) Act 1948 and Anti-Terrorism Act 1997 and any regulations made there under.

(2) The Company is prohibited, on an ongoing basis, from providing any financial services to proscribed/ designated entities and persons or to those who are known for their association

with such entities and persons, whether under the proscribed/ designated name or with a different name. The regulated person should monitor their business relationships with the entities and individuals on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the regulated person shall take immediate action as per law, including reporting to the FMU.

22. Record-Keeping Procedures:

The Company will ensure that all information obtained in the context of CDD is recorded. This includes both;

(i) recording the documents the Company is provided with when verifying the identity of the customer or the beneficial owner, and
(ii) Transcription into the Company owns IT systems of the relevant CDD information contained in such documents or obtained by other means.

The Company will maintain, for at least five years after termination, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity.

Where there has been a report of a suspicious activity or the Company becomes aware of a continuing investigation or litigation into ML/TF relating to a customer or a transaction, records relating to the transaction or the customer will be retained until confirmation is received from the relevant authority in writing that the matter has been concluded.

The Company will also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of five years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to relevant competent authorities upon request.

Beneficial ownership information will be maintained for at least five years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer of the Company.

Records relating to verification of identity will generally comprise:

(a) a description of the nature of all the evidence received relating to the identity of the verification subject; and
(b) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

Records relating to transactions will generally comprise:

(a) details of personal identity, including the names and addresses, of
    a. the customer; and
    b. the beneficial owner of the account or product
(b) details of securities and investments transacted including: a. the nature of such securities/investments;
(c) valuation(s) and price(s);
(d) memoranda of purchase and sale;
(e) source(s) and volume of funds and securities;
(f) destination(s) of funds and securities;
(g) memoranda of instruction(s) and authority(ies);
(h) book entries;
(i) custody of title documentation;
(j) the nature of the transaction;
(k) the date of the transaction;
(l) The form (e.g. cash, cheque) in which funds are offered and paid out.

23. Reporting of Suspicious Transactions / Currency Transaction Report

A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction will be considered unusual, and Company will put the case "on enquiry". The Company will also pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

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

Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result will be properly documented, and made available to the relevant authorities upon request. Activities which will require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

(a) any unusual financial activity of the customer in the context of the customer's own usual activities;
(b) any unusual transaction in the course of some usual financial activity;
(c) any unusually-linked transactions;
(d) any unusual method of settlement;

(e) any unwillingness to provide the information requested.

Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, the Company will need to approach such situations with caution and make further relevant enquiries. Company will set its own parameters at Rs. 25,000 for the identification and further investigation of cash transactions.

Where the Company will be unable to satisfy that any cash transaction is reasonable it will be considered as suspicious. The Company will also be obligated to file Currency Transaction Report ("CTR"), to FMU for a cash based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

If the Company decides that a disclosure should be made, the law requires the Company to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2015. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.

The process for identifying, investigating and reporting suspicious transactions to the FMU is clearly specified in the Company's KYC/CDD SOPs and communicated to all personnel through regular training.

The Company will also be required to report total number of STRs filed to the Commission on a bi-annual basis within seven days of close of each half year. The CO will ensure prompt reporting in this regard.

The Company will evolve a vigilance system for the purpose of control and oversight, which requires maintenance of a register of all reports made to the FMU. Such registers will be maintained and updated by CO and will contain details of:

(a) the date of the report;
(b) the person who made the report;
(c) the person(s) to whom the report was forwarded; and
(d) Reference by which supporting evidence is identifiable.

The Company as a matter of policy will turn away business where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration will be given to filing an STR to the FMU.

For existing customers, once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity, the Company will ensure that appropriate action is taken to adequately mitigate the risk of the Company being used for criminal activities. This will include a review of either the risk classification of the customer or account or of the entire relationship itself. In such cases an escalation will be made to the Chief Executive Officer to

determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

24. Sanctions Compliance

Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them. There are also sanctions that target those persons and organizations involved in terrorism. The types of sanctions that may be imposed include:

(a) targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly;
(b) economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly;
(c) currency or exchange control;
(d) arms embargoes, which would normally encompass all types of military and paramilitary equipment;
(e) prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;
(f) import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.; and (7) visa and travel bans.
(g) Targeted financial sanctions relating to the prevention, suppression and disruption of proliferation of Weapons of Mass Destruction (WMD) and its financing.

As required by Regulations Company will screen all its customers against consolidated sanctions list available on UNSC's website and will decline business relationship with the individuals/entities and their associates that are either, sanctioned under UNSC Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

The UNSC Resolution 1267 (1999), 1989 (2011), 2253 (2015) and other subsequent resolutions, which impose sanctions covering; asset freeze, travel ban and arms embargo, against individuals and entities associated to Al- Qaida, Taliban, and the Islamic State in Iraq (Daésh) organizations. The regularly updated consolidated lists are available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

The UNSC Resolution 1373 (2001), 1998 (2011) on terrorism and financing of terrorism requiring member states to proscribe individual and entities, who commit or attempt to commit terrorist act, freeze without delay the funds and other financial assets or economic resources, and prohibit making any funds or financial or other related services available to such proscribed persons and entities.

The UNSC Resolution 1718(2006), 2231(2015) and its successor resolutions [1] on proliferation of WMD and its financing, and Targeted Financial Sanctions (TFS) on countries and specifically identified individual and entities associated with it. The resolution requires, inter-alia freezing without delay the funds or other assets of, any person or entity designated, or under the authority of UNSC. The regularly updated consolidated lists of person and entities designated under UNSCRR 1718(2006) and its successor resolutions (on the DPRK) and listed under UNSCR 2231 (2015) (on Iran) is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/1718/materials
https://www.un.org/sc/2231/list.shtml

Government of Pakistan, Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 (Act No XIV of 1948) to give effect to the UNSC Resolutions and implement UNSC sanction measures in Pakistan. The said SROs are communicated to the Company, from time to time, and have a binding legal effect under the Act No. XIV of 1948. Company will ensure compliance with the sanctions communicated through SROs. A list of such SROs issued by the Federal Government till date is also available at the following links:

UNSCR1267http://www.mofa.gov.pk/contentsro1.php
http://www.mofa.gov.pk/contentsro2.php

UNSCR 1718 http://www.secdiv.gov.pk/page/sro-unscr-sanctions

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

The individuals and entities designated under the aforementioned resolutions are subject to sanctions including assets freeze, travel ban and ban on provision of any funds, financial assets or economic recourses. Such sanctions also extend to any funds, financial assets and economic

[1] The UNSC sanctions with respect to proliferation of WMD primarily encapsulate currently the Islamic Republic of Iran and the Democratic People's Republic of Korea's sanctions regime. The UNSC resolution on Iran is 2231 (2015). The UNSC resolution on Democratic People's Republic of Korea are 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), 2375 (2017) and 2397 (2017).

resources indirectly owned by the designated individuals, and to individuals or entities acting on their behalf or on their direction.

The Company will, taking note of the circumstances where customers and transactions are more vulnerable to be involved in TF and PF activities[2], identify high-risk customers and transactions, and apply enhanced scrutiny. Company will conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names in the abovementioned lists, to determine if the business relations involve any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

The Company will also screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list. Company will undertake reasonable efforts to collect additional information in order to identify, and avoid engaging in prohibited activities and, to enable follow-up actions.

Where there is a true match or suspicion, Company will take steps that are required to comply with the sanction's obligations including immediately –

(a) Freeze without delay[3] the customer's fund or block the transaction, if it is an existing customer;

(b) Reject the customer, if the transaction has not commenced;

(c) Lodge a STR with the FMU; and (d) notify the SECP and the MOFA.

The Company will submit an STR when there is an attempted transaction by any of the listed persons.

The Company will ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether it is a true match. In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, the Company will consider raising an STR to FMU.

Notwithstanding the funds, properties or accounts are frozen, Company will continue receiving dividends, interests, or other benefits, but such benefits shall still remain frozen, so long as the individuals or entities continue to be listed.

[2] The circumstances that the Company shall take note of where customers and transactions are more vulnerable to be involved in PF activities relating to both DPRK and Iran sanction regime are listed on Annexure 7 as PF Warning Signs/Red Alerts.[3] According to FATF, without delay is defined to be ideally within a matter of hours of designation by the UNSC

The Company will make their sanctions compliance program an integral part of their overall AML/CFT compliance program and accordingly should have policies, procedures, systems and controls in relation to sanctions compliance. Company will provide adequate sanctions related training to their staff. When conducting risk assessments, Company will take into account any sanctions that may apply (to customers or countries).

The obligations/ prohibitions regarding proscribed entities and persons mentioned in the above lists are applicable, on an ongoing basis, to proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed/ designated name or with a different name. Therefore, to mitigate the risk of having a sanctioned individual / entity in the portfolio of customer Company has implemented an in-house solution to screen the updated customer portfolio against Alerts are raised by the system on daily basis, which are reviewed and closed by CO on daily basis. Where there is a true match or suspicion, the CO raise the matter with the CEO with his proposal to comply with 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.

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

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

The Company will also educate its customers that in case of wrongful or inadvertent freezing, they may apply in writing for de-listing to Federal Government through relevant Ministry or to the UN's Ombudsman, as the case may be.

25. Internal Controls (Audit Function, outsourcing, employee screening and training)

The Company will put in place systems and controls that are comprehensive and proportionate to the nature, scale and complexity of its activities and the ML/TF risks they identified. The Company will establish and maintain internal controls in relation to:

(a) an independent internal audit function to test the AML/CFT systems, policies and procedures;
(b) outsourcing arrangements;
(c) employee screening procedures to ensure high standards when hiring employees; and
(d) an appropriate employee training program.

(i) Internal Audit Function:

The Company will, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit will be determined through annual risk assessment exercise and will commensurate with the

Company nature, size, complexity, and risks identified during the risk assessments. The scope of AML/CFT audits will cover assessment of the AML/CFT systems which include:

(a) testing the overall integrity and effectiveness of the AML/CFT systems and controls;
(b) assessing the adequacy of internal policies and procedures in addressing identified risks, including; (a) CDD measures;
(c) Record keeping and retention;
(d) Third party reliance; and
(e) Transaction monitoring;
(f) assessing compliance with the relevant laws and regulations;
(g) testing transactions in all areas of the Company, with emphasis on high–risk areas, products and services; (5) assessing employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
(h) assessing the adequacy, accuracy and completeness of training programs;
(i) assessing the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and
(j) Assessing the adequacy of the Company's process of identifying suspicious activity including screening sanctions lists.

(ii) Outsourcing

The 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, the 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.

(iii) **Employee Screening**

The Company's policy and procedures with regards to screening prospective and existing employees to ensure abidance with high ethical and professional standards are defined in these sections. The extent of employee screening will be proportionate to the particular risks associated with the individual positions.

Employee screening will be conducted at the time of recruitment and periodically thereafter, i.e., at least annually and where a suspicion has arisen as to the conduct of the employee.

The Company will 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 Company will:

(a) Verify the references provided by the prospective employee at the time of recruitment;
(b) Verify the employee's employment history, professional membership and qualifications from his resume and original copies of education documents.
(c) Verify details of any regulatory actions or actions taken by a professional body;
(d) Verify details of any criminal convictions; if possible and
(e) Verify whether the employee has any connections with the sanctioned countries or parties.

(iv) **Employee Training**

The Company will ensure that all staff, receive training on ML/TF prevention on a regular basis, ensure all staff fully understands the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

Training to staff will be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to the Company's business operations or customer base.

The Company will provide their staff training in the recognition and treatment of suspicious activities. Training will also be provided on the results of the Company's risk assessments. Additionally, this training will be structured to ensure compliance with all of the requirements of the applicable legislations pertaining to AML/CFT.

Training material will be designed to ensure staff is aware on the AML/CFT legislation and regulatory requirements, systems and policies. Additionally, focus will be given on the consequences should they fail to report information in accordance with internal procedures and legislation. One of the key focus of these training program will be active coordination with

customers and CO whereby all staff will be encouraged to provide a prompt and adequate report of any suspicious activities to the CO for inward reporting to FMU.

To make staff more accountable towards AML/CFT requirements, Company will obtain an undertaking from its staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read the Company's AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.

The Company is cognizant of the fact that all information regarding a potential or existing customer is not available on systems or on public domain immediately and human interaction plays an important role in identifying such information. Staff members who deal with the public such as traders are the first point of contact with potential money launderers, and their efforts are vital to an organization's effectiveness in combating ML/TF. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers. Training will be given on the factors which may give rise to suspicions about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.

Staff involved in the processing of transactions will receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. The training curriculum will contain information on types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff will also be made aware of the correct procedure(s) to be following in such circumstances.

The Company expects all staff to 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. In such cases whilst the Company may have previously obtained satisfactory identification evidence for the customer, the Company will take steps to learn as much as possible about the customer's new activities.

Although Directors and Senior Managers may not be involved in the handling of ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the Company itself given that these individuals are involved in approving AML/CFT policies and procedures. Hence the supervisors, managers and senior management (including the Board) will 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 will himself receive in-depth training on all aspects of the primary legislation, the Regulations, regulatory guidance and relevant internal policies. It will include 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

Procedure for Enhance Due Diligence:

To address the assessed ML/TF risk following controls are implemented and methods are used for high risk clients;

i) KYC/CDD process is performed for each client which includes the following;

- Approval from senior management for enhanced due diligence
- Biometric verification of the customer (Soft/Hard Copy)
- Verification of customer's identity
- Validation of identity documents through NADRA verisys (Soft/Hard Copy)
- Full name as per identity document;
- Father/Spouse Name as per identity document;
- Mother Maiden Name;
- Identity document number along with date of issuance and expiry;
- Existing residential address (if different from CNIC);
- Contact telephone number(s) and e-mail (as applicable);
- Nationality-Resident/Non-Resident Status
- FATCA/CRS Declaration wherever required;
- Date of birth, place of birth;
- Incorporation or registration number (as applicable);
- Date of incorporation or registration of Legal Person/ Arrangement;
- Registered or business address (as necessary);
- Nature of business, geographies involved and expected type of counter-parties (as applicable);
- Type of account/financial transaction/financial service;
- Profession / Source of Earnings/ Income: Salary, Business, investment income;
- Purpose and intended nature of business relationship;
- Expected monthly turnover (amount and No. of transactions); and
- Normal or expected modes of transactions/ Delivery Channels.
- Verification of customer's mailing and permanent addresses
- Verification of customer's source of income with supporting documents
- Identification of beneficial owner

ii) The photocopies of identity documents shall be validated through NADRA verisys or Biometric Verification. The regulated person shall retain copy of NADRA Verysis or Biometric Verification (hard or digitally) as a proof of obtaining identity from customer.

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

iv) In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that regulated person shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account.

v) For CNICs which expire during the course of the customer's relationship, regulated person shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, regulated person are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.

vi) The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the regulated person.

vii) The condition of obtaining 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 verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.

viii) Government entities accounts shall not be opened in the personal names of a government official. Any account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government.

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

Minimum documents required for CDD shall be in accordance with **Annex 1** of Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2020.

Screening of customers through UN sanctions committee's website, National Counter Terrorism Authority's website and different SROs issued by the Federal Government

Ongoing monitoring of the clients which includes monitoring of their trading activities and their receipts and payments, etc. Enhanced Due Diligence (EDD) process in which more documentary evidences are obtained from the customers to verify their source of income, etc.

Procedure: Account Opening, KYC CDD/EDD/AML Procedures and Other Processes

1. SUMMARY

1.1. This procedure defines the methods used to identify and (where applicable) the standard Account Opening, KYC/AML Procedures and Processes at Aba Ali Habib Securities (Pvt.) Ltd premises and services offered. This procedure includes methods:

1.1.1. To define the methods for identifying the standard Account Opening, KYC/AML Procedures and Processes at Aba Ali Habib Securities (Pvt.) Ltd premises and services offered (what they are)

1.1.2. Customer Identification (Customer visits, Biometric, NACTA Screening, NADRA verisys)

1.1.3. Risk Assessment (KYC, SDD, CDD, EDD, Receipt and Payment Monitoring, Trade monitoring, Risk profiling based on customer type, product and service, geography and transaction channels like (profession, residential status, PEP, high net worth, customer type, beneficial owner identification, high risk jurisdiction like cross boarder, transactions types)

1.1.4. Simplified Due Diligence

1.1.5. Customer Due Diligence

1.1.6. Enhanced Due Diligence

1.1.7. On-going Monitoring

1.1.8. Filing CTR/STR to FMU

1.1.9. Customer database maintenance

1.1.10. Periodic Reporting to Customers

1.1.11. Account Closing

1.1.12. SECP compliance relevant to AML/CFT

1.1.13. PSX, NCCPL, CDC Reporting

1.2. The compliance manager is responsible for implementation and risk management of this procedure.

2. APPLICATION

2.1. This procedure applies to all departments that are interlinked, deals with AAHSLs at all Aba Ali Habib Securities (Pvt.) Ltd facilities.

2.2. This procedure not only applies to typical services, but also deliverables from services, such as reports, schedules, etc.

3. DEFINITIONS

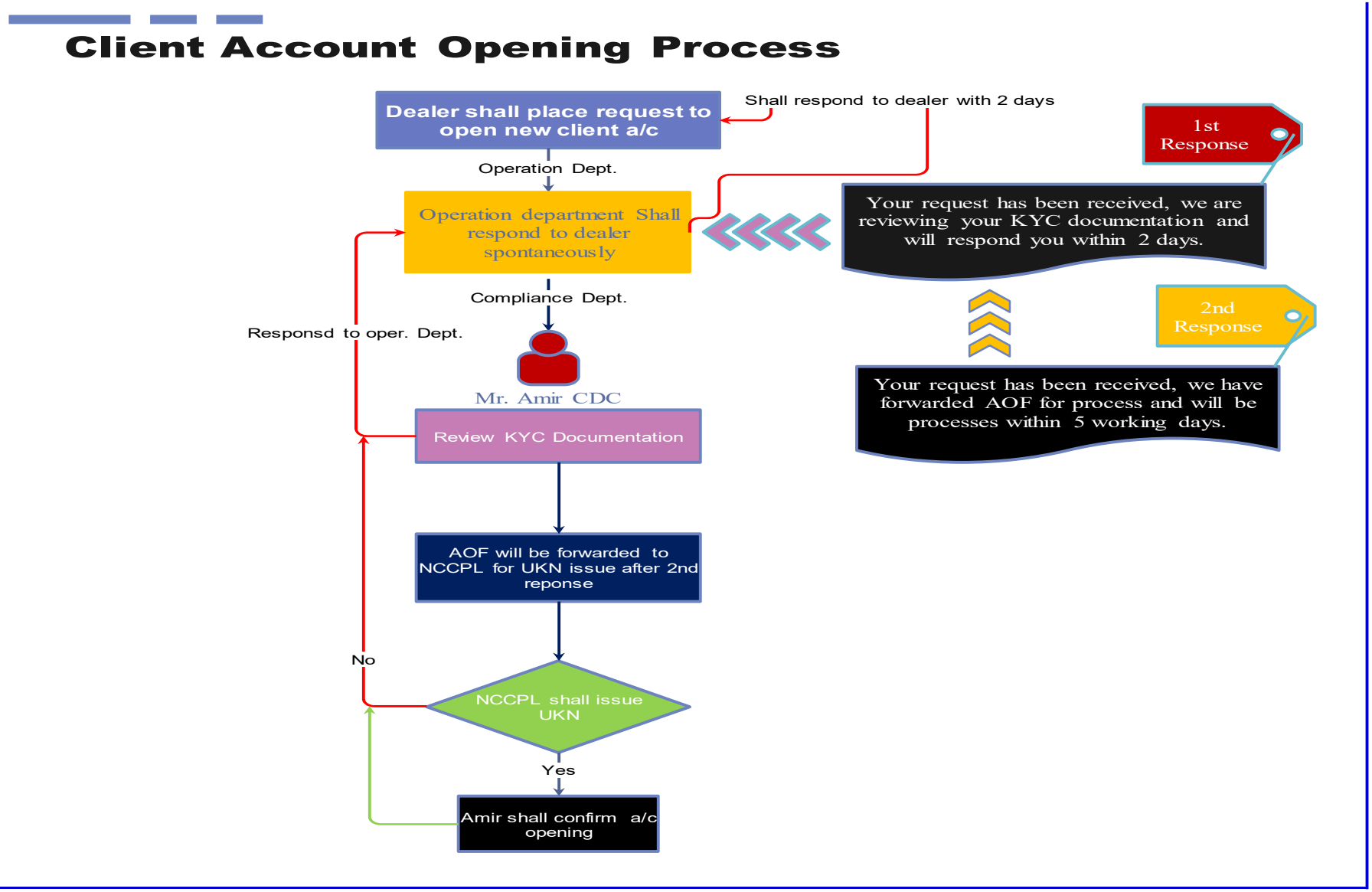
3.1. Service

3.1.1. “Service” includes any of the following:

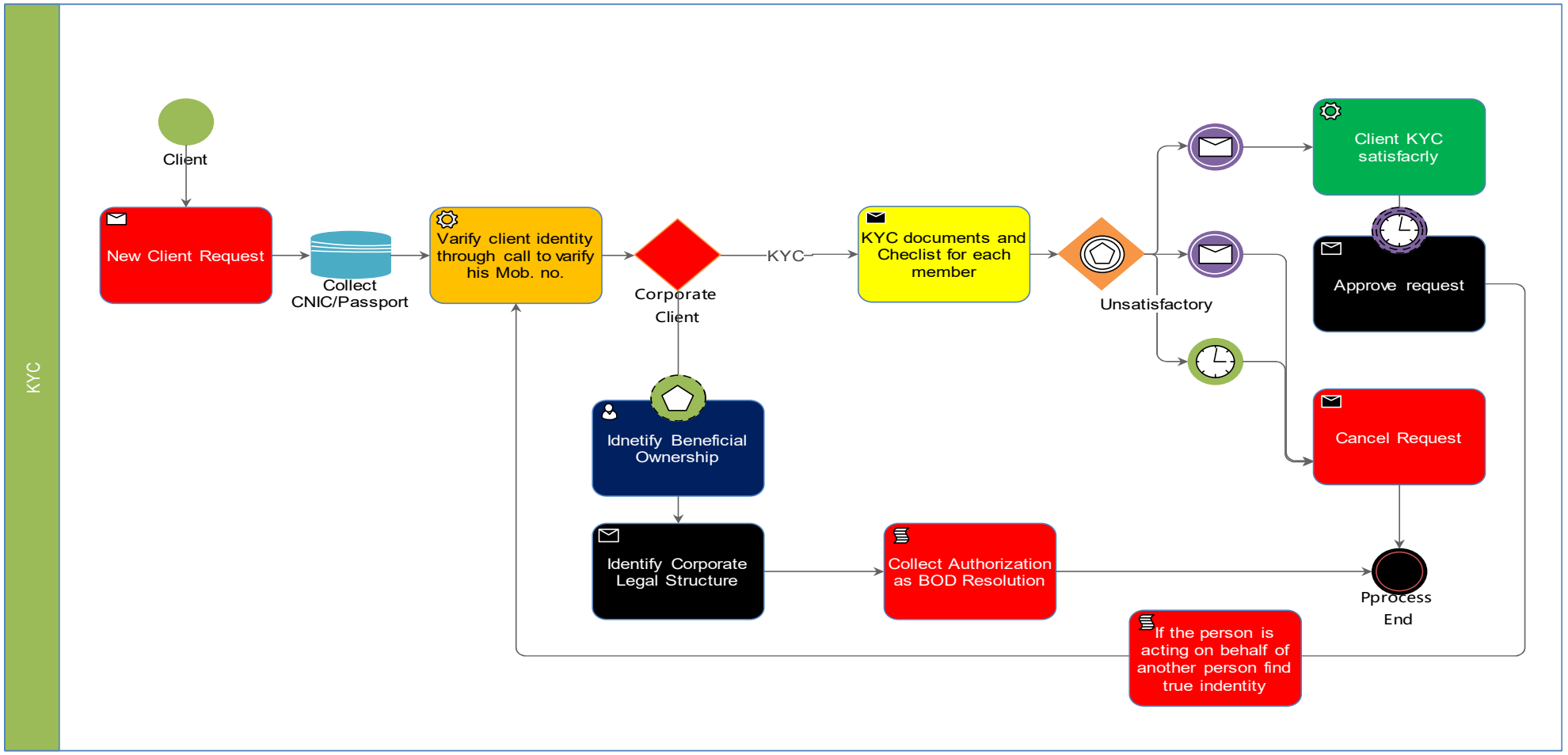
- Any the action of helping or doing work for someone
- Perform routine, maintenance or repair work

- Employee as a servant entered into his service agreemen

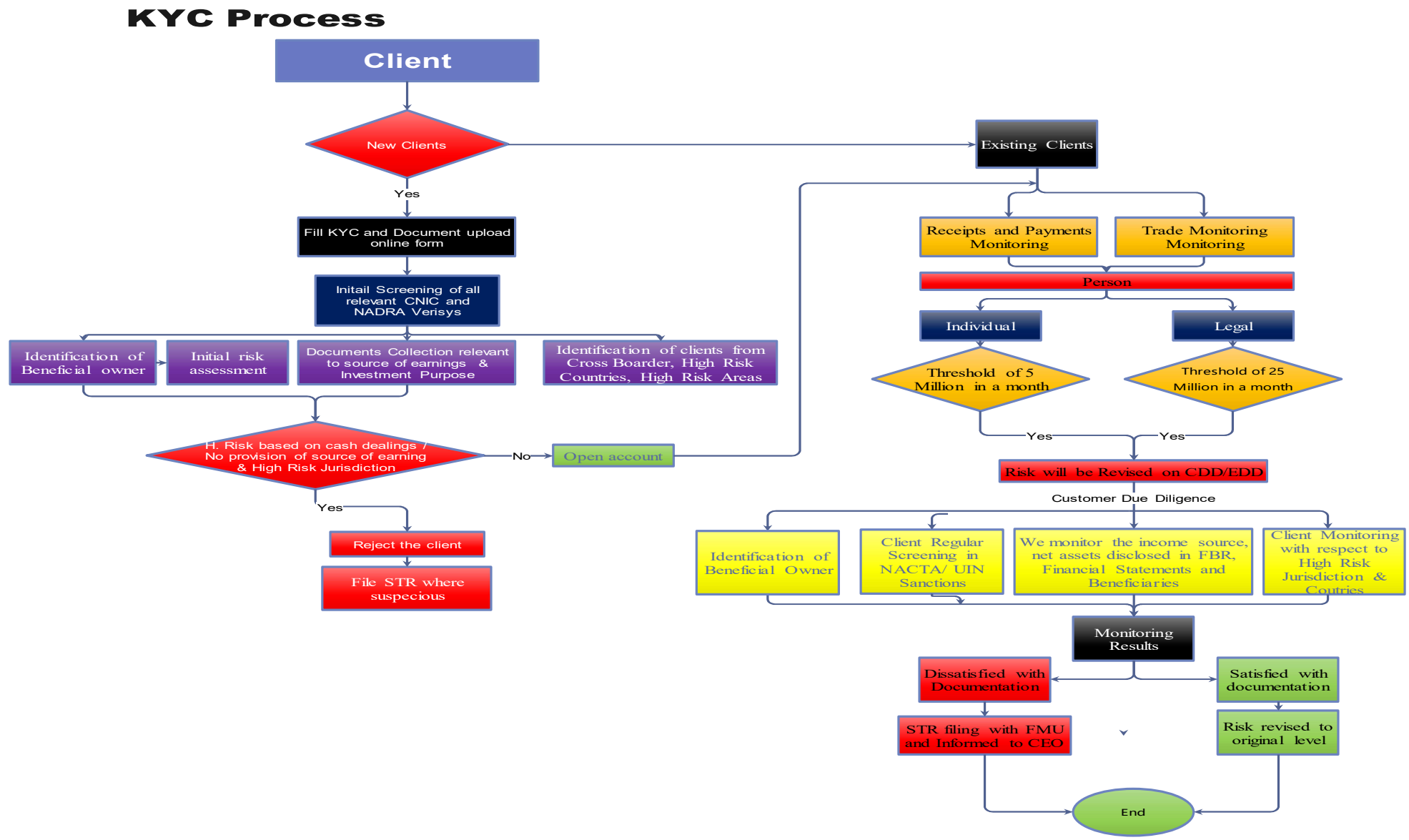
4. ACCOUNT OPENING PROCESS



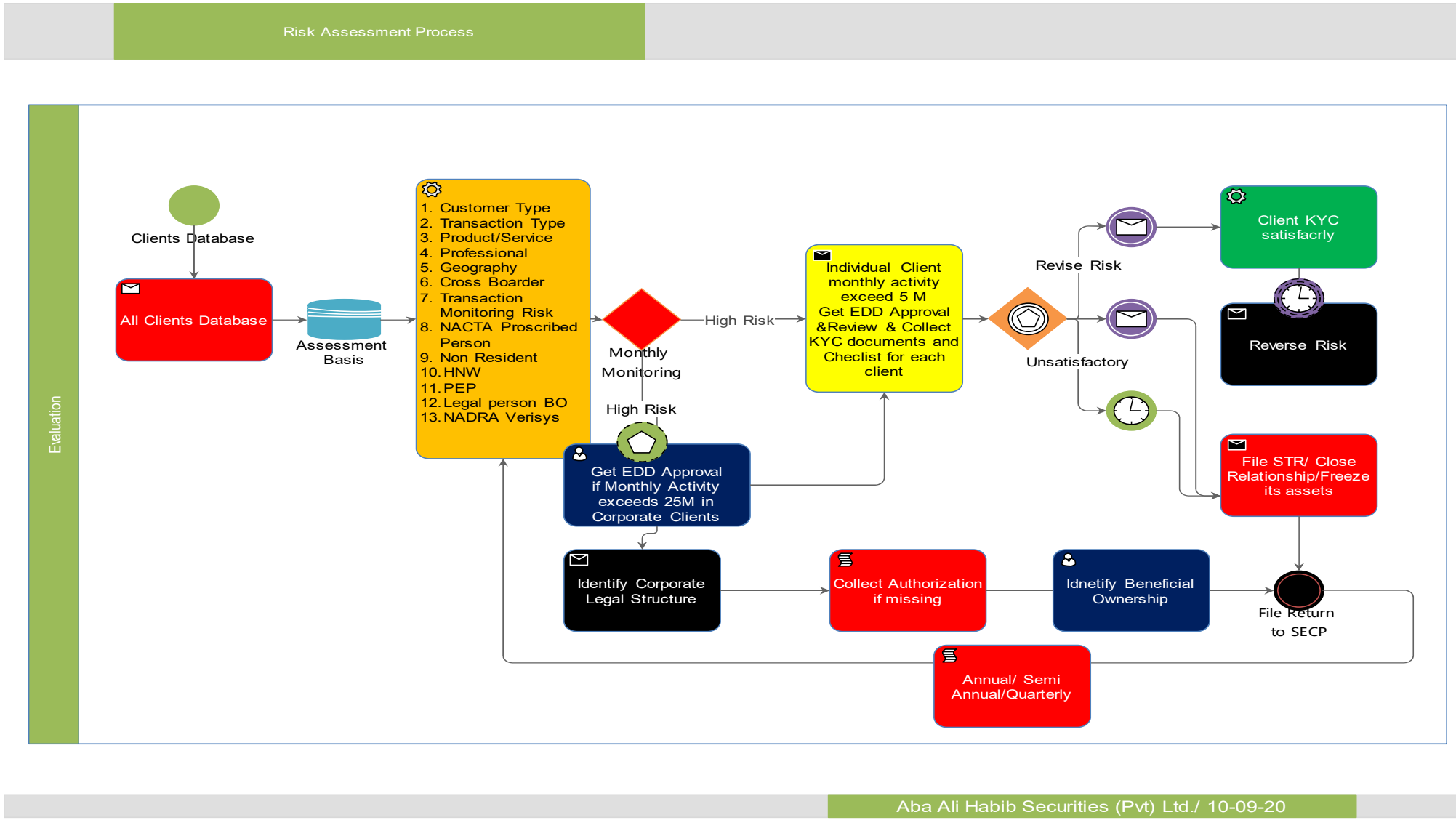
CUSTOMER IDENTIFICATION PROCESS



KYC PROCESS


KYC Process
Client
New Clients
Yes
Fill KYC and Document upload online form
Initail Screening of all relevant CNIC and NADRA Verisys
Identification of Beneficial owner
Initial risk assessment
Documents Collection relevant to source of earnings & Investment Purpose
Identification of clients from Cross Boarder, High Risk Countries, High Risk Areas
H. Risk based on cash dealings / No provision of source of earning & High Risk Jurisdiction
No
Open account
Yes
Reject the client
File STR where suspecious
Existing Clients
Receipts and Payments Monitoring
Trade Monitoring Monitoring
Person
Individual
Legal
Threshold of 5 Million in a month
Threshold of 25 Million in a month
Yes
Yes
Risk will be Revised on CDD/EDD
Customer Due Diligence
Identification of Beneficial Owner
Client Regular Screening in NACTA/ UIN Sanctions
We monitor the income source, net assets disclosed in FBR, Financial Statements and Beneficiaries
Client Monitoring with respect to High Risk Jurisdiction & Coutries
Monitoring Results
Dissatisfied with Documentation
Satisfied with documentation
STR filing with FMU and Informed to CEO
Risk revised to original level
End

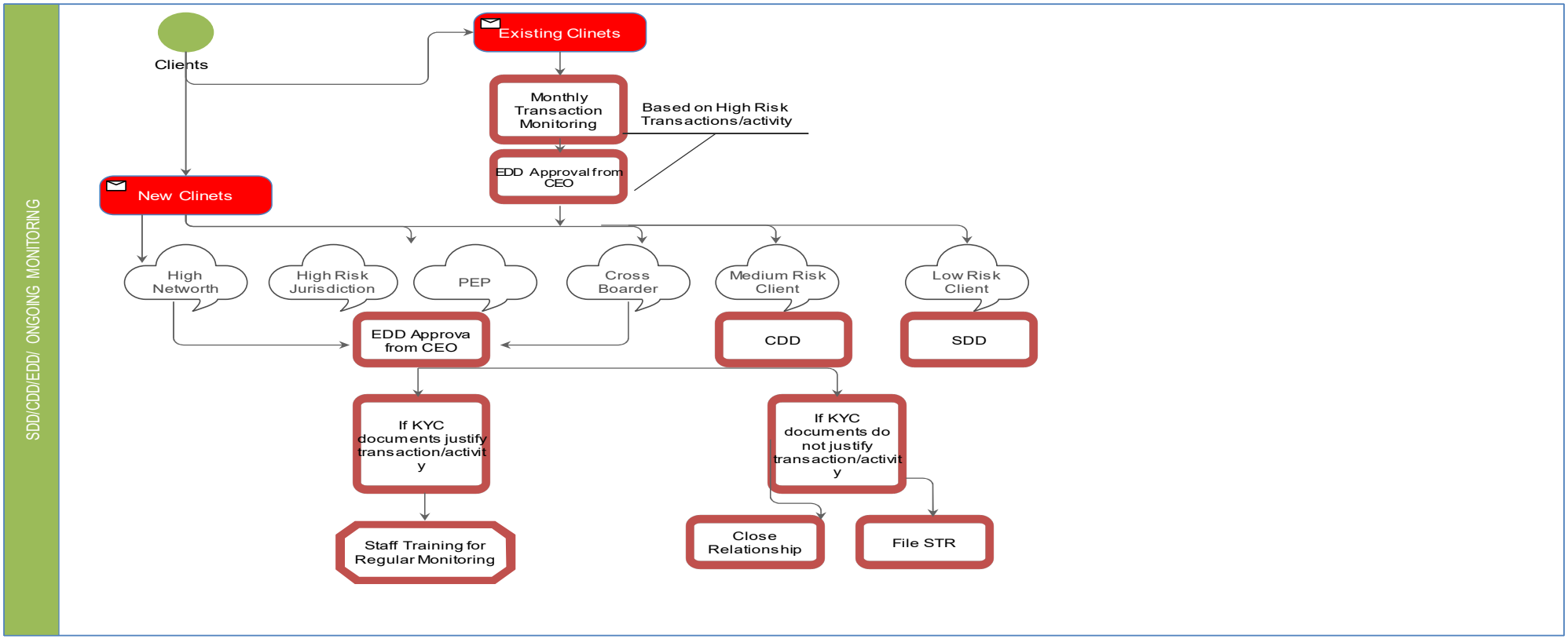
RISK ASSESSMENT PROCESS



Risk Assessment (KYC, SDD, CDD, EDD, Receipt and Payment Monitoring, Trade monitoring, Risk profiling based on profession, residential status, PEP, high net worth, customer type, beneficial owner identification, high risk jurisdiction like cross boarder) are prohibited as a matter of corporate policy.

CUSTOMER DUE DILIGENCE PROCESS

Customer Due Deligence Process

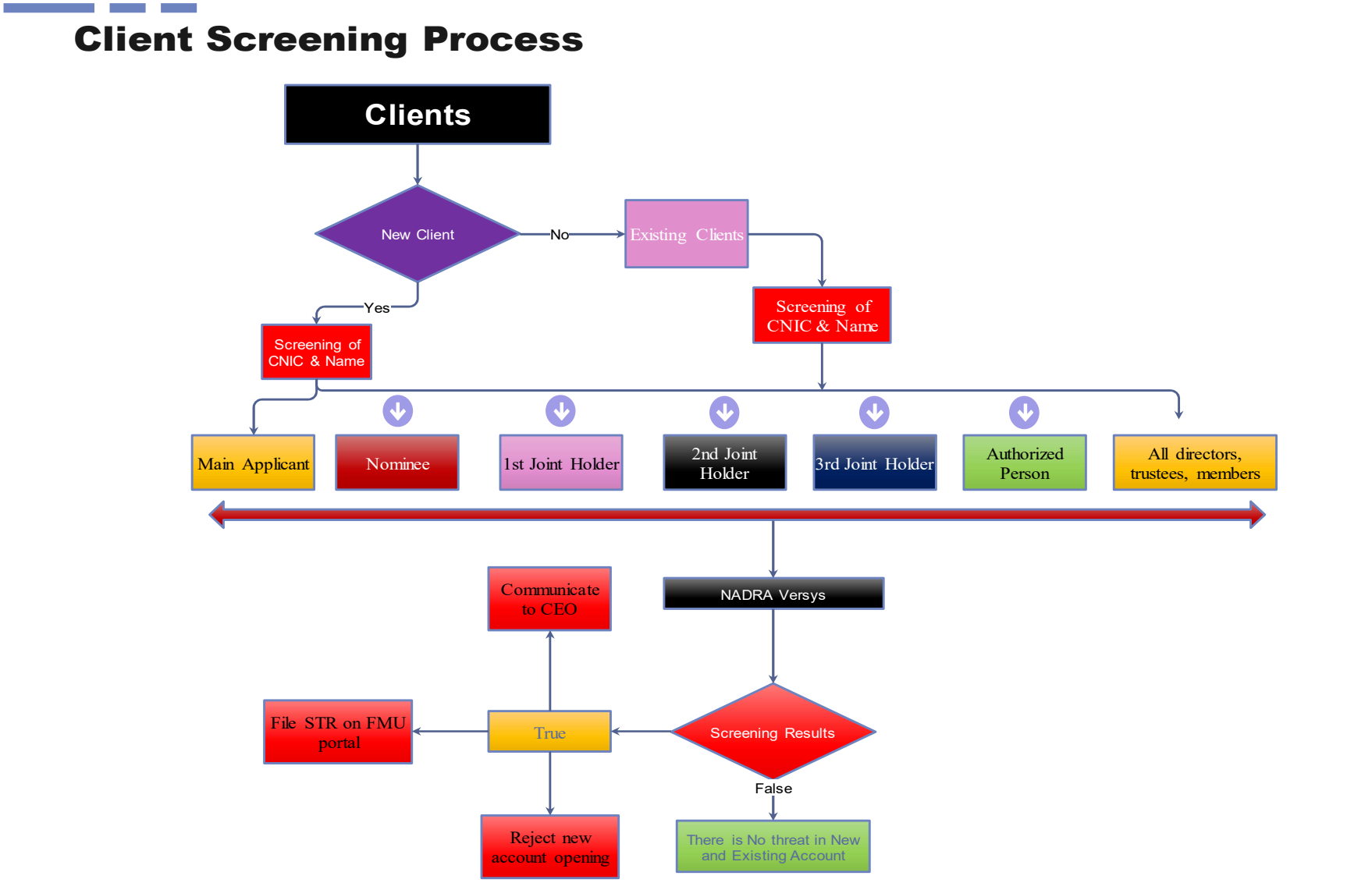


Aba Ali Habib Securities (Pvt) Ltd./ 10-09-20

The success of our business is dependent on the trust and confidence we earn from our employees, customers and shareholders. We gain credibility by adhering to our commitments, displaying honesty and integrity and reaching company goals solely through honorable conduct. It is easy to say what we must do, but the proof is in our actions. Ultimately, we will be judged on what we do.

RPs shall take steps to know who their customers are. RPs shall not keep anonymous accounts or accounts in fictitious names. RPs shall take steps to ensure that their customers are who they purport themselves to be. RPs 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.

5. CLIENT SCREENING PROCESS



6. Simplified Due Diligence

I. CO shall conduct SDD in case of lower risks identified by the CO. However, the CO shall ensure that the low risks is identified commensurate with the low risks justification. 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. The simplified measures should be commensurate with the low risk factors.

II. SDD is not acceptable in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF. Page 16 of 40

III. Where the risks are low and where there is no suspicion of ML/TF, the law allow the RPs to rely on third parties for verifying the identity of the applicants and beneficial owners.

IV. Where an RP decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

7. Customer Due Diligence

i. RPs shall take steps to know who their customers are. RPs shall not keep anonymous accounts or accounts in fictitious names. RPs shall take steps to ensure that their customers are who they purport themselves to be. RPs 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, risk assessment in compliance of NRA 2019 jurisdictions like Iran & Korea, beneficial ownership and control structure of the customer.

ii. RP shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the RP's knowledge of the customer, its business and risk profile (Annex 3), including, where necessary, the source of funds, funds received by foreign or non-resident clients. RPs shall conduct CDD when establishing a business relationship if: (1) There is a suspicion of ML/TF, Annex 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF. Although these may not be exhaustive in nature, it may help RPs recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose; or (2) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.

iii. In case of suspicion of ML/TF, an RP should: (1) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and (2) File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law.

iv. RPs shall monitor transactions to determine whether they are linked. Transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold.

v. RPs shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys. Similarly, RPs shall identify and verify the customer's beneficial owner(s) to ensure that the RP understands who the ultimate beneficial owner is.

vi. RPs shall ensure that they understand the purpose and intended nature of the proposed business relationship or transaction. RPs shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

vii. The Regulations require RPs to identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person"). The RP should also verify whether that authorized person is properly authorized to act on behalf of the customer. RPs shall conduct CDD on the authorized person(s) using the same standards that are applicable to a customer. Additionally, RPs shall ascertain the reason for such authorization and obtain a copy of the authorization document.

viii. RPs may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk Page 13 of 40 product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

ix. When performing CDD measures in relation to customers that are legal persons or legal arrangements, RPs should identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure.

8. Enhanced Due Diligence

I. RPs 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 with high risk assessment;
   a) business relationships and transactions with natural and legal persons when the ML/TF risks are higher;
   b) business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF;
   c) PEPs and their close associates and family members.

II. Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, RPs should conduct enhanced CDD measures, consistent with the risks identified. In particular, RPs 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.

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

IV. In case of accounts where the accountholder has instructed the RP not to issue any correspondence to the accountholder's address. Such accounts do carry additional risk to RPs, and they should exercise due caution as a result. It is recommended on a best practice basis that evidence of identity of the accountholder should be obtained by the RP. "Hold Mail" accounts should be regularly monitored and reviewed and the RP should take necessary steps to obtain the identity of the account holder where such evidence is not already in the RP file.

High-Risk Countries

i. Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to an RP. Conducting a business relationship with an applicant/customer from such a country exposes the RP to reputational risk and legal risk.

ii. RPs should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

iii. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability. Page 17 of 40

iv. RPs are advised to consult publicly available information to ensure that they are aware of the high-risk countries/territories. While assessing risk of a country, RPs are encouraged to 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) and Transparency international corruption perception index.

v. Useful websites include: FATF website at www.fatf-gafi.org and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

9. On-going Monitoring

i. Once the identification procedures have been completed and the business relationship is established, the RP 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. RPs shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps RPs to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

ii. RPs shall conduct on-going due diligence which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer.

iii. RP should develop and apply written policies and procedures for taking reasonable measures to ensure that documents, data or information collected during the identification process are kept up-to-date and relevant by undertaking routine reviews of existing records.

iv. RPs shall consider updating customer CDD records as a part its periodic reviews (within the timeframes 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:
    a. Material changes to the customer risk profile or changes to the way that the account usually operates;
    b. Where it comes to the attention of the RP that it lacks sufficient or significant information on that particular customer;
    c. Where a significant transaction takes place;
    d. Where there is a significant change in customer documentation standards;
    e. Significant changes in the business relationship.

v. Examples of the above circumstances include:
    a) New products or services being entered into,
    b) A significant increase in a customer's salary being deposited,
    c) The stated turnover or activity of a corporate customer increases,
    d) (A person has just been designated as a PEP,
    e) The nature, volume or size of transactions changes.

vi. RPs should be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be: (1) transaction type (2) frequency (3) amount (4) geographical origin/destination (5) account signatories

vii. However, if an RP has a suspicion of ML/TF 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

viii. 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.

ix. Whilst some RPs may wish to invest in expert computer systems specifically designed to assist the detection of fraud and ML/TF, it is recognized that this may not be a practical option for many RPs for the reasons of cost, the nature of their business, or difficulties of systems integration. In such circumstances RPs will need to ensure they have alternative systems in place for conducting on-going monitoring.

10. Filing CTR/STR to FMU

After suspicion filing STR/CTR to FMU through its online portal

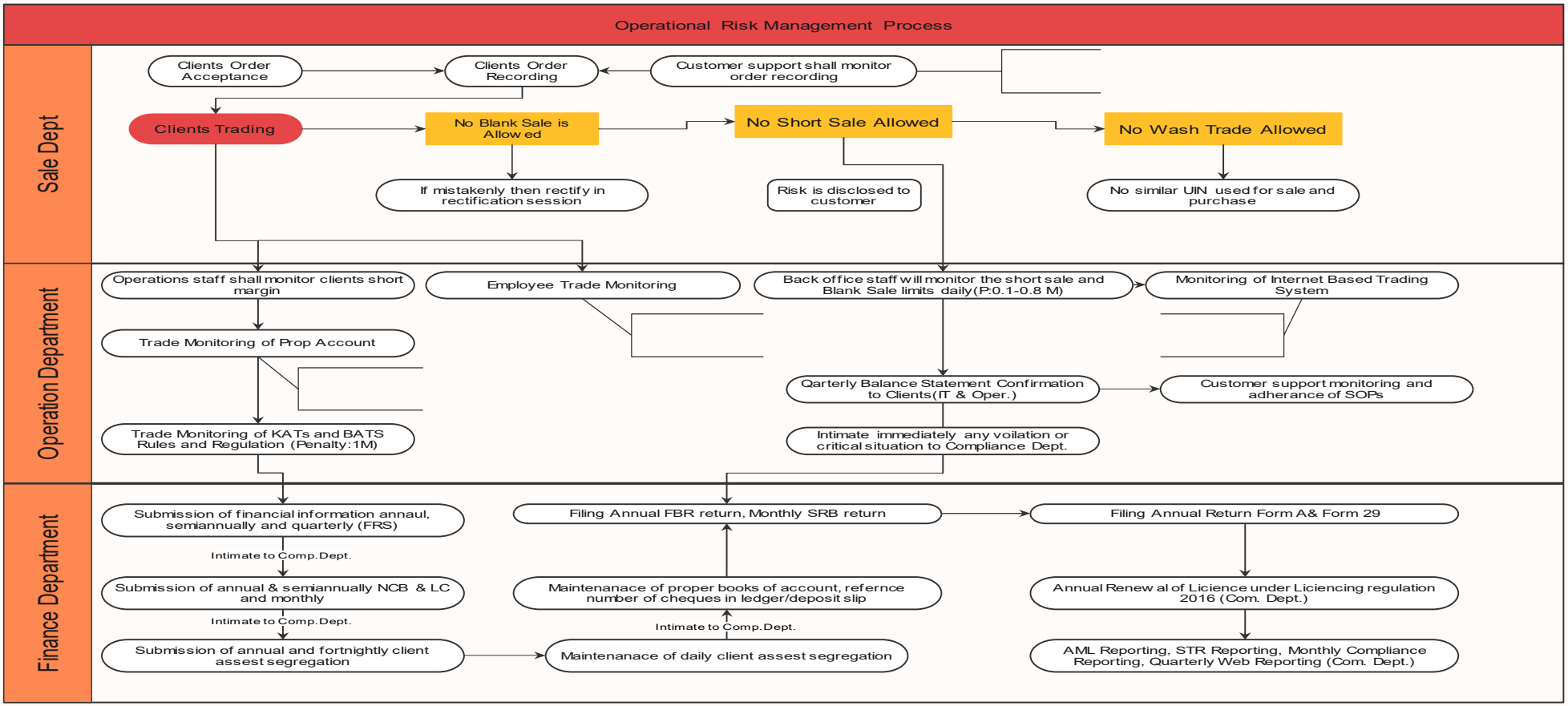
11. Customer database maintenance

Maintenance of proper KYC database of all active clients for their activity monitoring.

12. Periodic Reporting to Customers

Forwarding quarterly client balance statement through email/physically

13. Account Closing

Account closing after obtaining customer request and settling his/her all assets and liabilities outstanding with the house.

14. SECP compliance relevant to AML/CFT