

2025



ANTI MONEY LAUNDERING POLICY - 2025

VERSION 2.6 OF 2025
COMPLIANCE DEPARTMENT

AA EXCHANGE COMPANY (Pvt) LIMITED | Office No M-04, Mezzanine Floor, Islamabad Stock Exchange Tower, 55-B
Jinnah Avenue, Blue Area, Islamabad

TABLE OF CONTENTS

CHAPTER: 1 - INTRODUCTION	7
1.1 OBJECTIVES.....	7
CHAPTER: 2 - DEFINITIONS.....	8
2.1 MONEY LAUNDERING.....	8
2.2 REVERSE MONEY LAUNDERING	8
2.3 TERRORIST FINANCING	8
2.4 PROLIFERATION FINANCING	8
2.5 TARGETED FINANCIAL SANCTIONS (TFS)	9
2.6 ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM	9
CHAPTER: 3 - RISK BASED APPROACH (RBA).....	10
3.1 RISK CRITERIA.....	10
I - PRODUCTS AND SERVICES RISK.....	11
II - CUSTOMER RISK	12
III - COUNTRY / GEOGRAPHIC RISK.....	12
IV - DISTRIBUTION CHANNEL RISK.....	13
3.2 RISK ASSESSMENT	14
PURPOSE OF RISK ASSESSMENT	14
3.3 MONEY LAUNDERING RELATED THREATS ASSOCIATED WITH PREDICATE OFFENCES	15
3.4 TERRORISM AND TERRORISM FINANCING RELATED THREATS.....	17
3.5 ML/TF Threats Associated with Predicate Offenses (by NRA 2023).....	17
3.6 RISK INDICATORS.....	19
3.7 RISK MANAGEMENT AND INTERNAL CONTROLS.....	24
4 EPD CIRCULAR # 15 & EPD CIRCULAR # 17 Explanation	
4.1 RISK MANAGEMENT AND INTERNAL CONTROLS	24
KNOW YOUR CUSTOMER (KYC).....	24
CUSTOMER DUE DILIGENCE (CDD).....	24
ENHANCED DUE DILIGENCE (PROCEDURE & REQUIREMENTS)	25
KYC /CDD AND EDD LEVELS AND DESCRIPTION	25
REQUIREMENT OF DOCUMENTARY EVIDENCE ON HIGH RISK SCENARIOS.....	25
IDENTIFICATION AND VERIFICATION OF BENEFICIAL OWNERSHIP.....	26
ENHANCED DUE DILIGENCE PROCEDURE.....	26
PROCEDURE FOR CONDUCTING AND FILING EDD	26
REJECTION OF TRANSACTION.....	27
PROHIBITION TO DEAL WITH LEGAL PERSONS AND LEGAL ARRANGEMENTS.....	27
CHAPTER: 4 - OFFSITE MONITORING AND SURVEILLANCE.....	28
4.1 MONITORING TOOLS & PROCEDURES	28

TRANSACTION MONITORING SYSTEM	29
4.2 CLIENT MONITORING PROCESS	30
4.3 REMITTANCE MONITORING PROCESS.....	30
INWARD REMITTANCE	31
<hr/>	
OUTWARD REMITTANCE THROUGH MTOS	31
OUTWARD FOREIGN TELEGRAPHIC TRANSFER / FOREIGN DEMAND DRAFT	32
4.4 FOREIGN CURRENCY EXCHANGE / CASH TRANSACTIONS MONITORING PROCESS.....	33
4.5 KNOW YOUR PARTNER - OFFSITE DUE DILIGENCE PROCESS	33
SELECTION STAGE	33
PRE-AGREEMENT STAGE	34
POST AGREEMENT STAGE	34
CHAPTER: 5 - SANCTION SCREENING.....	35
5.1 WORLD CHECK	35
CHAPTER: 6 - SUSPICIOUS TRANSACTION REPORTING AND CURRENCY TRANSACTION REPORTING ..	36
6.1 FINANCIAL MONITORING UNIT- FMU	36
6.2 CURRENCY TRANSACTION REPORTING (CTR)	36
PROCEDURE	37
6.3 SUSPICIOUS TRANSACTION REPORTING (STR).....	37
SUSPICIOUS TRANSACTION / ACTIVITY INCLUDES	37
CHAPTER: 7 - CURRENCY EXPORT	38
7.1 CASH COLLECTION (FOREIGN CURRENCY TO BE EXPORTED)	38
7.2 SETTLEMENT AGASINT THE EXPORT	39
7.3 DUE DILIGENCE ON COUNTER PARTY	39
CHAPTER: 8 - PUNISHMENT FOR MONEY LAUNDERING AND RELATED OFFENCES	41
8.1 PUNISHMENT FOR MONEY LAUNDERING.....	41
8.2 FAILURE TO FILE SUSPICIOUS TRANSACTION REPORT AND FOR PROVIDING FALSE INFORMATION	42
8.3 DISCLOSURE OF INFORMATION (TIPPING OFF)	42
CHAPTER: 9 - UNSC, NACTA & OTHER RELEVANT INTERNATIONAL AGENCIES / EVALUATION BODIES	43
9.1 UNITED NATION'S SECURITY COUNCIL (UNSC).....	43
9.2 NATIONAL COUNTER TERRORISM AUTHORITY (NACTA)	44
9.3 OFFICE OF FOREIGN ASSET CONTROL (OFAC).	44
9.4 FINANCIAL ACTION TASK FORCE (FATF)	44
CHAPTER: 10 EMPLOYEE RECRUITMENT AND TRAINING	45
10.1 EMPLOYEE TRAINING	45

PURPOSE	45
PROCEDURES.....	46
10.2 TRAINING ASSESSMENT AND EFFECTIVENESS	46
10.3 TRAINING MEDIUM.....	46
10.3 APPOINTMENT/INDUCTION OF NEW DIRECTOR OR SHAREHOLDER	46
CHAPTER: 11 - DOCUMENT RETENTION	47
CHAPTER: 12 - ROLES AND RESPONSIBILITIES	48
12.1 BOARD OF DIRECTORS.....	48
12.2 SENIOR MANAGEMENT	49
12.3 CHIEF COMPLIANCE OFFICER / MANAGER	49
12.4 STAFF	49
CHAPTER: 13 - INDEPENDENT REVIEW OF COMPLIANCE PROGRAM AND ITS EFFECTIVENESS.....	50
ANNEXURE – I (EDD QUESTIONNAIRE).....	51
ANNEXURE – II (AML QUESTIONNAIRE FOR EXTERNAL CORRESPONDENT ENTITIES)	52
ANNEXURE – III (UNDERTAKING).....	56
ACRONYMS	57

VERSION CONTROL PAGE

NOMENCLATURE				REMARKS
DOCUMENT TITLE				AML/CFT Policy
VERSION				2.6 (2025)
REVIEWED BY				Mehran Khan
LAST REVIEW DATE				12 February, 2025
NEXT REVIEW DATE				December 31, 2026
APPROVED BY				Board of Directors
APPROVAL DATE				14 February, 2025
NOTABLE CHANGES				
VERSION	DATE	AUTHOR	NOTE	APPROVED BY
1.0	2010	Muhammad Asim	Revision of AML Policy	Board of Directors
1.1	2011	Ehtisham Ali Ehsan	Amendment /Updations- AML & KYC Policy	Board of Directors
1.2	2012	Ehtisham Ali Ehsan	Modified AML & KYC Policy	Board of Directors
1.3	2013	Ehtisham Ali Ehsan	Annual Revision- AML & KYC Policy	Board of Directors
1.4	30/09/2014	Ehtisham Ali Ehsan	Annual Updation- AML & KYC Policy	Board of Directors
1.5	28/09/2015	Mehak Tariq	Annual Updation- AML & KYC Policy	Board of Directors
1.6	17/02/2016	Mehak Tariq	Generalization of the Policy	Board of Directors
1.7	29/09/2016	Mehak Tariq	Annual Review and Updation- AML / CFT & KYC Policy	Board of Directors
1.8	29/09/2017	Mehak Tariq	Annual Revision Addition: RBA, PEP and Employee Recruitment Deletion: Products & Services	Board of Directors
1.9	29/09/2018	Mehak Tariq	Annual Revision Addition: Reverse Money Laundering, Thresholds, Splitting and Structuring, New EDD form, Refined Risk Criteria under RBA, Know Your Partner- Offsite Due Diligence Process, AML QA for External Parties / Correspondents, Bi-annual Screening of Sub-Agent Owner(s), Sanction Screening and World Check, UNSC and NACTA, Fourth Schedulers, Quarterly Independent Review of the AML / CFT Program and its Effectiveness, AML Employee Undertaking	Board of Directors
2.0	29/09/2019	Mehak Tariq	Annual Revision	Board of Directors

2.1	25/09/2020	Muhammad Amjad	Additions: Currency Export Policy, Proliferation Financing, Targeted Financial Sanctions, Categorization of PEPs, Threshold for Due Diligence, Prohibition to deal with legal persons, Induction procedure for new Director / Shareholder, Time-line for STR reporting	Board of Directors
2.2	14/12/2020	Muhammad Amjad	Scheduled Revision Document format, Addition of Transaction Monitoring System, Rejected Transaction's procedures Addition in TFS Addition in Staff Training regarding online training module Addition in Punishments against TFS	Board of Directors
2.3	30/12/2021	Muhammad Amjad	Additions: Contents of FE Circular 8 of 2021, New limits and thresholds, EDD for PEPs and additional PEPs screening and identification Client monitoring Process EPD Circular 16 of 2021	Board of Directors
2.4	01/10/2022 10/01/2024	Arsalan Tariq Arsalan Tariq	Additions: Currency Export Mechanism PEPs approval from Management EPD Circular 15 of 2022 EPD Circular 17 of 2022 Deletions: Old thresholds and limits Additions: No additions made as this Policy was up to date Deletions: Sub-agent due diligence	Board of Directors
2.5	25/06/2024	Mehran Khan	Policy was thoroughly reviewed and below changes were made. 1. 1.Addition: Ongoing Screening 2. Deletion: Sub-agent Risk 3. Revision of PEPs SOPs 4. Revision of Risk indicators and Risk rating (by NRA 2023) 5. Revision of Risk categories as Very High, High, Medium and Low (by NRA 2023)	Board of Directors

			<p>6. Revision of Products, Customers, Geographic Risk level.</p> <p>7. Addition of ML/TF Threats Associated with Predicate Offenses (by NRA 2023).</p>	
2.6	12/02/2025	Mehran Khan	<p>Referring the Regulatory Framework For Exchange Companies Of 2024, below changes were incorporated:</p> <p>1- Updation of Regulatory Requirements related to the Transactional thresholds (Chapter-3)</p> <p>2- Addition of "Recruitment Of CEO & Key Executives" (Chapter-10)</p>	Board of Directors

CHAPTER: 1 - INTRODUCTION

With the enactment of Anti – Money Laundering / Combating of Terrorist Financing and Know Your Customer (KYC) and Customer Due Diligence (CDD) legislations in Pakistan, AA Exchange Company (Pvt.) Ltd is giving increased attention to implementing these laws. The policy has been enriched by the enabling AML / CFT enacted, particularly by the relevant recognized evaluation bodies Recommendations, country laws, the guidelines of the foreign associates and regulations of Financial Monitoring Unit (FMU) and the State Bank of Pakistan. To provide a further guide and to avoid ambiguity, the guidance on KYC and CDD is also provided to assist the Company in the implementation of this policy.

Company has placed necessary checks and internal controls within the organization to counter money laundering and terrorist financing.

Diligent implementation of the provisions of this policy would not only minimize the risk faced by Company of being used to launder the proceeds of crime but also provide protection against fraud and reputational and financial risks.

This policy applies to all employees of the Company, without exception. This includes the Board of Directors / shareholders and Chief Executive Officer, officers, and other managers, all staff employed with the Company (collectively, the “Employees”). Policy should be read in conjunction with a number of related policies and procedures, including the following:

- I. Compliance Manual
- II. Sanction Screening Guidelines
- III. Fraud Prevention Policy
- IV. Record Retention Policy

1.1 OBJECTIVES

- I. The aim of this policy is to provide guidance on identifying and controlling risks associated with money laundering (ML) and financing of terrorism (TF) and to prevent criminal elements from using the Company for money laundering and terrorist activities.
- II. It also includes procedures for monitoring and reporting of activities possibly linked to money Laundering or terrorist financing or other predicate offences.

CHAPTER: 2 - DEFINITIONS

2.1 MONEY LAUNDERING

To acquire, possess or deal in a benefit obtained from a criminal act or to facilitate someone else to do so, when knowing or suspecting that the benefit was obtained from a criminal act. Money Laundering is a process by which money or other assets obtained as proceeds of crime are exchanged to “clean money” or other assets with no obvious link to their criminal origins.

There are three steps involved in the process of laundering money: placement, layering, and integration.

- I. **Placement** refers to the act of introducing / depositing criminal proceeds / "dirty money" (money obtained through illegitimate, criminal means) into the financial system
- II. **Layering** is the act of concealing the source / origin of the criminal proceeds through the use of layers of complex financial transactions and bookkeeping gymnastics. These layers are designed to obstruct the audit trail, disguise the origin of funds and provide anonymity.
- III. **Integration** refers to the act of placing the laundered proceeds back into the economy in such a way that they reenter the financial system as apparently legitimate funds.

2.2 REVERSE MONEY LAUNDERING

Reverse money laundering is the process where the money that starts out legitimate and grows “dirty” in its ultimate purpose. This means that instead of “washing” criminal proceeds to make them legal, legitimate funds are withdrawn from formal circulation and pushed into the informal sector to evade taxes, hand in bribes, pay “under-the-table” salaries and sidestep paperwork. Terrorist financing is also often referred to as reverse money laundering as it focuses on utilizing legal assets to carry out terrorist activities, which are often in the form of clean sources such as charitable organizations and legitimate business organizations.

2.3 TERRORIST FINANCING

Fundraising, possessing or dealing with property or facilitating someone else to do so, when intending, knowing or suspecting or having reasonable cause to suspect that it is intended for the purposes of terrorism. Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity.

A person commits the crime of financing of terrorism ‘if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out an offence of terrorism’

2.4 PROLIFERATION FINANCING

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non- legitimate purposes), in contravention of national laws or, where applicable, international obligations.

2.5 TARGETED FINANCIAL SANCTIONS (TFS)

FATF Recommendation 6 requires countries to implement the targeted financial sanctions regimes to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCR 1267(1999) and its successor resolutions, and UNSCR 1373(2001).

It is a regulatory requirement that all the regulated entities shall ensure compliance with TFS obligations. All the applicable lists should be embedded in company's MIS so it can be assured that no listed individual is can take advantage of the company's services.

NEC (National Executive Committee) is responsible to share the list of jurisdiction which are to be considered as High Risk and requires actions against such transactions. The lists are shared on <https://www.fmu.gov.pk/fatf-high-risk-jurisdiction-intl/>

2.6 ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

Anti-money laundering (AML) and Combating the Financing of Terrorism (CFT), refers to a set of Procedures, laws or regulations designed to stop the practice of generating income through illegal actions, to assist in identifying money laundering and terrorist financing schemes, blocking their funding, and ultimately halting terrorist's plans.

CHAPTER: 3 - RISK BASED APPROACH (RBA)

RBA to AML / CFT means to identify, assess and understand the ML/TF risks to which the Company is exposed and take AML / CFT measures proportionate to those risks in order to mitigate them effectively and efficiently.

A risk-based approach takes the following steps in assessing the most effective way to mitigate the money laundering and terrorist financing risks faced by the Company:

- I. Identify the money laundering and terrorist financing risks that are relevant to the Company
- II. Assess the level of associated risks
- III. Understand the impact of the reputational, financial or business risks
- IV. Design and implement controls to manage and mitigate the assessed risks

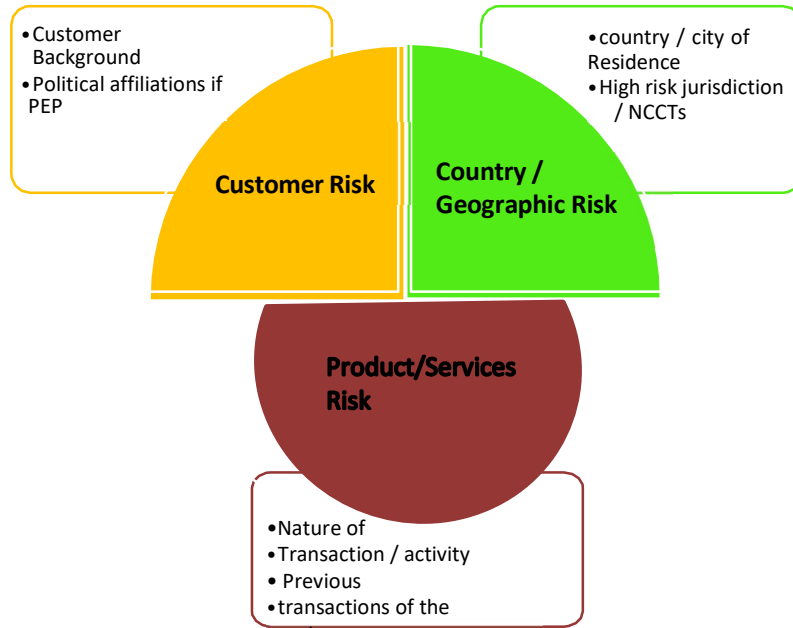


3.1 RISK CRITERIA

Money Laundering and Terrorist Financing risks can be measured by using the following various categories, which can be modified by risk variables. The most commonly used risk criteria are:

- I. Products / Services Risk
- II. Customer Risk
- III. Country / Geographic Risk

All the factors and criteria should be assigned a risk rating based on Internal Risk Assessment performed in the relevant tenure.



I - PRODUCTS AND SERVICES RISK

An overall risk assessment includes determining the potential risks presented by products and services offered by the Company. Following factors should be considered in order to determine the level of the risk associated with the Company's products and services on the basis of Internal Risk Assessment of 2024:

- I. Global reach of the Product / Services
- II. New Product / Services
- III. Demand of the product / services

PRODUCT		RISK LEVEL
Foreign Currency Sale		High
Purchase		Medium
Outward Money Transfer through Transfer Organizations	Money	Medium
Inward Money Transfer through Transfer Organizations	Money	High
Foreign Telegraphic Transfer and Demand	Draft	Low
Branchless Banking		High
Currency Export		Low

II - CUSTOMER RISK

Determining the potential money laundering risks posed by a customer provides significant input into the overall risk assessment.

Customer's categorizing according to customer's occupation, geographical location, Behavior or activity. Categories of customers whose business or activities may indicate a very high, high, medium or low level of risk may include:

CUSTOMER	RISK LEVEL
Non Resident and Foreign Nationals	Medium
Afghan Refugees*	High
Housewives	Low
Property Dealers /Real Estate Agents	Very High
Jewelers /Precious Metals and Gold dealers	High
Students	Low
Politically Exposed Person or PEP(s) (Domestic / International)	High
Lawyers, TCSPs and Notaries	Low
Accountants	Low

Note: Afghan refugees in abysmal circle of poverty and homelessness are perfect prey to exploitation, thus carrying a major TF risk.

*(POLITICALLY EXPOSED PERSONS)

Individuals who are, or have been, entrusted with prominent public functions either domestically or by a foreign country and their family members and close associates. Due to their status and influence, many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as terrorist financing (TF).

For example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials or persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

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

Foreign PEPs: Individuals who are or have been entrusted with prominent public functions by a foreign country.

Domestic PEPs: Individuals who are or have been entrusted domestically with prominent public functions.

International Organizations PEPs: Persons who are or have been entrusted with prominent function by an international organization.

PEP SCREENING /APPROVAL AND IDENTIFICATION BY THE REPORTING ENTITY:

1. Roles and Responsibilities:

- **Front Line Associates (FLAs):** Responsible for conducting PEP screenings and obtaining necessary approvals.
- **Chief Compliance Officer (CCO) / Money Laundering Reporting Officer (MLRO):** Responsible for performing PEP screenings through World Check, evaluating supporting documents, and making approval decisions.

2. PEP Screening by FLAs:

- **Initial Screening:** FLAs screen customers using the PEP database as per the directions of company policy.
- **Identification:** If a customer is identified as a PEP, FLAs must document the PEP status and proceed with the approval process.

3. Prior Approval Process:

- **Submission:** FLAs must obtain formal approval from higher management, including the CCO/MLRO, before proceeding with any PEP transaction.
- **Information Gathering:** FLAs submit detailed information regarding the PEP, including their source of funds, purpose of the transaction, and relationship with the counterparty, to the CCO/MLRO.

4. Screening and Evaluation by CCO/MLRO:

- **World Check Screening:** CCO/MLRO performs a thorough PEP screening using World Check to identify any adverse findings.
- **Supporting Document Evaluation:** CCO/MLRO evaluates the supporting documents provided, including the source of funds and the purpose of the transaction.
- **Transaction Assessment:** CCO/MLRO assesses the PEP's relationship with the counterparty to ensure the legitimacy of the transaction.

III - COUNTRY / GEOGRAPHIC RISK

Country / Geographical risks, in combination with other factors, provide useful information as to potential money laundering risks. Entities and individuals, in countries / geographical areas, identified by Financial Action Task Force or other credible sources as Non-cooperative in the fight against money laundering, providing funds and support for terrorist activities and with significant level of corruption or other criminal activities including illegal drugs, human trafficking and smuggling and illegal gambling, are considered high risk. Company may devise an internal list of high risk countries / geographical areas on the basis of its risk assessment.

In addition to the above, presence of 3 million (approximately) Afghan Refugees in Pakistan poses high vulnerability for transnational terrorism as terrorism financing amount can be transferred across the

border through illegal means. As per the Company's internal risk assessment, all branches in KPK and areas near to border are considered to be high risk.

Besides this in Punjab, regions like Sialkot, Faisalabad, and Sargodha are most material in terms of population affected by potential ML / TF incidences.

GEOGRAPHIC	RISK LEVEL
Khyber Pakhtunkhwa	High
Punjab	Medium
Sindh	High
Baluchistan	High
Countries identified by FATF as Blacklisted	High (NORTH KOREA,IRAN,MYANMAR)

3.2 RISK ASSESSMENT

Internal Risk Assessment is done in order to document the identified ML/TF/PF risks. IRAR shall cover ML/TF/PF risks including Transactional TF risks and other emerging risks to and from the company or organization.

IRAR shall take into account results of National Risk Assessment 2023, major international/domestic financial crimes and terrorism incidents that have probability of posing ML/TF/PF risks. Feedback from SBP, FMU, LEA's and other related stakeholders should be taken into account while conduction Internal Risk Assessment.

PURPOSE OF RISK ASSESSMENT

To effectively prevent money laundering and to combat the financing of terrorism, an assessment mechanism that adopts Risk based approach in accordance with the Company's AML and CFT policy is established to carry out overall assessment of money laundering and terrorist financing (ML/TF) risks so as to assess the procedures, controls, and their effectiveness, in order to address the gaps / deficiencies in the mechanism.

In order to ascertain the Company's inherent and residual risks, Company should conduct its internal risk assessment on an annual basis. Internal Risk Assessment report should include an action plan for review and approval by the Board of Directors.

The risk assessment forms the basis of a Company's RBA. It enables to understand how, and to what extent, the Company or its products and services is vulnerable to ML/TF. To address the above risks in consistency with the objective of fighting corruption, money laundering and terrorist financing, AA Exchange Company (Pvt.) Ltd. has a robust risk management system to detect, mitigate and prevent the business from any potential abuse by determining whether a transaction is a threat or is legitimate.

As the risk categories and criteria is defined above, the next step is to develop a risk assessment method by calculating each risk factor based on the level of impact and threat attributed giving the weightage and risk rating that will enable the classification of risk. Compliance has established risk ranges from 1 to 4 with 1 being the lowest and 4 being the highest to determine the level of associated Risks. The overall risk rating is based on the risk indicators given as under.

1. LOW



2. MEDIUM



3. HIGH



4. VERY HIGH



3.3 MONEY LAUNDERING RELATED THREATS ASSOCIATED WITH PREDICATE OFFENCES

Money laundering (ML) is a cognizable offence under the Anti-Money Laundering Act (AMLA) 2010. For the assessment of ML Threats, 23 major predicate offences were empirically examined in line with FATF methodology. Please note that predicate offences refer to crimes that generate proceeds that are subsequently laundered to make them appear legitimate. ML threat ratings were assigned to 21 predicate offences. As per the assessment, **corruption& bribery, illegal MVTs/ hundi/ hawala, tax crimes, smuggling and cash smuggling** were assessed as 'Very High' risk while **illicit trafficking in narcotic drug & psychotropic substances, trafficking in human beings & migrant smuggling, frauds & forgeries and cyber-crimes** were rated as "High" risk. The remaining predicate offences were assessed as "Medium" or "Low" ML threats from Pakistan's perspective. It is important to consider that the predicate offence of **Organized Crimes** was not separately assigned any rating as its impact has been considered in the assessment of all other predicates, to the extent of the involvement of organized groups in the commission of those crimes. Similarly, **Terrorism and Terrorism Financing** were not rated as their impact was covered under the TF Threats part of this NRA.

Rating Factors: The assessment of ML threats includes;

- i. A review of all the incidents based on the seriousness and magnitude of domestic and international crimes
- ii. The estimated amount of proceeds generated and the potential of money laundering;
- iii. The capacity and resources of criminal actors and their level of sophistication to launder proceeds (including third-party launderers);

- iv. The level of criminal actors to continue committing a crime sustainably, and
- v. The sectors and channels used to launder proceeds.

The tabular form of the ML threat rating against each predicate offence is provided below:

Table 3.3. (a) Ratings of ML Threats by Predicate Offence		
Sr. No.	Type of Crime in Pakistan	ML Threat Rating
		2023
1	Corruption and Bribery	VH
2	Illegal MVTs/Hawala/Hundi	VH
3	Tax Crimes (Related to Direct Taxes and Indirect Taxes)	VH
4	Smuggling; (Including Customs Duties and Taxes)	VH
5	Cash Smuggling	VH
6	Illicit Trafficking in Narcotic Drugs and Psychotropic Substances	H
7	Trafficking in Human Beings and Migrant Smuggling	H
8	Fraud and Forgery	H
9	Cyber Crime	H
10	Kidnapping, Illegal Restraint and Hostage-Taking	M
11	Illicit Arms Trafficking	M
12	Extortion	M
13	Insider Trading and Market Manipulation	M
14	Counterfeiting and Piracy of Products	M
15	Environmental Crimes	M
16	Robbery or Theft	M
17	Sexual Exploitation, Including Sexual Exploitation of Children	L
18	Illicit Trafficking in Stolen and Other Goods	L
19	Counterfeiting Currency	L
20	Murder, Grievous Bodily Injury	L
21	Maritime Piracy	L

Key ML Sources and Channels

The ML threat assessment of predicate offences indicated that most of the funds used in money laundering were the illegal proceeds generated from committing the predicate offences; however, the activities like underreporting of legal business income/trade volume/wages/investments, as well as hiding assets or funds in offshore accounts or other undeclared financial irregularities also resulted in money laundering. The major channels used to launder proceeds generated from predicate offences included illegal MVTs/ hundi/ hawala, cash smuggling, bank accounts, real estate, construction industry, cash-intensive businesses, DPMS, and front & shell companies, etc. A summary table of key sources and channels used for ML is provided below:

Table 3.3. (b) Key Sources and Channels used for ML	
Sr. No.	Major Sources
1	Illegal proceeds generated from committing predicate offences including but not limited to embezzlement, kickbacks/commissions/bribes, extortions, drug trafficking, human trafficking, bonded labor, illegal organ removal, corruption, smuggling, fraud, illegal gambling, smuggling of people and weapons, tax evasion, false tax claims/credits/refunds, hawala/Hundi or any other predicate offence listed in the Schedule-I of AMLA, 2010.
2	Under-invoicing or over-invoicing as well as underreporting of legal business income/trade-volume/wages/investments, as well as hiding assets or funds in offshore accounts or other undeclared financial irregularities.
Sr. No.	Major Channels
1	Cash/ Cash couriers
2	Illegal MVTs
3	Benami Accounts and properties
4	Shell companies
5	Front import & export companies
6	Offshore bank accounts
7	Trade-based funds transfers
8	Payment through intermediaries/ third parties
9	Investment in real estate/ Precious metals & stones/ other high-value assets
10	Investments in stocks/bonds/investment funds
11	Cryptocurrency

3.4 TERRORISM AND TERRORISM FINANCING RELATED THREATS

Pakistan has been fighting the menace of terrorism for the last two decades. Although terrorism incidents have been declining over the past few years since 2016, except for 2022, there remains a threat of terrorism and its financing due to the presence of terrorist organizations (TOs) in the region. Utilizing the expertise of National Counter Terrorism Authority (NACTA), Pakistan formed a working group to conduct the assessment of terrorism and terrorism financing threats. The working group was led by the NACTA and included federal and provincial authorities to get input and data from all the relevant stakeholders on the overall landscape of terrorism and terrorism financing in the country. The assessment also took into account international reports and reliable open-source information.

Pakistan has proscribed 78 terrorist organizations under the Anti-Terrorism Act 1997, which is available publicly on the NACTA website. Please note that all these 78 proscribed TOs are not active rather, most of them are inactive, dismantled or merged into other TOs. A detailed **assessment of TF threats** was carried out during the NRA 2023 process by assessing a total of 87 terrorist organizations (TOs), including 78 proscribed TOs as well as some other non-proscribed and UN-listed entities. Based on the data provided by LEAs and from the intelligence inputs, it was found that 41 terrorist organizations have been active in Pakistan with varying degrees of operations. The rest of the TOs have either been dismantled, merged into other organizations or inactive for long. Based on the assessment, **04 TOs were considered as “very high” risk, 08 as “high” risk, 07 as “medium” risk and the remaining 68 as “low” risk.**

Key TF Sources and Channels:

LEAs regularly consider and examine possible sources and channels during TF investigations which could be exploited or misused by terrorist organizations to fund their activities. A detailed assessment of these sources has been carried out during NRA 2023, considering their prevalence in TF investigations since 2019, use of the sources by TOs in funding their activities and the perceived TF threat posed by each source. A detailed assessment of the sectoral channels has also been carried out by considering TF investigations involving these channels since 2019, relevant terrorist organizations, if any and perceived TF threats posed by each channel, including potential for misuse in TF. A summary table of risk ratings of all sources and sectoral channels exploited for TF is provided below

Table 3.4. Key Sources and Channels exploited for TF		
Sr. No.	Sources	NRA 2023
1	Donations	Very High
2	Extortion	Very High
3	Narcotics trafficking	High
5	Cash smuggling	High
4	Misuse of Properties	Medium
6	Kidnapping for ransom	Medium
7	Goods/ Natural resources smuggling	Medium
8	Skin/ Hides collection	Low
Sr. No.	Channels	NRA 2023
1	Cash/ Cash couriers	Very High
2	Illegal MVTs	Very High
3	Banking	High
5	Branchless Banking	High
4	Virtual Currency	Medium
6	Exchange Companies	Medium
7	Securities	Low
8	Insurance	Low
9	NBFCs & <i>Modaraba</i>	Low
10	Microfinance	Low
11	Legal persons & legal arrangements	Low

Please note that Pakistan has a large, diverse, and vibrant Non-Profit Organization (NPO) sector and an overall assessment revealed that 6.75% of the NPOs are high-risk whereas 43.64% consists of Medium-risk and 49.61% are Low-risk

3.5 RISK INDICATORS

Activity(s) that could be an indicator of illegitimate transaction

SR. NO.	RISK INDICATORS	RATING
INTERNATIONAL MONEY TRANSFERS / REMITTANCES		
1	High volume / frequency of transactions (through MTOs ONLY) over a short period of time i.e. (i) More than one transaction on same / consecutive days	3
2	High Value Transactions through MTOs (Equivalent or above 500,000 PKR in a single transaction)	3
3	Suspicious / Lack of apparent relationship between the sender and beneficiary (the receiver)	3
4.	Transaction that apparently does not fall into the category of Home Remittance / Worker Remittance.	3
5.	Structuring / Splitting- (i) Customers who together, and simultaneously, use separate locations/branches to conduct multiple transactions (ii) Frequent transactions of small amounts in an apparent effort to avoid triggering identification or reporting requirements Identification and Reporting Thresholds <ul style="list-style-type: none"> For all transactions of equivalent to USD 1,000 or above, the Company will record the purpose and obtain supporting documents thereof. Maximum limit per person per day for buying foreign currency (in the form of cash or outward remittance) from all ECs is USD 10,000 or equivalent in other foreign currencies. Maximum limit per person per calendar year for buying foreign currency (in the form of cash or outward remittance) from all ECs is USD 100,000 or equivalent in other foreign currencies Threshold of USD 3,000 for all outward remittance transactions through Money Transfer Organizations ONLY 	3
6.	Multiple senders remitting funds to a single individual or vice versa.	3
7.	Funds are received by the same individual from different senders or vice versa.	3
8.	Consumer networking i.e. Transaction(s) among a network of customer(s).	3
9.	Transaction sent or received from high-risk jurisdictions / corridors without reasonable explanation. Note: Company shall pay special attention when establishing or continuing customer relationship with entities / person(s) which are located in jurisdictions that have been identified or called for by FATF for inadequate and poor AML / CFT standards in the fight against money laundering and financing of terrorism	3
10.	Customer using different/multiple IDs	2

11.	Customers incoming transfer or vice versa	2
12.	Customer offers a bribe or a tip other than where a tip is customary or is willing to pay unusual fees to have transactions conducted	3
13.	Customer makes unusual inquiries, threatens or tries to convince staff to avoid reporting	3
14.	Any customer identified as suspicious	3
	(i) The customer only seems to know which amount is being transferred after the staff has counted the cash and/or the customer shows no interest in the transfer costs/charges;	
	(ii) Volume of transaction not in line with the outlook of the Customer	
15.	Any transaction seems unusual or fraudulent.	3
16.	Customer is not the beneficial owner* of the transaction	3
	<p>Note: *Beneficial owner is the natural person(s) who ultimately owns or controls a customer And/or the natural person on whose behalf of transaction is being conducted.*</p> <p>✓ All ECs will not conduct any transaction with their customers on an authority letter Further, it is also reemphasized that ECs shall perform transaction from authorized outlets of the company and shall not provide delivery services to the customers (FE Circular No.08 of 2021)</p>	
17.	High Risk Customer's Occupations	
	i. Customers having association with NGOs / NPOs / Trusts / Clubs / Charities	3
	ii. Real Estate Owners / Property Dealers	4
	iii. Importers / Exporters	3
	iv. Employees / associates of Exchange Companies	2
	v. Employees of Banks	2
	vi. Dealers in precious metals and stones	3
	vii. Freelancers	2
	viii. Religious Scholars	2
FOREIGN CURRENCY EXCHANGE & CASH TRANSACTIONS		
	Exchange of large quantities of low denomination notes for higher denomination ones	3
	Large or frequent exchanges that are not related to the customer's profile	3
	High frequency of currency exchange transactions over a short period of Time	3
	Customer is not the beneficial owner* of the transaction	3
	Structuring / Splitting-	3
	Customers who together, and simultaneously, use separate locations /branches to conduct multiple transactions	
	Frequent transactions of small amounts in an apparent effort to avoid triggering identification or reporting requirements	

Identification and Regulatory Thresholds (Ref by Regulatory framework for EC's 24)

Recording of Transactions

- a) The Company will record all transactions in its centralized Core Business Application (CBA) on real time basis and no manual transaction will be executed with any customer. Further, any transaction not recorded in the CBA would be treated as out of books transaction.
- b) The Company will issue system generated receipt of each transaction carried out with the customer.
- c) The system generated receipt could be kept as record in physical or digital form.

Sale of Foreign Currency to Individuals

The Company may sell foreign currency to individuals' subject to compliance of the following:

- a) Sell foreign currency in "Ready" value date only.
- b) For all transactions, the Company will retain copy of identification document (in physical or digital form) i.e. Computerized National Identity Card (CNIC), National Identity Card for Overseas Pakistanis (NICOP), Pakistan Origin Card (POC), Passport (having valid visa on it or any other proof of legal stay of a foreigner in Pakistan) as the case may be; after having seen the original document.
- c) For all transactions equivalent to USD 500 or above, the Company will carry out biometric verification of Pakistani Nationals and maintain the record thereof.
- d) The company shall obtain original online Verisys slip issued by NADRA, in case biometrics of any individual cannot be verified from NADRA due to:
 - i) Customer's permanent physical disability, e.g. limbs disability, uneven texture/ erased / unclear fingerprints, etc.
 - ii) Customer's temporary issue e.g. wounded/ bandaged hands/ mehndi, etc.
 - iii) NADRA system/data/connectivity or technical issue beyond a reasonable time.
- e) For all transactions equivalent to USD 1,000 or above, the Company will record the purpose of the transaction and obtain supporting documents. The company shall also record the source of funds.
- f) For all transactions equivalent to USD 2,000 or above, the Company will receive contra credit in PKR through bank transfer or cheque from the personal account of the customer. The transaction or instrument reference number and the name of the bank transferring funds or issuing the instrument will be mentioned on the transaction receipt along with identification document number of the customer.

- g) In addition to the above requirements, the sale of foreign currency to individuals will be subject to the following:
 - i) Maximum limit per person per day (in the form of cash or outward remittance) from all Companies, is USD 10,000 or equivalent in other foreign currencies.
 - ii) Maximum limit per person per calendar year (in the form of cash or outward remittance) from all Companies, is USD 100,000 or equivalent in other foreign currencies.
 - iii) While selling the foreign currency to the individuals the Company will also adhere to purpose specific limits under the applicable regulations.
 - iv) In order to ensure compliance of limits mentioned under serial no (i & ii), the Company will obtain an undertaking from the customer, at the time of each transaction, that the customer has not already reached the daily and yearly limits and these limits will not be breached after the current transaction. The Company will ensure, through placement of appropriate checks in their information systems, that the above limits are not breached at their Company's level.

Purchase of Foreign Currency from Individuals

- v) The Company may purchase foreign currency from individuals in "Ready" value date only.
- vi) Where the transaction is equivalent to USD 2,500/- or above, the Company will retain copy of identification document i.e. Computerized National Identity Card (CNIC), National Identity Card for Overseas Pakistanis (NICOP), Pakistan Origin Card (POC), Passport (having valid visa on it or any other proof of legal stay of a foreigner in Pakistan), as the case may be.

Other Important Requirements

- a) Requirement of Currency Transaction Report on each transaction involving sale / purchase of Foreign Currency equivalent or above PKR 2 million.
- b) All ECs shall maintain DVR recording of at least six (06) months and its CCTV system should be operational 24/7 and 7 days a week.

AML POLICY - 2025 (v2.6)

6.	The customer buys currency that does not fit with what is known about the customer's destination or the customer buys currency from an unusual location in comparison to his/her own location	3
7.	The customer Apparently does not know the exact amount being Exchanged the customer does not watch the counting of money, and/or customer is happy with a poor rate.	3
8.	Client requests that a large amount of foreign currency be exchanged to Another foreign currency.	3
9.	Cash is in "used notes" and/or small denominations ("used notes" may imply that notes are worn, dirty, stained, give off unusual smell e.g. drugs, etc.)	3
10.	Customer to disclose the source of funds refuses	3
11.	Customer has made an unusual request for collection or delivery	3
12.	Significant discrepancy between customer's declaration of cash total and counted total	3
13.	Presence of counterfeit banknotes in the bankroll	3

14.	Cash transactions followed closely by transfer of funds on the same or next day	3
15.	Any transaction seems unusual and or fraudulent.	3
16.	High Risk Customer's Occupations	
	1. Customers having association with NGOs / Charities	/ 3
	2. Real Estate Owners / Property Dealers / Landlords	4
	3. Importers / Exporters	3
	4. Exchange Companies associates or their employees	/ 2
		3
	5. Banks or their employees	3
	6. Dealers in precious metals and stones	1
	7. Freelancers	2
	8. Religious Scholars	
POLITICALLY EXPOSED PERSON OR PEP Associates		
<i>Specific behavior and individual characteristics of PEPs may raise red flags or cause a suspicion:</i>		
1.	Inquiries about the Company's AML or PEP Policy	3
2.	Unable to explain the purpose of transaction	3
3.	Unable or reluctant to explain his / her profession / occupation	3
4.	Reluctant to provide information about source of funds	3
5.	PEP uses third parties for conducting transactions, i.e. use of family members, friends or close associates like employee's transactions on their behalf	4
Note: <i>Refusing a business relationship with a PEP should NOT be simply based on the Determination that the client is a PEP. Please follow the EDD process to determine a PEP.</i>		

In case of above mentioned indicators / “Red Flags”, please refer to Risk Management and internal controls to help assess the legitimacy of transaction.

Note: *Threshold Limits and list of High Risk Jurisdictions are subject to change according to the Company's and regulatory requirements. Please refer to the Company's circulars for updates.*

Important Points: -

- As per RFEC's-2024's chapter 7, Para 6 (a) & (b) Purchase and sale of foreign exchange in "Ready", "Tom" and "Spot" value dates from/to other Exchange Companies. Further, ECs shall settle Pakistan rupee consideration of all foreign currency purchase/sale transactions conducted with other Exchange Companies, only through their bank accounts.
- As per RFEC's-2024's chapter 7, Para 3 (a) & 5 (a)- Exchange Companies are authorized to deal in purchase and sale of foreign currency notes and coins from individuals in "Ready" value only.
- Exchange Companies are advised to ensure that CCTV should be operational at all times (i.e. 24 hours a day and 7 days a week), as required in terms of RFEC's-2024's chapter 5, Para 7 (a) (ii) for the purpose to real time transaction monitoring.
- In cases, where CCTV system is non-functional at an outlet for any reason, including technical faults, ECs shall not carry out any business activities in the said outlet during such time, until the functionality of the CCTV system is restored.
- Lastly, minimum preservation period of video recording as given in RFEC's-2024's chapter 5, Para 7 (a) (v) shall be of six months or until inspection of the company by SBP, whichever is earlier.
- The Company shall not establish any type of relationship with shell banks.

3.6 RISK MANAGEMENT AND INTERNAL CONTROLS

Risks need to be managed in order to successfully achieve the Company's objectives. The first step when implementing the AML / CFT risk management system is to create a set of internal controls.

Company has an effective AML / CFT risk management system in place to help understand, and quantify the risks associated with the business operations. Company's AML / CFT risk management system involves extra compliance procedures, such as requirements for Know your customer and due diligence procedures that shall help to predict the possible impact of risks and put appropriate controls in place to counter threats, and effectively pursue Company's objectives.

KNOW YOUR CUSTOMER (KYC)

Know Your Customer (KYC) is a set of guidelines designed for proper identification and verification of the identity of a customer. It is the collection and analysis of basic identity information such as identity documents.

Company's KYC procedures play a vital role for all AML / CFT measures in place to help manage the risks prudently. All reasonable efforts shall be made to determine true identity of every prospective customer who wants to make a transaction.

CUSTOMER DUE DILIGENCE (CDD)

Company performs KYC / CDD measures in order to establish and verify the identity of its customers which covers the following:

- i. Full Name of the Customer
- ii. Date and place of birth
- iii. Nationality
- iv. Existing Residential / Business Address
- v. Contact Number
- vi. Valid Form of ID (Original)
 - a. For Pakistan Nationals
 - i. CNIC (Computerized National Identity Card)
 - ii. NICOP (National Identity Card for Overseas Pakistanis)
 - iii. POC (Pakistan Origin Card)
 - iv. SNIC (Smart National Identity Card)
 - v. Passport
 - b. For Foreign Nationals
 - i. ARC (Aliens Registration Card, As per GOP Policy)
 - ii. POR (Proof of Registration for Afghan Citizen, As per GOP Policy)
 - iii. Valid Passport (having valid visa on it)
 - iv. Any other proof of legal stay
- vii. Occupation/Source Of Fund
- viii. NTN if necessary

Note: Front Line Associates (FLAs) should retain legible copies of all reference documents used for identification and verification. FLAs may also utilize NADRA Verisys facility for verification of customer's identity. Also, the FLAs must screen all customers in the sanctions lists, embedded in the system, before transaction execution. Against a possible match, FLAs are required to obtain additional information and report to compliance in case of evasion.

ENHANCED DUE DILIGENCE (PROCEDURE & REQUIREMENTS)

A rigorous and robust process of investigation over and above KYC and CDD procedures. Enhanced Due Diligence shall be applied in red flag scenarios and specially when:

- i. There is a reason to believe that the customer has been refused transaction by other financial institution/Exchange Company.
- ii. Conducting transactions for and on behalf of Politically Exposed Persons (PEPs).

‘Enhanced Customer due diligence measures’ (EDD) means –

- i. Identifying and verifying the customer’ identity, on the basis of documents, data or information obtained from reliable and independent source
- ii. Obtaining customer’s occupation, and source of funds
- iii. Obtaining information on the purpose and intended nature of the business relationship
- iv. Acquiring additional verification documents as evidence and conducting a thorough research if deemed necessary

Some customers may pose higher than average risk to the Company and should be considered for further assessment like customer’s background, country of origin, public or high profile position, and other risk indicators.

other risk indicators.

KYC /CDD AND EDD LEVELS AND DESCRIPTION

LEVEL 3 •Enhanced Due Diligence	LEVEL 2 •KYC / CDD and additional information	LEVEL 1 •Know Your Customer and Customer Due Diligence
---	---	--

- i. In low-risk scoring, staff shall adopt the regular KYC / CDD procedures.
- ii. In medium risk, staff shall conduct proper KYC and CDD and shall obtain additional information to assess the legitimacy of the transaction.
- iii. Enhanced due diligence in high risk instances should be conducted through a thorough search on the potential customer by filing enhanced due diligence forms and acquiring additional documents for verification if necessary.

REQUIREMENT OF DOCUMENTARY EVIDENCE ON HIGH RISK SCENARIOS

SR.	HIGH RISK SCENARIOS	REQUIRED DOCUMENTARY EVIDENCE
1.	Outward Transactions for the purpose of charity / donation	Documentary proof of Source of Funds, Occupation of the client & Correspondence with the counter-party
2.	Inward Transactions for the purpose of and charity / donation	Proof of occupation of both parties Correspondence with the counter-party
3.	Outward Remittance by Foreign Nationals / Nonresidents and Afghan Refugees	Documentary proof of Source of Funds / Occupation

IDENTIFICATION AND VERIFICATION OF BENEFICIAL OWNERSHIP*

Beneficial owner means a person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over the transaction. In this regard, FLA should

- i. Inquire whether there exist any beneficial owner in relation to the customer or transaction
- ii. In case of a beneficial owner, verifying the identity of the beneficial owner

ENHANCED DUE DILIGENCE PROCEDURE

It is the responsibility of the FLA to stop funds transfer at the time of transaction that could be used for:

- | | |
|---------------------------|--------------------------------|
| i. Money Laundering | vi. Bribery / Corruption |
| ii. Terrorist Financing | vii. Embezzlement |
| iii. Human Trafficking | viii. Tax Evasion |
| iv. Narcotics Trafficking | ix. Any other illegal activity |
| v. Extortion | |

PROCEDURE FOR CONDUCTING AND FILING EDD

FLA to check in its record if any special instructions related to the customer is provided by Head Office. If no instruction is available then FLA shall conduct enhanced due diligence following the method given hereunder:

- i. Open the URL <https://www.jotform.com/AAEX/enhanced-due-diligence-form>
- ii. Fill EDD Form sequence wise (Appendix-I); it is an attempt to determine the legitimacy of transaction.
- iii. If FLA is unable to determine the genuineness of transaction, he/she may ask customer to submit additional documents.
- iv. FLA may refuse the transaction, in case the EDD is unsatisfactory and select 'Unsatisfied' under EDD Assessment recording proper reason in the field of 'Additional Comments'
- v. For assistance, FLA may select 'Escalation to Compliance for Review' under EDD Assessment and contact the Compliance / relevant department at Head Office before transaction execution.
- vi. FLA must report any unusual activity/transaction to the Compliance team.
- vii. If the circumstances are suspicious, consideration should be given to filing an STR with the Financial Monitoring Unit (FMU).

Important Note: Please note that the proposed EDD questionnaire is a minimum set of information that may be obtained from customer to determine the genuineness of transaction, FLAs may satisfy themselves by using other methods or may ask more questions from customer to determine the legitimacy of transactions. In case of unsatisfactory or incomplete CDD measures, FLA should not conduct the transaction. However, in the post transaction scenario, if the circumstances are suspicious, consideration should be given to filing a Suspicious Transaction Report (STR) with the Financial Monitoring Unit (FMU)

REJECTION OF TRANSACTION

A transaction may be rejected/refused on the basis of lack of compliance or when a customer's Credentials are matched with a sanctioned person.

If any relationship is found with existing potential customer or occasional customer, following actions must be taken:

- I. Retain necessary information for the customer, may include retention of copy of Identity document, source of funds, occupation and purpose of the transaction (If possible).
- II. Reject/Refuse the transaction with delay without prior notice
- III. Inform compliance department regarding the case and fill-up rejected transaction form.

Further if FLA has conducted EDD on a specific transaction and finds any suspicion related to Money Laundering / Terrorist Financing or finds that there is no financial sense in the transaction concerned FLA is advised to follow below mentioned instructions:

Consult compliance department immediately without informing the customer or any other staff member regarding the suspicion

Compliance team may investigate the case meanwhile and advise FLA to proceed with one of the below mentioned instruction:

- i. Proceed with the transaction (In case customer is not willing to or unable to provide any other information)
- ii. Proceed with payment after acquiring relevant information / document
- iii. Proceed with cancellation / rejection but may request other documentary proof or information
- iv. Proceed with cancellation / rejection

In any of the above case, Suspicious Transaction Report is to be filed with the consent of Chief Compliance Officer if any suspicion is found.

In case of cancellation / rejection, FLA's are advised to fill up Rejected Transaction Form which is available at <https://form.jotform.com/202692150831046>

Record of all the rejected/refused transactions should be kept safe.

PROHIBITION TO DEAL WITH LEGAL PERSONS AND LEGAL ARRANGEMENTS

Dealing with Legal Persons and Legal Arrangements is prohibited, Business can be performed with regulated/supervised banks and exchange companies (within and outside Pakistan) for permissible businesses as per RFEC's Chapter 7 Para 13(B).

CHAPTER: 4 - OFFSITE MONITORING AND SURVEILLANCE

Offsite Monitoring and surveillance entails reviewing and analyzing the business operations, to assess the risk indicators on an ongoing basis and to investigate that the transaction is conducted, recorded and reported according to the rules and regulations of the Company.

Company has effective systems and tools in place, for offsite monitoring in order to detect irregularities and suspicious activities in a timely manner.

Procedures: Compliance team shall verify that:

- i. Employees are reporting suspicious activity/transactions.
- ii. Regulatory requirements are being met.
- iii. Quality of the KYC and EDD information being recorded is not ambiguous.
- iv. Updated AML and compliance information is provided to the new and existing employees.
- v. New and existing employees receive initial and ongoing AML and compliance training.

4.1 MONITORING TOOLS & PROCEDURES

- i. Transactions monitoring may be performed on Real time and Quarterly basis
- ii. Reports shall be extracted from Management Information System 'MIS' or any software assigned by the foreign associates to monitor irregular transaction patterns by the designated compliance officer.
- iii. Compliance officer shall retrieve the data from the MIS reports for monitoring.
- iv. Compliance officer shall identify and categorize High, Medium and Low risk cases for transactions analysis using Risk Based Approach.
- v. Transactions shall be filtered using multiple scenarios / red flag indicators
- vi. Once the monitoring is completed, compliance officer shall gather KYC/CDD/EDD and supporting data pertinent to each case for investigation and STR evaluation
- vii. Investigator reviews the KYC / CDD / EDD and supporting data retained by the Front Line Associates and add comments on the quality of transaction information against each highlighted case Compliance uses multiple tools for investigation i.e. Through electronic media, FBR Database, World Check by Refinitiv and other sources; the Compliance officer may also interview the Front Line Associate / customer and acquire further details of the transactions
- viii. Once the investigation is completed, the report is shared with the Chief Compliance Officer for review and decision for filing / non-filing of STR, interdiction and for putting the customer / Transactions under monitoring
- ix. Chief Compliance Officer shares the report with the Board of Directors for review, and internal enforcement actions where necessary

Chief Compliance Officer shall be independent in decision of filing / non-filing of STR, maintaining / terminating the business relationships, putting the customer under monitoring and for interdicting the client. Further, off-site report will be shared with the relevant branches for their information.

TRANSACTION MONITORING/SCREENING SYSTEM

AA Exchange has adopted a state-of-the-art transaction monitoring and screening system, through which transactional data is screened against all the embedded lists. Transaction Monitoring is being performed real time against all the predefined rules and criteria's.

Transaction monitoring can also be categorized as:

1. Systematic Monitoring
2. Manual Monitoring

Every transaction is first monitored through system then manually by compliance team (rule and name matched transactions).

SYSTEMATIC/AUTOMATIC MONITORING

Systematic monitoring system assess each transaction against predefined rules (mentioned above) and then proceed the transaction accordingly i.e. either release the transaction or block/hold for compliance review.

MONITORING PROCESS

System screens every transaction against set criteria i.e. Name matched based on percentage and Transactions Thresholds rule to assess the related risks accurately and quickly. After screening, the transaction will released automatically or blocked for compliance review (as elaborated below):

1. System will check if customer's name is matched with any of the listed person and then it will hold the transaction for compliance review.
2. In case of NACTA list, system will check Customer's CNIC/ID Number against NACTA listed person:
 - a. System will not let the transaction to be generated in case "CNIC matched" is found.
 - b. In case "CNIC not Matched" in NACTA list, system will check the name from other lists and will take a decision based on findings.
3. Based on findings i.e. percentage of matches, system will release or block the transaction
 - a. Released transaction will be forwarded for auto monitoring.
 - b. Blocked transaction will be reviewed manually by compliance team to decide either to "Release or Refuse".

TRANSACTION MONITORING RULES

System monitored associated risks with customer, product, geography and distribution channel through different rules (mentioned below) is monitored by implementing several rules in the system.

1. "Name matched Rule" based on Percentage of name matched with Lists i.e. UNSC, EU, SBP Year Limit, NACTA, FIA RED BOOK, HMT, OFAC, PEPs and Internal Block List.
2. "Amount Based Rule" (e.g. Regulatory Threshold limits) to trigger any possible structuring.
3. "Transaction Frequency" Based Rules to check the nature of customer business relationship with us/legitimacy of the transactions.
4. "Address Based Rules" to monitor transaction of the High Risk Jurisdiction customer more thoroughly, High Risk residential address, same address against multiple customers.
5. "Sender Count Rule" and "Receiver Count Rule" in IR and OR Remittance.
6. "Product Based" rules to monitor and assess the risk based on type of products a customer has used or willing to use.
7. Currency Checks (FCY)
8. Locations/Branches Count (IR/OR & FC)
9. Countries Check (Monitor Risk and count of countries)
10. Contact Number (Check if multiple customers are registered against same contact number)
11. Nationality Check (Monitor the risk based on customer's/sender's/receiver's nationality).

"These rules shall be reviewed regularly and can be updated according, rules can be add /deactivate with the passage of time depending upon the risk associated to the relevant factor".

After monitoring each transaction, transaction is rated according to the associated risks i.e. High, Medium, or Low.

MANUAL SCREENING

After a transaction is blocked (after systematic screening) compliance team reviews the transaction and customer's profile to confirm if transaction is fully compliant according to rules and regulation.

There are set procedures which are followed while manual screening (depending on the cases) i.e.

1. Compliance team will compare customer's credentials against matched individuals' credentials i.e. Name, Father Name, Date of birth, Address, ID number and Nationality (in Name matched Rule), and
 - a. In case sufficient evidences are found to verify that customer is different from matched sanctioned person, compliance team will release the transaction by adding reason/remarks to support their decision.
 - b. In case compliance team can't verify the difference (with the help of all available information), transaction will be refused after adding reason/remarks to support their decision.

- 2. Compliance team may require extra information (Including occupation, exact purpose, relationship withcounter party, Source of funds etc.) to confirm the financial sense of the transaction. EDD is advised accordingly and documentary proofs might also be collected as evidence (In Rule base transactions).

TRANSACTION PROCESSING FLOWCHART

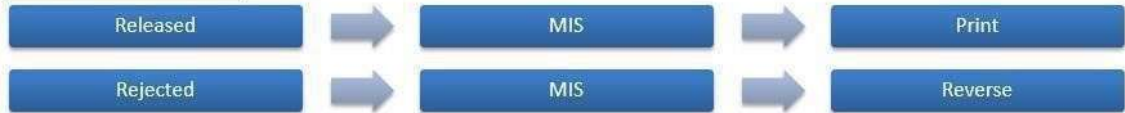
TRANSACTION GENERATION



TRANSACTION PROCESSING



TRANSACTION CONCLUSION



4.2 CLIENT MONITORING PROCESS

Company has a centralized monitoring/review process for high risk clients / PEPs. These structures help to ensure that all relevant internal information is carefully considered in specific cases.

Company's MIS and global sanctions database shall be used for offsite monitoring of high risk clients / PEPs in order to mitigate risk, and to actively manage the termination of a business relationship with a client / PEP, if and where deemed necessary.

4.3 REMITTANCE MONITORING PROCESS

Company's MIS or any monitoring tool assigned by the foreign associates shall be used to detect / identify the suspicious transaction patterns based on the below criteria, and to review the quality of the data. Compliance Manager / designated officer shall initiate investigation on the cases identified in offsite monitoring and take necessary actions where required.

INWARD REMITTANCE

- i. High Frequency Transactions (for example Ten or more transactions in a quarter)
- ii. High Value Transactions (for example Aggregated amount is equivalent or above PKR 1,000,000)
- iii. Transactions from High Risk Jurisdictions
- iv. Multiple beneficiaries receiving funds from same sender
- v. Same Beneficiary receiving funds from multiple senders
- vi. Customer using different / multiple IDs
- vii. Consumer Networking

OUTWARD REMITTANCE THROUGH MTOS

- i. High Frequency Transactions (for example 10 or more transactions in a quarter)
- ii. High Value Transactions (for example aggregated amount is equivalent to USD-10,000 or above in week/month)
- iii. Structuring and Splitting on same / consecutive days to avoid internal and regulatory requirements
- iv. Transactions to High Risk Jurisdictions
- v. Multiple senders remitting funds to same beneficiary
- vi. Same sender remitting funds to multiple beneficiaries
- vii. Customer using different / multiple IDs
- viii. Consumer Networking

OUTWARD FOREIGN TELEGRAPHIC TRANSFER / FOREIGN DEMAND DRAFT

- i. High Frequency Transactions (for example Three or more transactions in a quarter)
- ii. High Value Transactions (for example aggregated amount is equivalent to 20,000 USD)
- iii. Structuring and Splitting on same / consecutive days to avoid internal and regulatory requirements
- iv. Transactions to High Risk Jurisdictions
- v. Multiple senders remitting funds to same beneficiary
- vi. Same sender remitting funds to multiple beneficiaries
- vii. Customer using different / multiple IDs

Periodic review of the data collected shall be conducted and compliance team shall take appropriate action that may include staff training/ counseling, reporting the case to relevant authorities and penalizing the concerned Branch staff.

4.4 FOREIGN CURRENCY EXCHANGE / CASH TRANSACTIONS MONITORING PROCESS

Company's MIS or any monitoring tool assigned by the foreign associates shall be used to detect and identify suspicious transaction patterns on the basis of the Red Flags for Foreign Currency Exchange / Cash Transactions given as under.

- i. High Frequency Transactions (for example Ten (10) or more transactions in a quarter)
- ii. High Value Transactions (for example aggregated amount is equivalent or above 25,000 USD in a quarter)
- iii. Structuring and Splitting on same / consecutive days to avoid internal and regulatory requirements
- iv. More than one customers using same contact number
- v. More than one customers using same contact address
- vi. Customer using different / multiple IDs
- vii. High Risk Clients (Prominent Figures / PEP)
- viii. Sale / Purchase of Unusual / multiple currencies

Periodic review of the data collected shall be conducted and compliance team shall take appropriate action that may include staff training/ counseling, reporting the case to relevant authorities and penalizing the concerned Branch staff.

4.6 KNOW YOUR PARTNER - OFFSITE DUE DILIGENCE PROCESS

In order to comply with Company's obligations as prescribed by the KYC / AML / CFT regulations of the State Bank of Pakistan, the Company requires that all external parties with whom it carries out business apply ethical principles that are consistent with its own. External parties include, but are not limited to, Foreign Entities, Money Transfer Organizations and other Exchange Companies.

Proper due diligence procedures enable the Company to follow through on its commitment to act with integrity by protecting against partnering with companies and individuals that do not operate pursuant to ethical principles. Due Diligence procedures also minimize reputational and legal risks, by investigating potential correspondent entity's' past and current ethical standing.

SELECTION STAGE

- i. Only those entities that have effective AML / KYC policies and are effectively supervised by the relevant authorities should be selected for agency agreements.
- ii. No arrangements should be entered into or continued with a correspondent entity incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.
- iii. Company should pay particular attention, when continuing relationship with entities located in jurisdictions that have poor KYC standards or have been identified by Financial Action Task Force (FATF) as being "non-cooperative" in the fight against Money Laundering.

PRE-AGREEMENT STAGE

- i. Copy of License issued by the concerned regulatory body should be obtained and it should be confirmed that the entity has power to enter into or execute such arrangements.
- ii. Investigation of their credentials and market reputation
- iii. Network Size and its details
- iv. List of their existing partners / associates
- v. Ownership Structure and Details
- vi. AML / CFT Policy should be obtained
- vii. AML and KYC Questionnaire for External Correspondent Entities (Appendix-II) should be filled and signed by their Compliance Officer

All agreement arrangements should be made with the principal company

In case of agreement arrangements with a Foreign Entity, Company shall also have understanding of legal and regulatory framework of the jurisdiction involved with respect to the following:

- i. Rules related to licensing requirements
- ii. Rules regarding opening / closing / shifting of business locations
- iii. Anti-Money Laundering and KYC requirements
- iv. Laws and regulations related to overseas agency arrangements.

POST AGREEMENT STAGE

- i. Company should continuously monitor the market reputation and financial condition of the external partners / agents
- ii. Ensure that External Parties are made bound to immediately bring into the notice of the Company any change in laws, rules and regulations which may affect business arrangements and any change in its network
- iii. Ensure that prior approval from SBP is obtained for any subsequent changes in the agreement

CHAPTER: 5 - SANCTION SCREENING

Sanctions Screening is the process of reviewing sanctions lists to check if any individual(s) is or has been involved in financial crime or terrorism financing, in order to take appropriate measures.

To implement the targeted financial sanctions regimes to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCR 1267(1999) and its successor resolutions, and UNSCR 1373(2001) applicable lists i.e. UNSC and NACTA are embedded in the Company's Management Information System 'MIS' for transactions screening. To protect and safeguard the Company from any reputational damage, fines and to mitigate the TF risks, other lists including OFAC, HMT, EU, and FIA Redbook are also embedded in the system and updating regularly.

Note: *For complete procedure and mechanism, please refer to the Company's Sanction Screening Guidelines.*

5.1 WORLD CHECK

In addition, Company has a separate global sanctions database 'World Check' as a support tool for KYC verification and risk assessment in areas such as PEP monitoring, sanction screening, AML / CFT risk, and anti-bribery and corruption.

Note: *Compliance team shall frequently use electronic media as an independent source of information for the determination, monitoring, verification of information in relation to high risk customers / transactions.*

ON GOING SCREENING

Company shall perform screening of the Shareholders, Directors, CEO and Key Executives on an ongoing basis for designated/proscribed entities/persons and maintain proper record of screening.

CHAPTER: 6 SUSPICIOUS TRANSACTION REPORTING AND CURRENCY TRANSACTION REPORTING

6.1 FINANCIAL MONITORING UNIT- FMU

Financial Monitoring Unit is an independent Federal Government entity in Pakistan with an aim of combating money laundering and terrorist financing. FMU is the only designated agency in Pakistan to which Suspicious Transactions reports and Currency Transactions reports shall be made.

6.2 CURRENCY TRANSACTION REPORTING (CTR)

CTR shall be reported to FMU for each transaction involving sale/purchase of foreign currency that exceeds or is equivalent to the figure of Rs. 2 million, immediately, but not later than seven working days as provided in the Section 7(3) of AML Act 2010.

PROCEDURE

- i. Concerned Branch will fill and submit the CTR form embedded in the system
- ii. CTR form shall be submitted to FMU by the Finance department at Head office within the required time
- iii. Compliance team may verify whether the CTR(s) are being reported correctly and within time

Note: Every single cash transaction of two (02) million rupees or above is to be reported as CTR. If there is a suspicion that the customer is structuring the transaction into several broken cash transactions to evade reporting of CTR, same may be reported in the form of Suspicious Transaction Report.

6.3 SUSPICIOUS TRANSACTION REPORTING (STR)

A **suspicious transaction**, whether completed or attempted, is a transaction that could be related to money laundering or terrorist financing offence. STR shall be filed if the Chief Compliance Officer / MLRO, knows, identifies, suspects, or has reason to suspect that the transaction(s), involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime, or is involved in terrorism financing.

STR shall be filed immediately after forming that suspicion in respect of a particular transaction, irrespective of the fact that the transaction was executed or not.

Guidance notes for filling STR to FMU by the authorized CCO / MLRO;

[http://www.fmu.gov.pk/docs/Guidance_notes_to_Reporting_Entities_\(Non_Bank\).pdf](http://www.fmu.gov.pk/docs/Guidance_notes_to_Reporting_Entities_(Non_Bank).pdf)

SUSPICIOUS TRANSACTION / ACTIVITY INCLUDES

- i. Possible attempts to launder money
- ii. Transactions that serve no business or apparent lawful purpose
- iii. Transactions that are unusual and there is no reasonable explanation
- iv. Altered or false identification
- v. Inconsistent information
- vi. Possible Structuring
- vii. Any other transaction / activity relating to the predicate offence given under AML Act 2010

PROCEDURE

FLAs shall remain vigilant while attending to their day to day operations and pay attention to any red flags that might appear during the transactional activities of the customers.

FLAs shall obtain as much information as possible about the customer and report any unusual/suspicious activity that might arise to the Compliance Team at Head Office.

Compliance Team shall investigate the cases reported by the FLAs or identified during offsite monitoring.

- i. Chief Compliance Officer / MLRO shall review and verify all the information, before filing of STR.
- ii. STR shall be filed with FMU along with necessary KYC documents/evidences.
- iii. Copy of STR shall be retained along with any supporting documentation for 10 years.

CHAPTER: 7 - CURRENCY EXPORT

The core business of the exchange company is to deal in the sale and purchase of foreign currency and to collect several different currencies from different parties including following;

- i. Own locations.
- ii. Other exchange companies.

Hence there was a need to set up a structure which would assist the exchange companies in Pakistan to export the currencies outside Pakistan and bring back the designated USD after necessary conversions back to Pakistan. This exercise keeps the open market USD prices in check and liquidity position improves significantly.

7.1 CASH COLLECTION (FOREIGN CURRENCY TO BE EXPORTED)

Available cash (Foreign Currency to be exported) is deposited to the designated branches in each region. From there Cash is transferred to another designated branch, where it is counted again, checked and packed as per SBP's instructions.

Further following procedures should be followed:-

Exchange Companies are allowed to export all foreign currencies other than US Dollars on consignment basis through cargo/security companies. Prior approval from SBP is mandatory before starting the foreign currency export business. (EPD Circular letter No. 06- dated May 24, 2021) (Revision of Chapter 5)

- i. Currencies other than US Dollars are permissible to be exported by the SBP
- ii. Minimum of 10% of US Dollars received against export of foreign currencies are to be sold in interbank on an ongoing basis.
- iii. Currency Export is to be done through SBP & Pakistan Customs Joint Booths located at international departure lounges of designated airports i.e. Jinnah International airport-Karachi, Allama Iqbal International Airport -Lahore, Islamabad and Bacha Khan international Airport- Peshawar.
- iv. Foreign Currency Deal must be finalized with overseas entity before the shipment of each export consignment. The system generated deal ticket (specifying consignee name, address, contract details, amount, exchange rate etc.) must be accompanied with each request for exporting permissible foreign currencies.
- v. Currency carrier representative must approach the SBP & Customs joint booth 4 hours prior to the scheduled departure time of the flight through which export of currency is intended to be made or 02 hours prior to the closure time of the SBP –Custom joint booth whichever is earlier.

- vi. All currencies presented at SBP-Customs joint booth should be in packets Of 100 notes each of the same currency and denomination.
- vii. Loose notes can only be exported twice in week i.e. on Wednesday and Saturday
- viii. Following are the documents, should be with carrier.
 - a. Cover letter/Export declaration in triplicate
 - i. Containing UTN (**Unique Transaction Number**) on cover letter i.e. Company's Initials, Transaction Number and financial year
 - ii. Addressed to State Bank of Pakistan and Pakistan Customs
 - b. Summary of shipment
 - i. Including amount
 - ii. Including count of different currencies denomination notes
 - iii. Local bank account details in which settlement amount will be credited
 - iv. Counterparty's detail
 - c. Authorization letter
 - d. Deal tickets
 - e. Any other relevant documents including export permission letter and company's License must be presented at the SBP and customs joint booth with the currency which is to be exported.
- ix. All the documents should also be maintained for record keeping purpose.
- x. After all the checks (by SPB and customs) currency is cleared to be exported and can be carried only if SBP and customs sign and stamps are embossed on the currency packets.

After the recent instruction and new guidelines by the State Bank of Pakistan, currency export can be done using authorized currency cargo services provider.

All the mandatory documents, with the physical currency can be handled on behalf of AA Exchange Company by nominated cargo/security company:

- i. An agreement has been signed between AA Exchange and Cargo/security Company
- ii. Deal has been finalized with the counterparty after mandatory due diligence and ticket (Against the deal) has been generated
- iii. Cargo/security Company will initiate the export as per SBP and Pakistan customs directives.
- iv. Settlement against the export will be done in local bank FC account within 05 working days.

7.2 SETTLEMENT AGAINST THE EXPORT

- i. Local bank foreign currency (US – Dollars) account must be credited within 05 (Five) working days against the export of foreign currency other than USD
- ii. ECs should maintain separate FC accounts for receiving proceeds against export of permissible FCs for reconciliation purpose.
- iii. No other remittances and foreign currency cash shall be deposited in these accounts.

7.3 DUE DILIGENCE OF CARGO /SECURITY COMPANY

Proper due diligence procedures enable the Company to follow through on its commitment to act with integrity by protecting against partnering with companies and individuals that do not operate pursuant to ethical principles. Due Diligence procedures also minimize reputational and legal risks, by investigating potential correspondent entity's past and current ethical standing.

- i. EC's shall satisfy themselves before entering into the contract with the cargo/security company registered in Pakistan
- ii. EC's shall ensure that the contract /agreement with the cargo/security company is at Arm's length Basis.
- iii. Exchange companies shall ensure carrying out due diligence of the cargo/security company prior to the execution of the contract the contract/agreement and ensure its periodical updating /review

CHAPTER: 8 - PUNISHMENT FOR MONEY LAUNDERING AND RELATED OFFENCES

On any contravention of

- I. Section 7(1), 7(3) to 7(6) and 7A to 7H of the AML Act;
- II. AML/CFT Regulations; and
- III. Regulations issued by FMU

Any or all of the following sanctions may be imposed by the concerned AML/CFT regulatory Authority, namely:-

- a) Impose a monetary penalty in accordance with these rules
- b) Impose any condition, limitation or restriction on the reporting entity's business or product offerings, as it considers appropriate,
- c) Revoke license or de-registration of the reporting entities as applicable
- d) Impose a temporary or permanent prohibition on any natural person who holds an office or position involving responsibility for taking decisions about the management of the reporting entity, including but not limited to:
 - a. Issuing a written warning;
 - b. Imposing a temporary suspension; or
 - c. Removal from services.
- e) Issue a statement of censure/warning/reprimand;
- f) Issue a direction to the person to undertake any given actions, including but not limited to:
 - a. Comply with the requirements within a specified time period through a remedial plan;
 - b. Conduct internal inquiries; or
 - c. Take disciplinary action against directors, senior management and other officers
- g) Impose any other sanction permitted under the AML/CFT regulatory authority's enabling Legislation and any rules, regulations or directives issued thereunder.

8.1 PUNISHMENT FOR MONEY LAUNDERING

According to the AML Act 2010 (as amended up to September 2020), whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than one year but may extend to ten years and shall also be liable to fine which may extend to twenty-five (25) million rupees and shall also be liable to forfeiture of property involved in money laundering or property of corresponding value.

8.2 FAILURE TO FILE SUSPICIOUS TRANSACTION REPORT AND FOR PROVIDING FALSE INFORMATION

- i. Whoever willfully fails to comply with the suspicious transaction reporting requirement as Provided in section 7 of the AML Act 2010 or give false information shall be liable for imprisonment for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or both.
- ii. In the case of the conviction of the Company, the concerned regulatory authority may also revoke Company's license or take such other administrative action.

8.3 DISCLOSURE OF INFORMATION (TIPPING OFF)

According to the AML Act 2010, the directors, officers & employees of the Company are prohibited from disclosing, directly or indirectly, to any person involved in the transaction that the transaction has been reported. Tipping off is a criminal offence and shall be punishable by a maximum term of five years imprisonment or a fine which may extend to two million rupees or both.

Company can however make normal enquiries to learn more about the transaction or instruction to determine whether the activities of the customer arouse suspicion.

Note: *Employees of the company are strictly prohibited to disclose to the customer or any third person (s) that a suspicious transaction or related information is being or has been reported to any authority, except if required by law.*

CHAPTER: 9 -

UNSC, NACTA & OTHER RELEVANT INTERNATIONAL AGENCIES / EVALUATION BODIES

For the development and implementation of appropriate measures and procedures on a risk based approach, and Due Diligence Procedures, the Compliance team consults data, information and reports from;

9.1 UNITED NATION'S SECURITY COUNCIL (UNSC)

The UN Charter established six main organs of the United Nations, including the Security Council UNSC. It gives primary responsibility for maintaining international peace and security to the Security Council, which may meet whenever peace is threatened.

UNSC has the power to make decisions that member states are obligated to implement under the Charter. Security Council sanctions have taken a number of different forms, in pursuit of a variety of goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council has applied sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation.

The Consolidated Sanctions List includes all individuals and entities subject to sanctions measures. <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>

9.2 NATIONAL COUNTER TERRORISM AUTHORITY (NACTA)

National Counter Terrorism Authority (NACTA) is an Internal Counter-terrorism Authority of Pakistan. NACTA is mandated to devise a counter-terrorism strategy that should address short, medium and long-term goals and devise action plans for their implementation. NACTA maintains a list of Fourth Schedulers under Anti-Terrorism Act, 1997.

Any individual about whom either there is a credible intelligence-information or who has a history of being linked to a Proscribed Organization can be proscribed by Home Department of a Province and can be subjected to restrictions on travel, speech and business, under the Anti-Terrorism Act, 1997. After issuance notification by the Home Department, name of such proscribed person is included in the 4th Schedule under the Anti-Terrorism Act, 1997. Therefore, such proscribed persons are also referred to in local Police/ LEAs parlance as 4th Schedulers.

9.3 OFFICE OF FOREIGN ASSET CONTROL (OFAC)

A department of the U.S. Treasury that enforces economic and trade sanctions against countries and groups of individuals involved in terrorism, narcotics and other disreputable activities.

List issued by the Office of Foreign Assets Control (OFAC), USA.
<http://www.treasury.gov/offices/enforcement/ofac/sdn/>

9.4 FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is the main international body established to combat money laundering and terrorist financing.

FATF monitors countries progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and counter-measures; and, promotes the adoption and implementation of the FATF Recommendations globally.

FATF High Risk and Non-cooperative Jurisdictions

<http://www.fatf-gafi.org/Clauses/high-riskandnon-cooperativejurisdictions/>

CHAPTER: 10 EMPLOYEE RECRUITMENT AND TRAINING

Company should recruit after performing necessary background checks and screening the individual, and satisfy themselves that the staff they employ have integrity, are adequately skilled and possess the knowledge and expertise required to carry out their responsibilities, in particular where staff are responsible for implementing AML / CFT controls.

10.1 Appointment of CEO

- a. The Board will appoint the CEO and also determine the terms and conditions of his/her appointment.
- b. The CEO, subject to directions and control of the Board, will be entrusted with the powers of management of the affairs of the Company.
- c. The Company will be responsible to conduct prior self-assessment of the FPT of the CEO in accordance with criteria given in Annexure-B.
- d. Subsequent to above self-assessment, the Company will seek SBP's approval for appointment of CEO, submitting documents as per Annexure-B1 & B2.
- e. Subject to receipt of approval from SBP, the CEO will assume the charge and the Company will share copy of charge assumption report with SBP immediately.
- f. The Company can appoint an Acting CEO, for a period not exceeding three (03) months in case of vacation of the office of CEO due to any plausible reason (including resignation, removal, etc.). The Company can assign acting charge of CEO Office to any existing Key Executive, whose FPT has been cleared by SBP previously or who meets the FPT Criteria prescribed for the CEO.
- g. The Company will inform SBP within three working days of the assumption of charge by Acting CEO. Further, during the three (03) months' period of acting charge, the Company will initiate process for appointment of CEO and seek approval of SBP, as mentioned in (a) to (d), above.

10.2 Appointment of Key Executives

- a. The Company will ensure appointment of well qualified persons for all key executive positions including Chief Compliance Officer, Head of Operations etc.
- b. The Company will conduct prior self-assessment of FPT of the all Key Executives as per criteria given in Annexure-B to ensure they meet the relevant FPT criteria in letter and spirit and keep this assessment on record for review of SBP inspection.
- c. The appointment of all Key Executives will not require prior approval of SBP.
- d. The Company will inform SBP within seven (07) working days of assumption of the charge of the post by the incumbent and submit the information as per Annexure-B1 & B2.

10.3 Screening of Shareholders, Directors, CEO and Key Executives

- a. The Company will institute a proper mechanism for screening of the Shareholders, Directors, CEO and Key Executives, on an ongoing basis, as per criteria set under relevant resolutions of the United Nations Security Council Resolutions and Anti Terrorism Act, 1997 for designated/proscribed entities/persons.
- b. The Shareholder, Director, CEO or Key Executive will become disqualified if they become designated/proscribed or found associated directly or indirectly with any designated/proscribed entity or person.
- c. The Company will maintain proper record of such screening.
- d. The Company shall obtain annually a declaration from all Shareholders, Directors, CEO and Key Executives as per Annexure B3 that the information previously provided has not undergone change and where there is any change, requisite details have been furnished to SBP within fifteen (15) days of the change.

10.4 EMPLOYEE TRAINING

PURPOSE

To establish required processes for consistent training of all new and existing employees. It is important that staff receive AML / CFT training, which should be:

- i. Relevant to the Company's ML / TF risks, business activities and up to date with the latest legal

- and regulatory obligations, and internal controls
- ii. Mandatory for all relevant staff
- iii. Tailored to particular lines of business, preparing staff with an understanding of specialized ML/TF risks they are likely to face and their responsibilities in relation to those risks
- iv. Effective: training should have the desired effect
- v. Complemented by AML / CFT information and updates that are disseminated to relevant staff as appropriate.

Overall, the training should also seek to build up a working culture where compliance is embedded in the activities and decisions of the entire Company's staff.

PROCEDURES

- i. At the time of the induction every employee should be provided with the basic training covering key areas of operations, related Standard Operating Procedures (SOPs), fraud prevention and compliance policies, AML / CFT, KYC, record management and maintenance.
- ii. Compliance trainer should use the local and international Anti-Money Laundering Compliance Program to provide initial training.

In addition to the above, various training sessions should be conducted throughout the year at the following different levels

- i. Quarterly Internal Audit refresher training program
- ii. Training at Regional levels
- iii. On the Job and offsite trainings
- iv. Annual Seminar

10.5 TRAINING ASSESSMENT AND EFFECTIVENESS

Effectiveness of the training can be evaluated by requiring the staff to solve case studies and pass tests, by monitoring levels of compliance, interviewing during internal audit or by mystery shopping. Training tests on AML and CFT should be score based to assess the efficiency of the employees.

Note: All Company's employees are required to sign the AML / CFT undertaking(Annexure- III).

10.2 TRAINING MEDIUM

Different mediums are available for the trainings. Company may choose the relevant one for the specific type of training i.e. to train the distant staff virtual training may be organized.

10.3 APPOINTMENT/INDUCTION OF NEW DIRECTOR OR SHAREHOLDER

Company shall conduct prior self-assessment of fitness and propriety for all fresh inductions/appointments of shareholders, Directors and CEO before seeking approval of SBP.

Self-assessment of fitness and propriety includes (but not limited to);

- i. Police Character Certificate & Verification Letter
- ii. Disclosure of all bank accounts held in the past 05 years along with statements
- iii. Disclosure of Directorship, Partnership, Sole proprietor or any key position held in any other business entity in last 10 years
- iv. Income Tax and wealth Tax return for last 03 years
- v. CNIC
- vi. Family registration certificate from NADRA
- vii. Attested copy of passport along with travel history for 05 years
- viii. Detailed CV (along with passport size picture) including qualification and all work experience
- ix. World check and Media search report
- x. Declaration that individual is not debarred for being shareholder, Director, CEO and key Executive or in similar capacity of an Exchange Company or any other financial institution.
- xi. Declaration that no stakes of any kind in any other exchange company or similar businesses were ever held both in Pakistan and/or abroad.

CHAPTER: 11 - DOCUMENT RETENTION

Company has a separate record retention policy that describes who is responsible for record keeping and outlines the necessary retention timeline for each type of record. It is important to keep and preserve the record for ten (10) years as required by regulatory authorities.

Note: *For additional details, please refer to the company's record retention policy.*

CHAPTER: 12 - ROLES AND RESPONSIBILITIES

Responsibility of the Compliance is defined at four levels:

12.1 BOARD OF DIRECTORS

- i. Board of Directors shall review and approve the AML and CFT policy at least annually.
- ii. Board has to ensure that the Compliance team is authorized to contact the Board of Directors directly, as deemed necessary
- iii. Responsible for establishing a permanent Compliance function within the organization including Chief Compliance Officer (CCO)

12.2 SENIOR MANAGEMENT

- i. Responsible for overall compliance of the company and ensuring adequate resources are provided for the proper training of staff and the implementing of risk systems
- ii. Senior management will be sent regular updates by the Chief Compliance Officer / Compliance Managers on compliance matters
- iii. Responsible for reviewing the efficiency of implementation of this policy on a regular basis

12.3 CHIEF COMPLIANCE OFFICER / MANAGER

- i. Chief Compliance Officer (CCO) / Compliance Manager will regularly update the Chief Executive Officer on compliance matters and Serve as a contact point between the Chief Executive Officer (CEO) and senior management of the Company with regard to implementation of AML / CFT policy
- ii. Chief Compliance Officer will be responsible for / to;
 - a) Effective compliance of regulatory requirements and policies and procedures relating to combating money laundering and terrorist financing
 - b) Offsite Monitoring & Surveillance
 - c) Submission of Quarterly Offsite Transaction Monitoring Reports to the Board of Directors
 - d) Coordinate with relevant external bodies and regulators on compliance matters; exercise any specific legal responsibilities such as reporting suspicious transactions related to money laundering and terrorism financing
 - e) Disseminating updates in the regulatory rules and regulations to Internal Compliance for enforcement
 - f) Report violations of compliance or regulatory standards to duly authorized enforcement agencies as appropriate or required
 - g) Preparing offsite compliance reports and assimilate the investigation results and evidences, and share the report with senior executive management for necessary actions and dissemination of reports to the respective locations if required.
 - h) Working closely with all external and internal stakeholders, examine the violations contained in the internal / external audit and Offsite Compliance Reports and take necessary enforcement actions against concerned individuals, advising immediate compliance and submission of timeline action plans. In addition, the department facilitates other departments of the company as and when required.

- i) Formal discussions with management and Branch managers to resolve serious issues and agree on course of action for corrective measures.
- j) Coordinate in all compliance related matters and make amendments in the policies and control mechanism to address the deficiencies / improve them.

Chief Compliance Officer / Managers will update the Senior Management on the status and efficiency of the implementation of this manual on annual basis (including, but not limited to the achievement of compliance-related objectives, the main risks detected by the Compliance function and the corrective action taken and preventive measures to mitigate these risks).

12.4 STAFF

It is important to stress that the staff members remain personally responsible for


- i. Handling business operational activities in a prudent and compliant manner
- ii. Adherence to the compliance guidelines and Company's rules and regulations in their respective operational activities
- iii. Reporting all breaches thereof promptly to the Compliance Function
- iv. Reporting of all suspicious circumstances to the MLRO / Compliance Manager.

CHAPTER: 13 - INDEPENDENT REVIEW OF COMPLIANCE PROGRAM AND ITS EFFECTIVENESS

Company shall maintain an independent audit function in line with Code of Corporate Governance that is adequately resourced and able to regularly assess the effectiveness of the Company's Compliance Program. An independent audit of the Company's network shall be conducted on a regular basis to evaluate the effectiveness of the procedures and control mechanisms applied to safeguard the business, from the risks of legal or regulatory sanctions, financial loss, or loss to reputation, and for the prevention of Money Laundering and Terrorist Financing.

Internal Audit Team shall also conduct a quarterly review of the Compliance Program of the Company to assess its appropriateness. This review shall point out the anomalies and deficiencies, on the basis of which the Internal Audit team shall make recommendations for resolving these issues and adopting corrective measures.

ANNEXURE – I (EDD QUESTIONNAIRE)


AA EXCHANGE®

Enhanced Due Diligence Form

Transaction Date *

Location Name *

Nature of Transaction *

Reference No. *

Transaction Code

Reason for Due Diligence *

☐ Possible Structuring

☐ High Frequency

☐ Multiple Senders

☐ High Value Amount

☐ Multiple Beneficiaries

☐ Lack of Relationship

☐ High Risk Jurisdiction

☐ Other

Customer Name *

Customer ID Number *

Customer Phone Number *

Occupation *

Source of Funds *

Counter-party's Occupation

(optional)

Purpose and Intended Nature of Transaction *

☐ Family Support and Maintenance

☐ Medical Expenses

☐ Travelling and Accommodation Expenses

☐ Educational Expenses

☐ Loan Payment

☐ Other

Relationship with Counter-party

☐ Family

☐ Employee / Employer

☐ Teacher / Student

☐ Friend

☐ Business Partner

☐ Purchaser / Seller

☐ Other

Third Party / Beneficial Owner *


☐ Yes ☐ No

Additional Comments *

FLA Name and Signatures *

EDD Assessment *

ANNEXURE – II (AML QUESTIONNAIRE FOR EXTERNAL CORRESPONDENT ENTITIES)


AA EXCHANGE®

QUESTIONNAIRE
(TO BE FILLED BY OUR CORRESPONDENT ENTITIES & BANKS)

Anti-Money Laundering, Combating Terrorist Financing and Know Your Customer

In order to comply with Company's obligations as prescribed by KYC/AML/CTF Laws of the State Bank of Pakistan, we kindly require all our Correspondent to fill up the KYC, CTF and AML questionnaire below.

Section I – General Information

1.	Legal Name Of Institution:	
2.	Full Legal Name of the ultimate parent (if different from the Entity completing the document)	
3.	Principal Place Of Business (Address):	
4.	Corporate Legal Form:	
5.	Date Of Establishment:	
6.	Is there any Regulatory Authority for Supervision of your Institution?	
7.	Name of Local Licensing Authority And Regulator:	
8.	Regulator License No: (Provide a Copy of the License):	
9.	Date Of Incorporation:	
10.	Network Size: (Provide a List)	
11.	External Auditor:	
12.	Official Website Address:	

Section II – Non Shell Bank Arrangements

1.	Institution is not a Shell Bank*	<input type="checkbox"/>
2.	Institution does not maintain accounts for Shell Banks and does not conduct business with Shell Banks.	<input type="checkbox"/>

* Shell Bank means a bank incorporated in a jurisdiction in which it has no physical presence and which is affiliated financial group (i.e. FATF Fully Recommended).

Section III – Ownership and Management Information

1.	Is your Institution is listed with any Stock Exchange If Yes provide us detail:

2. Please list the names of all owners* in the table below and their ownership interest (add further rows if necessary):		
Name	Nationality	Ownership Interest (%)

* An "owner" is any person or legal entity that, directly or indirectly, owns or controls any class of securities or other voting interests in the Institution.

3.	Have there been any significant changes in ownership over the last five years? If yes, please provide details:	<input type="checkbox"/> Yes <input type="checkbox"/> No

4.	Are there any Politically Exposed Persons*** among your Institution's ownership structure and executive management? If yes, please provide details (name and role):	<input type="checkbox"/> Yes <input type="checkbox"/> No

5.	Confirm if the FI or the regulator is a member of Financial Action Task Force (FATF) or regional FATF style bodies? If yes, then please provide details:	<input type="checkbox"/> Yes <input type="checkbox"/> No

6	Confirm that the FI has not been prosecuted or fined for failure to comply with Anti-Money Laundering laws and / or Sanctions violation in the last 5 years? If your answer is "No", then please provide details: _____	<input type="checkbox"/> Yes <input type="checkbox"/> No
7	No negative comments / observations have been made by your Regulator or External Auditor on your AML, KYC and Sanctions policies and processes in last two years.	<input type="checkbox"/> Yes <input type="checkbox"/> No

Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public function, for example Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, or their family members or close associates. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories (cf. FATF Party Recommendations).

Section IV - Business Activity

1.	Please provide the principal types of Business Activity
a.	
b.	
c.	
d.	
e.	

Anti-Money Laundering Questionnaire

Section I - General AML Policies, Practices and Procedures:

1.	Does the AML compliance program require approval, atleast annually, of the FI's Board or a senior committee thereof?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2.	Does the FI have a legal and regulatory compliance program that includes a designated Compliance officer that is responsible for coordinating and overseeing the AML program on a day-to-day basis, which has been approved by senior management of the FI?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.	Has the FI developed written policies and procedures consistent with the applicable AML, CTF and Sanctions regulations and requirements to reasonably prevent, detect and report suspicious transactions that has been approved by senior management?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.	In addition to inspections by the government supervisors/regulators, does the FI Customer have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?	<input type="checkbox"/> Yes <input type="checkbox"/> No
5.	Does the FI have policies covering relationships with politically exposed persons consistent with industry best practices?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.	Does the FI have appropriate record retention procedures pursuant to applicable law?	<input type="checkbox"/> Yes <input type="checkbox"/> No
7.	Does the FI require that its AML policies and practices be applied to all branches and subsidiaries of the FI both in the home country and in locations outside of the home country?	<input type="checkbox"/> Yes <input type="checkbox"/> No
8.	Does your institution provide training to employees regarding KYC/AML/CTF?	<input type="checkbox"/> Yes <input type="checkbox"/> No
9.	Is the FI fully compliant with the FATF 49 recommendations?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Section II - Risk Assessment

10.	Does the FI have a risk focused assessment of its customer base and transactions of its customers?	<input type="checkbox"/> Yes <input type="checkbox"/> No
11.	Does the FI have policies in place to assess the risks of relationships with PEPs, including their family and close associates? Does the FI review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	<input type="checkbox"/> Yes <input type="checkbox"/> No
12.	Does the FI determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Section III - Know Your Customer, Due Diligence and Enhanced Due Diligence

13.	Has the FI implemented systems for the identification of its customers, including customer information in the case of recorded transactions, account opening, etc. (for example; name, nationality, street address, telephone number, occupation, age/date of birth, number and type of valid official identification, as well as the name of the country/state that issued it)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
14.	Does the FI have a requirement to collect information regarding its customers' business activities?	<input type="checkbox"/> Yes <input type="checkbox"/> No
15.	Does the FI collect information and assess its FI customers' AML policies or practices?	<input type="checkbox"/> Yes <input type="checkbox"/> No
16.	Does the FI have procedures to establish a record for each customer noting their respective identification documents and Know Your Customer Information collected at account opening?	<input type="checkbox"/> Yes <input type="checkbox"/> No
17.	Does the FI take steps to understand the normal and expected transactions of its customers based on its risk assessment of its customers?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Section IV - Reportable Transactions and Prevention & Detection of Transactions with Illegally Obtained Funds

18.	Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	<input type="checkbox"/> Yes <input type="checkbox"/> No
19.	Does the FI have policies or practices to identify transactions structured to avoid large cash reporting requirements?	<input type="checkbox"/> Yes <input type="checkbox"/> No
20.	Does the FI have policies or practices to screen customers or transactions the FI deems to be of significantly high risk (which may include individuals, entities or countries that are contained on the lists issued by government/international bodies such as UNSC, NACTA, OFAC, HM TREASURY, EU) that special attention to such customers or transactions is necessary prior to completing any such transactions?	<input type="checkbox"/> Yes <input type="checkbox"/> No
21.	Does the FI have policies to reasonably ensure that they will not open accounts and conduct transactions with or on behalf of shell banks through any of its accounts or products?	<input type="checkbox"/> Yes <input type="checkbox"/> No
22.	Does the FI have policies to reasonably ensure that it only operates with correspondent banks, exchange houses and money transfer agents that are licensed?	<input type="checkbox"/> Yes <input type="checkbox"/> No

V. Transaction Monitoring

23	Does the FI have a monitoring program for suspicious or unusual activity that covers funds transfers and monetary instruments (such as travellers checks, money orders, etc.)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
----	--	--

VI. AML Training

24	Does the FI provide AML training to relevant employees that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?	<input type="checkbox"/> Yes <input type="checkbox"/> No
25	Does the FI retain records of its training sessions including attendance records and relevant training materials used?	<input type="checkbox"/> Yes <input type="checkbox"/> No
26	Does the FI have policies to communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?	<input type="checkbox"/> Yes <input type="checkbox"/> No
27	Does the FI employ agents to carry out some of the functions of the FI and if so does the FI provide AML training to relevant agents that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?	<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby confirm that the statements given above are true and correct. I also confirm that I am authorized to complete this document.

--	--

Signature of Compliance Officer of the Institution

Completed by

Date: _____

Official Contact Address: _____

Telephone No(s): _____

E-mail Address: _____

Please send your response by e-mail to aaec.compliance@aaexchange.com.pk

ANNEXURE – III (UNDERTAKING)

**UNDERTAKING**

I fully agree and accept that it is my personal responsibility to adhere to the Company's AML / CFT & KYC Policy and any amendment / modification thereof and to comply with all of the provisions stated therein in true letter and spirit. I understand and accountable for any consequence or any violations of the policy whether committed or knowingly facilitated by me. I further undertake to abide by the AML / CFT & KYC Policy guidelines as a condition of my employment and my continuing employment in the Company.











Employee Signature:

Employee Name:

ACRONYMS

✓	AAE	AA Exchange
✓	AML /CFT	Anti-Money Laundering and Combating the Financing of Terrorism
✓	ARC	Aliens Registration Card
✓	CNIC	Computerized National Identity Card
✓	CTR	Currency Transaction Report
✓	EDD	Enhanced Due Diligence
✓	FATF	Financial Action Task Force
✓	FC	Foreign Currency
✓	FDD	Foreign Demand Draft
✓	FLA	Front Line Associates
✓	FMU	Financial Monitoring Unit
✓	FTT	Foreign Telegraphic Transfer
✓	KYC	Know your Customer
✓	MIS	Management Information System
✓	ML	Money Laundering
✓	MLRO	Money Laundering Reporting Officer
✓	NADRA	National Database & Registration Authority
✓	NCCTs	Not Cooperative Countries and Territories
✓	NICOP	National Identity Card for Overseas Pakistanis
✓	NTN	National Tax Number
✓	OFAC	Office of Foreign Assets Control
✓	PEP	Politically Exposed Person
✓	POC	Pakistan Origin Card
✓	POR	Proof of Registration
✓	RBA	Risk Base Approach
✓	SBP	State Bank of Pakistan
✓	SOP	Standard Operating Procedures
✓	STR	Suspicious Transaction Report
✓		

References:

-  AML ACT 2010
-  EXCHANGE COMPANIES MANUAL 2020
-  FMU RED FLAGS FOR EXCHANGE COMPANIES
-  NATIONAL RISK ASSESSMENT OF PAKISTAN 2019
-  INTERNAL RISK ASSESSMENT ON ML/TF (2019)
-  AML/ CFT/ CPF REGULATIONS FOR SBP RE's
-  ARTICLE 52 OF THE UNCAC 'UNITED NATIONS CONVENTION AGAINST CORRUPTION'
-  FATF 40+9 RECOMMENDATIONS
-  WOLFSBERG PRINCIPLES FOR RISK ASSESSMENT
-  UNSC AND NACTA