Global Anti-Money Laundering, Combating Financing of Terrorism, Countering Proliferation Financing & Know Your Customer Policy

Confidential

Global Anti Money Laundering, Combatting Financing of Terrorism, Combating Proliferation Financing & Know Your Customer Policy	
Approval Sheet	
Document Owner: Global Compliance and Conduct Group Document Version: 3.0	
Implementation Responsibility: Head Financial Crime Compliance for Pakistan / Country Compliance Head for International Branches	
Custodian: Financial Crime Compliance	
Operating Jurisdiction: HBL- Pakistan & Overseas Branches	
Review Frequency: 1 year or earlier if required	
Review Responsibility: Financial Crime Compliance Last Approval Date: September 22, 2022	
Approval Date: Dec 15, 2023 Effective Date: Date of Publication Next Review Date: Dec 15, 2024	
Prepared by:	
(Email approval on record) _____ Kashif Abdur Rahman Head Financial Crime Compliance	
Reviewed by:	
(Email approval on record) _____ Armughan Ahmed Kausar Chief Compliance Officer	
Concurred and Recommended by:	
(Email approval on record) _____ Muhammad Aurangzeb President & CEO	
Board Committee's Approval	Board's Approval
(Email approval on record) Board's Compliance & Conduct Committee: Date of Approval: Dec 15,2023	(Email approval on record) Board of Directors: Date of Approval: Dec 15,2023

Table of Contents

1. Overview

HBL is licensed by the State Bank of Pakistan (SBP) as a commercial bank and is registered with the Securities and Exchange Commission of Pakistan. It is also listed on the Pakistan Stock Exchange. HBL's compliance structure is based on a strong foundation of local and international regulatory requirements and best practices. Accordingly, HBL ensures meticulous compliance with all applicable laws and regulations governing Anti-Money Laundering (AML), Combating Financing of Terrorism (CFT) & Combating Proliferation Financing (CPF) activities; including, but not limited to:

- Anti-Money Laundering (AML) Act 2010, as updated up to September 2020.
- Anti-Terrorism Act (ATA) 1997, updated up to July 2020;
- SBP's AML/CFT/CPF Regulations updated up to November 2022;
- BPRD/AMLD-01/2023-2073 - Anti-Money Laundering, Combating the Financing of Terrorism & Countering Proliferation Financing (AML/CFT/CPF) Regulations (dated March 10, 2023 - UBO)
- BPRD/AMLD-01/2021-2282 (dated 25 February 2021 – Senior Management)
- AML/CFT Guidelines on Risk Based Approach, updated up to December 2019;
- Counter-measures for High-Risk Jurisdiction Rules 2020, updated as of October 2020;
- Framework for Managing Risks of Trade Based Money Laundering (TBML) and Terrorist Financing (TF), issued by SBP in October 2019; and
- National Risk Assessment (NRA), updated up to 2019.Or any other AML/CFT/CPF related instructions updated from time to time.

Keeping in view its international presence and the importance of countering Money Laundering (ML), Terrorist Financing (TF) & Proliferation Financing (PF) risks in jurisdictions that it operates in, HBL aims to comply with international standards, Financial Action Task Force (FATF) recommendations and Wolfsberg Group's guidelines in the areas of ML/TF/PF.

HBL Pakistan shall ensure that it complies with any updates to the SBP's AML/CFT/CPF Regulations as and when these are updated, and the policy should be read in conjunction with these regulations as amended from time to time. International locations are to ensure compliance with their relevant regulations as amended from time to time along with the instructions given in Section 1.2. "Scope and Applicability".

1.1. Objectives

The primary objective of this policy is to establish governing principles and minimum requirements to protect HBL (also referred as "Bank" or "the bank") from being used as a conduit for ML, TF (including Transnational TF), and PF activities. This policy requires the bank and its staff to comply with applicable laws and regulatory requirements, including those related to the identification and reporting of suspicious activities. This policy also aims to enhance the awareness of staff regarding their obligations with regards to the conduct of business in accordance with the applicable AML/CFT/CPF laws, rules, local and international regulation.

1.2. Scope and Applicability

This policy sets out the minimum requirements & standards to be adopted by the bank's domestic and international branches. Compliance with this Policy and the related procedures is mandatory and applies to:

- All HBL's domestic & international branches.
- All employees, including contractual and outsourced, working on behalf of the bank; and
- The Board of Directors of the bank.

All International branches and subsidiaries must also comply with the AML/CFT/CPF & KYC regulations applicable in the jurisdiction in which they operate and shall follow the higher standard between this policy and local regulations to the extent that the laws of the host country or jurisdiction so permit.

Where the laws of the host country conflict with the AML/ CFT requirements of Pakistan so that the overseas branch is unable to fully observe the higher standards, HBL through its head office shall report this to the State Bank of Pakistan and comply with further directions as may be issued.

In accordance with Approval Framework for Policies and Associated Documents (AFPAD), this Policy shall act as a Global Policy, and shall apply to the bank's domestic and overseas operations. Each international branch is responsible for identifying any inconsistency in this policy vis-à-vis statutory/regulatory framework of the host country and developing an addendum to this policy that incorporates all local regulatory requirements.

All Country Addendums will be approved by country management except for those overseas locations where the host country regulations require BOD approval for Country addendums.

Country Addendum owner should consult the Country Compliance team and international compliance team at the time of renewal to confirm if the country addendum requires BoD approval, in light of the prevailing host country regulations.

HBL subsidiaries should use this policy as a guiding document while developing their own policy.

1.3. Dispensations & Waivers

Exception(s) to this policy must be recommended by Head - FCC with concurrence of the Chief Compliance Officer (CCO) and approved by President & CEO. Exceptions must be reported to the Board Compliance and Conduct Committee (BC&CC). Exceptions to any regulatory requirements shall not be granted.

2. Roles and Responsibilities

Compliance Committee of Management (CCM) is responsible for maintaining and promoting a strong compliance culture by ensuring that all employees understand their responsibilities with respect to compliance and feel comfortable in raising any event of non-compliance without any fear of negative consequences. In this respect, the senior management/EXCO should create an enabling compliance culture that not only ensures that its employees comply with legal & regulatory requirements, standards and market best practices but also encourages the required ethical conduct that underlies such requirements. The "Board Compliance & Conduct Committee (BC&CC)" assists the Board in overseeing implementation of FCC framework along with governance over AML, CFT, CPF & KYC controls.

2.1. Board of Directors

The Board is responsible for:

- Approving the bank's Internal Risk Assessment Report (IRAR);
- Approving the AML/CFT/CPF & KYC Policy and overseeing its effectiveness;
- Overseeing that the AML/CFT/CPF & KYC Policy is effectively communicated enterprise-wide; and
- Ensuring (through management) that FCC within GCC is adequately supported with sufficient capacity, authority, and independence to exercise its responsibility effectively.
- Ensuring adequate, reliable, periodic management information, from senior management, for ensuring effective oversight, monitoring, and accountability

2.2. Board Compliance & Conduct Committee (BC&CC)

The BC&CC supports the Board on:

- Inculcating a compliance and conduct culture in the bank;
- Providing guidance on enterprise-wide design of compliance program;
- Overseeing the bank's compliance with legal & regulatory requirements, internal policies, and procedures;
- Reviewing reports and significant issues in domestic/overseas jurisdictions and related mitigating plans; and
- Overseeing implementation of SBP's Framework for Managing Risks of Trade Based Money Laundering (TBML) and Terrorist Financing (TF).

2.3. Compliance Committee of Management (CCM)

The CCM is responsible for:

- Implementation of an enterprise-wide Financial Crime Compliance (FCC) program;
- Ensuring senior management focuses on the AML/CFT/CPF issues and their resolution;
- Promoting high levels of compliance culture and addressing weaknesses, if any;
- Ensuring required ownership from the first line of defense and other functions; and
- Monitoring implementation of time-bound action plan developed for mitigation of governance, risk and control weaknesses identified in the IRAR.

2.4. Chief Compliance Officer (CCO)

CCO is responsible for:

- Evaluating the adequacy and effectiveness of Compliance controls over AML/CFT/CPF & KYC risks.
- Independent monitoring and reviews based on findings noted in the IRAR,
- Advising the Board, through BC&CC, on adequacy and strength of the AML/CFT/CPF & KYC controls

2.5. Senior Management

HBL's Senior Management, ExCo, and Extended Leadership Team (ELT) is responsible for:

- Establishing an appropriate culture of compliance and conduct at all levels in the bank by way of clear and effective communication;
- Implementing AML/CFT/CPF & KYC policy, Procedures, and controls in their respective business areas;
- Ensuring that ML/TF/PF/TBML risks are identified, assessed, monitored, adequately controlled, and reported in accordance with regulatory and internal requirements;
- Ensuring that the bank has implemented effective AML/CFT/CPF controls (preventive measures) related to ML, TF & PF;
- Ensuring that appropriate disciplinary actions are initiated in case of violations of this Policy or related policies and procedures;
- Overseeing timely completion of AML/CFT/CPF & KYC training requirements; and
- Effective, enterprise-wide implementation of three lines of defense model.

2.6. Three Lines of Defense Model

HBL gives utmost importance to preventing the bank from being used as a channel, directly or indirectly, for ML/TF/PF purposes and considers compliance of AML/CFT/CPF Regulations as everyone's

responsibility within the bank. The 'three lines of defense' model in HBL defines relationships among various functions and clearly demarcates their responsibilities. The detailed roles and responsibilities of the three lines are discussed in Compliance Program; however, a brief description with respect to AML/CFT/CPF & KYC risks is as under:

2.6.1. First Line of Defense – Business & Operations

The bank's business units and operations (support and back-office) functions act as the first line of defense and carry the primary responsibility for identifying, managing, and mitigating AML/CFT/CPF & KYC risks as part of the bank's day-to-day operations. The first line also designs and executes controls required to manage these risks.

2.6.2. Second Line of Defense – Compliance

The FCC department within the GCC acts as a part of second line of defense and provides advice, educates, guides, supports, monitors, and challenges the first line of defense to ensure AML/CFT/CPF & KYC risks are adequately identified and managed. FCC is also responsible to closely coordinate with other risk management functions of the bank to monitor the adequacy and efficacy of AML/CFT/CPF & KYC controls, where required.

2.6.3. Third Line of Defense - Internal Audit

Internal Audit (IA) is the third line of defense for the bank. It reports to; and is responsible for providing independent assurance to the Board and the Board Audit Committee on the quality, effectiveness and adequacy of governance, risk management and control environment including effectiveness of the first and second lines of defense to achieve organizational risk management and control objectives

3. Financial Crime Risk Framework

3.1. Financial Crime Risk Appetite

HBL's risk appetite comprises of the following element:

HBL shall conduct periodic risk assessment based on the comprehensive methodology outlined in its Risk Assessment document. Based on the risk assessment, the Bank shall develop its Financial Crime Risk Appetite Statement and Strategy along with tolerance limits that shall be reviewed and approved by the BC&CC and BoD on recommendation of CCM.

3.2. Unacceptable Customers & Transactions

HBL will not conduct business with or on behalf of individuals or entities that it believes are engaged in illicit activity or present an unacceptably high risk to the bank. Details of these are set out below.

HBL will not, at any time, open or maintain the following type of accounts or relationships:

- Numbered accounts, or accounts in the name of anonymous or fictitious persons, or benami accounts;
- Where the bank is not able to satisfactorily complete required CDD or EDD measures.
- Unauthorized financial service provider, dealers in financial instruments, unregistered charities or businesses engaged in Hundi/Hawala;
- Parties involved in unauthorized, defense procurement, arm & ammunitions and explosive.
- Client or business segments the bank has decided not to do business with, based on this Policy, Sanctions Compliance Policy, or SBP instructions.
- Shell Banks/Companies and Bearer Share Companies;
- Casinos and other businesses associated with gambling;
- Government accounts opened in the personal names of government officials;

- Pawnbrokers;
- Storage facilities for any form of Virtual Assets (VAs), including cryptocurrency and non-fungible tokens (NFTs), whether in hosted or un-hosted wallets;
- Virtual Asset Service Providers; including those who are dealing in VAs, Convertible Virtual Currencies (CVCs), Designated Contract Markets; digital assets trading platforms; and any providers engaged in exchange services between virtual currencies and fiat currencies and the same should be reported to FMU
- Customers who are nationals of or are resident in jurisdictions having country level embargoes/sanctions by UN, OFAC or Local/Host country sanctions;
- Nationals or residents, whether individuals or corporates, of Israel or any other country which may be notified by the Government of Pakistan (Relevant for HBL-Pakistan only, other countries to follow their own applicable laws/regulations).
- The following types of transactions fall outside of HBL's risk appetite:
- Payments that appear to relate to any form of illegal activity, including without limitation money laundering, proliferation financing, terrorist financing, human trafficking, modern day slavery, wildlife smuggling, child pornography and corruption;
- Payments that do not appear to have a legitimate purpose, including without limitation payments without underlying justification/transactional documents and payments lacking transparency regarding originator and beneficiary;
- Payments involving businesses associated with gambling;
- Payments involving Virtual Currency Exchanges e.g. Bitcoin, NFTs etc.
- Payments from foreign nationals (individuals or majority-owned entities) in the accounts of political parties; and
- Requests from occasional/walk-in customers for financial instruments such as pay order, demand drafts, call deposit receipts, requests from bearers of prize bonds etc. (except situations where such services are required under regulatory or legal mandate)
- Transactions where the identity documents do not appear to be genuine.

3.3. Entity wide Internal Risk Assessment

SBP has emphasized the application of risk-based approach (RBA) to ensure that measures to prevent or mitigate ML, TF and PF are appropriate to the identified ML, TF and PF risks. RBA should allow for efficient allocation of resources across AML/CFT/CPF regime and the implementation of risk-based measures.

Bank shall conduct an Enterprise-Wide Internal Risk Assessment Report (IRAR/FCRA), which should cover ML/TF/PF risks including Transnational TF and other emerging risks to and from Bank. IRAR shall identify, assess, and understand inherent ML/TF/PF risks at entity level for customers, products & services, geographies, delivery channels and technologies. IRAR/FCRA should factor in the results of National Risk Assessment (NRA), major international/ domestic financial crimes and terrorism incidents that have probability of posing ML/TF/PF risks to the entity itself or to the larger financial sector.

IRAR shall also assess the control environment that the bank has in terms of design and effectiveness, including AML/CFT/CPF & KYC and Sanctions policies, effectiveness of reporting (CTRs, STRs) and Targeted Financial Sanctions (TFS). Based on the identified inherent risks and the assessed control environment, the residual risks on ML/TF/PF will be evaluated and the bank will make further decisions on different areas of business / operations, including changes in policies for the application of due diligence measures as per evaluated risk ratings in each risk dimension or based on regulatory instructions.

The BCNC will review Internal Risk Assessment Report comprising of assessment on Money Laundering, Terrorist Financing, Proliferation Financing including Transnational TF risks and Trade Based Money Laundering risks along with a time bound action plan, if any and recommend to the Board for approval.

IRAR/FCRA shall be conducted at least annually unless local regulatory requirements/NRA when updated on national level call for more frequent assessments.

3.4. New Technologies, Products and Services

HBL shall identify and assess the ML/TF/PF risks that may arise in relation to their development for both new and pre-existing products, especially those that have vulnerability regarding ML/TF/PF risks and identity theft, anonymity, and cyber-crimes. Further, ML/TF/PF risk assessments shall be undertaken prior to the launch or use of such products, services, vendors, partners, alliances, business practices and technologies. Appropriate measures shall be taken to manage and mitigate the identified risks.

3.5. Country Risk Assessment

Both domestic branches and foreign locations can be characterized as high-risk based on several factors. Geographic risks shall feed into a client's risk assessment and due diligence procedures as a risk factor. The Country Risk Guidelines document is dynamic and reviewed at least annually by FCC. HBL shall comply with the obligations imposed in the Counter Measures for High-Risk Jurisdictions Rules 2020 as issued by Ministry of Finance, Government of Pakistan.

4. Know Your Customer (KYC)

Know Your Customer is the bank's best defense to prevent the bank from being used by criminal elements. The basics of KYC are built upon following:

- Identification & Verification (ID&V)
- Due Diligence Standards

4.1. Identification & Verification (ID&V)

HBL shall apply ID&V measures for establishing business relationships. Every customer and the beneficial owner shall be identified and verified on the basis of documents, data or information obtained from reliable and independent sources, wherever practicable. All efforts shall be made to understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship, and for ongoing monitoring.

For identification of customer/occasional customer at minimum, HBL shall obtain information mentioned in Annexure-I. For the purposes of verification of identity of the customer/ occasional customer, at minimum, documents mentioned in the Annexure-II shall be obtained. However, overseas branches may introduce more stringent process wherever local regulation require the same identities of the customers (natural persons) and ultimate beneficial owners (natural persons) of legal entities shall be verified from relevant authority's databases where required by regulations. Other reliable, independent sources may also be used, for example, World Check if necessary and copies of all reference documents used for identification and verification shall be retained on record.

In Pakistan, the Bank shall conduct biometric verification for all Pakistani citizens and Afghan refugees holding Proof of Registration (PoR) Cards before establishing new relationships, except in cases of genuine reasons or technical issues as prescribed by SBP on use of Biometric Technology. Other countries should also conduct identity verification as per their local regulatory requirements.

Non- face-to-face Identification and verification using digital methods may be applied, in accordance with home/host country regulatory standards.

4.1.1. Identification & Verification of Natural Persons Acting on Behalf of Customer

Where one or more natural persons are acting on behalf of a customer by way of bona fide mandate, or a power of attorney, occasional customer / walk-in customer or where customer is a legal person or legal arrangement, Bank shall identify and verify such persons using the prescribed methods and record in the system.

Moreover, the bank shall seek information on powers (legal basis or authority) that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement. For customers that are legal persons or legal arrangements, bank shall identify the customer and verify its identity by obtaining the following information in addition to the information required in Annexure-I and Annexure-II of the SBP regulations1

- The name, legal form, and proof of existence,
- Powers (legal basis or authority) that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement.
- The address of the registered office and if different, a principal place of business.
- Understanding and as appropriate obtaining information on the purpose and intended nature of business relationship
- In addition, for customers that are legal persons or legal arrangements the bank shall understand the nature of the customer's business, its ownership & control structure.

4.1.2. Identification & Verification of Ultimate Beneficial Owners (UBO) of Legal Entities & Arrangements

Reasonable measures shall be taken to obtain information to identify and verify the identities of the beneficial owner(s) in relation to a customer, using relevant information or data obtained from reliable source such that beneficial owners and the controlling person(s) of an entity are evident. For this purpose, any natural person(s) who has ultimate effective control of 25% or more of a legal entity or arrangement. The entire ownership structure should be unwrapped down to the identification of natural person(s)2.

For legal persons, HBL shall identify the customers and verify their identity by obtaining the information as set out in this Policy and Bank's procedural manual(s) in each country.

In case there is doubt as to whether the person(s) with controlling ownership interest is/are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity

[1] ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM & COUNTERING PROLIFERATION FINANCING
(AML/ CFT/ CPF) REGULATIONS FOR STATE BANK OF PAKISTAN'S REGULATED ENTITIES (SBP-REs) (Updated up to November 28, 2022)

[2] Refer Annxure-3 of SECP' guidelines on AML/ CFT/ CPF for better understanding of Ultimate Beneficial Ownership (UBO) of LP / LA customers (https://www.secp.gov.pk/document/secp-aml-cft-guidelines-updated-jan-2021/)

of the natural persons (if any) exercising control of the legal person or arrangement shall be identified and verified through other means. Where no natural person is identified, the identity of the relevant natural person who holds the position of senior managing official shall be verified along with other due diligence measures.

For customers that are legal arrangements, Bank shall identify and take reasonable measures to verify identity of beneficial owners through following information:

- For trusts; identity of the settlor, trustee(s), protector (if any), beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership as ascertained during CDD/EDD).
- For other types of legal arrangements, identity of the persons in equivalent or similar positions.

Bank shall obtain the ultimate beneficial ownership information from legal entities, i.e.; natural persons or individuals who ultimately own or control the company, that are required to maintain such information.

In the case of an entity with abbreviated name or title, the bank shall satisfy itself that the subject name/title is in accordance with the constituent documents of the entity. No account/relationship shall be allowed in abbreviated name in cases where entity has its complete name (non-abbreviated) in the constituent documents.

4.1.3. Timing of Verification

Verification of the identity of the customers and beneficial owners must be completed before business relations are established. Hence, the process with respect to Annexure I & II must be completed before the establishment of any business relationship. For accounts opened via branches, biometric verification needs to be performed before opening the account. However, for Digital Account Opening (DAO) SBP instructions need to be followed in line with section 4.1.5 “Customer Digital Onboarding."

4.1.4. Dormant Accounts

For customers, whose accounts are dormant or in-operative, Bank may allow credit entries without changing the dormancy status of such accounts. Debit transactions/withdrawals shall not be allowed until the account is activated on the request of the account holder. For activation, the bank shall review and update KYC where necessary. Bank may use the NADRA Verisys and a formal request (through any authenticated medium, including their mobile banking applications, internet banking portals, ATMs, call centers, postal address or email address or registered mobile number or landline number) for activation of dormant account by customers. Bank should retain the NADRA Verisys for record keeping requirements (digitally or hard copy). International Branches shall follow the dormant activation process as per regulatory guidelines in respective jurisdiction. However, a re-identification process should at minimum be in place before activation of account.

Debits under recovery of loans and markup, permissible bank charges, government duties or levies and on instructions issued under any law or from the court shall not be subject to debit or withdrawal restriction.

Following measures for dormant accounts shall be followed:

- Prior to marking the account as dormant, Bank shall send prior notice explaining the activation process/channels to the account holder through registered medium as per defined frequency of one (1) month, seven (7) days and one (1) day

- Bank shall not allow debit transactions/ withdrawals until the account is activated. However, transactions e.g. debits under the recovery of loans and markup etc., any permissible bank charges, government duties or levies and instruction issued under any law or from the court will not be subject to debit or withdrawal restriction
- Bank shall activate the dormant account upon receipt of a formal request from the customer through any authenticated medium, including their mobile banking applications, internet banking portals, ATMs, call centers, surface mail, email, registered mobile or landline number, etc.

Bank shall follow the requirement in line with SBP BPRD Circular Letter # 33, of 2023 dated November 28, 2022.

4.1.5. Customer Digital Onboarding

In line with SBP BPRD Circular letter # 15 of 2022 "Customers' Digital Onboarding Framework" for opening of bank accounts digitally by Resident Pakistanis, HBL shall ensure effective compliance with AML Act, 2010 (particularly Sections (7A – 7I), AML/CFT/CPF Regulations and all other applicable laws/ regulatory instructions including but not limited to Foreign Exchange Regulations updated from time to time.

4.2. Due Diligence Standards

CDD/EDD measures are applied when:

- Establishing business relationship,
- Dealing with occasional/walk-in customers (in which case their valid CNIC numbers or local identity number in other countries shall be captured in the system),
- There is suspicion of money laundering/financing of terrorism regardless of threshold, and
- There are doubts about the veracity or adequacy of previously obtained customer identification information.

4.2.1. Client Risk Assessment & Profiling

HBL shall risk assess each customer before classifying them on different risk levels based on the quantified risk scoring/Rule based model. HBL's Customer Risk Rating Methodology (CRRM) is based on two assessment models, as follows:

Rule Based Assessment Model: Customers rated as high risk by default (including those with specific criteria of client acceptance) for which the first line of defense must conduct EDD.

Algorithm Based Assessment Model: Customer's risk rating is based on the following factors:

- Customer Profiles
- Geographic Risks
- Delivery Channels
- Products and Services

These factors lead to each customer being rated as high, medium, or low, based on the score assigned at the time of on-boarding/periodic reviews/event-based reviews.

4.3. Enhanced Due Diligence (EDD)

EDD measures are called for when the bank assesses a customer to be inherently high risk, requiring the bank to obtain additional information or enhance the applied level of controls, as the case may be. This includes but is not limited to business relationships and transactions with natural and legal persons from countries mentioned in Counter Measures for High-Risk Jurisdictions Rules, 2020 which are already incorporated in Financial Crime Country Risk Guidelines.

HBL shall apply EDD measures at the time of onboarding and annually at the time of periodic review which shall include but not be limited to one or more of the following measures:

- Obtaining information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating identification data of the customer and beneficial ownership yearly;
- Obtaining information on the intended nature of the business relationship/ transactions;
- Obtaining information on the source of funds or source of wealth of the customer;
- Obtaining additional information on the reasons for intended or performed transactions and purpose of transaction;
- Taking necessary measures to establish the source of funds and wealth involved in the transaction or business relationship to be satisfied that they do not constitute the proceeds from/for crime
- Obtaining approval of the senior management (GM and above)[3] to commence or continue the business relationship or execute the high-risk financial transaction.
- Clearance from Compliance through CCO or his/her delegate wherever required, who may be Head FCC (or delegate as per EDD matrix), or any direct report of the CCO in-line with the Risk Appetite, or any additional clearance requirement under this policy;
- Conducting enhanced monitoring of the business relationship by reviewing its nature and frequency of controls applied and selecting patterns of transactions that need further examination
- Where available, requiring the first payment to be deposited through an account in the customer's name with a bank subject to similar CDD standards.
- Adverse Media to be searched via Google Search Engine or World Check Report of an Individual or Non-Individual customer.
- Business relationships and transactions with natural and legal persons from countries mentioned in Counter Measures for High-Risk Jurisdictions Rules,2020.
- Significant information and documents that are required to be obtained at the time of performing EDD in connection with the essential data points and checks are listed in the table below:

ENHANCED DUE DILIGENCE MATRIX

	Customer Type	Risk	Approval Level	Type of Document & Process
Individuals	Politically Exposed Persons (PEPs)	Default High	EDD Business Head and Clearance from Head FCC	***For Individuals Only:*** **<u>Source of Wealth (Accumulated)</u>** ▪ Wealth Return, or ▪ Inheritance or property documents, or ▪ Self-declaration as per Annexure III, or ▪ Any Supporting Document **<u>Source of Funds / Income</u>**
	Foreign Nationals (Non-Residents)	Default High	EDD Head Distribution and Clearance from Head FCC or delegate	
	Unemployed	Conditional High	High Risk EDD & Approval of Head Distribution	

[3] This should be read in conjunction to the definition of senior management (refer section 10).

	Customer Type	Risk	Approval Level	Type of Document & Process
	High Net Worth and Ultra High Net Worth Individuals	Conditional High	High Risk EDD & Approval of Business Head	▪ Bank Statement, and ▪ Assessment of tax or wealth return **Address Verification** ▪ Utility Bills, or ▪ Rental Agreement, or ▪ Property Document **First transaction through banking Channel** ▪ Cheque/ Payment instruments for transfer/ clearing containing the details or information on paper. ▪ If there is no other account to execute the first transaction through banking channel, an undertaking to be obtained as per Annexure IV **Adverse Media** ▪ WorldCheck reports or ▪ Google Searches
	Landlords	Conditional High	High Risk EDD & Approval of Business Head	
	Self Employed	Conditional High	High Risk EDD & Approval of Business Head	
	Minor	Conditional High	High Risk EDD & Approval of Head Distribution	
	Student	Conditional High	High Risk EDD & Approval of Head Distribution	
	Housewife	Conditional High	High Risk EDD & Approval of Distribution Head	
	Non-Resident (Nationals)	Conditional High	As per Country Risk Guidelines	
	Foreign Nationals (Resident)	Conditional High	As per Country Risk Guidelines	
Business	Money Service Businesses (MSB)/Money or Value Transfer Service Businesses (MVTS)	Default High	EDD – Business Head and Clearance from Head FCC	***For Legal Entities only*** **Controlling Person:** ▪ Identity Documents ▪ Sanctions Screening Operating Locations and Customer Type (Walk In/Referral/Solicited) ▪ Only Information to be obtained. **Government Approval where needed, based on entity type (Foreign / Local / Private / Public), for NGO / NPO / Trusts etc.** ▪ Approval as per applicability, such as
	Vostro Accounts (Financial Institution)	Default High	EDD – Business and Global Head FIGRB. and Clearance from Head FCC	
	Hedge Funds	Default High	EDD – Business Head and Clearance from Head FCC	
	Private Equity/Venture Capital Businesses	Default High	EDD – Business Head and Clearance from Head FCC	
	Investment Advisors	Default High	EDD – Business Head and Clearance from Head FCC	

	Customer Type	Risk	Approval Level	Type of Document & Process
	Mutual Funds	Default High	EDD – Business Head and Clearance from Head FCC	Ministry of Interior, Economic Affairs Division etc. **Source of Donation** ▪ Supporting Documents **Names of Major Donors (Charitable Institutes & Organizations)** ▪ List of Donors with Addresses **Details of foreign students in relation to Madaris - If yes, details** ▪ Details with nationality, and ▪ Identity details ▪ In case of any Sanctions hit, customer will not be onboarded or will be de-risked. **Source of Funds / Income** ▪ Bank Statement **Address Verification** ▪ Physical Verification Reports **First transaction through banking channel** ▪ Cheque/ Payment instruments for transfer/ clearing containing the details or information on paper. ▪ If no other account to execute the first transaction through banking channel, an undertaking that customer has no existing/previous banking relationship with reasoning **Adverse Media**
	Credit Card Services Companies	Default High	EDD – Business Head and Clearance from Head FCC	
	Precious Metals / Gems / Jewelers	Default High	EDD – Business Head and Clearance from Head FCC	
	Authorized/Licensed Arms & Ammunition	Default High	EDD – Business Head and Clearance from Head FCC	
	Arts Galleries/Dealers	Default High	EDD – Business Head and Clearance from Head FCC	
	Rent a car Service	Default High	EDD & Approval from Business Head	
	Hotels & Other accommodation	Default High	EDD & Approval from Business Head	
	Used Car Dealer	Default High	EDD & Approval from Business Head	
	Real Estate / Construction	Default High	EDD & Approval from Business Head	
	Travel Agent / Operator	Default High	EDD & Approval from Business Head	
	General Trading	Default High	EDD & Approval from Business Head	
	Trade Customers	Conditional High	As per Risk Profiling Mechanism of SBP TBML guidelines subject to EDD along with Business Head Approval & clearance from Head FCC or delegate	
Legal Structure	NGO, INGO, Trust	Default High	EDD – Business Head and clearance from Head FCC	
	Charity, Clubs, Association	Default High	EDD – Business Head and clearance from Head FCC	

	Customer Type	Risk	Approval Level	Type of Document & Process
	Madrasah / Masjid / Religious Entities	Default High	EDD – Business Head and clearance from Head FCC	▪ World Check reports or ▪ Google Searches **<u>Vostros & MSBs</u>** ▪ Wolfsberg or internal questionnaire ▪ Identification documents of Directors and UBOs ▪ AML policy statement ▪ Assessment through FCC Call ▪ Physical visit for MSBs, as required.
	Off-shore Entities	Default High	EDD & Approval of Business Head	
	Free Zone Offshore	Default High	EDD & Approval of Business Head	
	Free Zone Onshore	Default High	EDD & Approval of Business Head	
	Branch Office/Liaison Office of entities incorporated abroad	Default High	EDD & Approval of Business Head	
	Sole Proprietors	Conditional High	EDD & Approval of Business Head	
	Embassies	Conditional High	As per Country Risk Guidelines	

Note: Any customer assessed as High Risk through Customer Risk Rating Model through algorithm, will also be subjected to same documentation requirement as described in above table under individual or entity, as the case may be. The business head approval will also be required in such High-Risk relationships.

4.2.2. Politically Exposed Persons (PEPs)

PEPs are individuals who are or have been entrusted with a prominent public function either domestically or by a foreign country, or in an international organization and includes but is not limited to:

- Domestic and foreign PEPs which include heads of state or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations and important political party officials;
- For International Organization PEPs, members of senior management or individuals who have been entrusted with equivalent functions and
- middle ranking or more junior individuals in the above referred categories are not included in the definition of PEP
- Family members and close associates of PEPs are also classified as PEP and are subject to enhanced due diligence.
- Family members of PEPs include Direct family members, i.e.; spouses, children and their spouses, siblings, lineal descendants, and ascendants of the PEP.
- Close Associates of PEPs include:
  - An individual(s) known to have joint beneficial ownership of a legal person or a legal arrangement or any other close business relations with a PEP;
  - Any individual(s) who have beneficial ownership of a legal person or a legal arrangement which is known to have been set up for the benefit of a PEP;

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

4.2.2.1. PEP Categorization

At minimum, following persons or beneficial owners of the account would be considered as PEP including non-individual relationships. Taking a risk-based approach to PEP onboarding, PEPs have been divided into two categories:

Category 'A': Political PEPs are PEPs that hold elected office and include

- Heads of States such as President and Prime Minister of Pakistan & Azad Jammu Kashmir (AJK);
- Provincial Governors and Chief Ministers;
- Federal Ministers including Ministers of State and Provincial Ministers, including those of AJK;
- Members of National Assembly, Senate, and Provincial assemblies;
- Federal, State and Provincial Ministers and Advisors and Special Assistants to Chief Ministers, Governors, President, and Prime Minister;
- Heads of political parties at Federal or Provincial level and their central executive committee or governing body members;
- Nazims and Mayors; and
- Heads and Leaders of Trade Unions.

Category 'B': Service PEPs are PEPs that hold prominent government positions and include:

- All Justices of Supreme Court, Federal Shariat Court and High Courts, Federal Ombudsmen, Banking Ombudsmen.;
- Attorney General of Pakistan and Advocate Generals;
- Senior-most Federal and Provincial Secretaries;
- High Ranking Officials (3 star & above) of Armed Forces/Paramilitary, including:
  - Pakistan Army: Equivalent to or above the rank of Lieutenant General (3 Star);
  - Pakistan Navy: Equivalent to or above the rank of Vice Admiral;
  - Pakistan Air Force: Equivalent to or above the rank of Air Marshal;
  - Head of Pakistan Rangers;
- Heads (including Provincial Heads) and Deputy Heads of investigative agencies including Intelligence Bureau, FIA, NAB, etc.;
- Divisional & Deputy Commissioners;
- All Inspector Generals of Police include IGs (Special Charge) and Additional Inspector Generals of Police;
- Heads of state-owned enterprises, corporations, and autonomous bodies such as PIA, PSO, SSGC, PEPCO, OGDC, PPL, Civil Aviation, etc.;
- Heads of Government established Boards, Commissions, Bureaus, Authorities (such as NADRA, WAPDA, NHA), Programs such as (BISP) and national level committees, etc.;
- Heads of regulatory authorities, such as SECP, PTA, Election Commission, PEMRA, NEPRA, OGRA, Competition Commission, and Bait-ul-mal, etc.;
- Governor and Deputy Governor of the State Bank of Pakistan;
- Chairman FBR (Federal Board of Revenue), Chief Commissioner Income Tax and Collector of Customs;
- Vice Chancellors of Universities established under Government Acts;

- Heads of International Organization and agencies that exercise genuine political or economic influence, e.g., UN, IMF, WB; WTO, ILO, etc.;
- Senior Diplomats i.e., Ambassadors, High Commissioners, Counsel General, Chargés d'affaires only;
- Head of International and local sporting bodies e.g., FIFA, ICC, PCB, PHF, etc.;

This category has been further divided into three sub-categories under a defined process.

- "B1-Active Service PEPs",
- "B2-Retired Service PEPs for less than 3 years" and
- "B3-Retired Service PEP for 3 years and more"

For Category 'B' cases, if any adverse media is found, the approval process of category 'A' shall be followed of PEP

The same principles for classification for both categories stated above would apply for foreign PEPs.

Overseas branches will use PEP classification as per their local regulatory requirements.

4.2.2.2. PEP Controlled Entities (PCE):

PCEs are those entities which are made for the benefit of a PEP or where the PEP Owns and controls 50% or more of the entity (excluding SOEs). This should be covered in Business remarks when conducting Due Diligence of PCEs.

4.2.2.3. Declassifying PEPs

Upon being classified as a PEP, the classification must be retained in a following manner:

- At least five years for Category A - Political PEPs after the individual ceases to hold office, and;
- At least three years for Category B – Service Level PEPs after the individual ceases to hold office.

After the lapse of stated periods, PEP classification can be removed for PEPs where the risks appear demonstrably reduced and there is no adverse media. This decision will also require prior approval from the Business Head and clearance from Head – FCC.

However, the following PEPs will remain PEPs without the option of declassification throughout their life:

- Former Heads of State, President, and Prime Minister
- Former Governors and Chief Ministers,
- Former Heads of Armed Forces

The risk rating of Declassified PEPs will be calculated as per effective CRRM model which is automated.

4.4. NGOs/NPOs/Charities

HBL shall conduct EDD (including obtaining senior management approval) while establishing relationship with Non-Governmental Organizations (NGOs)/Not-for-Profit Organizations (NPOs) and Charities to ensure that these accounts are used for legitimate purposes and the transactions are commensurate with the stated objectives and purposes.

Accounts shall be opened in the name of relevant NGO/INGO/NPO as per their constituent documents. The individuals who are authorized to operate these accounts and all members of their governing bodies

shall be subject to CDD separately. HBL shall ensure that these persons are not affiliated with any proscribed/designated entity or person, whether under the same name or a different name.

In the case of advertisements through newspapers or any other medium, especially when a bank account number is mentioned for donations, the Relevant Business segment shall ensure that title of the account is same as that of the entity soliciting donations. In case of any difference, immediate caution should be marked on such accounts by engaging relevant team in Operations and the matter considered for filing Internal STR.

Personal accounts shall not be allowed to be used for charity purposes/collection of donations.

All existing relationships of NGOs/INGOs/NPOs/Charities shall be reviewed and monitored to ensure that these organizations, their authorized signatories, members of their governing body and the beneficial owners are not linked with any proscribed/designated entity or person, whether under the same name or a different name. In case of any positive match, the bank would consider filing STR and/or take other actions as per the law.

Business shall ensure at the time of on-boarding and also during the relationship that:

- The entity has operations in line with the articles and memorandum/trust deed/rules etc.;
- The funds are utilized in the manner and in the areas as was stated in the documents and recorded at the time of CDD.

4.5. Trade Finance Customers

Bank shall undertake CDD measures for asset side/trade finance customers as prescribed in the AML/CFT/CPF Regulations and ensure monitoring of such customers regarding ML/TF/PF risks. The bank has also implemented SBP's Framework for Managing Risk of Trade Based Money Laundering (TBML) and Terrorist Financing (TF) which was issued in October 2019.

A dedicated Trade Compliance Advisory (TCA) Unit exists to facilitate the Business in trade transactions. For all transactions being escalated, TCA ensures that appropriate controls are in place to deal with TBML through a risk-based approach, which relates to analysis of the risks in relation to the parties involved, the type of transaction and monetary values of the transaction. TCA also ensures that due diligence is conducted at the time of trade advisory by acquiring relevant details such as details of local and international counter parties, line of business of customer, nature of goods in which the client or counterparty is dealing, price verification, vessel checking and details on counter party geographies.

HBL must ensure that high risk customers are subject to EDD and high-risk trade transactions undergo more extensive documentary/diligence checks. The use of Trade Finance to obscure the illegal movement of funds includes methods to misrepresent the price, quality, or quantity of goods. Generally, these techniques rely upon collusion between the seller and buyer, since the intended outcome from such arrangements is obtaining a benefit in excess of what would be expected from an arm's length transaction. The transfer of value may be accomplished in a variety of techniques as mentioned below:

- Over-invoicing and under-invoicing of goods by the exporter;
- Multiple invoicing for goods;
- Over - shipment and under-shipment of goods;
- Describing goods on the invoice and other documentation as being of a higher quality than actual;
- Supply of dual-use goods;
- Third Party Payments.

- Related parties registered in free trade zones or Tax Haven Countries

In order to mitigate TBML risk, the bank must ensure that due diligence with reference to trade is being conducted at the time of customer on-boarding by acquiring relevant details, which is not limited to:

- Details of customer interest in trade products and services of the bank;
- Detail of local and international counterparties;
- Line of business of customer;
- Nature of goods in which client or counterparty is dealing
- Detail of counterparty geographies.

The trade in dual-use items - goods, software and technology that can be used for both civilian and military applications and/or can contribute to the proliferation of Weapons of Mass Destruction (WMD) – is subject to controls to prevent the risks that these items may pose for both national, international security and the bank. It is the responsibility of the first line of defense to potentially identify the customers at the time of onboarding CDD/KYC customer who deal in such goods and should monitor them throughout the relationship.

4.5.1. Trade Based Money Laundering

As per SBP Trade Based Money Laundering (TBML) Guidelines, the bank is required to ensure that a risk-based approach is adopted while conducting CDD of trade-related customers. Bank shall capture the relevant information about trade related activities of the customer and incorporate it in the Customer's Risk Profile giving due weightage to various risk factors. The assessment for risk profiling may include, but not limited to the following:

- The goods/services in which the customer usually trade in and prices thereof, where available;
- Customer's key buyers/ suppliers, # of year relationship, volume of sale/purchase in %;
- Annual volume of trade transactions of customer;
- Number of offices within and outside of the country if any and its affiliates exists
- Approximate amount of trade transactions during the month
- Average /Max ticket size of trade transaction (USD)- Import/Export.
- Trade cycle/tenor of the customer;
- Nature of Transaction (i.e trade Product)
- The countries of origin of goods in which the customer trades;
- The jurisdictions/countries of business;
- Modes of transportation for goods;
- Port(s) of loading/discharge;
- Usual mode of trade and terms of payments;
- Related business concerns (domestic as well as international) and third parties such as shipping agents, insurance companies, inspection companies etc.;
- Active membership of customer with Chamber of Commerce/Trade Association;
- Group Companies / Related and Third-Party information
- List of Bank, # of account with has/had business relationship
- Disclosure on any Trade related overdue and penalties
- Person(s) authorized to sign Trade Document / Instructions to the Bank on behalf of customer;
- Legal structure of the customer;
- Ultimate beneficial owner of the customer/transactions along with his/her stakes in the trade transactions, directly or indirectly; and
- Conduct of customer's personal PKR/FCY Account.

Additionally, the bank must comply with instructions issued by SBP from time to time including but not limited to due diligence requirements with respect to import of Solar Panels and related accessories.

The Control Framework to Manage Trade Related ML/TF Risks must include the following components as base-line standards:

- Price related Due Diligence;
- Vessel Check
- Dual Usage of Goods
- Transaction level due diligence as per Foreign Exchange Manual;
- High Risk Transactions and Enhanced Due Diligence;
- Development and Maintenance of Goods/HS related MIS;
- Transaction Monitoring;
- Suspicious Transaction Reporting;
- Technology Based Solutions;
- Staffing Requirements;
- Risk Awareness and Trade related ML/TF Risks Training;
- Collaboration with Stakeholders including Customs, Shipping Companies, chamber of commerce etc.;
- Internal Audit as third line of defense.

4.5.2. Government Accounts & Accounts of Autonomous Bodies

Government accounts shall not be opened in the personal names of the government official(s). Under the existing statutory and legal framework, no government ministry, division, department/attached departments, and subordinate offices can operate their bank accounts other than the principal account of the federal/ provincial government residing at the SBP. The list of all such entities falling in the above-mentioned categories shall be available at the Finance Division's website, www.finance.gov.pk

HBL shall only open and maintain accounts of autonomous bodies, incorporated under an act of Parliament or the Companies Act 2017, after obtaining necessary approval/resolution from their respective board/ governing bodies; and constituted through a cabinet resolution/ notification of federal or a provincial government, after obtaining a no objection certificate (NOC) issued by the Finance Division or relevant finance departments of the provinces, as the case may be with respective Business Head sign-off.

Further in compliance with SBP BPRD circular no.1 of 2021 for Implementation of Cash Management & Single Treasury Account Rules, 2020, in terms of Rule 4 (2) of the CM & TSA Rules, 2020, HBL must conduct regular KYC on existing bank account(s), maintained by the Federal Government offices.

Further, HBL shall not open account of Federal Government Offices i.e. Ministries, Divisions, their Executive Departments, Attached Departments, Subordinated Offices and Other Office(s) or Department(s) except under the authority of Finance Division as provided under Section 31 of the PFMA, 2019.

4.5.3. Correspondent Banking

The bank shall take following measures in line with functions and powers prescribed under relevant law, for providing correspondent banking services:

- Assess the suitability of respondent bank by taking following steps:
- Gather adequate information about the respondent bank to completely understand the nature of the respondent bank's business, including but not limited to the following, where applicable:

- Know Your Customer Policy (KYC)
- Information about the respondent bank's management and ownership
- Major business activities;
- Their geographical presence/jurisdiction (country) of correspondence;
- Money Laundering prevention and detection measures
- CDD
- AML/CFT/CPF controls and procedures
- Purpose for which the account or service shall be used;
- Identity of any third party that shall use correspondent banking services (i.e., in case of payable through accounts); and
- Condition of the banking regulation and supervision in the respondent's country.

- Determine from any available sources' reputation of the respondent bank and, as far as practicable, quality of supervision over the respondent bank, including where possible whether it has been the subject of money laundering or financing of terrorism investigation or regulatory action; and
- Assess respondent bank in the context of sanctions/embargoes and advisories about risks.
- Clearly understand and document the respective AML/CFT/CPF responsibilities of each bank;
- Obtain approval of senior management, before establishing new correspondent banking relationship;
- HBL shall neither offer payable-through accounts nor shall it allow nesting;
- Bank shall apply enhanced due diligence when establishing or continuing correspondent relationships with banks/financial institutions pertaining to high-risk countries & jurisdictions as per the Financial Crime Country Risk Guidelines.
- HBL shall not enter into or continue correspondent banking relations with a shell bank and shall take appropriate measures when establishing correspondent banking relations to satisfy itself that respondent banks do not permit their accounts to be used by shell banks. HBL shall further ensure that its platform is not used by any shell bank for execution or provision of financial services.
- In the case where HBL is availing correspondent banking services from a bank/financial institution abroad, the CDD measures specified above shall be applied, as considered necessary to mitigate ML/TF/PF risks.

4.5.4. Branchless Banking (BB)

BB provides a convenient and cost-effective alternative to conventional branch-based banking. BB includes mobile wallet accounts, wallet-to-wallet transfers, account-to-person transfers, merchant and bill payments, cash in and cash outs, and receipt of home remittances. Although branchless banking products are retail in nature, HBL offers these products under a separate business segment in view of its rapid growth. BB accounts are for individuals only and shall not be opened in the name of legal persons and legal arrangements, high-risk customers and high-risk geographies as identified by the bank in the process of internal ML/TF risk assessment. Risk-Based Customer Due Diligence include following:

Risk Assessment and Mitigation:

In line with SBP regulations, BB is a part of HBL's IRAR/FCRA together with other business segments;

Simplified Due Diligence:

As per Branchless Banking Regulations, HBL shall adopt simplified due diligence procedures for BB accounts and adhered the regulation 2 section 18 of AML/CFT/CPF regulations, except:

a. When there is a suspicion of money laundering or financing of terrorism;
b. In case certain high-risk factors are identified by the SBP or by HBL in its own internal risk assessment; or as per international standards viz-a-viz FATF Recommendations, etc.;
c. In relation to customers that are from or in jurisdictions which have been identified for inadequate AML/CFT measures by FATF or identified by the bank itself having poor AML/CFT standards, or otherwise identified by the SBP.

For the purpose of Simplified Due Diligence, HBL shall:

a. Categorize BB accounts in two levels; Level-0 (Basic Banking Account with low KYC requirements and low transaction limits) and Level-1 (Entry Level account with simplified KYC requirements commensurate with transaction limits);
b. Onboard and monitor agents as per criteria laid down in "Framework for Branchless Banking Agent Acquisition & Management' issued vide BPRD Circular No. 06 dated 21st June 2016, as amended from time to time. Agent accounts including level-2 account holders shall be treated as full-fledged KYC/CDD accounts and are subject to SBP's AML/CFT Regime as amended from time to time.
c. Not open BB accounts on behalf of other individuals and shall not allow operation in these accounts to any individual on behalf of the account holder;
d. Apply simplified Customer Due diligence (CDD) measures for level-0 and level-1 accounts. The simplified CDD measures shall be commensurate with lower risk factors and these procedures shall not be applicable on specific higher risk scenarios;
e. Verify the identity of the customers before opening of their accounts;
f. Not keep anonymous accounts or accounts in obvious fictitious names;
g. Undertake CDD measures when there are doubts about the veracity or adequacy of previously obtained customer identification data;
h. Understand and, if required, obtain information on the purpose, and intended nature of the business relationship;
i. Not allow agents to perform elements of CDD measures including identification of the customer, identification of the beneficial owner and understanding the nature of business to introduce business etc.
j. The role of BB agent is only limited to facilitating the customers and to forwarding their information to HBL through an electronic channel. HBL shall conduct all CDD measures by itself;
k. Not open account where it is unable to comply with relevant CDD measures at the time of account opening;
l. Not conduct the transaction; and terminate the business relationship; and file Suspicious Transaction Report (STR) in relation to a customer, where it is unable to comply with relevant CDD measures at the time of performing the transactions of customers;
m. Not pursue the CDD process and instead file an STR, where the bank forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process shall tip-off the customer;
n. Scrutinize transactions undertaken throughout the course of the relationship through Automated Transaction Monitoring System (ATMS) to ensure that the transactions are consistent with Bank' knowledge of the customers, their business and risk profile,

including, where necessary, the source of funds; and report suspicious transaction including attempted transactions to Financial Monitoring Unit (FMU) as per law.

a) ***Types of BB Accounts:***
KYC requirements, transactional limits, record retention and Bank's responsibilities applicable to 'level 0'and level '1' accounts are tabulated in the Branchless Banking Regulations issued by SBP which shall be covered in the Branchless Banking Procedures;

b) ***Domestic Funds Transfers:***
The minimum requirements applicable to funds transfer service for Account to Person are tabulated in the Branchless Banking Regulations which shall be covered in the Branchless Banking Procedures. Further/specific details are covered in the internal procedures of Branchless Banking.

4.5.5. Wire Transfers/Fund Transfers

The following requirements shall apply as per functions and powers prescribed under relevant law, during the course of sending or receiving funds by wire transfer except transfers and settlements between local banks where both are acting on their own behalf as originator and the beneficiary of the wire transfers.

4.5.5.1. Responsibility as an Ordering Institution

- HBL as an ordering institution (whether for domestic or cross border wire transfer) shall: identify and verify the originator and obtain details of beneficial owner(s) of funds;
- Record adequate details of the wire transfer so as to permit its reconstruction, including the date of the wire transfer, the type and amount of currency involved, the value date, the purpose and details of the wire transfer beneficiary and the beneficiary institution, and relationship between originator and beneficiary, as applicable, etc.;
- Include following information in the message or payment instruction which should accompany or remain with the wire transfer throughout the payment chain:

  a) Name of the originator;
  b) Originator's account number (or unique reference number which permits traceability of the transaction);
  c) Originator's applicable identity document number;
  d) Name of the beneficiary;
  e) Beneficiary's applicable identity document number;

- Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information (originator's account number or unique transaction reference number) and full beneficiary information that is fully traceable within the beneficiary country.

4.5.5.2. Responsibility as a Beneficiary Institution

- Verify identity of the beneficiary and record this information as per the relevant record keeping requirements;
- Adopt risk-based internal policies, procedures, and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator or beneficiary information. The incomplete originator or beneficiary information may be considered as a factor in assessing whether to execute or terminate the transaction, and in assessing whether the transaction is suspicious and merits reporting to FMU;

- Limit or prohibit transactions with institutions that do not comply with the standard requirements set out for wire transfers by limiting or even terminating business relationship.

4.5.5.3. Responsibility as an Intermediary Institution

- In passing onward, the message or payment instruction, maintain all the required originator and beneficiary information with the wire transfer;
- Keep a record of all the information received from the ordering financial institution or another intermediary financial institution, as per relevant record keeping requirements;
- Take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or beneficiary information; and
- Have risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information.

4.5.6. Incomplete CDD Measures

In compliance with legal and regulatory requirements, in case the bank is not able to satisfactorily complete required CDD measures, account shall not be opened, nor any service provided. Consideration shall be given if the circumstances are suspicious so as to warrant filing of a Suspicious Transaction Report (STR).

If the bank is unable to satisfactorily comply with CDD measures of an existing customer, the relationship shall be terminated, and reporting of suspicious transaction be considered as per law. Further, the bank shall serve prior notice and record cogent reasons for terminating business relationships.

In cases where the bank forms suspicion of money laundering, terrorist financing or other criminal activity, and reasonably believes that performing the CDD process shall tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FMU (or as applicable in case of international locations).

4.5.7. Employee Due Diligence

HBL has a comprehensive employee due diligence/screening policy and procedure in place to ensure high standards and integrity which is followed at the time of hiring all employees, whether permanent, contractual, or through outsourcing to ensure high standards. This includes but is not limited to screening of all employees against lists of designated and proscribed individuals, on an ongoing basis, and maintaining proper record of screening. Accordingly, employees shall be disqualified from service if they are designated/proscribed or associated directly or indirectly with such persons.

The bank shall also ensure that no employee is or has been convicted, involved in any fraud, forgery, financial crime etc. and is or was not associated with any illegal activities involving the banking business, foreign exchange business, financial dealing, or other employment. In this regard, the bank shall obtain appropriate responses from candidates during their onboarding process and verify their antecedents as per obtained information. Employees will be disqualified from services if they have been found to have provided false information regarding their previous employment or activities.

As per BPRD Circular No. 09 of 2018, In view of potential risk arising from money laundering, terrorism financing and proliferation financing, it is imperative that any person(s) linked to any criminal activities or affiliated to any terrorist organizations are not on-boarded. HBL shall ensure compliance with SBP's Fitness & Proprietary Test (F&PT) criterion required for sponsor shareholders & board approval and senior management.

4.5.8. Reliance on 3rd party Financial Institutions for CDD Measures

All CDD measures are to be carried out by HBL's staff. The CDD measures as required under Annexures I & II will not be carried out by a 3rd party Financial Institution, unless recommended by the CCO and approved by the board. In such cases, the ultimate responsibility of the CDD measures carried out will rest with HBL, including ongoing monitoring of customers & reporting of STRs/CTRs.

HBL shall also ensure that the 3rd party Financial Institution:

a) Has appropriate measures in place for compliance with CDD, record keeping, data security and privacy requirements as prescribed by SBP in its AML/CFT/CPF Regulations and other instructions issued from time to time;
b) Is a regulated, supervised and monitored Financial Institution;
c) Is not located or based in a High-Risk Jurisdiction as per the bank's Country Risk Rating Methodology.

5. AML/CFT Monitoring

As per regulatory requirements and best international practices, the bank is required to implement a risk-based AML/CFT/CPF monitoring mechanism, which is divided into different monitoring processes at various stages of the customer life-cycle management.

5.1. Ongoing Monitoring (Customers & Transactions)

Ongoing Monitoring comprises of event-based and periodic review for customer relationships and transactions.

5.1.1. Customer Screening

As part of the onboarding process, branches perform due diligence in line with this policy and complying with the regulatory requirements. The due diligence process includes sanction screening from the applicable sanction regimes as per the "Sanctions Compliance Policy" of the bank. The process also encompasses screening of the local lists in the respective jurisdiction. (For Pakistan – ATA proscribed persons).

5.1.2. Expired Identification Documents

With respect to HBL Pakistan, SBP has issued Regulations that allow banks to block accounts without valid Identity Document (after serving one-month prior notice) for all debit transactions/ withdrawals, irrespective of mode of payment, until the subject regulatory requirement is fulfilled. However, debit block from the accounts shall be removed upon submission of valid identity document and verification of the same. However, in case of expiry of CNIC or other ID documents in low-risk accounts, bank may allow continuity of relationship/operation in the account up to three months from the date of expiry. However, the Bank shall obtain the ID renewed CNIC/ID documents within the stipulated time period.

5.1.3. Periodic and Ongoing Monitoring

HBL business segments/branches shall ensure that they update customer information as part of the Customer Risk Profiling (CRP) on an ongoing basis.

All business relations with customers shall be monitored on an ongoing basis in order to ensure that the transactions are consistent with the Bank's knowledge of the customers, their business, risk profile and the sources of funds/wealth.

Bank shall obtain information and examine, as far as possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or

visible lawful purpose. The background and purpose of these transactions shall be inquired, and findings shall be documented with a view to making this information available to the relevant competent authorities when required.

Bank shall periodically review the adequacy of information obtained in respect of customers and beneficial owners including Ultimate Beneficial Owner (UBO) of Legal person/ Legal arrangement (LP/ LA), and ensure that the information is kept up to date, as per the following frequency:

High	Once a year
Medium	Once in 2 years
Low	Once in 3 years

The above defined review frequency is based on industry norms; however, this may change based on any specific regulation, best practices or due to any other reason with the approval of Chief Compliance Officer (CCO).

Regardless of predefined frequencies, if any material change is observed in the relationship i.e. customer's profile, UBO of Legal Person / Legal arrangement, in terms of transaction volumes/pattern, address, etc., KYC review shall be triggered and updated immediately. In relation to the above review, customers' profiles shall be revised keeping in view the spirit of KYC(CDD/EDD) and the basis of revision documented; customers may be consulted, if necessary.

HBL branches/businesses shall keep records of their customers updated with regard to their postal and email address or registered mobile and landline number, or source of income where applicable for ensuring efficient and reliable communications.

5.1.4. Transaction Monitoring

HBL has implemented adequate, reliable, efficient automated systems and technologies proportionate to the ML/TF/PF risks posed to the bank's business and operational models. The current transaction monitoring system is FCCM Oracle 8.0.4 that provides risk-based transaction monitoring. Based on the coverage assessment with known typologies and IRAR, HBL has implemented AML/TF scenarios under different customer segments with dynamic parameters.

The parameters and scenarios are reviewed for stability and suitability commensurate to the business/risk on an ongoing basis. Transaction monitoring scenario/parameter optimization is an important activity that should be performed at least annually.

A team of AML professionals has been assigned to handle the alerts as per Standard Operating Procedures of FCC.

Any alerts that require investigation are escalated to case management for a SAR/No SAR decision.

5.1.5. Reporting of Transactions (STRs/CTRs)

HBL shall:

a) Comply with the provisions of Section 7 of the AML Act, rules and regulations issued for reporting suspicious transactions/currency transactions in the context of money laundering, financing of terrorism and financing of proliferation.
b) implement appropriate internal policies, procedures, and controls for meeting its obligations under AML Act.

c) Pay special attention to attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions shall, as far as possible, be examined, the findings established in writing, and shall assist the relevant authorities in the inspection and investigation.
d) Make use of technology and upgrade systems and procedures in accordance with the changing profile of various risks. Accordingly, HBL has implemented automated Transaction Monitoring Systems (TMS) capable of producing meaningful alerts based on pre-defined parameters/thresholds and customer profile, for analysis and possible reporting of suspicious transactions. Criteria for management of such alerts is available in the FCC Procedures document.
e) Place adequate number of analysts for monitoring and reporting purpose. Moreover, steps shall be taken to develop the knowledge and skills of staff and utilize technology solutions required for effective Targeted Financial Sanctions (TFS) monitoring and reporting of suspicious transactions.
f) Review transactions, which are out of character or are inconsistent with the history, pattern, or normal operation of the account including through heavy deposits, withdrawals, and transfers, with suspicion, investigate properly and where required, report to FMU under the AML Act.
g) Ensure that STRs, including actual or attempted structured transactions, are reported regardless of the amount of the transactions; and the CTRs are reported for the transactions of rupees two million and above as per requirements of the AML Act.
h) Document the basis of deciding whether an STR is being filed or not and keep it on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.
i) Strictly prohibit the employees from disclosing the fact to the customer or any other quarter that a suspicious transaction or related information is being or has been reported to any authority, except if required by law. This shall be made part of the Code of Ethics to be signed by employees and directors of the bank.
j) Not assign reporting of suspicious transactions/currency transactions in the context of money laundering, financing of terrorism or financing of proliferation to outsourced employees.
k) The bank shall assess the matter of continuity of relationships subject of SARs reported to the regulatory authority taking into consideration the element of potentially tipping off the customer.

5.2. Combating Financing of Terrorism (CFT) Desk and List Management

The Combatting Financing of Terrorism (CFT) function is responsible for CFT related controls (preventive measures). CFT Desk is also responsible for ensuring quality and coverage of STRs reporting in the areas of terrorism, TF, PF and Targeted Financial Sanctions (TFS), if any. In compliance with the requirement, FCC has a dedicated CFT Desk.

CFT Desk shall analyze major terrorist incidents that occur within the country or abroad for assessing the possibility of use of Bank's products, services or delivery channels and consider reporting STRs, if warranted.

In case an account needs to be closed due to incomplete CDD, the bank shall follow the usual account closure process. Further, business may escalate the matter to FCC as an internal STR if there are obvious reasons to do so, including unusual and unexplainable large transactions. Bank shall maintain record of all accounts involuntarily closed by branch on CDD deficiencies including a central MIS.

If any of the local regulator does not allow termination of account on CDD related deficiencies, branches may still raise internal STR/SAR with respective AML Unit based on the rationale mentioned above.

CFT Desk shall;

a) Through adverse media and desktop review processes, analyze actual/potential terrorist incidents in conjunction with country directly or indirectly for assessing the TF risk exposed through bank's customers, products, services, or delivery channels and take appropriate measure that include incident reporting to SBP & reporting of SAR to FMU (If warranted);
b) Ensure that no new relationship should be established with Designated/Proscribed Individuals and Entities directly or indirectly;
c) Ensure that local and international relevant lists are updated timely and appropriate actions that include regulatory reporting, freezing/de-freezing are undertaken timely in compliance of regulatory & legal framework in the prescribed manner;

5.3. Use of personal accounts for business purposes

The bank shall not allow personal accounts to be used for business purposes except proprietorships, small businesses, and professions where constituent documents are not available and the bank is satisfied with KYC profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status and nature of business of that customer. The International Branches shall follow regulatory guidelines in their respective jurisdictions which may be more stringent.

The first line of defense shall monitor such accounts/relationships to ensure that their turnovers remain within the acceptable limits as per their approved procedures and where there is a turnover breach, either a regular business account shall be opened immediately or having a valid rationale recorded in the customer KYC comments or filing an internal STR as per the bank's implemented process.

5.4. AML/TF Red Flags

The Bank shall maintain and continuously update a list of red flags as risk indicators for ML/ TF/ TBML and all transactions/ activities as per the red flags shall be analyzed and/or escalated, even if the transactions otherwise appear in order. For details refer to annexure V.

6. Sharing Information at Group Level

Foreign Branches need to inculcate in their policies the following protocol in line with their local legal & regulatory requirements as follow:

For sharing information with Head Office required for the purpose of CDD and Risk Management. This should also include the details about sharing information with the International Compliance Department and Internal Audit Department based at Head Office.

Sharing of information for AML/CFT purpose with Head Office or other HBL Branches at different locations with GCC, Internal Audit at Head Office.

Confidential information should only be shared with the intended recipients to prevent tipping off.

Foreign Branches should also include consequences if information is shared with staff other than intended ones without permission from Head Office. Such information includes but is not limited to internal audit reports, board documents, regulator reports and any other information which is confidential as mentioned by senior management.

In the case of corporate group, in addition to compliance with SBP AML/CFT/CPF Regulation 13, sharing of customer information at group level without any legitimate purpose is restricted.

However, sharing of customers' and supervisory information shall only be possible wherever legal statue permits and after initial assessment and approval by respective units of GCG to prevent confidential information to be tipped-off. Details will be covered in respective procedures.

7. Training & Development

Adequate training and development of staff is a key factor in their growth and success, enabling and equipping them to perform their assigned tasks with the tools they need. Training and developing the bank's staff in the areas of AML/CFT/CPF is recognized as a core focus area by the Board and Management.

The bank has implemented a suitable annual training program for relevant employees, which is developed after a formal training needs assessment in the area of AML/CFT/CPF. The Annual Training Program ensures training sessions are conducted for sponsor shareholders, BoD, senior management, line management, and field staff.

HBL ensures that content of training and methodology used is updated with regard to emergent risks identified by the bank through IRAR, updates on National Risk Assessment (NRA) threats & vulnerabilities, update on international standards and best practices including by FATF in the area of AML/CFT/CPF, regulatory/ supervisory updates, update on legal framework, issuance and sharing of guiding documents and analysis by government specially FMU, MOFA, NACTA in the areas of AML/ CFT/ CPF.

Training is imparted to improve the knowledge and skills of Bank staff in the area of AML/CFT/CPF. Training employees directly/indirectly responsible for AML/CFT/CPF enables them to understand new developments, money laundering and financing of terrorism techniques, methods, and trends. The training includes their responsibilities relating to AML/CFT especially requirements relating to TFS, CDD and analysis of abnormal /out of pattern transactions and alerts generated thereof for possible reporting of suspicious transactions. HBL realizes that the relevant AML/CFT training combined with optimum use of technology is becoming inevitable due to ever changing nature of methods and trends in illicit activities. It is also important to test the capability and knowledge of the relevant staff on a periodic basis. Therefore, HBL also uses online trainings and AML/CFT tests of varying nature that are available in the market offering opportunity for banks to equip their staff with relevant skills as per respective roles and responsibilities within the institution.

HBL, from time to time, also plans and arranges outreach and awareness sessions covering ML/TF/PF risks and the AML/ CFT obligations including TFS for TF & PF and STR/CTR for its staff.

8. Record Management

Following are requirements for record management:

1. The bank shall ensure compliance with the record keeping instructions for maintaining record of documents and information obtained digitally or in hard form for CDD and other purposes;
2. Records of identification data obtained through CDD process, including but not limited to copies of identification documents, account opening forms, KYC forms, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a period of ten years after the business relationship is ended. The identification records shall be maintained in document as originals or copies attested by the bank.
3. Bank shall maintain all records on transactions, both domestic and international, including the results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, unusual or large transactions) and shall also keep and maintain all records related to STRs and CTRs filed by it for a minimum period of ten years from completion of the transaction;

4. For the purpose of STRs, all related customer records other than transactions, including those related to account opening shall be retained even after 10 years of termination/closure of relationship.
5. The records retained shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence if required by Law Enforcement Agencies and other relevant authorities as per the law for prosecution of criminal activity. The transaction records shall be maintained in paper or electronic form or on microfilm, as admissible as evidence in a court of law.
6. Those records where transactions, customers or accounts are involved in litigation, or where such records are required by court or other competent authority shall be retained for longer period; until they are no longer needed, and the bank is given explicit permission to destroy these records;
7. The bank shall satisfy itself in a timely manner, on any enquiry or order from the relevant competent authorities including law enforcement agencies and FMU for supply of information and records as per law.

9. Annexures

Annexure-I
(List of Information Required for Customer Identity)

Basic Identification Information

1. Full name as per identity document
2. Mother's Maiden name
3. Date of Birth
4. Place of Birth
5. Permanent Address
6. Identity document number, whichever applicable
7. Date of expiry of applicable identity document

Other basic information

8. Father/ spouse name as per identity document
9. Date of issuance of applicable identity document
10. Contact Number: Mobile Number (s)/ Land Line Number
11. Purpose of account/ transaction/ business relation
12. Beneficial ownership/ controlling rights

Other relevant Information for natural persons, as applicable

13. Current/ Mailing Address
14. Personal Email Address (as applicable)
15. Nationality – Resident/ Non-Resident Status
16. FATCA/ CRS Declaration, wherever required
17. Profession/ Source of Income/ Funds: Salary, Business, investment income
18. Next of Kin
19. Attested Passport Size Photo (in case of Photo Account instructions)
20. Live Photo (in case of digital onboarding)

Information for Legal Persons/ Legal Arrangements

21. Registration/ incorporation number or business registration number (as applicable)
22. Date of incorporation or registration of legal person or arrangement (as applicable)
23. Place of incorporation or registration of legal person or arrangement (as applicable)
24. National Tax Number (NTN)
25. Nature of business, geographies involved and expected type of counter-parties (as applicable)
26. Registered or business address
27. Intended nature of business relations
28. Purpose of account or transaction (where accounts are not maintained, and transactions are done by walk in/ occasional customers)
29. Type of account/ financial transaction/ financial service
30. Expected monthly credit turnover (amount and No. of transactions)
31. Normal or expected modes of transactions/ delivery channels

32. Wherever instructed/ advised, regulatory limits imposed such as: credit and debits/ deposit and withdrawals/ execution of financial transaction/ types of financial services allowed/ restricted.

Additional Information in case of "Trusts"

33. Whether the Trust is a Public Trust or Private Trust including foreign and national trust
34. Trust Deed whereby the Trust has been created;
35. Details of Settlor (this shall also be available in the Trust Deed);
36. Objects of the trust (this shall also be available in the Trust Deed);
37. Trustee of the trust (whether trustee is associated person of the settlor);
38. Description of each class or type of beneficiary (this information may also be checked from Trust Deed);
39. Details of any possibility of influence of any other person on trustee regarding management and control of trust property;
40. In the case of "Private Trust" if the beneficiary of a trust is also the beneficial owner of the trust, identification and verification of the beneficiary is required otherwise the name and CNIC of each beneficiary of a trust should be obtained.

Annexure-II

Minimum Documents to be obtained for Identification of Customer/ Occasional Customer

Sr. No.	Type of Customers	Documents/ papers to be obtained.
1)	Individuals (including Walk in/ Occasional customers)	Copy of the applicable valid identity document
2)	Joint Account	1. Copy of the applicable valid identity document for each joint account holder 2. In the case of joint accounts, CDD measures on all the joint account holders shall be performed as if each of them is an individual customer of the Bank.
3)	Sole Proprietorship	Copy of the applicable valid identity document; 41. Any one of the following documents: a. Registration certificate for registered concerns b. Sales tax registration or NTN certificate, wherever applicable c. Certificate or proof of membership of trade bodies etc., wherever applicable d. Declaration of sole proprietorship on business letterhead e. Account opening requisition on business letterhead
4)	Small businesses and professions including freelance professionals	42. Copy of the applicable valid identity document of the account holder/s 43. Any one of the following documents: a. Registration certificate for registered concerns. b. Sales tax registration or NTN certificate, wherever applicable. c. Certificate or proof of membership of trade bodies etc., wherever applicable. d. Proof of source of funds/ income
5)	Partnership	44. Copy of the applicable valid identity document of all partners and authorized signatories 45. All the following documents: a. Attested copy of 'Partnership Deed' duly signed by all partners of the firm. b. Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. c. Authority letter, in original, signed by all partners for opening and operating the account.
6)	Limited Liability Partnership (LLP)	46. Copy of the applicable valid identity document of all partners and authorized signatories 47. All the following documents: a. Certified Copies of:

Sr. No.	Type of Customers	Documents/ papers to be obtained.
		i. Limited Liability Partnership Deed/ Agreement ii. LLP-Form-III having detail of partners/ designated partner in case of newly incorporated LLP. iii. LLP-Form-V regarding change in partners/ designated partner in case of already incorporated LLP. iv. Authority letter signed by all partners, authorizing the person(s) to operate LLP account.
7)	Limited Companies/ Corporations	48. Copy of the applicable valid identity document of all directors and authorized signatories 49. Certified copies all the following documents: a. Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; b. Memorandum and Articles of Association; c. Certified copy of Latest 'Form-A/Form-B' d. Incorporate Form II in case of newly incorporated company and Form A/ Form C whichever is applicable; and Form 29 in already incorporated companies
8)	Branch Office or Liaison Office of Foreign Companies	50. Copy of the applicable valid identity document of senior official and/ or authorized signatories 51. All the following documents: a. Copy of permission letter from relevant authority i.e.; Board of Investment b. List of directors on company letterhead or prescribed format under relevant laws/ regulations. c. Certified copies all the following documents: i. Form II about particulars of directors, Principal Officer etc. in case of newly registered branch or liaison office of a foreign company ii. Form III about change in directors, principal officers etc. in already registered foreign companies branch or liaison office of a foreign company d. Letter from Principal Officer of the entity authorizing the person(s) to open and operate the account.
9)	Trust, Clubs, Societies and Associations etc.	52. Copy of the applicable valid identity document of: a. All members of Governing Body/ Board of Directors/ Trustees/ Executive Committee, if it is ultimate governing body, b. all authorized signatories c. settlor, the trustee(s), the protector (if any), and the beneficiaries d. Declaration from Governing Body/ Board of Trustees/ Executive Committee/ sponsors on ultimate control, purpose, and source of funds etc. 53. Certified copies all the following documents:

Sr. No.	Type of Customers	Documents/ papers to be obtained.
		a. Certificate of Registration/ Instrument of Trust b. By-laws/ Rules & Regulations c. Resolution/ Documentation of the Governing Body/ Board of Trustees/ Executive Committee, if it is ultimate governing body, authorizing any person(s) to open and operate the account
10)	NGOs/ NPOs/ Charities	54. Photocopy (after original seen) of the applicable identity documents of all members of Governing Body/ Board of Directors/ Trustees/ Executive Committee, if it is ultimate governing body, and authorized signatories. 55. Certified copies all the following documents: a. All relevant Registration documents/ Certificate of Incorporation/ license issued by SECP, as applicable b. Memorandum & Article of Association c. Incorporation Form II in case of newly incorporated company and Form B-29 in case of already incorporated company d. Resolution of the Governing Body/ Board of Directors/ Trustees/ Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account 56. Annual accounts/ financial statements or disclosures in any form, which may help to ascertain the detail of its activities, sources, and usage of funds in order to assess the risk profile of the prospective customer
11)	Agents Accounts	57. Copy of the applicable valid identity document of the agent and principal 58. Certified copy of 'Power of Attorney' or 'Agency Agreement' 59. The relevant documents/ papers from Sr. No. 2 to 10, if agent or the principal is not a natural person
12)	Executors and Administrators	60. Copy of the applicable valid identity document of the Executor/ Administrator 61. Certified copy of Letter of Administration or Probate
13)	Minor Accounts	62. Copy of the applicable valid identity document of the minor and his/her parent or natural or Court Appointed Guardian 63. Certified copy of order of appointment of Guardian appointed by Court, if applicable
14)	Mentally Disordered Person Account	64. Copy of applicable valid identity documents of mentally disordered person and court appointed manager under the applicable laws related to mental health 65. Certified true copy of court order for appointment of manager for mentally disordered person. 66. Verification of identity document through biometric verification from NADRA for both persons i.e.; mentally disordered person and the manager appointed by court.

Sr. No.	Type of Customers	Documents/ papers to be obtained.
		67. Verification of court order from the concerned court (to be obtained by bank). 68. An account would be opened in the name of a mentally disordered person and the same would be operated by the court appointed manager. 69. All CDD requirements should be conducted / completed for both persons 70. In case of change of manager by the court, the CDD formalities will be conducted for the new appointed manager by the bank afresh.

1) Requirement for copy of applicable valid identity document can be fulfilled by either:

a. obtaining photocopies of identity documents, invariably attested by Gazetted officer/ Nazim/ Administrator or an officer of the SBP RE after original seen; or

b. retaining copy of NADRA Verisys or Biometric Verification, for (hard or digital as proof of obtaining identity from customer)

2) In case of an individual with shaky/ immature signatures, in addition to CNIC or any of valid document mentioned at Sr. No 1, a passport size photograph of the new account holder besides taking his right and left thumb impression on the specimen signature card will be obtained.

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

4) The requirement of obtaining NTN depends upon availability/ issuance of NTN by tax authorities. The requirement of NTN should not be the reason for refusal of financial services to the customers, especially, where bank account is a prerequisite for obtaining NTN as per FBR's criteria. The SBP REs should facilitate their customers in opening bank accounts and subsequently obtain NTN when issued by the FBR.

5) The condition of obtaining photocopies of identity documents of directors of Limited Companies/ Corporations is relaxed in case of Government/ Semi Government entities, where SBP REs should obtain photocopies of identity documents of only those directors and persons who are authorized to open and operate the account. However, SBP REs shall validate identity information including CNIC numbers of other directors from certified copies of relevant list(s) required to be filed under Companies Act, 20

Annexure III

(To be obtained from customers who do not have a formal wealth statement)

Date:

The Branch Manager
Habib Bank Limited
_____Branch

Subject: Declaration of Wealth

Dear Sir/Madam,

This refers to my account opening request at HBL, in the context of which I would like to inform you that there is no formal document available with me to update you on my wealth. However, I hereby declare the following details of wealth as follows, for the purpose of account opening:

1. Total Value of Assets owned: _____

    a. Details of major Assets: (For example; bank balance, property, jewelry, cars, businesses etc.)
        i. _____
        ii. _____
        iii. _____
        iv. _____
        v. _____
        vi. _____

(Add more in case required)

2. Source of Wealth (For example; Inheritance, savings etc.): _____

3. Additional Information, if any: _____

Thanks,

Yours Sincerely,

_____
Customer/Authorized Signatory

Annexure IV

For Customers who do not maintain any account with any bank for conducting the first transaction through a banking channel

Date:

The Branch Manager
Habib Bank Limited
_____Branch

Subject: First Payment by any channel other than own Cheque deposit

Dear Sir/Madam,

Due to the following reason (s), I cannot make initial deposit via check deposit in my new account no. _____ opened at HBL:

Please tick the relevant option

☐ I/we do not maintain an account in any bank.
☐ I/we do not maintain an account in any bank in Pakistan
☐ I/we will transfer the first payment through online banking from my/our account number _____ maintain with _____ (mention the name of the bank and account number)
☐ I/we am/are an existing customer of HBL and maintaining account no. _____with _____ Branch
☐ Any other reason _____

Thanks,

Yours Sincerely,

_____
Customer/Authorized Signatory

Annexure V

AML/TF Red Flags

Red Flags are risk indicators for ML/TF/PF; which are related to, but not limited to customer profiles, documentation, transactions, sanctions, and goods. These must be analyzed and/or escalated, even if the transactions otherwise appear in order. Such indicators may also be taken as a means of highlighting the ways in which money may be laundered or financed for illegal/illegitimate activities. While each individual situation may not be sufficient to suggest that ML/TF/PF/TBML is taking place, a combination of such situations may be indicative of such transactions.

Transactions which do not make economic sense

a) A customer-relationship that does not appear to make economic sense, for example, a customer having a large number of accounts with the same financial institution, frequent transfers between different accounts or exaggeratedly high liquidity;
b) Transactions in which assets are withdrawn immediately after being deposited unless the customer's business activities furnish a plausible reason for immediate withdrawal;
c) Transactions that cannot be reconciled with the usual activities of the customer, for example, the use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business;
d) Transactions which, without plausible reason, result in the intensive use of what was previously a relatively inactive account, such as a customer's account which shows virtually no normal personal or business-related activities but is used to receive or disburse unusually large sums which have no obvious purpose or relationship to the customer and/or his business;
e) Provision of bank guarantees or indemnities as collateral for loans between third parties that are not in conformity with market conditions;
f) Unexpected repayment of an overdue credit without any plausible explanation; or
g) Back-to-back loans without any identifiable and legally admissible purpose.

Transactions Inconsistent with the Customer's Business

a) The currency transaction patterns of a business show a sudden change inconsistent with normal activities;
b) A large volume of cashier's cheques, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity;
c) A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location;
d) Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals; or
e) Goods or services purchased by the business do not match the customer's stated line of business.

High Value Cash Transactions

a) Large cash withdrawals made from a business account not normally associated with cash transactions;
b) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments;

c) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account;
d) The deposit or withdrawal of cash in amounts which fall consistently just below identification
e) The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements;
f) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, if any, particularly if the instruments are sequentially numbered;
g) Exchanging an unusually large number of small-denominated notes for those of higher denomination;
h) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the financial institution;
i) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
j) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
k) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g., cheques, letters of credit, bills of exchange, etc.;
l) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial;
m) The deposit of unusually large amounts of cash by a customer to cover requests for bankers' cheques, money transfers or other negotiable instruments;
n) Customers whose deposits contain counterfeit notes or forged instruments;
o) Customers making large and frequent cash deposits, but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their business; or
p) Customers who together, and simultaneously, use separate branches/booths to conduct large cash transactions or foreign exchange transactions.

Transactions involving structuring to avoid reporting or identification requirements

Structuring transactions are conducted to evade reporting and identification requirements. A person structures a transaction by breaking down a single currency sum exceeding the specified threshold into smaller amounts that may be conducted as a series of transactions at or less than a specified amount. Money launderers and criminals have developed many ways to structure large amounts of currency to evade the reporting and identification requirements. Unless currency is smuggled out of a country or commingled with the deposits of an otherwise legitimate business, any money laundering scheme that begins with a need to convert the currency proceeds of criminal activity into more legitimate-looking forms of financial instruments, accounts, or investments, will likely involve some form of structuring. Bank employees should be aware of and alert to the following structuring schemes:

1) A customer makes currency deposit or withdrawal transactions, so that each is less than the CTR filing threshold;
2) A customer uses currency to purchase official bank cheques, money orders, or traveler’s cheques with currency in amounts less than the specified amount to avoid having to produce identification in the process;
3) Deposits are structured through multiple branches of the bank or by groups of people who enter a single branch at the same time;

4) A person customarily uses the automated teller machine capable of accepting deposits, to make several deposits below a specified threshold;
5) Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers; or
6) The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

In addition, structuring may occur before a customer brings the funds to the bank. In these instances, the bank may be able to identify the aftermath of structuring. Deposits of money instruments that may have been purchased elsewhere might be structured to evade the reporting and record keeping requirements. These instruments are often numbered sequentially in groups totaling less than the specified amount; bear the same handwriting (for the most part) and often the same small mark, stamp, or initials; or appear to have been purchased at numerous places on the same or different days.

Transactions involving accounts

a) Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out;
b) A dormant account containing a minimal sum suddenly receives deposit or series of deposits followed by daily cash withdrawals that continue until the sum so received has been removed;
c) When opening an account, the customer refuses to provide information required by the bank, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify;
d) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship);
e) An account opened by a legal entity or an organization that has the same address as other legal entities or organizations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.);
f) An account opened in the name of a recently formed legal entity and in which a higher-than-expected level of deposits are made in comparison with the income of the promoter of the entity;
g) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer;
h) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organization;
i) An account opened in the name of a legal entity, a foundation, or an association, which may be linked to a terrorist organization and that shows movements of funds above the expected level of income;
j) Matching of payments out with credits paid in by cash on the same or previous day;
k) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts;
l) High velocity of funds through an account, i.e., low beginning and ending daily balances, which do not reflect the large volume of funds flowing through an account;
m) Multiple depositors using a single account;
n) Accounts opened in the name of an exchange company that receives structured deposits; or
o) Accounts operated in the name of an offshore company with structured movement of funds.

Transactions involving transfers to and from abroad

a) Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements;
b) Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected;
c) Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries;
d) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern;
e) Transfer of money abroad by an interim customer in the absence of any legitimate reason. An interim customer is one who is not a regular customer of the financial institution in question, or does not maintain an account, deposit account, safe deposit box, etc.;
f) A customer which appears to have accounts with several financial institutions in the same locality, especially when the financial institution is aware of a regular consolidated process from such accounts prior to a request for onward transmission of the funds elsewhere;
g) Repeated transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash;
h) Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries associated with (i) the production, processing or marketing of narcotics or other illegal drugs or (ii) criminal conduct;
i) Substantial increase in cash deposits by a customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer;
j) Building up large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas;
k) Cash payments remitted to a single account by a large number of different persons without an adequate explanation;
l) Funds transfer activity occurs to or from a financial secrecy haven without an apparent business reason or when the activity is inconsistent with the customer’s business or history;
m) Many small, incoming transfers of funds are received, or deposits are made using cheques and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer’s business or history;
n) Incoming funds transfers with limited content and lack of remitter’s information; or
o) Unusually large number and variety of beneficiaries are receiving funds transfers from one company;

Investment Related Transactions

p) Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent standing;
q) Requests by a customer for investment management services where the source of funds is unclear or not consistent with the customer's apparent standing;
r) Larger or unusual settlements of securities transactions in cash form; or

Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

Transactions Involving Unidentified Parties

a) Provision of collateral by way of pledge or guarantee without any discernible plausible reason by third parties unknown to the financial institution and who have no identifiable close relationship with the customer;
b) Transfer of money to another financial institution without indication of the beneficiary;
c) Payment orders with inaccurate information concerning the person placing the orders;
d) Use of pseudonyms or numbered accounts for effecting commercial transactions by enterprises active in trade and industry;
e) Holding in trust, shares in an unlisted company whose activities cannot be ascertained by the bank; or
f) Customers who wish to maintain a number of trustee or clients' accounts that do not appear consistent with their type of business, including transactions that involve nominee names.

Transactions Involving Embassy and Foreign Consulate Accounts

a) Official embassy business is conducted through personal accounts;
b) Account activity is not consistent with the purpose of the account;
c) Accounts are funded through substantial currency transactions; or
d) Accounts directly fund personal expenses of foreign nationals without appropriate controls.

Characteristics of the Customer or His/ Her Business Activity

e) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types;
f) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.);
g) Stated occupation of the transactor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area);
h) Regarding non-profit or charitable organizations, financial transactions for which there appears to be no logical economic purpose, or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction;
i) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown, or such activity does not appear to justify the use of a safe deposit box; or
j) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

Transactions Linked to Locations of Concern

k) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF High Risk countries and territories, etc.);
l) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF High Risk and territories, etc.);

m) A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern;
n) The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern;
o) A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations;
p) The opening of accounts of financial institutions from locations of specific concern; or
q) Sending or receiving funds by international transfers from and/or to locations of specific concern.

Miscellaneous Transactions

r) Purchase of bank cheques on a large scale by an interim customer;
s) Extensive or increased use of locker facilities that do not appear to be justified by the customer's personal or business activities;
t) Lockers are used by individuals who do not reside or work in the institution's service area despite the availability of such services at an institution closer to them;
u) Unusual traffic patterns in the lockers area. For example, more individuals may enter, enter more frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or valuable items;
v) A customer rents multiple lockers to park large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the financial system;
w) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation;
x) To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments;
y) A customer purchases several open-end stored value cards for large amounts. Purchases of stored value cards are not commensurate with normal business activities;
z) Suspicious movements of funds occur from one financial institution to another, and then funds are moved back to the first financial institution;
aa) Purchase of real estate on price higher that the determinable value; or
bb) A series of purchases of real estate within a relatively short span of time.

10. Definitions

As per AML/CFT/CPF Regulations, following definitions shall be adopted:

1. "Act" means the Anti-Money Laundering Act 2010 as updated from time to time.
2. "Bank" or "Banking Company" shall have the same meaning as under section 5 of the Banking Companies Ordinance (BCO) 1962.
3. "Banking Business" shall include the businesses stipulated under section 7 of BCO.
4. "Banking" means the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawable by cheque, draft, order or otherwise.
5. "Beneficial Owner" shall have the same meaning as under section 2(iv) of the Act.
6. "Beneficiary Institution" means the financial institution that receives the funds on behalf of the wire transfer or fund transfer beneficiary.
7. "Beneficiary" means the person to whom or for whose benefit the funds are sent or deposited in a bank or person who has beneficial interest in financial transaction to be executed.
8. "Biometric Verification System" or "BVS" means the technology enabled system (verifiable from NADRA or the relevant Government authority) that allows financial institutions to obtain biometrics of the customers at the time of opening of account or conducting the transactions.
9. "Branch" or "Branch Office" means any branch or branch office or other place of business of the bank, authorized in terms of respective laws administered by SBP.
10. "Business Relationship" shall have the same meaning as under section 2(v) of the Act.
11. "Class of Beneficiaries" for beneficiary(ies) of trusts that are designated by characteristics or by class, financial institutions shall obtain sufficient information concerning the beneficiary to satisfy the financial institution that it shall be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.
12. "Close associate of a PEP" means—
    a. an individual known to have joint beneficial ownership of a legal person or a legal arrangement or any other close business relations with a PEP;
    b. any individual(s) who have beneficial ownership of a legal person or a legal arrangement which is known to have been set up for the benefit of a PEP; or
    c. an individual who is reasonably known to be closely connected with the PEP for any other reason, including socially or professionally.
13. "Company" shall have the same meaning as under section 2(vii) of the Act.
14. "Competent Authorities" shall have the same meaning as under section 2(viii) of the Act.
15. "Control" in relation to a legal person, means the power to exercise a controlling influence over the management or the policies of the undertaking, and, in relation to shares, means the power to exercise a controlling influence over the voting power attached to such shares.
16. "Corporate Group" shall have the same meaning as under section 2(ix) of the Act.
17. "Correspondent Bank" means the banks in Pakistan, which provide correspondent banking services to banks or financial institution situated abroad and vice versa;
18. "Correspondent Banking" means provision of banking services by one bank (correspondent) to another bank (respondent) including but not limited to opening and maintaining accounts in different currencies, fund transfers, cheque clearing, payable through accounts, foreign exchanges services or similar other banking services.
19. "Court appointed Manager" means a person appointed by the competent court to operate a bank account of a mentally disordered person under the applicable laws on mental health.

20. "Cross-Border Wire Transfer" means a wire transfer where the ordering institution and the beneficiary institution are in different countries or jurisdictions;
21. "Currency Transaction Report (CTR)" shall have the same meaning as under section 2(xi) of the Act.
22. "Customer" means a person (natural & legal) having relationship with the bank and availing financial services from the bank which includes but not limited to holding of deposit/deposit certificate/or any instrument representing deposit/placing of money with the bank, availing other financial services, locker facility, safe deposit facility, or custodial services.
23. "Deposit" shall include the deposits under Section 26A of BCO.
24. "Designated Person (DP)" individual or entity designated under UNSC Act.
25. "Domestic Wire Transfer" means any wire transfer where the originator and beneficiary institutions are in Pakistan regardless the system used to affect such wire transfer is located in another jurisdiction.
26. "Dormant or In-Operative Account" means. the account in which no customer-initiated transaction (debit or credit) or activity (e.g. login through digital channels) has taken place during the preceding one year.
27. "Electronic Money Institution (EMI)" shall have the same meaning as under Section 2(1)(u) of Payment Systems & Electronic Funds Transfer (PS&EFT) Act.
28. "Exchange Companies" shall have the same meaning as under Sections 3, 3A and 3 AA of the Foreign Exchange Regulations Act (FERA). SBP issues authorization/ license to REs known as ECs/ ECs-B to deal in foreign exchange including foreign currency, foreign currency notes, transfers, coins, postal notes, money orders, bank drafts, and traveler's cheques to individuals only i.e., to natural persons. Since ECs/ ECs-B don't deal with legal person and legal arrangements and don't maintain business relationship (accounts) therefore those requirements in these regulations which pertains to legal person and legal arrangement and business relationships shall not be applicable on them.
29. "Family member of a PEP" includes—
    a. spouse of the PEP; and
    b. lineal descendants and ascendants of the PEP and siblings of PEP.
30. "FATF Recommendations" means the Recommendations of Financial Action Task Force as amended from time to time.
31. "Financial Institution" shall have the same meaning as under Section 2(xiv) of the Act.
32. "FMU" means the Financial Monitoring Unit established under Section 6 of the Act;
33. "Foreign Banking Company" means a banking company, not incorporated in Pakistan, which has a branch or branches doing banking business in Pakistan under a license issued by SBP in this behalf.
34. "Fund Transfer/ Wire Transfer" means any transaction carried out by financial institutions on behalf of originator person by way of electronic means or otherwise to make an amount of money available to beneficiary person at another beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.
35. "Identity Document" means the following documents for identification of natural persons as applicable:
    a. Valid CNIC/ SNIC/ NICOP/ SNICOP for Pakistani citizens;
    b. Valid Passport for foreign citizens;
    c. Valid POC for persons of Pakistani origin;
    d. Valid ARC for registered Aliens in Pakistan;
    e. Valid POR Card for Afghan refugees; and
    f. Valid Form-B/ Juvenile Card for Pakistani citizens who are minors.
36. "Intermediary Institution" is an intermediary in the wire transfer payment chain; that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution.

37. "Microfinance Bank (MFB)" shall have the same meaning as under Section 2(ia) of Micro Finance Institutions Ordinance 2001 (MFIO).
38. "Monetary Threshold" expressed in Pakistani Rupees includes a reference to the equivalent amount expressed in any other currency.
39. "Money Laundering (ML)" shall have the same meaning as under Section 2 of the Act.
40. "Non-Face to Face Transactions or business relationship" non-face-to-face interactions are considered to occur remotely - meaning the parties are not in the same physical location and conduct activities by digital or other non-physically present means, such as mail or telephone or internet.
41. "Numbered Account" means account where the names of the customer and beneficial owner are known to the bank but are substituted by an account number or code name in subsequent documentation.
42. "Occasional Customer" (also called walk in customer) means the person conducting occasional transactions and is not a permanent customer; not having account/ permanent customer relationship with the bank. For those SBP REs which do not maintain permanent customer relationship/ customer accounts, every customer would be treated as occasional or walk in customer. Occasional/ Walk in customers may have frequent visit for execution of transaction on counter of the bank.
43. "Occasional Transactions" shall have the same meaning as under Section 2 (xxii) of the Act.
44. "Online Transaction" means deposit or withdrawal of cash, fund transfers, payments against goods and services, etc. using different branches of SBP REs through electronic means.
45. "Ordering Institution" means the financial institution that initiates a wire transfer on the instructions of the wire transfer originator for transferring the funds.
46. "Originator" means the person who allows or places the order to initiate a fund transfer/ wire transfer or an online transaction.
47. "Outsourcing" means use of a third party (affiliated or un-affiliated) to perform activities, functions, or processes normally to save money, time and/or use the skills/technology of another entity on a continuing basis that would normally be undertaken by the bank, now or in the future. However, it does not cover consultancy services, purchase contracts for tangible/intangible items, for example, contracts to purchase standardized products such as furniture, Software/IT solutions, ATM etc.
48. "Payable-through Account" means an account maintained at the correspondent bank by the respondent bank which is accessible directly by a third party to affect transactions on its own (respondent bank's) behalf.
49. "Payment Services" means the services that enable the customers to make payments for goods and services, bill payments, fund transfers, cash deposit and withdrawal and any other service endorsed by SBP from time to time.
50. "Payment System" shall have the same meaning as under Section 2(1) (zd) of PS&EFT Act.
51. "Person with Mental Disorder" means a person with mental illness as defined in the applicable laws on mental health.
52. "Politically Exposed Person (PEP)" means an individual who is or has been entrusted with a prominent public function either domestically or by a foreign country, or in an international organization and includes but is not limited to:
    a. for foreign PEPs, Heads of State or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations and important political party officials;
    b. for domestic PEPs, Heads of State or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, important political party officials;
    c. for international organization PEPs, members of senior management or individuals who have been entrusted with equivalent functions; and

d. Provided that middle ranking or more junior individuals in the above referred categories are not included in the definition of PEPs.

53. "Prescribed" means prescribed under applicable rules, circulars, directions, orders or by laws.
54. "Proscribed Person (PP)" means an individual or entity proscribed under Anti-Terrorism Act 1997 (ATA)
55. "PSOs/ PSPs" mean the same as defined in the Rules for PSOs/ PSPs issued and revised by SBP from time to time.
56. "Regulated Entities (REs)" mean financial institutions licensed/ authorized and regulated by the SBP under any law administered by SBP, and includes:
    a. Banks;
    b. Development Finance Institutions (DFIs);
    c. Microfinance Banks (MFBs);
    d. Exchange Companies (ECs)/ Exchange Companies of 'B' Category (ECs-B);
    e. Payment Systems Operators (PSOs);
    f. Payment Service Providers (PSPs);
    g. Electronic Money Institutions (EMIs); and
    h. Third Party Payment Service Providers (TPSPs).
57. "Regulations" means the AML/CFT/CPF Regulations for SBP REs
58. "Respondent Bank" means the bank or financial institution outside Pakistan to whom correspondent banking services in Pakistan are provided and vice versa.
59. "Senior Management" means chief executive officer, managing director, deputy managing director, chief operating officer, company secretary, chief financial officer, chief compliance officer, chief regulatory officer, and any holder of such positions by whatever name called. For High-Risk Approvals, Head – Financial Crime Compliance or any designated officer reporting directly to the Chief Compliance Office shall also be considered as part of "Senior Management".
60. "Settlor" are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
61. "Shell Bank" means a bank that has no physical presence (mind and management) in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
62. "State Bank of Pakistan (SBP)" means SBP established under Section 3 of the State Bank of Pakistan Act, 1956 (XXXIII of 1956).
63. "Third Party Payment Service Provider (TPSP)" shall have the same meaning as in SBP's Regulations for Mobile Banking Interoperability, updated from time to time.
64. "Transfer" means sale, lease, purchase, mortgage, pledge, gift, loan or any other form of transfer of right, title, possession or lien.
65. "Trust" means an obligation annexed to the ownership of property and arising out of the confidence reposed in and accepted by the owner or declared and accepted by him for the benefit of beneficiary.
66. "Trustee" means any person who accepts the confidence of the author of the trust to the benefit of the beneficiary.
67. "Ultimate Effective Control" or" Ultimately Owns or Controls" means situations in which ownership/ control is exercised through a chain of ownership or by means of control other than direct control.

Other terms used in the policy but not defined here, shall have the same meaning as ascribed to them in the Act. However, if not defined in the Act, shall have the meaning ascribed to them in the respective laws/regulations/rules/circulars governing the subject.