AML/CDD/CFT POLICY

For Prevention of Money Laundering/Terrorist Financing

HBL

Owner:

GLOBAL COMPLIANCE

Revision Date:

September, 2013

AML/CDD/CFT POLICY

APPROVAL SHEET

Policy Owner: Global Compliance

Implementation Responsibility: Chief Compliance Officer

Custodian: Anti Money Laundering Department, Global Compliance

Operating Jurisdiction: All Domestic and International HBL Operations

Review Frequency: 3 years or earlier if required

Review Responsibility: Anti Money Laundering Department, Global Compliance

Approval Date: October 25, 2013

Effective Date: November 01, 2013

Next Review Date: October 31, 2016

Recommended by:	Concurred by:
_____ **Jamil Iqbal** **Chief Compliance Officer**	_____ **Nauman K. Dar** **President & CEO**

Approved By:	
_____ **Board Audit Committee**	_____ **Board of Directors**

Slogan for HBL

‘Compliance is My Responsibility’

ABBREVIATIONS USED IN AML/CDD/CFT POLICY

CFT	Combating Financing of Terrorism
TF	Terrorist Financing
FATF	Financial Action Task Force
CCO	Chief Compliance Officer
MLRO	Money Laundering Reporting Officer
ML	Money Laundering
PEPs	Politically Exposed Person
BOD	Board of Directors
OFAC	Office of Foreign Assets Control
MSB	Money Service Business
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
SDD	Simplified Due Diligence

TABLE OF CONTENTS

INTRODUCTION

Habib Bank ('the Bank') is a pioneer financial institution of Pakistan, having largest domestic network of branches, a well-known brand locally with a substantial international presence.

To protect itself from the increasing danger of organized criminal activity, money laundering and Terrorist Financing, it is essential for the Bank to have a clearly laid down "Anti-Money Laundering" (AML)/"Customer Due Diligence" (CDD)/' Combating the Financing of Terrorism (CFT) Policy to ensure that the Bank remains protected from the menace of money laundering and is not used by existing &/or prospective customers for any criminal activity.

METHODOLOGY

1 METHODOLOGY

1.1 OBJECTIVES OF AML/CDD/CFT POLICY

The objective of this policy is to ensure that the products and services of the Bank are not used to launder the proceeds of crime and that all of the Bank's staff is aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing. The document also provides a framework to comply with applicable laws, Regulatory guidelines specially related with detection and reporting of suspicious activities.

In case of any clarification contact AML Department of Global Compliance at HOK comphelp@hbl.com or MLROs in respective countries.

1.2 SCOPE

This policy is applicable to the All Domestic and International HBL Operations including bank's subsidiaries, representative offices where it has majority ownership.

Particular attention shall be paid to overseas branches and subsidiaries located in countries which do not or insufficiently comply with FATF recommendations (as determined by FATF or identified by State Bank of Pakistan time to time).

Furthermore, HBL AML/ CFT policies shall be applied to all branches and subsidiaries outside Pakistan to the extent that laws and regulations of the host country permit. Where the AML/CFT requirements in the host country or jurisdiction differ from those in Pakistan, overseas branches or subsidiaries shall apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

1.3 AMENDMENT AND UPDATES

Amendment and updates to Policy shall be approved by the President on pre-facto basis on the recommendation of Chief Compliance Officer. All such Amendment and updates shall be subsequently ratified by the Board.

1.4 DEFERRAL

Deferral against procedural requirement can only be allowed by CCO under special circumstances.

Respective relationship management and operational staff will be responsible for monitoring and regularization of the deficiency before expiry of deferrals.

Policy coverage will include:

- Compliance with AML Act 2010.
- Compliance of SBP Prudential Regulations on AML/ CDD/CFT.
- Compliance of local country legislations/ regulations on AML/ CDD/CFT & subsequent updates.

- FATF Recommendations .
- International Standards and guidelines, including Basel and Regulatory sanctions as applicable.

1.5 MONEY LAUNDERING

Definition:

Money Laundering is the criminal practice of processing ill-gotten gains or "dirty" money, through a series of transactions, so that they appear to be the proceeds from legal activities, it is also the process to change the identity of illegally obtained money by using banking channel so that it appears to have originated from a legitimate source.

1.6 STAGES OF MONEY LAUNDERING

Money laundering can be a diverse and often complex process. The first step in the laundering process by the criminal is to attempt to get the proceeds of their crimes into a bank or other financial institution, sometimes using a false identity. The funds can further be transferred to other accounts, locally or internationally or used to buy other goods or services. It eventually appears to be like legally earned money and becomes difficult to trace back to its criminal origin. The criminals can then invest or spend it or, as is often the case, use it to fund more crime/s.

The laundering process is often described as taking place in three stages:-

1. Placement
2. Layering
3. Integration.

1. Placement

The first stage is referred to as Placement. At this stage Illegal funds or assets are first brought into the financial system. When illegal funds are placed in the financial system, they become more liquid. There are numerous Placement techniques, including the following:

- Smurfing
- Alternative Remittances
- Electronic Transfers
- Asset Conversion
- Bulk Movement
- Securities Dealing

Smurfing: It involves the deposit of small amounts of illegal cash into account(s). Typically, smurfing deposits are in small amounts in order to avoid Regulatory requirements of reporting cash transactions '

Alternative Remittances: It refers to the transfer of funds through 'alternative' or illegal money transfer system. These systems are unregulated and illegal, but they are used to transfer both legitimate and illegal funds. Alternative Remittances also go by the names of underground or parallel banking. There are very large networks of these systems in operation around the world.

Electronic Transfers: In the money laundering context, an electronic transfer involves the transfer of money through electronic payment systems that do not require sending funds through a bank account. If the amount is below the CTR (Cash Transaction Reporting) limit then it will not be reported as per prevailing regulations.

Asset Conversion: Asset Conversion simply involves the purchase of goods. Illegal money is converted into other assets, such as real estate, diamonds, gold and vehicles, which can then be sold and proceeds can be deposited in the account.

Bulk Movement: It involves the physical transportation and smuggling of cash and monetary instrument/s such as money orders and cheques.

Securities Dealing: Illegal funds are placed with securities firms which are used for buying bearer securities and other easily transferable instruments

2. Layering

Layering is the second stage of money laundering. In this stage illegal funds or assets are moved, dispersed and disguised to conceal their illegal origin. There are numerous techniques and institutions that facilitate layering, including the following:

- Offshore Banks
- Shell Corporations
- Trusts
- Walking Accounts
- Intermediaries

Offshore Banks: Offshore Banks accept deposits from non-resident individuals and corporations. A number of countries have well-developed offshore banking sectors; in some cases, combined with loose anti- money laundering regulations.

Shell Corporations: A Shell Corporation is a company that is formally established under applicable corporate laws, but does not actually conduct a business. Instead, it is used to engage in fictitious transactions or hold accounts and assets to disguise their actual ownership

Trusts: Trusts are legal arrangements for holding specified funds or assets for a specified purpose. These funds or assets are managed by a trustee for the benefit of a specified beneficiary or beneficiaries. Trusts can act as layering tools as they enable creation of false paper trails and transactions. The private nature of trusts make them attractive to money launderers.

Walking Accounts: A Walking Account is an account for which the account holder has provided standing instructions that upon receipt all funds should be immediately transferred into one or more accounts. By setting up a series of walking accounts, criminals can automatically create several layers as soon as any fund transfer occurs.

Intermediaries: Lawyers, accountants and other professionals may be used as Intermediaries or middlemen between the illegal funds and the criminal. Professionals engage in transactions on behalf of a criminal client who remains anonymous. These transactions may include use of shell corporations, fictitious records and complex paper trails.

3. Integration

Integration is the third stage of money laundering process. In this stage, illegal funds are successfully legitimized by mixing with legitimate funds in the financial system.

There are various Integration techniques, including the following:

- Import /Export Transactions
- Business Recycling
- Asset Sales & Purchases
- Consultants
- Credit & Debit Cards
- Corporate Financings

Import /Export Transactions to bring illegal money into the criminal's country of residence, the domestic trading company will export goods to the foreign trading company on an over-invoiced basis. The illegal funds are remitted and reported as export earnings. The transaction can work in the reverse direction as well.

Business Recycling Legitimate businesses also serve as conduits for money laundering. Cash-intensive retail businesses, real estate, jewelers, and restaurants are some of the most traditional methods of laundering money. This technique combines the different stages of the money laundering process.

Asset Sales & Purchases This technique can be used directly by the criminal or in combination with shell corporations, corporate financings and other advanced means. The end result is that the criminal can treat the earnings from the transaction as legitimate profits from the sale of the real estate or other assets.

Consultants The use of consultants in money laundering schemes is quite common. The consultant could be fake. For example, the criminal could himself be the consultant. In this case, the criminal is channeling money back to himself. This money is declared as income from services performed and can be used as legitimate funds.

Credit & Debit Cards:

Credit cards are an efficient way for launderers to integrate illegal money into the financial system. By maintaining an account in an offshore jurisdiction through which payments are made, the criminal ensures there is a limited financial trail that leads to his country of residence.

Debit Cards Individuals first transfer illegal funds into an offshore account and also signs up for a debit card from the bank to utilize the funds.

Corporate Financings Corporate financings are typically combined with a number of other techniques, including use of offshore banks, electronic funds transfers and shell corporations.

The three basic stages may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap.

1.7 SOURCES OF MONEY LAUNDERING:

Money laundering may not just involve wealth related to Drug Trafficking / Terrorism financing. List of crimes identified by Financial Action Task Force (FATF) as generators of criminal wealth also included:

1. Illegal arms sales.
2. Gun running
3. Organized crime including drug trafficking and prostitution
4. Embezzlement
5. Smuggling (including movement of nuclear materials)
6. Counterfeiting (including making of imitation and copies of original products/goods)
7. Fraud, especially computer-supported fraud
8. Benefiting from insider trading.
9. Bribery and kickbacks
10. Tax evasion
11. Under and over-invoicing of trade transactions.
12. Bogus trade transactions to launder money through round-tripping
13. Facilitating illegal immigration
14. Real Estate Transactions

1.8 TERRORIST FINANCING

Terrorist Financing can be defined as the financial support, in any form, to terrorism or of those who encourage, plan, or engage in terrorism. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organization.

1.9 THE NEED TO COMBAT MONEY LAUNDERING (ML) AND TERRORIST FINANCING (TF)

The prevention of ML and TF from the point of view of the Bank has three dimensions:

- **Ethical** - taking part in the prevention of crime.
- **Professional** - ensuring that the Bank is not involved in recycling the proceeds of crime that would call into question its reputation, integrity and, if fraud is involved, its solvency.

- **Legal** - complying with Laws and Regulations that impose a series of specific obligations on financial institutions and their employees.

The need also arises due to the severe nature of consequences of ML and TF. Following are some examples:

- Unexplained changes in supply and demand for money,
- Volatility of capital flows and exchange rates due to un-anticipated cross border asset transfers,
- Contamination of legal financial transactions,
- Threat to the functioning of economy's financial system,
- Systemic risk,
- Unlawful enrichment by perpetrator of crime,
- Dampening effect on foreign direct investment,
- Weakening of the social, collective ethical standards,
- Drug trafficking, Human trafficking,
- Political corruption,
- Terrorism crimes cause a great deal of human misery.
- Prudential risks to bank soundness arising from these developments.

1.10 REGULATORY OVERSIGHT & COMPLIANCE RISKS

HBL has used SBP/FMU guidelines and International Regulatory guidelines/standards as applicable to formulate its own AML/CDD/CFT Policy. The consequence of contravening the Regulations or failing to comply can be significant and include disciplinary measures, imprisonment or fine or both under local laws as well as the loss of reputation for the bank.

Notwithstanding the statutory and regulatory penalties, increased vigilance by Management and staff will protect the Bank from the following risks:

- Reputational
- Operational
- Legal
- Financial

Reputational risk: The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong AML/CDD/CFT policy helps to prevent a business from being used as a vehicle for illegal activities.

Operational risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If AML/CDD/CFT policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time

and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

Legal risk: If a business is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations.

Financial risk: If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone he/she is not. The consequences of this may be far reaching. If a business does not know the true identity of its customers, it will also be difficult to retrieve money that the customer owes.

LEGAL AND REGULATORY OBLIGATIONS

2 LEGAL/ REGULATORY OBLIGATIONS

2.1 LEGAL OBLIGATIONS

The bank is obligated to comply with the requirements of the AML Law and with the relevant provisions of the Banking Act as and when they are promulgated. In addition, the bank under NAB Ordinance 1999, Anti Terrorism Act 1997 and Control of Narcotics Substance Act 1997 is obligated to take prompt and immediate notice of all unusual or large transactions in customer account, which apparently have no genuine economic or lawful purpose.

Overseas branches should follow regulatory requirement of the host country under relevant legislations.

2.2 REGULATORY OBLIGATIONS

Under State Bank of Pakistan/ Financial Monitoring Unit (FMU) and international Regulations there are personal obligations on every member of the management and staff to report suspicious activities

If a person is aware or suspects that a transaction or instruction is related to any crime, he/ she must report the transaction to Global Compliance /MLRO even if he/ she is not directly handling the transaction, instruction or funds in question.

The Bank itself has similar obligations.

It is a regulatory requirement for an institution to have in place policy and procedures to combat money laundering/terrorist financing. The policy / procedures as a minimum must include:

- Setup a compliance unit with a full time CCO
- The verification of new client identification, CDD (Know Your Customer) profiling, update customer's information and record at reasonable interval.
- Risk-based controls
- Awareness raising and training of staff members.
- Recognition and reporting suspicions of money laundering/terrorist financing.
- Retention of records.
- Independent testing (internal/external Audits);
- CCD Measures for Occasional Customers/ Walk-in Customers.
- Handling wire transfers/ fund transfers.
- ML/CFT threats that may arise from the use of new or developing of new products and technologies.

Overseas branches/ subsidiaries should follow host country regulatory requirements or that of the State Bank whichever are more exhaustive. Moreover, if the law of the host country conflicts with the AML/ CFT requirements of HBL or SBP which are more stringent and Branch is unable to fully observe the higher standards, branch shall report this to the Head office for further reporting to State Bank of Pakistan and comply with such further directions as may be issued.

It is a criminal offence if management or staff:

1. Acquire proceeds of a crime or assist anyone whom they know or suspect has committed, or benefited from any criminal conduct. **(Acquire, Possess & Assist)**
2. Prejudice an investigation by informing the subject of a suspicion, or any third party that a disclosure has been made either internally or externally, or that the authorities may act or propose to act or investigate. **(Tip Off)**
3. Acquire knowledge or a suspicion, or has reasonable grounds to know or suspect, that benefit has been gained from criminal conduct or that the proceeds of crime have been laundered, and have not reported the same as soon as possible. Bank staff negligent in this respect would be liable for prosecution. **(Failure to Report)**
4. Have not implemented effective systems, controls and procedures to guard against money laundering. **(Systems & Controls)**

2.3 OFFENCES AND PENALTIES (KEY ELEMENTS)

The AML Act 2010 and other local Laws deal with AML/CDD/CFT related violations which include imprisonments or fine or both.

2.3.1 AML ACT 2010

Offences (Section 3)

A person shall be guilty of offence of money laundering, if the person;

a. Acquires, converts. possesses, uses or transfers property, knowing or having reason to believe that such property is proceeds of crime conceals or disguises the true nature, origin, location, disposition, movement or ownership of property, knowing or having reason to believe that such property is proceeds of crime.
b. Holds or possesses on behalf of any other person any property knowing or having reason to believe that such property is proceeds of crime
c. Participates in, associates, conspires to commit, attempts to commit, aids, abets, facilitates or counsel the commission of the acts specified in the above clauses.

Penalties (Section 4)

Whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than one year but may extend to ten years and shall also be liable to fine which

may extend to one million rupees and shall also be liable to forfeiture of property involved in the money laundering. The aforesaid fine may extend to five million rupees in case of a company and every director, officer or employee of the company found guilty shall also be punishable under this law.

2.3.2 NAB ORDINANCE 1999

Offences (Section 9)

Corruption and corrupt practices: Committed by holder of public office or any other person is cognizable offence under NAB Ordinance

Penalties (Section 10)

A person who commits the offence of corruption and corrupt practices shall be punishable with imprisonment for a term which may extend to 14 years and with fine, assets and property of such person which are found to be disproportionate to the known sources of his/her income or which is acquired by money obtained through corruption and corrupt practices whether in his/her name or in the name of any of his/her dependents, or benamidars shall be liable to be forfeited.

2.3.3 CONTROL OF NARCOTIC SUBSTANCES ACT 1997

Offences (Section 67)

Reporting of Suspicious financial transactions: Notwithstanding anything contained in any for the time being in force, all banks and financial institutions shall pay special attention to all unusual patterns of transactions, which have no apparent economic or lawful purpose and upon suspicion that such transactions could constitute or be related to illicit narcotics activities , the manager or director of such financial institution shall report the suspicious transactions to the Director General of ANF.

Penalties (Section 67)

Whoever fails to supply the information in accordance with the above shall be punishable with rigorous imprisonment which may extend to three years.

2.3.4 ANTI TERRORISM ACT 1997

Offences (Section 11-K)

A Person commits an offence if he/she enters into or becomes concerned in any arrangement which facilitates the retention or control, by or on behalf of another person of terrorist property.

(a) By concealment,
(b) By removal from the jurisdiction.
(c) By transfer of nominees, or
(d) In any other way.

Penalties (Section 11-N)

Any person who commits an offence shall be punishable on conviction with imprisonment for a term not less than six months and not exceeding five years and with fine.

Similarly, in the overseas network where the bank operates, respective Regulators also have stringent laws to deal with AML/CDD/CFT related violations and violators.

THE BANK'S POLICY FOR AML/CDD/CFT

3 THE BANK'S POLICY FOR AML/CDD/CFT

Keeping in view of Global threat, the bank has taken various steps to counter the menace of money laundering and terrorist financing. The bank is stringently focusing on core Compliance functions and has adopted a robust Policy across HBL network to remain compliant with AML/CFT regimes in all jurisdictions.

3.1 AML/CFT

It is the Policy of HBL that:

- Statutory, regulatory & legal obligations to prevent ML and TF are fully complied with.
- Systems and controls are implemented and reviewed on set frequency in order to minimize the risk of the Bank's services being abused for the purposes of ML and TF.
- A money laundering risk assessment of the Bank's services and customer base including correspondent banks and MSBs (Money Service Businesses) are undertaken and appropriate policies, procedures and due diligence controls are applied proportionate to that risk.
- The bank would not do business with
    - Individuals / entities subject to UN sanctions
    - Individuals / entities under OFAC or local country sanctions as applicable
    - Unauthorized money changers/prize bond dealers
    - Anonymous customers
    - Customers hiding beneficial ownership of the account
    - Client or business segment black listed by the Bank or by the Regulators.
    - Shell Banks & off shore corporate clients
    - Government officials willing to open government's accounts in their personal names.
- To carry out enhanced due diligence before establishing relationships with the following High risks customers
    - Trusts ,NGOs, NPOs, Foundations, Welfare Association, Religious Entities, Club, Societies, Financial Institution, Authorized Money Exchange Cos., Controversial entity, Jewelers, Arms Dealers.
    - Politically Exposed Persons (PEPs)
    - Correspondent Relationships
    - Customers using their personal accounts for business transactions
    - Private Banking Customers
    - Institutions / Individuals whose association with HBL could be considered controversial
    - Any individual or entity that has caused or has been related to a credit, operational or reputational loss to HBL
    - Extending Banking facilities refused by other banks
    - Customers belonging to countries where AML/CDD/CFT rules are lax
    - Non-face to face / on-line customers,
    - Accounts of foreign nationals belonging to sanctioned countries
    - Walk in customers
    - Non- resident customers

- Customers in cash based business
- High risk geographies
- Customers reportedly having previous unsatisfactory / suspicious social status
- High net worth customers with no clearly identifiable source of income
- Companies that have nominee shareholders or shares in bearer form
- Legal persons or arrangements that are personal asset holding vehicles
- There is a doubt about the veracity or adequacy of available identification data on the customer

- Any customer relationship where the customer's conduct gives the Bank reasonable cause to believe or suspect involvement with illegal activities is required to be reported to the Regulators or relevant authorities.
- In countries where local regulators call for a money laundering compliance reports, respective country MLROs are responsible for preparation and submission of these reports. CCO would submit a quarterly compliance report (including significant AML/CFT issues)to Board Audit Committee.
- Management shall establish criteria of identifying and assessing ML/FT risks that may arise in relation to new products, services, business practices and delivery mechanisms including the review of existing products and services on on-going basis.

3.2 CUSTOMER DUE DILIGENCE (CDD)

CDD is closely associated with the fight against money-laundering. Supervisors around the world are increasingly recognizing the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can be exposed to reputational, operational, legal and financial risks

It is a Policy of the Bank that:

- Prior to establishing a relationship with a new customer, basic background information about the customer should be obtained including identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from customer and/or from reliable and independent sources, furthermore, understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship, information related with customer's business and source/utilization of funds and the expected level of activity.
- Prior to establishing relationships with correspondent banks or agents, appropriate steps must be taken to confirm the identity, integrity and due diligence procedures of those representatives or agents and, where necessary, the identities of underlying clients.
- Bank shall take reasonable measures to identify and verify identities of beneficial owner (s) in relation to a customer. Furthermore, in case of a legal person, trust or similar legal arrangement, measures shall be taken to understand the ownership and control structure of the legal person or entity.
- Customer's profile must be updated periodically based on risk profiling of the customer. Customer activity must be monitored against a pre-determined profile on ongoing basis, paying special attention to higher risk customers or activities, furthermore, to take prompt action when there is

material departure from usual and expected activity through regular matching with information already available with bank.

- To apply appropriate CDD measures for walk-in customers including cash deposits, withdrawals, online transfers and remittances while ensuring compliance of regulatory guidelines.
- In the case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them were individual customers of the bank
- All new relationships should be filtered through automated solution for possible name matching with individuals / entities appearing on various negative lists maintained by the bank. In case of exact match, relationship should be terminated, besides reporting to concerned authorities.
- Physical verification of Sole proprietorship/Self employed/ Individual business in case of unsatisfactory verification matter should be referred to AML Unit, HOK
- Prior approval of Regulatory Operations and compliance department, Global Compliance (ROCD-GC) is to be obtained for opening of any account related to NGOs/NPOs/Trust/ Foundation /Religious entities and Charities account.

Basic Concept Of Risk Based Approach

Keeping in view of growing sensitivities on domestic and international front, there is need to focus on the areas where related risks are relatively high in order to allocate resources in the most effective way. Therefore, based on SBP guidelines and international best practices on AML/CFT risk management, bank is fully committed to develop on ongoing basis necessary internal policies, procedures and risk parameters to ensure alignment with regulatory frame work and best practices in this regard.

In view of above, following guidelines on enhanced due diligence (EDD) and Simplified Due diligence (SDD) shall be observed as per circumstances of the case.

3.3 ENHANCED DUE DILIGENCE (EDD)

Enhanced due diligence (EDD) is a process of “digging deep” into a high risk customer / transaction. It’s a process of applying measures that are over and above the standard (KYC) procedures already in place and are effective and commensurate to the level of risks.

Following EDD measures shall be applied as per applicability on different high risk elements/scenarios:

- Obtaining additional information on the customer (occupation, volume of assets, address, information available through public databases, internet, etc);
- Reducing interval for updating and reviewing customer risk profile; including updating the identification data of customer and beneficial owner;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining additional information on the sources of funds or sources of wealth of the customer;
- Obtaining the approvals of senior management to commence or continue the business relationship;

- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
- A signatory who is neither a beneficial owner nor a key principal may also be verified if they were the principal contact with the bank acting on behalf of directors or owners with whom the bank had little or no direct contact; and
- Documentary evidence may be sought to support transaction where possible, e.g. purchase of property etc.

3.4 SIMPLIFIED DUE DILIGENCE (SDD)

There may be circumstances where the risk of money laundering or financing of terrorism may be low, for example where information on the identity of the customer and the beneficial ownership is publicly available and/or the turnover in the account is meager . In such circumstances, and provided there has been an adequate analysis of the risk by the banks/DFI, SDD measures may be applied.

Following low risk scenarios/factors shall be considered for SDD:

- Basic Banking Accounts (BBA);
- Low value accounts having monthly credit turnover up to Rs. 25,000;
- Salary accounts of individuals subject to the condition that account is not used for other than salary purposes;
- Pension accounts for direct credit of pensions;
- Remittance cards restricted to receive inward remittances only; and
- Other financial products or services that provide appropriately defined and limited services to certain types of customers so as to increase access to financial services.

SDD measures shall include:

- Decreasing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable monetary threshold; and
- Not collecting specific information (no exemption shall be presumed in respect of minimum documents prescribed in 'Annexure-I' of AML/CFT Regulations) or carrying out specific measures to understand the purpose and intended nature of the business relationship, but intended purpose and nature of account may be ascertained from the relationship established or from the type of transactions.

SDD measures should not be considered in following situations:

- When there is a suspicion of money laundering or financing of terrorism;
- There are no exceptions in reporting suspicion to FMU within the provisions of AML Act.

3.5 AML/ CDD/CFT ASSOCIATED POLICIES

Following associated policies form an integral part of the AML/CDD/CFT Policy and have been developed specifically to achieve the objectives outlined in the Bank's Policy and the regulatory requirements of the State Bank of Pakistan/Financial Monitoring Unit.

3.5.1 Internal control Compliance and Audit

It is a Policy of the Bank:

- To design and implement processes, systems, and controls to comply with all applicable AML/CFT laws and regulations.
- To conduct risk assessment and develop risk profiles of the Bank's customers, products & services and to apply appropriate policies and procedures to manage such risks.
- To undertake enhanced due diligence for 'High Risk' customers.
- AML/CFT policy duly approved by their Board of Directors shall be circulated down the line to each and every business location and concerned employees for meticulous compliance. The detailed procedures and controls shall be developed by banks in the light of policy approved by the Board.

  To conduct risk assessment and develop risk profile of the bank's customer, product & services and apply appropriate policies and procedure to manage such risk. Risk profiling of customer shall be based on various factors including customer, product and services, delivery channel and geography.

3.5.2 Recognition and reporting of suspicion

It is a Policy of the Bank:

- To establish and follow procedures that requires employees to refer promptly any suspicious activity to Global Compliance or respective country MLRO for further review and to determine whether STR should be filed with the Regulators.
- To report all cash transactions exceeding Rs. 2.5 M to the Financial Monitoring Unit (FMU) in a manner as prescribed by the Regulator. For overseas locations, the limit may be set as per the requirement set by local regulators.
- To remain vigilant on unusual or suspicious transactions or other activities that appear not to make good business or economic sense, or activities that appear to be inconsistent with the given profile of the customer, including activities that may be indicative of criminal conduct, terrorism or corruption.
- To act competently and honestly while assessing information and circumstances that might give reasonable grounds to suspect ML or TF.

- To provide Global Compliance or respective country MLRO at his/her request with access to all customer, correspondent or counterparty information that are within the possession of the bank.
- To co-operate with law enforcement authorities in investigations concerning possible ML or TF within the confines of applicable laws, and in consultation with Global Compliance or respective country MLRO.
- Not to alert or provide any information to any person regarding suspicion or inquiry on his or her account or transactional activities or any indication of being reported to the Regulators.
- To comply with the provisions of AML Act, rules and regulations issued there under for transactions/currency transactions in the context of money laundering or financing of terrorism.
- To establish criteria in their AML/CFT procedures for management of alerts arising from automated transaction monitoring systems.
- To pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The back ground and purpose of such transactions shall, as far as possible, be examined, the findings established in writing, and be available to assist the relevant authorities in inspection and investigation.
- The 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, shall be viewed with suspicion, be properly investigated and to be considered for possible reporting to FMU under AML Act.
- To report attempted transactions regardless of the amount. AML/CFT procedural document shall provide guidelines on reporting of attempted transactions.
- The employees of the banks are strictly prohibited to disclose 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.

3.5.3 Awareness raising and training

It is a Policy of the Bank:

- To make all management and staff aware of what is expected of them to prevent money laundering or terrorist financing and to advise them of the consequences for them and for the Bank if they fall short of that expectation.
- To chalk out and implement suitable training program for relevant employees through L& D, in order to effectively implement the regulatory requirements and banks own policies and procedures relating to AML/ CFT. Furthermore, Management shall pay special attention on comprehensive AML/CFT Computer-based/online Training Programs and Tests to meet training and development need of relevant bank's staff.
- That Management and staff are required to sign a memorandum confirming they have read and understood the Bank's AML/CDD/CFT policy and relevant procedures. Changes made on set frequencies or on adhoc basis to this policy should also be communicated to the staff

3.5.4 Record keeping

It is a Policy of the Bank:

- To retain identification and transaction documentation for the minimum period as required by applicable Laws and Regulations.
- The transactions records may be maintained in paper or electronic form or on microfilm, provided it is admissible as evidence in a court of law.

- To retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority. All such record shall be destroyed after approval of Head Office.
- To be in a position to retrieve, in a timely fashion, records that are required by law enforcement agencies as part of their investigations.
- To keep records of AML/CDD/CFT training provided to the employees, nature of the training and the names of staff who received such training.

3.5.5 Bank's' policy on politically exposed persons (PEPs)

Definition

PEPs are individuals who are or have been entrusted with prominent public functions in a country, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials. Senior executives of state owned corporations, important political party officials, business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. PEPs include the following:

- Current and Ex-Head & Deputy head of state or National Government (President, Prime Minister, Government Ministers, Provincial Governors, Cabinet Members their Deputies (assistants), Senior Ministerial staff, and Secretaries.
- Current and ex-Members of National and Provincial Assemblies and Senate.
- Senior Civil Servants including Senior Government Officials, Heads of Government Departments, Police Service etc
- Senior Judicial & Military officials,
- Senior Executives of state-owned Corporations,
- Influential Religious leaders of National / International repute
- High ranking Officers in Diplomatic Service (Ambassadors, High Commissioners, Envoys, Attachés, Consul Generals, Consuls, Honorary Consuls, Counselors etc)
- Senior Political Party Officials and functionaries such as Leader, Chairman, Deputy leader, Secretary General, and Executive Committee or any other Senior ranks in party (does not include middle ranking or more junior individuals)
- Close family members of PEPs includes: Spouses, children, parents, siblings and may also include other blood relatives and relatives by marriage.
- Closely associated persons includes: Close business colleagues and personal Advisors/ Consultants to the politically exposed person as well as persons who are expected to benefit significantly by being close to such a person.

Relationships with PEPs shall be established with the prior approval of respective Functional Business Heads and Global Compliance / MLRO.

Branches are required to conduct enhanced due diligence of close family members / closely associated persons of politically exposed persons in line with the afore-mentioned policy references.

Policy Rationale

PEPs and related individuals can pose unique reputation and other risks, in particular:

- Some corrupt PEPs around the globe have used traditional banking products and services as safe havens for misuse of funds, illegal activities and associated practices, including money laundering;
- PEPs enjoy prominence and are therefore under continuous public spotlight. Their financial affairs are highly magnified and could easily trigger adverse publicity and franchise risks for the Bank;
- There is a growing attention worldwide to the misuse of public funds and increased reaction against corruption at high government levels;
- There is increasing responsibility and liability for banks and bank personnel to undertake due diligence for establishing source of wealth and investigate fund flows of PEPs.

It is a Policy of the Bank:

- That relationships with PEPs should be established with the prior approval of respective business Heads & Global Compliance/MLRO
- All such relationships should be classified under High Risk category for effective monitoring through automated AML solutions used by the bank

3.5.6 Bank's' policy on Correspondent Relationships / MSBs

It is a Policy of the Bank:

- To obtain sufficient information about correspondent banks/MSBs to understand the nature of their business & activities
- To determine from available sources the reputation of the respondent bank and, as far as practicable, the 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;
- To assess the respondent bank's AML/CFT systems and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates;
- To Clearly understand and document the respective AML/CFT responsibilities of each bank;

- Special attention shall be paid when establishing or continuing correspondent relationship with banks/ financial institutions which are located in jurisdictions that have been identified or called for by FATF for inadequate and poor AML/CFT standards in the fight against money laundering and financing of terrorism.

- Not enter into a relationship or continue correspondent banking relations with a shell bank and shall take appropriate measures when establishing correspondent banking relations, to satisfy them that their respondent banks do not permit their accounts to be used by shell banks.

- All FIs relationships are subject to prior approval from FID/ Global Compliance/MLRO

3.5.7 Wire Transfers/ Fund Transfers

Management shall clearly understand and implement regulatory requirements and responsibilities on wire transfers / funds transfers as ordering institute/remitter , beneficiary institute/beneficiary and intermediary institute and take appropriate measures to ensure implementation of the same in bank.

3.5.8 Prohibition for Using Personal Accounts for Business Purposes

Personal accounts shall not allow to be used for business purposes except proprietorships, small businesses and self employed 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 & nature of business of that customer.

3.5.9 Use of automated AML solutions

It is a Policy of the Bank:

- To make maximum use of technology and upgrade the systems and procedures in accordance with the upcoming challenges ML/TF
- To implement /use automated AML solutions across its network for effective transaction monitoring /real time filtering of payment instructions in line with the best industry practices.

3.6 NON COMPLIANCE WITH BANK'S AML/CDD/CFT POLICY

Failure to abide by the Policy set by the Bank to prevent money laundering and terrorist financing will be treated as a disciplinary issue. Any deliberate breach will be viewed as gross misconduct. Such cases will be referred to HR for onward initiation of disciplinary action that could lead to termination of employment and could also result in criminal prosecution and imprisonment for the concerned staff member.

3.7 ACCOUNTABILITIES AND RESPONSIBILITIES

3.7.1 The Board is Responsible for:

- Ensuring that adequate systems and controls are in place to deter and recognize criminal activity, money laundering and terrorist financing.
- Seeking compliance reports through BAC from the CCO (including coverage of AML/CFT issues) on quarterly basis and taking necessary decisions required to protect the bank from use by criminals for ML & TF activities.
- Approval of appropriate policies on AML/CFT on recommendations of senior management along with periodic review of the same for necessary updation etc.

3.7.2 Management is Responsible for:

- Ensuring that AML/CDD/CFT policy is implemented in letter and spirit.
- Ensuring that Global Compliance and respective country MLROs are promptly advised where there are reasonable grounds to know or suspect that transactions or instructions are linked to criminal conduct, money laundering or terrorist financing.
- Ensuring that Global Compliance and respective country MLROs are provided with all relevant information to carry out complete assessment of underlying transaction.
- Ensuring that CDD and EDD is being carried out as per bank's policy and regulatory requirements

  (a) At the time of establishing business relationship;

  (b) conducting occasional transactions above rupees one million whether carried out in a single operation or in multiple operations that appear to be linked;

  (c) carrying out occasional wire transfers (domestic / cross border) regardless of any threshold;

  (d) there is suspicion of money laundering / terrorist financing; and

  (e) there is a doubt about the veracity or adequacy of available identification data on the customer
- Ensuring that EDD is being carried out for high risk relationships and following minimum steps are taken:
  - Approval of all high risk relationships are obtained as required
  - Names of prospective customers are filtered through automated solution for possible name matching with individuals / entities appearing on various negative lists maintained by the bank. In case of an exact match, relationship should be discontinued.
  - Additional documentations as appropriate besides the minimum required documents
- Ensuring that Global Compliance and respective country MLROs are provided with adequate resources to carry out their duties effectively.

3.7.3 Global Compliance / MLRO are Responsible for:

- Developing and maintaining policy in line with evolving statutory and regulatory obligations.
- Making use of technology and upgrading Bank's systems and procedures in accordance with the changing compliance risks.
- Undertaking the required money laundering /terrorist financing risk assessment for customers, products or services.
- Developing and ensuring that the internal procedures remain up-dated at all times.
- Monitoring and Identifying transactions of suspicious nature and reporting to the Regulators in a timely manner.
- Ensuring that staff is aware of their personal obligations and adequately trained in prevention of ML/TF.
- Representing the Bank to all external agencies and any other third party enquiries in relation to money laundering prevention, investigation or compliance.
- Preparing quarterly reports on AML compliance for onward submission to the Board Audit Committee.
- Ensuring that all employees sign-off an undertaking confirming having read and understood Bank's policy on AML/CDD/CFT.
- Responding promptly to any request for information made by the Regulators or law enforcement agencies.
- Take appropriate action against the staff found involved in any of such activities that comes under the domain of AML / CFT

3.7.4 All Employees are Responsible for:

- Remaining vigilant to the possibility of money laundering / terrorist financing through use of bank's products and services.
- Complying with all AML/CFT policies and procedures in respect of customer identification, account monitoring, record keeping and reporting.
- Promptly reporting to Global Compliance or respective country MLRO where they have knowledge or grounds to suspect a criminal activity or where they have suspicion of money laundering or terrorist financing whether or not they are engaged in AML / CFT monitoring activities.
- Ensuring that the customer is not disclosed any information related to inquiry or filing of a suspicious activity report (STRs) or Cash Transactions Report (CTRs)
- Understanding Bank's Policy and Procedures on AML/CDD/CFT and to sign-off on the required Form.
- Employees who violate any of the Regulations or the Bank's AML/CDD/CFT policies and procedures will be subject to disciplinary action.