ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) REGULATIONS

Course designed by
Training & Organization Development Division
in consultation with
Compliance Group

June, 2015

Reference & effective date

BPRD Circular No. 02 of 2012 September 13, 2012

These regulations will take effect from October 31, 2012.

Banks/DFIs may align their AML/CFT risk assessment procedures in accordance with aforesaid Guidelines within six months from issuance of this circular.

ACRONYMS

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
ARC	Aliens Registration Card
CNIC	Computerized National Identity Card
CRP	Customer Risk Profiling
CTR	Currency Transaction Report
DDs	Demand Drafts
DFI	Development Finance Institution
EDD	Enhanced Due Diligence

ACRONYMS

FATF	Financial Action Task Force
FI	Financial Institution
FMU	Financial Monitoring Unit
FT	Financing of Terrorism
KYC/CDD	Know Your Customer/ Customer Due Diligence
ML	Money Laundering
MTs	Mail Transfers

ACRONYMS

NADRA	National Database & Registration Authority
NARA	National Aliens Registration Authority
NGOs/NPOs	Non-governmental Organizations or Non-profit Organizations
NICOP	National Identity Card for Overseas Pakistanis
NTN	National Tax Number
PEP	Politically Exposed Person

ACRONYMS

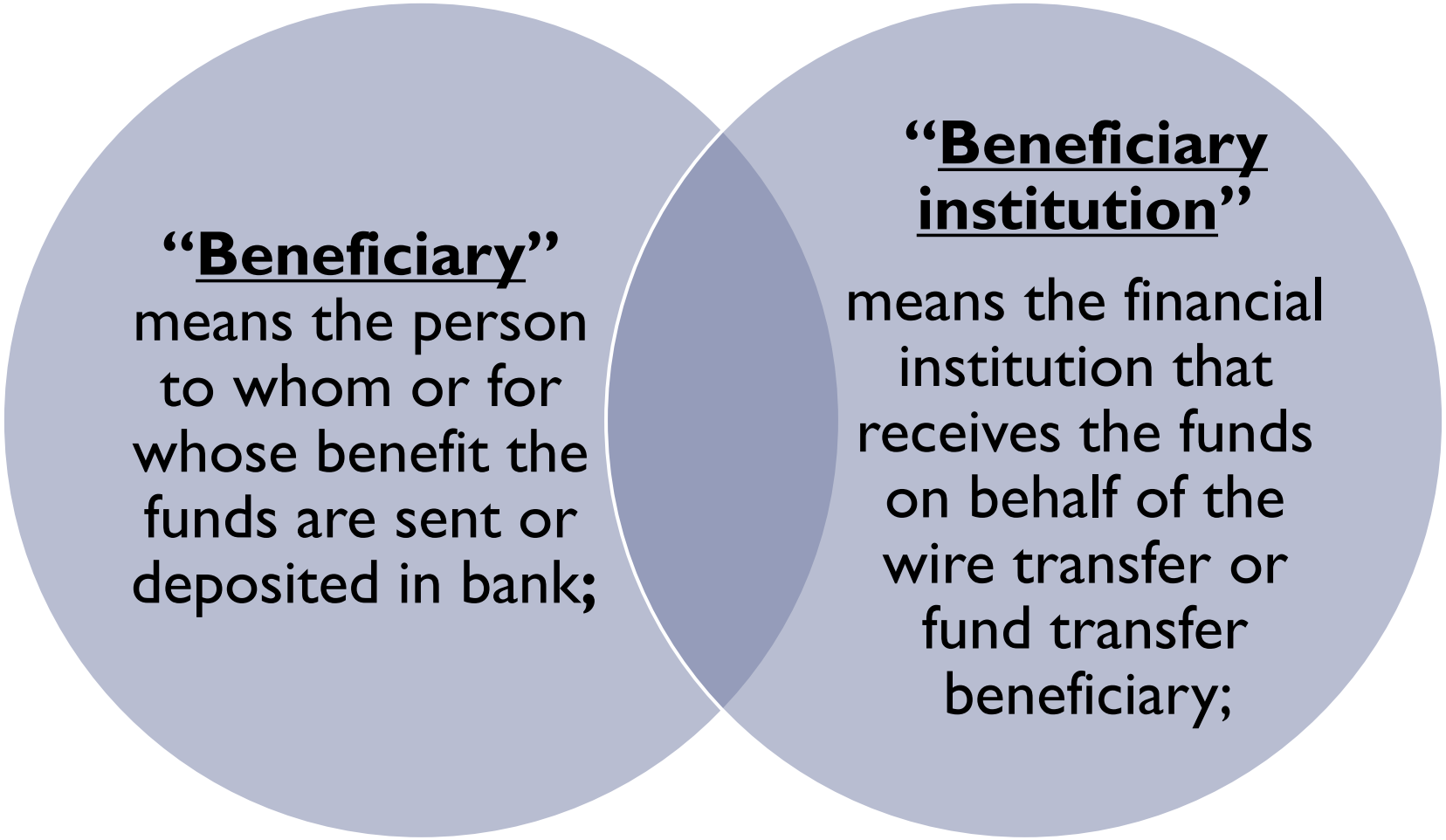
POs	Payment Orders
POC	Pakistan Origin Card
RBA	Risk Based Approach
SBP	State Bank of Pakistan
SDD	Simplified Due Diligence
SECP	Securities & Exchange Commission of Pakistan
STR	Suspicious Transaction Report
TMS	Transaction Monitoring System

CONTENTS

STAGE - I
DEFINITIONS

"<u>Beneficial owner</u>"
in relation to a customer of a bank/DFI, means the natural person(s) who ultimately own(s) or controls a customer or the person on whose behalf a transaction is being conducted and includes the person(s) who exercise(s) ultimate effective control over a person or a body of persons whether incorporated or not;

STAGE - I
DEFINITIONS



STAGE - I
DEFINITIONS

- **"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;
- **"Correspondent bank"** means the bank in Pakistan which provides correspondent banking services to bank or financial institution situated abroad and vice versa**;**

STAGE - I
DEFINITIONS

- **"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.
- **"Cross-border wire transfer"** means a wire transfer where the ordering institution and the beneficiary institution are located in different countries or jurisdictions;
- **"Currency Transaction Report or CTR"**

  as defined under AML Act;

STAGE - I
DEFINITIONS

- **"Customer"** means a person having relationship with the bank which includes but not limited to holding of deposit/deposit certificate/ or any instrument representing deposit/placing of money with a Bank/DFI, availing other financial services, locker facility, safe deposit facility, or custodial services from the Bank/DFI**;**
- **"Customer due diligence or CDD"** in broader terms includes**;**
  a) 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;

STAGE - I
DEFINITIONS

b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, to verify his identity so that the Bank/DFI is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement;

c) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

STAGE - I
DEFINITIONS

d) monitoring of accounts/transactions on an ongoing basis to ensure that the transactions being conducted are consistent with the Banks/DFIs knowledge of the customer, their business and risk profiles, including, where necessary, the source of funds and updating records and data/ information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with Bank/DFI.

STAGE - I
DEFINITIONS

- **"Domestic wire transfer"** means any wire transfer where the originator and beneficiary institutions are located in Pakistan regardless the system used to effect such wire transfer is located in another jurisdiction;
- **"Dormant or in-operative account"** means the account in which no transaction has been taken place for the last one year;
- **"FATF Recommendations"** means recommendations of Financial Action Task Force as amended from time to time;
- **"FMU"** means Financial Monitoring Unit established under the AML Act;

STAGE - I
DEFINITIONS

- "**Fund transfer/wire transfer**" means any transaction carried out by financial institution 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;
- "**Government entity**" means federal or provincial government, a ministry within such a government, a local government or an agency specially established by any such government, or a department, organization or corporation owned or controlled by such government under federal, provincial or local law;

STAGE - I
DEFINITIONS

- **"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;
- **"Monetary threshold"** expressed in Pak rupee includes a reference to the equivalent amount expressed in any other currency;
- **"Money laundering and financing of terrorism or ML/TF"** has the same meaning as ascribed to them in AML Act;
- **"Occasional customer" or "walk-in-customer"** means the person conducting occasional transactions and is not a customer; having relationship with the Bank/DFI;

STAGE - I
DEFINITIONS

- **"Occasional transaction" or "walk-in-transaction"** means a transaction carried by or on behalf of a person who is not a customer; having relationship with the Bank/DFI**;**
- **"Online transaction"** means deposit or withdrawal of cash using different branches of a bank through electronic means**;**
- **"Ordering institution"** means the financial institution that initiates a wire transfer on the instructions of the wire transfer originator in transferring the funds**;**
- **"Originator"** means the person who allows or places the order to initiate a fund transfer/wire transfer or an online transaction**;**

STAGE - I
DEFINITIONS

- **"Payable-through account"** means an account maintained at the correspondent bank by the respondent bank which is accessible directly by a third party to effect transactions on its own (respondent bank's) behalf**;**
- **"Person"** has the same meaning as ascribed to it under the AML Act, 2010**;**
- **"Politically exposed persons or PEPs"** are individuals who are entrusted with prominent public functions either domestically or by a foreign country, or in an international organization, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations/departments/autonomous bodies. This does not intend to cover middle ranking or more junior individuals in the foregoing categories;

STAGE - I
DEFINITIONS

- **"Respondent bank"** means the bank or financial institution outside Pakistan to whom correspondent banking services in Pakistan are provided and vice versa**;**
- **"Risk"** refers to risk associated with money laundering and financing of terrorism;
- **"Senior management"** means the officer(s) not below the rank of Executive Vice President as designated by the Board of a Bank/DFI for the purpose of AML/CFT regulations**;**

STAGE - I
DEFINITIONS

- **"Shell bank"** means a bank that has no physical presence (mind and management), in the country in which it is incorporated and licensed and/or which is not affiliated with a regulated financial services group that is subject to effective consolidated supervision; and
- **"Suspicious transaction report or STR"** As defined under AML Act.

STAGE - II
REGULATIONS

REGULATION - 1
CUSTOMER DUE DILIGENCE (CDD)

When CDD measures are to be applied ?

1. Banks/DFIs shall apply CDD measures;
    a. when establishing business relationship;
    b. while dealing with occasional customers/ walk-in customers;
    c. in other situations/scenarios when there is suspicion of money laundering/financing of terrorism, regardless of threshold.

STAGE - II
REGULATIONS

a. CDD Measures for Establishing Business Relationship

Identification of Customers:

Every customer shall be identified for establishing business relationship. For this purpose, details of documents required for opening of accounts of different categories is included in **Stage III** course material.

STAGE - II
REGULATIONS

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

i. Full name as per identity document;
ii. CNIC/Passport/NICOP/POC/ARC number or where the customer is not a natural person, the registration/ incorporation number or business registration number (as applicable);
iii. Existing residential address, registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable);
iv. Date of birth, incorporation or registration (as applicable);

STAGE - II
REGULATIONS

v. Nationality or place of birth, incorporation or registration (as applicable);
vi. Nature of business, geographies involved and expected type of counter-parties (as applicable);
vii. Purpose of account;
viii. Type of account;
ix. Source of earnings;
x. Expected monthly credit turnover (amount and No. of transactions); and
xi. Normal or expected modes of transactions.

STAGE - II
REGULATIONS

Verification of Identity:

- The Bank/ DFI shall verify "identities of the customers (natural persons) and in case of legal persons, identities of their natural persons from relevant authorities or where necessary" using other reliable, independent sources and retain on record copies of all reference documents used for identification and verification.

- The verification shall be the responsibility of concerned Bank/DFI for which the customer should neither be obligated nor the cost of such verification be passed on to the customers.

STAGE - II
REGULATIONS

Identification and Verification of Natural Persons Acting on Behalf of Customer:

- In relation to above, where one or more natural persons are acting on behalf of a customer or where customer is legal person, Bank/ DFI shall identify the natural persons who act on behalf of the customer and verify the identity of such persons.

- Authority of such person to act on behalf of the customer shall be verified through documentary evidence including specimen signature of the persons so authorized.

STAGE - II
REGULATIONS

Identification and Verification of Identity of Beneficial Owners :

- In case of beneficial owner(s) in relation to a customer, reasonable measures shall be taken to obtain information to identify and verify the identities of the beneficial owner(s).

Where the customer is not a natural person, the Bank/DFI shall

i. take reasonable measures to understand the ownership and control structure of the customer for obtaining information required under the subsequent para and;

ii. determine that the natural persons who ultimately own or control the customer.

STAGE - II
REGULATIONS

Information on the Purpose and Intended Nature of Business Relations :

- Banks/ DFIs shall obtain from customers information as to the purpose and intended nature of business relations.

Timing of Verification :

- Verification of the identity of the customers and beneficial owners shall be completed before business relations are established including verification of CNIC/NICOP/POC from NADRA wherever required for customers under these regulations.

STAGE - II
REGULATIONS

In exceptional cases, banks/ DFIs may allow business relationship without prior verification if the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations and the risks can be effectively managed.

STAGE - II
REGULATIONS

In relation to the above para, Banks/DFIs shall define criteria in their AML/CFT Policies clearly specifying the circumstances, authority levels and types of customers where such deferral will be allowed. In this regard, following should also be observed :

i. Verification shall be completed as soon as it is reasonably practicable but not later than 5 business days from the date of opening of the account.

ii. No debit will be allowed or cheque book is issued until positive verification is completed.

iii. Half yearly list is to be maintained by banks/DFIs highlighting all accounts/deposits where the business relationship needed to be closed on account of negative verification.

STAGE - II
REGULATIONS

b. CCD Measures for Occasional Customers/ Walk-in Customers and Online Transactions

Banks/DFIs shall;

1. in case of occasional customers/walk-in- customers :
   - obtain copy of CNIC while conducting cash transactions above rupees 0.5 million; and
   - obtain copy of CNIC while issuing remittance instruments e.g. POs, DDs and MTs etc.
   - obtain copy of CNIC (regardless of threshold) while conducting online transactions by occasional customers/walk-in-customers (except deposits through Cash Deposit Machines or cash collection/management services).

STAGE - II
REGULATIONS

- If transaction exceeds Rs. 100,000 the name and CNIC No. shall be captured in system and made accessible along with transaction details at beneficiary's branch.

STAGE - II
REGULATIONS

c. in other situations/scenarios when there is suspicion of money laundering/financing of terrorism, regardless of threshold

Where CDD Measures are Not Completed :

- In case banks/ DFIs are not able to satisfactorily complete required CDD measures, account shall not be opened or any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR.
- If CDD of an existing customer is found unsatisfactory, the relationship should be treated as high risk and reporting of suspicious transaction be considered as per law and circumstances of the case.

STAGE - II
REGULATIONS

- **Ongoing Monitoring :**
  - ✓ All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the bank/ DFI's knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.
  - ✓ Banks/DFIs 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.

STAGE - II
REGULATIONS

- ✓ Banks/ DFIs shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers. The review period and procedures thereof should be defined by Banks/DFIs in their AML/CFT policies, as per risk based approach.
- ✓ In relation to above Para, customers' profiles should be revised keeping in view the spirit of KYC/CDD and basis of revision shall be documented and customers may be consulted, if necessary.

STAGE - II
REGULATIONS

- **Anonymous or Fictitious Accounts :**

✓ Banks/DFIs shall not open or maintain anonymous accounts or accounts in the name of fictitious persons or numbered accounts.

- **Review of Products and services :**

✓ Banks/DFIs shall establish criteria for 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 an on-going basis.

- **Joint Accounts :**

✓ 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/DFI.

STAGE - II
REGULATIONS

- **Government Accounts :**

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

STAGE - II
REGULATIONS

However, in case of **autonomous entities and Armed Forces including their allied offices**, banks/DFIs may open bank accounts on the basis of **special resolution/ authority from the concerned administrative department or highest executive committee/ management committee of that entity duly endorsed by their respective unit of finance**.

The banks/DFIs shall also take into account any rules, regulations or procedures prescribed in the governing laws of such entities relating to opening and maintaining of their bank accounts.

STAGE - II
REGULATIONS

- **Existing Customers :**
  - ✓ A Bank/DFI shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk but without compromise on identity and verification requirements.
  - ✓ For existing customers who opened accounts with old NICs, banks/DFIs shall ensure that attested copies of CNICs shall be present in bank's/DFI's record. Banks/DFIs shall block accounts without CNIC (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 attested copy of CNIC and verification of the same from NADRA

STAGE - II
REGULATIONS

- ✓ Banks/ DFIs shall not provide any banking services to proscribed entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

- ✓ The banks/DFIs should monitor their relationships on a continuous basis and ensure that no such relationship exists. If any such relationship is found, the same should be immediately reported to Financial Monitoring Unit (FMU) and other actions shall be taken as per law.

STAGE - II
REGULATIONS

Dormant accounts :

- For customers whose accounts are dormant or in-operative, bank/DFIs may allow credit entries without changing at their own, the dormancy status of such accounts. Debit transactions/ withdrawals shall not be allowed until the account holder requests for activation and produces attested copy of his/her CNIC if already not available and bank/DFI is satisfied with CDD of the customer.

- In relation to the above paras, it may be noted that 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.

STAGE - II
REGULATIONS

- **Prohibition of personal accounts for business purposes :**
  - ✓ Banks/DFIs 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 Banks/DFIs are 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.

STAGE - II
REGULATIONS

- **Politically Exposed Persons (PEPs)**

In relation to PEPs and their close associates or family members, banks/DFIs shall:

- ✓ implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP;
- ✓ obtain approval from the bank's senior management to establish or continue business relations where the customer or a beneficial owner is a PEP or subsequently becomes a PEP;
- ✓ establish, by appropriate means, the sources of wealth or beneficial ownership of funds; as appropriate; including bank/DFI's own assessment to this effect; and
- ✓ conduct during the course of business relations, enhanced monitoring of business relations with the customer.

STAGE - II
REGULATIONS

- **NGOs/NPOs/ Charities' accounts**

  - ✓ Banks/DFIs should conduct enhanced due diligence (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 commensurate with the stated objectives and purposes.
  - ✓ The accounts should be opened in the name of relevant NGO/NPO as per title given in its constituent documents of the entity. The individuals who are authorized to operate these accounts and members of their governing body should also be subject to comprehensive CDD. Banks/DFIs should ensure that these persons are not affiliated with any proscribed entity, whether under the same name or a different name.

STAGE - II
REGULATIONS

- ✓ In case of advertisements through newspapers or any other medium, especially when bank account number is mentioned for donations, Banks/DFIs will ensure that the title of the account is the same as that of the entity soliciting donations. In case of any difference, immediate caution should be marked on such accounts and the matter should be considered for filing STR.
- ✓ Personal accounts shall not be allowed to be used for charity purposes/collection of donations.

STAGE - II
REGULATIONS

- All existing relationships of NGOs/NPOs/Charities should 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 entities and persons, whether under the same name or a different name. In case of any positive match, Banks/ DFIs should consider filing STR and/or take other actions as per law.

STAGE - II
REGULATIONS

REGULATION - 2
CORRESPONDENT BANKING

- ✓ In addition to measures required under Regulation 1 (as deemed necessary by the Bank/DFI), Banks/ DFIs shall take the following measures for providing correspondent banking services :

STAGE - II
REGULATIONS

1. assess the suitability of the respondent bank by taking the following steps:

   a. gather adequate information about the respondent bank to understand fully the nature of the respondent bank's business, including 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.

STAGE - II
REGULATIONS

- ✓ Money laundering prevention and detection measures.
- ✓ The purpose of the account or service.
- ✓ The identity of any third party that will use the correspondent banking services (i.e. in case of payable through accounts).
- ✓ Condition of the bank regulation and supervision in the respondent's country.
- ✓ determine from any 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; and
- ✓ assess the respondent bank in the context of sanctions/embargoes and Advisories about risks;

STAGE - II
REGULATIONS

b. clearly understand and document the respective AML/CFT responsibilities of each bank; and

c. obtain approval of senior management, before establishing new correspondent banking relationship.

STAGE - II
REGULATIONS

2. Where the cross-border banking services involve a payable-through account, the correspondent bank shall be satisfied that :

   a. the respondent bank has performed appropriate CDD measures at least equivalent to those specified in Regulation I on the third party having direct access to the payable-through account; and

   b. the respondent bank is able to perform ongoing monitoring of its business relations with third party and is willing and able to provide customer identification information to the correspondent Bank/ DFI upon request.

STAGE - II
REGULATIONS

3. Banks/DFIs shall pay special attention 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.

4. No Bank/ DFI shall enter into 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.

STAGE - II
REGULATIONS

5. In case where a Pakistani bank/DFI is availing correspondent banking services from a bank/financial institution abroad, the CDD measures specified under Para 1(a), 1(b) 1(c), 3 and 4 above should be applied, as considered necessary to mitigate ML/TF risks.

STAGE - II
REGULATIONS

REGULATION - 3

WIRE TRANSFERS/ FUND TRANSFERS

1. The requirement under this Regulation shall apply to a Bank/ DFI during the course of sending or receiving funds by wire transfer except transfer and settlement between the banks where both the banks are acting on their own behalf as originator and the beneficiary of the wire transfer;

STAGE - II
REGULATIONS

2. Responsibility of the Ordering Institution :

   Bank/DFI as ordering institution (whether domestic or cross border wire transfer and regardless of threshold) shall;

   a. identify and verify the originator (if it has not already done under Regulation 1); and obtain details of beneficial owner(s) of funds; and

   b. 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.

STAGE - II
REGULATIONS

3. Bank/DFI shall include the following information in the message or payment instruction which should accompany or remain with the wire transfer throughout the payment chain:

   a. the name of the originator;

   b. the originator's account number (or unique reference number which permits traceability of the transaction); and

   c. the originator's address or CNIC/passport number;

STAGE - II
REGULATIONS

4. Responsibility of the Beneficiary Institution

- ✓ Beneficiary institution shall adopt risk-based internal policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator information. The incomplete originator information may be considered as a factor in assessing whether the transaction is suspicious and whether it merits reporting to FMU or termination thereof is necessary.
- ✓ Banks/ DFIs shall remain cautious when entering into relationship or transactions with institutions which do not comply with the standard requirements set out for wire transfers by limiting or even terminating business relationship.

STAGE - II
REGULATIONS

5. Responsibility of Intermediary Institution

- ✓ A bank/DFI that is an intermediary institution shall, in passing onward the message or payment instruction, maintain all the required originator information with the wire transfer.
- ✓ In the context of Regulation-3 (Wire Transfers/ Fund Transfers), it is clarified that the requirements may not apply to domestic fund transfer transactions through e-banking channels (e.g. ATM, internet banking & mobile banking etc) and RTGS provided bank/DFI has put in place appropriate controls. (Annexure to BPRD Circular Letter No. 22 of 2013)

STAGE - II
REGULATIONS

REGULATION - 4

REPORTING OF TRANSACTIONS (STRs/CTRs)

1. Banks/ DFIs shall comply with the provisions of AML Act, rules and regulations issued thereunder for reporting suspicious transactions/currency transactions in the context of money laundering or financing of terrorism.

2. Banks/DFIs shall implement appropriate internal policies, procedures and controls for meeting their obligations under AML Act.

STAGE - II
REGULATIONS

3. Banks/ DFIs shall 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.
4. Examples and characteristics of some suspicious transactions (Red Alerts) that may be a cause for increased scrutiny for AML/CFT purposes are listed in Stage III reading material.

STAGE - II
REGULATIONS

5. Banks/DFIs are advised to make use of technology and upgrade their systems and procedures in accordance with the changing profile of various risks. Accordingly, all Banks/DFIs are advised to implement 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. Further, Banks/DFIs shall establish criteria in their AML/CFT Policies and/or Procedures for management of such alerts.

6. 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 referred to Compliance Officer for possible reporting to FMU under AML Act.

STAGE - II
REGULATIONS

7. Banks/ DFIs should note that STRs, including attempted transactions, should be reported regardless of the amount of the transactions; and, the CTRs should be reported above the threshold of Rs. 2.0 million as per requirements of AML, Act.
8. The basis of deciding whether an STR is being filed or not shall be documented and kept 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.
9. Banks/ DFIs, without disclosing the contents of STRs, shall intimate to State Bank of Pakistan on bi-annual basis the number of STRs reported to FMU.

   The status report (indicating No. of STRs only) shall reach to Director, BPRD within seven days of close of each half year.

STAGE - II
REGULATIONS

10. The employees of the Banks/ DFIs 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. This shall be made part of Code of Ethics to be signed by employees and Directors of the Bank/DFI.

STAGE - II
REGULATIONS

REGULATION - 5
RECORD KEEPING

1. Banks/ DFIs shall maintain all necessary 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 large transactions) for a minimum period of ten years from completion of the transaction.

STAGE - II
REGULATIONS

2. The records 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 for prosecution of criminal activity. 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.

STAGE - II
REGULATIONS

3. The records of identification data obtained through CDD process like 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 minimum period of ten years after the business relationship is ended. The identification records may be maintained in document as originals or copies subject to bank's attestation.

4. Banks/DFIs shall, however, retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority.

5. Banks/ DFIs shall satisfy, on timely basis, any enquiry or order from the relevant competent authorities including law enforcement agencies and FMU for supply of information and records as per law.

STAGE - II
REGULATIONS

REGULATION - 6

INTERNAL CONTROLS, POLICIES, COMPLIANCE, AUDIT AND TRAINING

1. Bank/DFIs own AML/CFT policies, procedures & controls :

- Each Bank/ DFI shall formulate its own AML/CFT policy duly approved by their Board of Directors and cascade the same down the line to each and every business location and concerned employees for strict compliance.
- The detailed procedures and controls shall be developed by banks/ DFIs in the light of policy approved by the Board.

STAGE - II
REGULATIONS

2. The policies, procedures and controls shall include, amongst other things, CDD measures, record retention, correspondent banking, handling wire transfers, risk assessment procedures, the detection of unusual and/or suspicious transactions and the obligation to report suspicious transaction etc.
3. In formulating policies, procedures and controls, banks/ DFIs shall take into consideration money laundering and financing of terrorism threats that may arise from the use of new or developing technologies, especially those having features of anonymity or inconsistency with the spirit of CDD measures.

STAGE - II
REGULATIONS

4. Foreign Branches and Subsidiaries :

   Banks/ DFIs shall pay particular attention to their 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) and ensure that their AML/ CFT policy is observed by branches and subsidiaries in those countries.

5. Banks/ DFIs shall apply their AML/ CFT policies to all of their 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, bank/ DFI shall require their overseas branches or subsidiaries to apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

STAGE - II
REGULATIONS

6. Where the law of the host country conflicts with the AML/ CFT requirements of Pakistan so that the overseas branch or subsidiary is unable to fully observe the higher standards, the bank/ DFI through its head office shall report this to the State Bank of Pakistan and comply with such further directions as may be issued.

7. Compliance :

   Banks/ DFIs shall develop appropriate AML/CFT compliance program, including at least, the appointment of a management level officer as the compliance officer in line with Regulation G-1 (Para D) of Prudential Regulations on Corporate/ Commercial Banking as amended from to time.

STAGE - II
REGULATIONS

8. Banks/DFIs shall ensure that the compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they may require to discharge their functions.
9. Audit

   Banks/ DFIs shall maintain an independent audit function in line with Code of Corporate Governance that is adequately resourced and able to regularly assess the effectiveness of the bank's internal policies, procedures and controls, and its compliance with regulatory requirements.

STAGE - II
REGULATIONS

10. Employee Due Diligence :

The Banks/ DFIs shall develop and implement a comprehensive employee due diligence policy and procedure to be implemented/ carried out at the time of hiring all employees permanent, contractual, or through outsourcing. This shall include but not limited to verification of antecedents and screening procedures to verify that person being inducted/ hired has a clean history.

STAGE - II
REGULATIONS

11. Training :

Banks/ DFIs shall chalk out and implement suitable training program for relevant employees on annual basis, in order to effectively implement the regulatory requirements and banks'/DFIs' own policies and procedures relating to AML/ CFT. The employees training shall enable them to understand new developments, money laundering and financing of terrorism techniques, methods and trends. The training should also include their responsibilities relating to AML/CFT especially requirements relating to CDD and analysis of abnormal/out of pattern transactions and alerts generated thereof for possible reporting of suspicious transactions.

STAGE - II
REGULATIONS

12. Banks/ DFIs should note 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 periodic basis.

    The online trainings and AML/CFT Tests of varying nature are available in the market offering opportunity for Banks/DFIs to equip their staff with relevant skills as per respective roles and responsibilities within the institution.

STAGE - II
REGULATIONS

As the periodic training of the front end staff is crucial, which is the first point of contact with customer; Banks/DFIs shall either purchase or internally develop comprehensive AML/CFT Computer-based/online Training Programs and Tests under a comprehensive plan with clear timelines for its implementation.

STAGE - II
REGULATIONS

Bank`s Reference:

- Instruction Circular No 88/2012 dated October 08, 2012
- Instruction Circular No 93/2012 dated November 02, 2012
- Instruction Circular No 98/2012 dated November 20, 2012
- Instruction Circular No 102/2012 dated November 30, 2012
- Instruction Circular No 112/2012 dated December 11, 2012
- Instruction Circular No 29/2013 dated March 21, 2013
- Instruction Circular No 72/2013 dated July 08, 2013
- Instruction Circular No 113/2013 dated October 14, 2013

Stage III

Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

Documents/papers to be obtained

Sr. No	Type of Customers	Documents To be Obtained
1	Individuals	A photocopy of any one of the following valid identity documents; i. Computerized National Identity Card (CNIC) issued by NADRA ii. National Identity Card for Overseas Pakistani (NICOP) issued by NADRA iii. Pakistan Origin Card (POC) issued by NADRA iv. Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only) v. Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2	Sole Proprietors	i. Photocopy of identity document as per Sr. No. 1 above of the proprietor ii. Registration certificate for registered concerns iii. Sales tax registration or NTN, wherever applicable iv. Certificate or proof of membership of trade bodies etc. wherever applicable v. Declaration of sole proprietorship on business letter head vi. Account opening requisition on business letter head.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

Sr. No	Type of Customers	Documents To be Obtained
3	Partnership	i. Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories ii. Attested copy of 'Partnership Deed' duly signed by all partners of the firm iii. 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 iv. Authority letter from all partners, in original, authorizing the person(s) to operate firm's account.
4	Limited Companies/ Corporations	Certified copies from Company Secretary/Public Notary of: i. Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account ii. Memorandum and Articles of Association iii. Certificate of Incorporation iv. Certificate of Commencement of Business, wherever applicable v. Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account vi. List of Directors on 'Form-A/Form-B' issued under Companies Ordinance 1984, as applicable vii. Form-29, wherever applicable

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

Sr. No	Type of Customers	Documents To be Obtained
		viii. For individual (natural person) shareholders holding 5% or above stake in company/corporation, photocopies of identity document as per Sr. No. I ix. For legal persons holding shares equal to 5% or above, in addition to any other relevant document including certificate of incorporation, photocopies of identity document as per S. No. I above of their individual shareholders holding 5% or more stake.
5	Branch Office or Liaison Office of Foreign Companies	i. A copy of permission letter from relevant authority i-e Board of Investment ii. Photocopies of valid passports of all the signatories of account iii. List of directors on company letter head or prescribed format under relevant laws/regulations iv. A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account.
6	Trust, Clubs, Societies and Associations etc	i. Certified copies of • Certificate of Registration/Instrument of Trust • By-laws/Rules & Regulations ii. Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

Sr. No	Type of Customers	Documents To be Obtained
		iii. Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body
7	NGOs/NPOs/Charities	i. Certified copies of : a. Registration documents/certificate b. By-laws/Rules & Regulations ii. Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account iii. Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees/ Executive Committee, if it is ultimate governing body iv. Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

Sr. No	Type of Customers	Documents To be Obtained
8	Agents Accounts	i. Certified copy of 'Power of Attorney' or 'Agency Agreement' ii. Photocopy of identity document as per Sr. No. 1 above of the agent and principal iii. The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person.
9	Executors and Administrators	i. Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator ii. A certified copy of Letter of Administration or Probate.
10	Minor Accounts	i. Form-B, Birth Certificate or Student ID card (as appropriate) shall be obtained from minor ii. Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

Additional Guidelines:

1. The photocopies of identity documents shall invariably be attested by Gazetted officer/ Nazim/Administrator or an officer of bank/DFI after original seen.
2. In case of a salaried person, in addition to CNIC, an attested copy of his service card, or any other acceptable evidence of service, including, but not limited to a certificate from the employer will be obtained.
3. In case of an individual with shaky/immature signatures, in addition to CNIC, 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.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

4. In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that Bank/DFI shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account. For CNICs which expire during the course of the customer's banking relationship, Banks/DFIs shall design/update their systems which can generate alerts about the expiry of CNICs at least one month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired.
5. A copy of CNIC without photograph duly attested by the same person who attested the photograph.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

6. In case the CNIC does not contain a photograph, Bank/DFI shall obtain following:
   a. A duly attested copy of either driving license, service card, Nikkah Nama, birth certificate, Educational degree/certificate, pension book, insurance certificate.
   b. A photograph duly attested by gazetted officer/Nazim/ Administrator/Bank officer.
   c. A copy of CNIC without photograph duly attested by the same person who attested the photograph.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

7. Banks/DFIs shall obtain copies of CNICs of all the members of Governing and Executive Bodies of DHA or ask for delegation of power to Administrator under section (7) & (8) of the Pakistan Defence Housing Authority Order, 1980 and accept copy of CNIC of Administrator as well as authorized signatories for the purpose of opening accounts of DHA or similar other authorities subject to compliance of other requirements.
8. The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for opening bank accounts to the satisfaction of their banks.

Examples or Characteristics of Suspicious Transactions (Red Alerts)

The following are examples or characteristics of possible suspicious transactions for money laundering or financing of terrorism. This list of situations may be taken as a means of highlighting the basic ways in which money may be laundered. The examples provided are not exhaustive and may serve only as guidance of banks/DFIs to recognize suspicious activities.

While each individual situation may not be sufficient to suggest that money laundering is taking place, a combination of such situations may be indicative of such a transaction. A customer's declarations regarding the background of such transactions shall be checked for plausibility and explanation offered by the customer may be accepted after reasonable scrutiny.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

2. Transactions which do not make economic sense or inconsistent with customer's business or profile :
   i. A customer's relationship having a large number of accounts with the same bank, frequent transfers between different accounts or exaggeratedly high liquidity;
   ii. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal;
   iii. 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;
   iv. Provision of bank guarantees or indemnities as collateral for loans between third parties that are not in conformity with market conditions;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

v. Unexpected repayment of an overdue credit without any plausible explanation;

vi. Back-to-back loans without any identifiable and legally admissible purpose;

vii. Paying in large third party cheques endorsed in favour of the customer;

viii. 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;

ix. 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;

x. 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;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

xi. 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;

xii. The structuring of deposits through multiple branches of the same bank or by groups of individuals who enter a single branch at the same time;

xiii. The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds;

xiv. 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;

xv. Customers making large and frequent deposits but cheques drawn on the accounts are mostly to counter-parties not normally associated with customer's business;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

xvi. Extensive or increased use of safe deposit facilities that do not appear to be justified by the customer's personal or business activities;

xvii. Goods or services purchased by the business do not match the customer's stated line of business;

xviii. Goods or services purchased by the business do not match the customer's stated line of business;

xix. A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location;

xx. Loans are made for, or are paid on behalf of, a third party with no reasonable explanation;

xxi. Suspicious movements of funds occur from one financial institution to another, and then funds are moved back to the first financial institution.

xxii. The deposit of excess balance in the accounts linked to credit cards/store value cards.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

xxiii. Unusual pattern of purchase through credit cards/store value cards etc.

3. Transactions involving large amounts of cash

   i. Exchanging an unusually large amount of small-denominated notes for those of higher denomination;

   ii. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;

   iii. Frequent withdrawal of large amounts by means of cheques, including traveler's cheques;

   iv. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit locally or from abroad;

   v. Large cash withdrawals made from a personal or business account not normally associated with customer's profile;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

vi. 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.;

vii. 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;

viii. The deposit of unusually large amounts of cash by a customer to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments;

ix. Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

x. 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.

4. Transactions involving locations of concern & wire transfers

i. Transactions involving foreign currency exchanges or deposits that are followed within a short time by wire transfers to locations of specific concern (for example, countries identified by national authorities/international bodies, UN or FATF etc.);

ii. A personal or business account through which a large number of incoming or outgoing wire transfers take place without logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern (as mentioned above);

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

iii. 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 (as mentioned above);

iv. Obtaining credit instruments or engaging 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 (as mentioned above);

v. The opening of accounts of financial institutions from locations of specific concern (as mentioned above);

vi. The business relationships conducted in unusual circumstances e.g. significant unexplained geographic distance between the bank and the customer;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

vii. The receipt of small or large amounts (in cash, using online or otherwise) from various locations from within the country 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;

viii. 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;

ix. Building up large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas;

x. Transfer of money abroad by an interim customer in the absence of any legitimate reason;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

xi. Repeated transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash;

xii. Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries or geographic areas identified by credible sources as having significant levels of corruption, or other criminal activity; as providing funding or support for terrorism activities; as associated with the production, processing or marketing of narcotics or other illegal drugs etc.

xiii. Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements;

xiv. 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;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

xv. 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.

xvi. Customer who generally use credit cards/store value cards out of their defined geographical location or locations prone to money laundering and terrorist financing.

5. Transactions involving unidentified parties

i. Provision of collateral by way of pledge or guarantee without any discernible plausible reason by third parties unknown to the bank and who have no identifiable close relationship with the customer;

ii. Transfer of money to another bank without indication of the beneficiary;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

iii. Payment orders with inaccurate information concerning the person placing the orders;

iv. Use of pseudonyms or numbered accounts for effecting commercial transactions by enterprises active in trade and industry;

v. Customer's holding in trust of shares in an unlisted company whose activities cannot be ascertained by the bank;

vi. 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.

6. Other suspicious accounts or customers

i. Large sums deposited through cheques or otherwise in newly opened accounts which may be suspicious;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

ii. The customers who are reluctant to provide minimal information or provide false or misleading information or, when applying to open an account, provide information that is difficult or expensive for the bank to verify;

iii. An account opened in the name of a moneychanger that receives structured deposits;

iv. Customers whose deposits contain counterfeit notes or forged instruments;

v. An account operated in the name of an offshore company with structured movement of funds;

vi. 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;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

vii. A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the sum so received has been removed;

viii. 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);

ix. 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.)

x. 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;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

xi. An account opened in the name of a legal entity that is believed to be involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorism organization;

xii. An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorism organization and that shows movements of funds above the expected level of income;

xiii. 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.);

xiv. Stated occupation of the customer 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);

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

xv. 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;

xvi. 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;

xvii. Safe deposit boxes 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;

xviii. 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);

xix. Official embassy business is conducted through personal accounts.

xx. Large deposits on pretext of transfer/disposition of property.

xxi. Frequent and unusual advance payments against imports.

Customer Risk Profiling (CRP)

1. Banks/DFIs may conduct their internal money laundering and financing of terrorism risk assessments (for their customers, products & services, transactions channels and geographic areas) with the purpose to develop their own policies and procedures, in order to identify, assess, manage and mitigate related risks on on-going basis. It is always advisable that measures to prevent ML/FT risks are commensurate to the risks identified for effective mitigation. Such risk assessments are generally based on perception, subjective judgment and experience of banks about risk regarding aforesaid elements. In this regard, the major considerations for banks/ DFIs may be:

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

a. Quantification of Risk through Risk Matrix: A matrix which quantifies likelihood and impact/consequences on two dimensions may be developed thereby categorizing risk as low, medium, high or any appropriate scale. It is pertinent to mention here that without proper quantification of risks, it may be difficult to decide which customer qualifies for simplified due diligence (SDD) or enhanced due diligence (EDD).

b. Risk Register: A risk register may be developed whereby risks emanating from various business aspects can be accounted for. These may include the following:

   i. Customers: Identifying risk determinants while establishing relationships with customer;

   ii. Products: Envisaging risk attributes resulting from customer's need for financial services and appropriate controls;

iii. Delivery Channels: Identifying risks associated with delivery channels which may vary from customer to customer depending on their needs; and

iv. Geographic/Jurisdictional: Risks resulting from customer geographic presence and jurisdiction in which the customer is operating.

v. Controls: After assessing the risks the controls are reviewed and assessed whether these are effective to cater to the risks.

vi. Residual Risk: In the next step, after assessing the risks controls are accounted for to quantify the residual risks.

vii. (Risk decision: After identification and quantification of inherent risks, controls and residual risks, the decision should be taken. For example, while establishing relationship the decision whether to take the customer on-board, mark as high risk or refuse to accept the customer etc.

c. Risk Profiling of Customers

2. Banks/ DFIs should profile every new customer using their own judgment and information obtained through CDD/KYC process. A template of Customer Risk Profiling (CRP) is provided at the end of this reading material.

3. SPECIFIC HIGH RISK ELEMENTS AND RECOMMENDATIONS FOR EDD

Some of the relatively high risk elements identified by SBP and recommended actions for EDD may be as under;

S. No	Customers	Recommendations for EDD
a.	NPOs/NGOs/ Charities, Trusts, Clubs, Societies, and Associations etc.	In relation to these customers, banks/DFIs may: i. obtain a declaration from Governing Body/Board of Trustees/Executive Committee/sponsors on ultimate control, purpose and source of funds etc; ii. obtain an undertaking from Governing Body/Board of Trustees/Executive Committee /sponsors to inform the bank/DFI about any change of control or ownership during operation of the account; and iii. obtain a fresh Resolution of the Governing Body/Executive Committee of the entity in case of change in person(s) authorized to operate the account.

SPECIFIC HIGH RISK ELEMENTS AND RECOMMENDATIONS FOR EDD

S. No	Customers	Recommendations for EDD
b.	Housewife accounts	In relation to housewife accounts, banks/DFIs may i. obtain a self-declaration for source and beneficial ownership of funds; ii. Update details of funds providers, if any along with customer's profile; and iii. Identify and verify funds providers if monthly credit turnover exceeds an appropriate threshold to be decided by banks/DFIs.
c.	Proprietorships and self-employed individuals/ professionals	In relation to these accounts, following measures may be taken by banks/DFIs: i. The business transactions in personal accounts of proprietors may only be permitted by linking it with account/business turnover. For example, such customers having monthly credit turnover of Rs. 5 million or above may be required to open a separate account for business related transactions; and ii. In order to verify the physical existence of business or self-employment status, banks/DFIs may conduct physical verification within 05 working days of the opening of account and document the results thereof on account opening form. In case of unsatisfactory verification, bank/DFI may consider reporting it to FMU and/or may change risk profile, as appropriate.
d.	Landlords	In relation to such customers, banks/DFIs may apply any recommend methods for assessment of source of funds/income e.g. Passbook of landholding records etc.

4. SPECIFIC HIGH RISK ELEMENTS AND RECOMMENDATIONS FOR EDD

S. No	Products & Services	Recommendations for EDD
a.	Online transactions	In relation to online transactions, Banks/DFIs should pay special attention to geographical factors/locations for movement funds.
S. No	Delivery Channels	Recommendations for EDD
a.	Cash	In relation to cash transactions, Banks/DFIs may: (i) monitor cash transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and (ii) pay special attention on cash based transactions considering examples of Red Alerts given in Stage III reading material.
b.	Wire transfers	In relation to wire transfers, banks/DFIs may: (i) monitor such transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and (ii) Ensure that funds transfers which are out of character/ inconsistent with the history, pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

GENERAL HIGH RISK SCENARIOS/ FACTORS : In addition, following high risk elements/ factors should also be considered as per international standards.

Customers	Products and Delivery Channels	Geography or Locations
• Non-resident customers • Correspondent banks' accounts • Customers with links to offshore tax havens • Customers in high-value items etc. • High net worth customers with no clearly identifiable source of income • There is a doubt about the veracity or adequacy of available identification data on the customer • There is reason to believe that the customer has been refused banking facilities by another bank/ DFI • Companies that have nominee shareholders or shares in bearer form • Legal persons or arrangements that are personal asset holding vehicles	• Non-face-to-face business relationships or transactions • Cash intensive or other forms of anonymous transactions • Payment received from unknown or un-associated third parties • Private banking relationships	• The jurisdictions which have been identified for inadequate AML/CFT measures by FATF or called for by FATF for taking counter-measures • Countries identified by credible sources such as mutual evaluations or detailed assessment reports, as having inadequate AML/CFT standards • Countries subject to sanctions, embargos, for example, the United Nations • Countries identified by credible sources as having significant levels of corruption, or other criminal activity • Countries or geographic areas identified by credible sources as providing funding or support for terrorism activities

5. In respect of general high risk elements mentioned at Para above, banks/DFIs may conduct EDD measures which are effective and commensurate to the level of risks. In particular, they may increase the degree and nature of on-going monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of such EDD measures may include:

a. Obtaining additional information on the customer (occupation, volume of assets, address, information available through public databases, internet, etc);
b. Reducing interval for updating and reviewing customer risk profile;
c. Reducing interval for updating the identification data of customer and beneficial owner;
d. Obtaining additional information on the intended nature of the business relationship;
e. Obtaining information on the reasons for intended or performed transactions;
f. Obtaining additional information on the sources of funds or sources of wealth of the customer;

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

g. Obtaining the approvals of senior management to commence or continue the business relationship;

h. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;

i. 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/DFI acting on behalf of directors or owners with whom the bank/DFI had little or no direct contact; and

j. Documentary evidence may be sought to support transaction where possible, e.g. purchase of property etc.

6. GENERAL HIGH RISK SCENARIOS/ FACTORS

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. In such circumstances, and provided there has been an adequate analysis of the risk by the banks/DFI, SDD measures may be applied. Examples of such low risk scenarios/factors may include:

Low risk factors for Customers	• A financial institution regulated/ supervised by the State Bank of Pakistan except exchange companies/ money remitters; • A Non-Bank Finance Company (NBFC) regulated/ supervised by Securities and Exchange Commission of Pakistan (SECP) unless an entity is notified for application of the requirements; • A government entity; • A foreign government entity; • Public administrations or enterprises; • An entity listed on any stock exchange in Pakistan; and • An entity listed on a stock exchange outside Pakistan that is subject to regulatory disclosure requirements and its information is publically available.

STAGE - III
Documentation, Suspicious Transaction Reporting (STR) & Customer Risk Profile (CRP)

Low risk factors for Products and Transaction Channel	• 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.
Low risk factors for Geography or Locations	• Country identified by credible sources such as mutual evaluation or detailed assessment reports, as adequately complying with and having effectively implemented the FATF Recommendations; and • Country identified by credible sources as having a low level of corruption, or other criminal activity.

7. In respect of general low risk elements mentioned above, Banks/ DFIs may perform such SDD measures as it considers adequate to effectively establish the identity of the customer, a natural person appointed to act on behalf of the customer and any beneficial owner. The SDD measures should be in accordance with pre-defined criteria within AML/CFT policy of a Bank/DFI and should commensurate with the low risk factors e.g. the SDD measures could relate only to customer acceptance measures or to aspects of on-going monitoring. Examples of such SDD measures may include:
   a. Decreasing the frequency of customer identification updates;
   b. Reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable monetary threshold; and
   c. Not collecting specific information (no exemption shall be presumed in respect of minimum documents in 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.

8. In relation to above Paras, SDD measures should not be considered in following situations:

   a. When there is a suspicion of money laundering or financing of terrorism;
   b. There are no exceptions in reporting suspicion to FMU within the provisions of AML Act.
   c. In case of certain high risk factors are identified by SBP, by bank/DFI in its own internal risk assessment or as per international standards viz-a-viz FATF Recommendations etc.
   d. 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 State Bank of Pakistan.

A Template of Customer Risk Profiling (CRP) Form

Risk Determinants	Risk Variables/ Determinants	Assigned Risk Weight
Customers	Exceptions in getting KYC related information from customer	0
	High net worth customer or high value transactions	10
	Politically exposed person, its close associate or family member	0
	Relatively complex control/ ownership structure	0
	Reliability of verification measures	5
	Unclear source of funds or income from undocumented sources	10
	Beneficial ownership of funds may not belong to customer	5

A Template of Customer Risk Profiling (CRP) Form

Product & Services	Use of products & services which entail non face-to-face conduct	10
	Customer seeks private banking or other riskier services	0
	Excessive use of funds remitting instruments	10
	Customer subscribes for International/ foreign products & services	5
Channels	Large wire-in/wire-out or inland online transfers	10
	Level of cash based transactions	20
	Element of anonymity in transactions	5
Locations	Customer is based or linked to High Risk Jurisdictions as per FATF	0
	Customer is based or linked to UN Sanctioned Countries	0
	Customer's link to offshore centers or tax heavens	0
	Name matches with databases i-e World Check, OFAC, EU lists etc.	0
Others	Transaction pattern matches with SBP's examples on Red Alerts or guidance provided by FMU on ML/FT typologies	5
	Any other risk factors etc	--

An example of Customer Risk Profiling (CRP)

Total Risk Score		95
Scale	Please note that risk weight assigned as above have been selected according to prevalence of risk i-e. Never = 0 Low = 5 Moderate = 10 High = 20	--
Benchmarking		
Risk Score Range		RATING
Below 50		1
51 – 80		2
→81 – 110		3
111 – 140		4
141 – 170		5
170 & above		6
Rating	Customer Risk Profiling	Check
1 - 2	Low Risk	
→3 - 4	Moderate Risk	√
5 - 6	High Risk	
Customer Risk Profile is re-considered in line with pre-defined criteria of SBP or Bank's own Internal Risk Assessment		Mod. Risk
Prepared by:	Reviewed by:Approved by:	Prepared by:
xxxxxx	xxxxxx xxxxxx	Xxxxxx