SUB-MODULE: BANKING AND FINANCE

1) **Definitions**
2) **General Banking Operation:**

- **Account Opening**

AML/CFT of SBP Reference REGULATION – 1 CUSTOMER DUE DILIGENCE (CDD) & Basic Documentation required for account opening process

- Minimum Documents to be obtained from Various Types of Customers under Reference SBP AML/CFT Regulations
- Review of the Instructions on Service Charges on PLS Deposit Account reference SBP BPD Circular No. 23 Prudential Regulation # XIII -
- Guideline for banking services to visually impaired/blind persons reference**(SBP/CPD/2014/C6-Annex)**

- **Account Operations**

Account operations for different type of customers;

- Joint account holders
- Government accounts
- Existing customers
- Dormant Accounts
- Prohibition of personal accounts for business purposes
- Politically Exposed Persons (PEPs)
- NGOs/NPOs/ Charities' accounts
- Shaky & Immature Signatures treatment
- Expired CNIC's treatment of an account holder
- Unclaimed Deposits reference SBP(BPD Circular No. 07 of 2006)

- **Remittances (Local & Foreign)**

- INWARD AND OUTWARD REMITTANCES reference SBP(FE Manual 2002 CHAPTER X)

WIRE TRANSFERS/ FUND TRANSFERS;

- Responsibility of the Ordering Institution
- Responsibility of the Beneficiary Institution
- Responsibility of Intermediary Institution

3) Banking Financing

- **Types of Credits**

- Types of products/facilities offered – fund based & non-fund based facilities
- Credit Approval, Initiation & Management
- Import & Export Documentation

4) Compliance Requirements of State Bank of Pakistan & Modern Trends in Banking

- **Understanding Money Laundering & Terrorist Financing.**

- **Stages of Money Laundering Process** – *Placement, layering & Integration.*
- **International initiatives for AML/CFT**
  - **FATF's 40 recommendations**
  - **Basel document on customer due diligence**
- **Measures to prevent Money Laundering (Local Regulations)**
- **SBP's PRs – R1 to R6** ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) REGULATIONS FOR BANKS & DFIs((Updated up to March 31, 2015)

(BF-1) Banking and Finance

1) DEFINITIONS

1) Account Holder means a person who has opened any account with a bank directly or through branchless banking agent or is a holder of deposit/deposit certificate or any instrument representing deposit/placing of money with a bank/DFI or has borrowed money from the bank/DFI.
2) "Banking" means the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawable by cheque, draft, order or otherwise;
3) "Banking company" means any company which transacts the business of banking in Pakistan and includes their branches and subsidiaries functioning outside Pakistan of banking companies incorporated in Pakistan
4) "branch" or "branch office", in relation to a banking company, means any branch or branch office, whether called a pay office or sub-pay office or by any other name, at which deposits are received, cheques cashed or moneys lent, and for the purposes of section 40 includes any place of business where any other form of business referred to in sub-section (1) of section 7 is transacted;
5) "Beneficial owner" 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;
6) "Beneficiary" means the person to whom or for whose benefit the funds are sent or deposited in bank;
7) "Beneficiary institution" means the financial institution that receives the funds on behalf of the wire transfer or fund transfer beneficiary;
8) Branchless Banking Agent means an agent providing banking services to the customers of a bank/DFI on behalf of the bank/DFI/MFBs under a valid agency agreement.
9) Bank means a banking company as defined in the Banking Companies Ordinance, 1962.
10) Borrower or Obligor means a person on whom a bank/DFI has taken any exposure during the course of business.
11) "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;
12) "Correspondent bank" means the bank in Pakistan which provides correspondent banking services to bank or financial institution situated abroad and vice versa;
13) "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;
14) "Cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are located in different countries or jurisdictions;
15) "Currency Transaction Report or CTR" means as defined under AML Act;
16) "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;

17) "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;

    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 AML/CFT Regulations 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

d) monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the banks/DFIs knowledge of the customer, their business and risk profile, 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.

18) Chief Executive Officer (CEO), in relation to bank/DFI means an individual who, subject to the control and directions of the Board of Directors, is entrusted with the whole, or substantially the whole, of the powers of management of the affairs of the bank/DFI occupying the position of Chief Executive Officer and includes President, acting President, Managing Director, Country Head of Foreign bank, Executive assuming charge of the bank for interim period or by whatever name called, and whether under a contract of service or otherwise.
19) Contingent Liability means:

a) A possible obligation that arises from past events and whose existence will be confirmed only by the occurrence or non-occurrence of one or more uncertain future events not wholly within the control of the enterprise; or

b) A present obligation that arises from past events but is not recognized because:

i) It is not probable that an outflow of resources embodying economic benefits will be required to settle the obligation; or

ii) The amount of the obligation cannot be measured with sufficient reliability;

And includes letters of credit, letters of guarantee, bid bonds/performance bonds, advance payment guarantees and underwriting commitments.

20) Control refers to an ownership directly or indirectly through subsidiaries, of more than one half of voting power of an enterprise.
21) Corporate Card means credit card issued to the employees of an entity where the repayment is to be made by the said entity.
22) "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;
23) "Dormant or in-operative account" means the account in which no transaction has been taken place from last one year;
24) Derivative means a type of financial contract the value of which is determined by reference to one or more underlying assets or indices. The major categories of such contracts include forwards, futures, swaps and options. Derivative also includes structured financial products that have one or more characteristics of forwards, futures, swaps and options.
25) DFI means Development Financial Institution and includes the, Saudi Pak Industrial and Agricultural Investment Company Limited, Pak Kuwait Investment Company Limited, Pak Libya Holding Company Limited, Pak Oman Investment Company (Pvt.) Limited, House Building Finance Company Ltd., Pak Brunei Investment Company Limited, PAIR Investment Company Limited, Pak-China Investment Company Limited, and any other financial institution notified under Section 3-A of the Banking Companies Ordinance, 1962.
26) Documents include vouchers, cheques, bills, pay-orders, promissory notes, securities for leases/advances and claims by or against the bank/DFI or other papers supporting entries in the books of a bank/DFI, or any other document which establishes relationship between the bank/DFI and its customers.
27) Director means any person occupying the position of a director on the Board of a bank/DFI and includes sponsor, nominee and alternate director or by whatever name called.

28) Equity of the Bank/DFI includes paid-up capital in respect of ordinary shares, general reserves, and balance in share premium account, reserve for issue of bonus shares, statutory reserves, and retained earnings /accumulated losses as disclosed in latest annual audited financial statements. In case of branches of foreign banks operating in Pakistan, equity will mean capital maintained, free of losses and provisions, under Section 13 of the Banking Companies Ordinance, 1962.
29) Exposure shall include:

A) Financing Facilities whether fund based or non-fund based extended by a bank/DFI and include:

i.) Any form of financing facility extended or Bills purchased/discounted, Bills purchased/discounted on the guarantee of the person.

ii.) Credit facilities extended through Corporate Cards.

iii.) Any financing obligation undertaken on behalf of the person under a letter of credit including a stand-by letter of credit, or similar instrument.

iv.) Loan repayment financial guarantees issued on behalf of the person.

v.) Any obligations undertaken on behalf of the person under any other guarantees including underwriting commitments.

vi.) Acceptance/endorsements made on account.

vii.) Any other liability assumed on behalf of the person to advance funds pursuant to a contractual commitment.

B) Subscription to or investment in shares, Participation Term Certificates, Term Finance Certificates, Sukuk or any other Commercial Paper by whatever name called issued or guaranteed by the persons.

(C) Exposure (Net open position) on account of derivative transactions allowed under Financial Derivatives Business Regulations (FDBR) issued vide BSD Circular No. 17 dated November 26, 2004.

For the purpose of calculating exposure, the sanctioned limits, or outstanding, whichever are higher, will be considered. However, in case of fully drawn term loans where there is no scope for re-drawal of any portion of the sanctioned limit bank/DFI may consider the outstanding as exposure.

30) Family Member as defined in sub-section (ff) of section 5 of Banking Companies Ordinance 1962.
31) Financial Institutions for the purpose of these regulations mean banks, Development Financial Institutions (DFIs) and NBFCs.
32) Forced Sale Value (FSV) means the value which fully reflects the possibility of price fluctuations and can currently be obtained by selling the mortgaged/pledged assets in a forced/distressed sale conditions.
33) “FATF Recommendations” means the Recommendations of Financial Action Task Force as amended from time to time;
34) “FMU” means financial monitoring unit established under the AML Act;
35) “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;
36) Government Securities shall include such types of Pak. Rupee obligations of the Federal Government or a Provincial Government or of a Corporation wholly owned or controlled, directly or indirectly, by the Federal Government or a Provincial Government and guaranteed by the Federal Government as the Federal Government may, by notification in the Official Gazette, declare, to the extent determined from time to time, to be Government Securities.
37) Group means persons, whether natural or juridical, if one of them or his dependent family members or its subsidiary, have control or hold substantial ownership interest (as defined in these regulations) over the other

For the purpose of this definition:

a) Subsidiary will have the same meaning as defined in Section 3 of the Companies Ordinance, 1984 i.e. a company or a body corporate shall deemed to be a subsidiary of another company if that other company or body corporate directly or indirectly controls, beneficially owns or holds 3 more than 50% of its voting securities or otherwise has power to elect and appoint more than 50% of its directors.

b) Control refers to an ownership directly or indirectly through subsidiaries, of more than one half of voting power of an enterprise.

c) Substantial ownership/affiliation means beneficial shareholding of more than 25% by a person and/or by his dependent family members, which will include his/her spouse, dependent lineal ascendants and descendants and dependent brothers and sisters. However, shareholding in or by the Government owned entities and financial institutions will not constitute substantial ownership/affiliation, for the purpose of these regulations.

38) "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;

39) "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;

40) Key Executive means key executives of banks/DFIs and includes the following functional responsibilities for the present:

a) Any executive, acting as second to CEO including Chief Operating Officer, Deputy Managing Director or by whatever name called.

b) Chief Financial Officer/Head of Finance/Head of Accounts

c) Head of Internal Audit

d) Country Treasurer

e) Head of Credit/Risk Management

f) Head of Operations

g) Head of Compliance

h) Head of Human Resource

i) Head of Information Technology

j) Head of Islamic Banking

k) Head of overseas operations of a bank at head office level

l) Country Head/Regional Head (where a region is consisting of more than one foreign country)

m) CEO/Head of subsidiary banking company outside Pakistan

n) CEO of Joint Venture (where majority stake is with the bank incorporated in

Pakistan & authority to appoint CEO)

The above list will be reviewed from time to time by SBP.

41) Large Exposure means an exposure of 10% or more of a bank's/DFI's equity to a single obligor or a group.

42) Liquid Assets are the assets which are readily convertible into cash without recourse to a court of law and mean encashment/realizable value of government securities, bank deposits, certificates of deposit, shares of listed companies which are actively traded on the stock exchange, NIT Units, certificates of mutual funds, Certificates of Investment (COIs) issued by DFIs/NBFCs rated at least 'A' by a credit rating agency on the approved panel of State Bank of Pakistan, listed TFCs rated at least 'A' by a credit rating agency on the approved panel of State Bank of Pakistan and certificates of asset management companies for which there is a book maker quoting daily offer and bid rates and there is

active secondary market trading. These assets with appropriate margins should be in possession of the banks/DFIs with perfected lien.

43) "Monetary threshold" expressed in Pak rupee includes a reference to the equivalent amount expressed in any other currency;
44) "Money laundering and financing of terrorism or ML/TF" has the same meaning as ascribed to them in AML Act;
45) Major Shareholder of a bank/DFI means any person holding 5% or more of the share capital of a bank/DFI either individually or in concert with family members.
46) NBFC means Non-Banking Finance Company as defined in Section 282A of Companies Ordinance 1984 and includes Leasing Company, Housing Finance Company, Investment Bank, Discount House, Asset Management Company and a Venture Capital Company. For the purpose of these regulations Modaraba will also be considered as NBFC.
47) "Occasional customer" or "walk-in-customer" means the person conducting occasional transactions and is not a customer; having relationship with the bank/DFI;
48) "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; AML/CFT Regulations
49) "Online transaction" means deposit or withdrawal of cash using different branches of a bank through electronic means;
50) "Ordering institution" means the financial institution that initiates a wire transfer on the instructions of the wire transfer originator in transferring the funds;
51) "Originator" means the person who allows or places the order to initiate a fund transfer/wire transfer or an online transaction;
52) "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;
53) "Person" has the same meaning as ascribed to it under the AML Act, 2010;
54) "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;
55) PBA means Pakistan Banks Association.
56) Person means and includes an individual, a Hindu undivided family, a firm, an association or body of individuals, whether incorporated or not, a company and every other juridical person.
57) "Respondent bank" means the bank or financial institution outside Pakistan to whom correspondent banking services in Pakistan are provided and vice versa;
58) "Risk" refers to risk associated with money laundering and financing of terrorism;
59) Recognized Rating Agency means rating agency either on the approved panel of State Bank of Pakistan or Standard & Poor's, Moody's, Fitch or Japan Credit Rating Agency (JCRA)
60) Related Party in respect of a bank / DFI means:

    a.) Directors, CEO, sponsor shareholders, employees or any of their family members.

    b.) Any entity (proprietorship, firm, company or trust) in which a bank / DFI or any of the above persons are interested as director, proprietor, partner or as a shareholder holding 5% or more of paid-up capital in that entity.

    c.) Any other entity which for its business acquisition or provision of services relies / depends to a greater extent on the bank/DFI i.e. major portion (50% or more) of its business (upstream or downstream) is with the bank/DFI.

    d.) The relationship of the related party on the basis of Nominee Director appointed by Federal/Provincial government by virtue of their shareholding shall be excluded from this definition. However, it shall include personal/family business interests of such director.

61) "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;

62) "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
63) "Suspicious transaction report or STR" means as defined under AML Act.
64) Secured means exposure backed by Liquid Assets, pledged stock, mortgage of land, plant, building, machinery and any other fixed assets, hypothecation of stock (inventory), trust receipt, assignment of receivables, lease rentals and contract receivables, but does not include hypothecation of household goods. The unsecured exposure will be considered as clean.
65) Sponsor Shares mean 5% or more paid-up shares of a bank, acquired by a person(s) individually or in concert with his family members (including his spouse, lineal ascendants and descendents and dependent brothers and sisters), group companies, subsidiaries, and affiliates/associates. Such acquisition of shareholding will include all the shares acquired by aforesaid person(s) including, interalia, through (a) as original subscriber/promoter of the bank; (b) subsequent right/bonus issues; (c) market based acquisition deal; (d) reconstruction/restructuring of a bank carried out by SBP; (e) strategic sale through privatization (f) amalgamation of banking companies; or (g) any other mode of acquisition. All shares acquired by common shareholders, who are also sponsor shareholders, of amalgamating banking companies in amalgamation transaction shall be considered Sponsor Shares.
66) Sponsor Shareholders mean all those shareholders of a bank holding sponsor shares.
67) Sponsor Director means the member of the Board of Directors of a bank holding sponsor shares.
68) Strategic Investment is an investment which a bank/DFI makes with the intention to hold it for a period of minimum 5 years.

    The following must be noted further in respect of strategic investment:

    a. The bank should mark strategic investment as such at the time of investment.

    b. If there are a series of purchases of stocks of a company, the minimum retention period of 5

    Years shall be counted from the date of the last purchase.

69) Underwriting Commitments mean commitments given by commercial banks/DFIs to the limited companies at the time of new issue of equity/debt instrument that in case the proposed issue of equity/debt instrument is not fully subscribed, the un-subscribed portion will be taken up by them (commercial banks/DFIs)

2) General Banking Operation:

- **Account Opening**

AML/CFT Regulations of SBP Reference REGULATION – 1 CUSTOMER DUE DILIGENCE (CDD)

- **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 in line with Para 13 below;

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

CDD Measures for Establishing Business Relationship

Identification of Customers

2. Every customer shall be identified for establishing business relationship. For this purpose, 'Annexure–I' provides range of documents which shall be obtained for different types of customers.

3. 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;

(a) Full name as per identity document;

(b) CNIC/Passport/NICOP/POC/ARC number or where the customer is not natural person, the registration/ incorporation number or business registration number (as applicable);

(c) Existing residential address, registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable);

(d) Date of birth, incorporation or registration (as applicable);

(e) Nationality or place of birth, incorporation or registration (as applicable);

(f) Nature of business, geographies involved and expected type of counter-parties(as applicable);

(g) Purpose of account;

(h) Type of account;

(i) Source of earnings;

(j) Expected monthly credit turnover (amount and No. of transactions); and

(k) Normal or expected modes of transactions.

Verification of Identity;

4. The Bank/ DFI shall verify identity documents of the customers from relevant authorities/document issuing bodies and 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.

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

5. In relation to Para 4 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.

6. 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.

Identification and Verification of Identity of Beneficial Owners;

7. 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).

8. 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 Para 9 below and (ii) determine that the natural persons who ultimately own or control the customer.

Information on the Purpose and Intended Nature of Business Relations;

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

Timing of Verification;

10. 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.

11. 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.

12. In relation to Para 11 above, 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;

(a) 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.

(b) No debit will be allowed or cheque book is issued until positive verification is completed.

(c) 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.

CCD Measures for Occasional Customers/ Walk-in Customers;

13. Banks/DFIs shall;

(a) obtain copy of CNIC from occasional customers/walk-in customers conducting cash transactions above rupees 1.0 million whether carried out in a single operation or in multiple operations that appear to be linked;

(b) Obtain originator information along with copy of CNIC while carrying out online transactions (regardless of threshold) by occasional customers/walk-in customers or where such person is conducting transaction on behalf of an account holder;

(c) In relation to Para 13 (b) above, name and CNIC No. of originator shall be captured in system and made accessible along with transaction details at corresponding branch if (i) online transaction exceeds Rs. 100,000; and (ii) transaction is taking place between two branches of different cities.

(d) Obtain copy of CNIC from occasional customers/walk-in-customers who wish to purchase remittance instruments e.g. POs, DDs and MTs etc.

Where CDD Measures are Not Completed;

14. 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.

Ongoing Monitoring;

15. 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.

16. 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.

17. 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.

18. In relation to Para 17 above, in order to avoid the risk where front-end staff do not follow the desired procedures and update the KYC/CDD form of the customer based on their personal knowledge/perception rather than interviewing the customer, banks/DFIs shall obtain sign-off from the customer on every revision of KYC/CDD form.

- Minimum Documents to be obtained from Various Types of Customers under AML/CFT Regulations for account opening Purpose;

Sr. No	Type of Customers	Documents/papers 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
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.

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; (viii) For individual (natural person) shareholders holding 5% or above stake in company/corporation, photocopies of identity document as per S. No. 1 above; and (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. 1 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 (a) Certificate of Registration/Instrument of Trust (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 AML/CFT Regulations 20 Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.
7	NGOs/NPOs/Charities	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
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

- Instructions Given by Central bank(State Bank of Pakistan) regarding PLS Account;

a) All terms and conditions of operation of an account shall be made known to the opener of the account at the time of opening of the account. The terms and conditions shall be clearly, explicitly & elaborately documented in the account opening form/application and must be signed by the prospective depositor/account holder to signify having been read and understood.

b) All account opening forms must be filled in by the account holder in duplicate, one copy of which must be returned to the depositor/account holder duly verified by the authorized official(s) of the branch under proper acknowledgement.

c) The banks can levy service charges on all types of PLS deposits provided these charges are indicated in their half yearly schedule of charges.

d) In case of accounts where no express clause was provided in account opening form for levy of service charges, i.e. accounts opened prior to 17th March, 2001, the banks may recover service charges provided each of the following conditions are met meticulously.

i. A reasonable time i.e. at least six months is allowed in advance to account holders intimating the intention of the bank to levy service charges.

ii. Account holders have been informed about the levy of these charges through a letter while dispatching the half yearly statement of accounts.

iii. The banks display the effective date for levy of service charges in each of their branches for information of their customers in the light of instructions given in para (a) above.

iv. Account holders have been advised through newspapers and other means of communication.

3. Banks are further directed that accounts maintained by (i) Students (ii) Mustahiqueen of Zakat (iii) employees of Government/Semi-Government institutions for salary and pension purposes shall be exempted from levy of service charges in any manner whatsoever.

In case of non-compliance;

4. In case it is found, on the basis of complaints received or during the course of on-site inspection by SBP, that the banks, without completely complying with the above instructions, are levying/recovering service charges, punitive action will be taken under the relevant provisions of Banking Companies Ordinance.

- GUIDELINES FOR BANKING SERVICES TO VISUALLY IMPAIRED/BLIND PERSONS BY CENTRAL BANK(SBP)

1) General Guidelines:

1.1) the bank/MFB shall render the same services to visually impaired/blind person as it would to any other person without discrimination through all branches.

1.2) before establishing banking relationship with visually impaired/blind persons, the bank/MFB must clearly explain them all possible risks involved in the operation and usage of any product/services being offered.

1.3) the bank/MFB shall not equate literate visually impaired/blind persons with illiterate customers.

1.4) if the visually impaired/blind customers need to complete a form, deposit slip, cheque etc., the branch staff member shall read out the questions, and write down the answers on the customers' behalf in the presence of witness who is personally known to the customer, if so desired.

1.5) the bank/MFB shall clearly mark the account of all such customers as "Visually Impaired/Blind Person Account".

1.6) the bank/MFB shall develop and put in place internal control procedures to deal with any possible financial exploitation of visually impaired/blind customers.

1.7) the bank/MFB shall arrange special training programs for its staff working at branch level or in a Call Centre so that they can support and facilitate banking for visually impaired/blind customers in a dignified manner.

1.8) when the visually impaired/blind customers intend to leave the branch premises, the branch staff shall ensure that they have picked up all of their belongings.

2) Opening and Operation of Account:

2.1) the bank/MFB shall not deny opening of individual account by a visually impaired/blind person.

2.2) Clear option should be provided to a visually impaired/blind person for opening of an account either singly or jointly with any other person.

2.3) No restriction shall be placed on opening of a joint account including with person(s) who is /are visually impaired/blind.

2.4) Minimum documentation requirements under related regulation will also be applicable to all such accounts.

2.5) The Manager/Operations Manager of the branch shall read out the rules of business/ terms and conditions governing the operation of the account in the presence of a witness known to the concerned illiterate visually impaired/blind person before signing the account opening forms/documents. However, the same may not be required in case of joint account and for literate visually impaired/blind customer.

2.6) The Manager / Operations Manager of the branch must inform a visually impaired/ blind customer of his / her rights and obligations before opening an account.

2.7) Illiterate visually impaired/blind person shall operate the bank account personally in the presence of a witness. The bank/MFB will not be responsible for any losses, claims, demands and consequences that may arise out of operation in the absence of any witness. However, in case of a literate visually impaired/blind person, the condition of presence of witness may not be required on providing duly witnessed undertaking by him/her stating that he/she would be responsible for all the transactions made in the account.

2.8) visually impaired/blind customer, if desires, may be allowed to appoint a person / persons as Power of Attorney or Mandate Holder to operate his / her bank account. This appointment will be duly witnessed by a person known to the concerned visually impaired person in the presence of a bank/MFB official.

3) Cash Withdrawal/Cheque Book:

3.1) the bank/MFB may allow the operations of the account of illiterate visually impaired/blind customers as it may deem feasible.

3.2) On the basis of undertaking (as stated at 2.7 above) by a literate visually impaired/blind person, the bank/MFB shall:

3.2.1) not restrict the operations of account to self-withdrawal only;

3.2.2) provide cheque book facility in a manner as provided to other customers;

3.2.3) adopt the same procedure for use of cheque as is being used for other customers;

3.2.4) honor the cheques issued in favor of third party (ies), if otherwise found in order;

3.2.5) allow over the counter cash payments in the presence of another bank official;

3.2.6) allow to get banking instruments issued through transfers from the account;

3.2.7) allow transfer of funds/online transaction in the account;

4) Phone/Internet Banking Facilities:

4.1) if requested, visually impaired/blind customer shall be provided with mobile or tele/phone banking facilities as are available to other customers.

4.2) Internet banking facility will be provided to literate visually impaired/blind persons.

4.3) the banks/MFBs are encouraged to develop web, desktop and mobile applications accessible to visually impaired/blind customers as per internationally recognized accessibility standards. Further,

the banks/MFBs shall device alternate methods of user authentication/password verification for its visually impaired/ blind customers.

5) ATM/Debit Cards:

The bank/MFB shall not deny issuance of ATM / Debit card to literate visually impaired/blind account holders against duly witnessed undertaking. However, for the purpose of installing Talking ATMs, the banks/MFBs shall follow the instructions issued vide CPD Circular No. 02 of February 13, 2014.

6) Credit Cards:

The bank/MFB shall allow issuance of credit card to visually impaired/blind customers upon duly witnessed request, if otherwise found eligible. However, prior to signing of contract, all such customers must be made aware of the likely risks associated with the handling/usage of the credit card.

7) Loans:

7.1) while dealing loan applications of visually impaired/blind persons, the bank/MFB shall adopt the same procedure/criteria as it follows in the case of other applicants.

7.2) the bank/MFB shall not impose additional terms and conditions on loan offering to visually impaired/ blind persons except requisite/standard conditions.

8) Lockers:

8.1) visually impaired/blind persons shall be provided with locker facility on the same terms and conditions as are applicable for other customers.

8.2) the bank/MFB shall preferably allot conveniently located lockers to visually impaired/ blind customers.

8.3) visually impaired/blind customers shall be allowed locker operations with the assistance of any person of their choice to ensure that all their belongings have been safe-In/out in the locker properly. That person needs to be registered by the visually impaired/blind person at the time of account opening.

8.4) The Branch Manager/Operations Manager shall ensure that the locker has been properly closed by the visually impaired/blind customers and nothing has been left behind.

- ## Account Operations

- Account operation Directives for different type of customers under Central Bank (SBP Guidelines) AML/CFT Regulations;

a) **Joint account holders** ; 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.

b) **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.

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

c) **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.

Banks/ DFIs shall not provide any banking services to proscribed entities and persons or to those who are associated 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.

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.

d) **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 afresh attested copy of his/her CNIC and bank/DFI is satisfied with CDD of the customer.

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.

e) **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.

f) **Politically Exposed Persons (PEPs);** In relation to PEPs and their close associates or family members, banks/DFIs shall:

(1) Implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP;

(2) 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;

(3) Establish, by appropriate means, the sources of wealth or beneficial ownership of funds; including obtaining a self-declaration to this effect; and

(4) Conduct during the course of business relations, enhanced monitoring of business relations with the customer.

g) **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 are 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.

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. 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

h) **Shaky & Immature Signatures treatment** ;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.

i) **Expired CNIC's treatment of an account holder;** 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 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired.

BPD Circular No. 07 of 2006 - TREATMENT FOR UNCLAIMED DEPOSIT UNDER CENTRAL BANK (SBP) DIRECTIVES

In terms of Section 31 of Banking Companies Ordinance, 1962 all Banks/DFIs in Pakistan are required to surrender to State Bank of Pakistan (SBP) all those deposits which have not been operated upon during the period of last ten years, except deposits in the name of a minor or a Government or a court of law, as stipulated under Subsection (1) of Section 31 of Banking Companies Ordinance (BCO), 1962.

2. In order to facilitate Banks/DFIs, instructions on the subject relating to definition, reporting, surrendering of unclaimed deposits, issuance of notice to the account holder, insertion of information in account opening form and procedure for refund of unclaimed deposits, etc issued since 1968 till to date have been reviewed and consolidated hereunder:-

i) DEFINITION OF UNCLAIMED DEPOSIT / INSTRUMENT

A debt payable either in Pakistani currency or any other (foreign) currency is owing by a banking company by reason of a deposit (time/demand deposit, or any other kind of deposit) or a financial instrument (pay slips / pay orders / D.Ds / T.Ts / M.Ts, or any other financial instrument), not being recorded in the name of a minor or a government or a court of law, in respect of which no transaction has taken place and no statement of account has been requested or acknowledged by the creditor during a period of ten years as reckoned under Subsection(1) of Section 31 of BCO 1962, will be classified as unclaimed deposit/instrument

ii) REPORTING OF UNCLAIMED DEPOSITS/ INSTRUMENTS

All Banks/DFIs will submit branch wise list of unclaimed deposits / instruments separately for Pak Rupee (PKR) and in foreign currency (FCY) on Form-XI (enclosed as Annexure-A) through soft copy (in MS-Excel format) as well as authenticated hard copy of the same within thirty days after the close of each calendar year.

iii) SURRENDER OF UNCLAIMED DEPOSIT

a) The amount of unclaimed PKR & FCY deposits/instruments will be surrendered during the first week of April of each calendar year along with a list of unclaimed deposits/instruments, which have been refunded by Banks/DFIs during the period i.e. from the date of reporting the unclaimed PKR & FCY deposits/instruments at the end of each calendar year and date of surrender of the outstanding amount thereof to SBP.

b) The Banks/DFIs will surrender the outstanding amount of the unclaimed FCY deposits / instruments through SBP nostro accounts maintained in any one of the six currencies namely US dollar-USD, Japan Yen-JPY, Euro-Eur, British Pound-GBP, Swiss Franc-CHF, United Arab Emirates Darham-AED.

c) Unclaimed FCY deposit/instrument maintained in other than the aforesaid six currencies will be surrendered by converting the same into US dollar.

d) In case of Frozen FCY deposits/instruments of 1998, as and when become unclaimed, the Banks/DFIs will surrender the equivalent PKR to SBP

iv) NOTICE TO THE HOLDER OF UNCLAIMED DEPOSIT/INSTRUMENT

a) All Banks/DFIs upon completion of a ten-year time period as stipulated in relevant provision of BCO, shall serve a three-month notice in writing by registered post acknowledgement due to the creditor or the beneficiary of the deposit/instrument on his/her address last made known to the banking company.

b) Banks/DFIs are required to maintain complete record of letter/envelope etc. posted at the address of the unclaimed deposit/instrument holder, at their respective branches as per the format enclosed (Annexure-B).

c) Apart from giving a notice to the respective account holder at the end of ten year period, Banks/DFIs should also make cognizable effort from time to time to contact such account holders where there has been no activity in the respective accounts for a considerable period.

d) Banks/DFIs would be required to intimate in-writing to the government departments/agencies, court of law and minors (after acquiring the age of maturity) for settlement of their deposits/instruments lying with them for more than ten years.

v) PRESERVATION OF DOCUMENTS

Banks/DFIs shall continue to preserve all signature cards and documents indicating “signing authorities” given to them and other documents relating to the debt or instrument until it is informed by SBP in writing that they need not be preserved any longer.

vi) INFORMATION IN ACCOUNT OPENING FORM (AOF)

Banks/DFIs shall insert a clause in “bold words” in their respective AOF indicating that a deposit/instrument, which remains inoperative for a period of ten years, shall become unclaimed and will be surrendered to SBP as per the provisions of BCO. The existing account holders should also be informed about the same through a letter to be sent with the bi-annual statement of account or any other methods as deem feasible by the Bank/DFI.

vii) PROCEDURE FOR REFUND OF UNCLAIMED DEPOSIT SURRENDERED TO SBP

Banks/DFIs while forwarding any claim for refund will provide legible and duly attested, copies of the following documents

I. Original application for refund along with verification of attested signature/thumb impression of the claimant by the concerned branch manager with name and stamp. Claimant’s address and contact number (if any) should be ensured in the application.

ii. Copy of three months’ notice served by the Banks/DFIs on the holder of the unclaimed deposit/instrument.

iii. Attested copy of Computerized National Identity Card (CNIC) of the claimant.

iv. Certificate as per enclosed format (Annexure-C).

v. Copy of relevant page of record furnished to SBP.

vi. Succession certificate in case of deceased customer.

- # Remittances (Local & Foreign)

1. **Inward Remittances;** The term 'inward remittance" means purchase of foreign currencies in whatever form and includes not only remittances by M.T., T.T., draft etc., but also purchase of travelers cheques, drafts under travelers letters of credit, bills of exchange, currency notes and coins etc. Debit to banks' non-resident Rupee accounts also constitutes an inward remittance. This chapter, however, does not cover purchase of foreign currency notes and coins which is dealt with in Chapter XI.

2. **Inward Remittance - No Restrictions;** There is no restriction on receipt of remittances from abroad either in foreign currency or by debit to non-resident Rupee accounts of banks' overseas branches or correspondents. Authorised Dealers may freely purchase T.Ts, M.Ts, drafts, bills etc.,

expressed and payable in foreign currencies or drawn in Rupees on banks' non-resident Rupee accounts. There is also no objection to their obtaining reimbursement in foreign currency from their overseas branches and correspondents in respect of Rupee bills and drafts which are purchased by them under letters of credit opened by non-resident banks or under other arrangements.

3**. Outward Remittances;** The term "outward remittance" means sale of foreign exchange in any form and includes not only remittances by T.Ts, M.Ts, drafts etc., but also sale of travellers cheques, travellers letters of credit, foreign currency notes and coins etc. Outward remittance can be made either by sale of foreign exchange or by credit to non-resident Rupee account of banks' overseas branches or correspondents. Authorised Dealers may sell foreign exchange for approved transactions only in accordance with the procedure outlined in this chapter. This chapter does not cover sale of foreign currency notes and coins which is dealt with in Chapter XI.

4. **Mode of Remittances;** Authorized Dealers should normally avoid issuing drafts in cover of outward remittances whenever remittance can be made by T.Ts, or M.Ts, etc. Where, however, the normal means of transfer is likely to result in unnecessary hardship or inconvenience to the remitter, drafts may be issued in the name of the beneficiaries of the remittance but such drafts should be crossed by the issuing bank as "Account Payee only".

INSTRUCTIONS FOR WIRE TRANSFERS/ FUND TRANSFERS UNDER AML/CFT REGULATIONS;

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;

Responsibility of the Ordering Institution

2. 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.

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 wire transfer originator;

(b) The wire transfer originator’s account number (or unique reference number assigned by the ordering institution where no account number exists);

(c) The wire transfer originator’s address, CNIC/passport number, date or place of birth or where originator is a legal person, necessary details such as registration number, date and place of incorporation; and

(d) A System Track Audit Number (STAN)

Responsibility of the Beneficiary Institution

4. 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 as for possible, shall determine that cross border transactions on behalf of customers are in compliance with the regulations of other country (originator’s country). 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.

Responsibility of Intermediary Institution

5. 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.

3) Banking Financing

Types of Credits

- Types of products/facilities offered – fund based & non-fund based facilities

What is fund based lending? What are the various forms in which fund based lending may be made by banks?

Fund based lending, where the lending bank commits the physical outflow of funds. The various forms in which fund based lending may be made by banks:

1) Loan
2) Overdraft
3) Cash Credit
4) Bills Purchased/Discounted
5) Working Capital Term Loans
6) Packing Credit

What is non-fund based lending? What are the various forms in which non- fund based lending may be made by banks?

The credit facilities given by the banks where actual bank funds are not involved are termed as 'non-fund based facilities'. These facilities are divided in three broad categories as under:

I. Letters of credit
II. Guarantees
III. Co-acceptance of-bills/deferred payment guarantees.

Credit Approval, Initiation & Management under Central Bank (SBP Risk Management Guidelines for Commercial Banks & DFIs).

Credit Origination;

Banks must operate within a sound and well-defined criteria for new credits as well as the expansion of existing credits. Credits should be extended within the target markets and lending strategy of the institution. Before allowing a credit facility, the bank must make an assessment of risk profile of the customer/transaction. This may include

a) Credit assessment of the borrower's industry, and macro-economic factors.

b) The purpose of credit and source of repayment.

c) The track record / repayment history of borrower.

d) Assess/evaluate the repayment capacity of the borrower.

e) The Proposed terms and conditions and covenants.

f) Adequacy and enforceability of collaterals.

g) Approval from appropriate authority

In case of new relationships consideration should be given to the integrity and repute of the borrowers or counter party as well as its legal capacity to assume the liability. Prior to entering into any new credit relationship the banks must become familiar with the borrower or counter party and be confident that they are dealing with individual or organization of sound repute and credit worthiness. However, a bank must not grant credit simply on the basis of the fact that the borrower is perceived to be highly reputable i.e. name lending should be discouraged.

While structuring credit facilities institutions should appraise the amount and timing of the cash flows as well as the financial position of the borrower and intended purpose of the funds. It is utmost important that due consideration should be given to the risk reward trade –off in granting a credit facility and credit should be

priced to cover all embedded costs. Relevant terms and conditions should be laid down to protect the institution's interest.

Institutions have to make sure that the credit is used for the purpose it was borrowed. Where the obligor has utilized funds for purposes not shown in the original proposal, institutions should take steps to determine the implications on creditworthiness. In case of corporate loans where borrower own group of companies such diligence becomes more important. Institutions should classify such connected companies and conduct credit assessment on consolidated/group basis.

In loan syndication, generally most of the credit assessment and analysis is done by the lead institution. While such information is important, institutions should not over rely on that. All syndicate participants should perform their own independent analysis and review of syndicate terms.

Institution should not over rely on collaterals / covenant. Although the importance of collaterals held against loan is beyond any doubt, yet these should be considered as a buffer providing protection in case of default, primary focus should be on obligor's debt servicing ability and reputation in the market.

Limit setting

An important element of credit risk management is to establish exposure limits for single obligors and group of connected obligors. Institutions are expected to develop their own limit structure while remaining within the exposure limits set by State Bank of Pakistan. The size of the limits should be ba sed on the credit strength of the obligor, genuine requirement of credit, economic conditions and the institution's risk tolerance. Appropriate limits should be set for respective products and activities. Institutions may establish limits for a specific industry, economic sector or geographic regions to avoid concentration risk.

Sometimes, the obligor may want to share its facility limits with its related companies. Institutions should review such arrangements and impose necessary limits if the transactions are frequent and significant.

Credit limits should be reviewed regularly at least annually or more frequently if obligor's credit quality deteriorates. All requests of increase in credit limits should be substantiated.

Credit Administration

Ongoing administration of the credit portfolio is an essential part of the credit process. Credit administration function is basically a back office activity that support and control extension and maintenance of credit. A typical credit administration unit performs following functions:

a. **Documentation**. It is the responsibility of credit administration to ensure completeness of documentation (loan agreements, guarantees, transfer of title of collaterals etc) in accordance with approved terms and conditions. Outstanding documents should be tracked and followed up to ensure execution and receipt.

b. Credit Disbursement. The credit administration function should ensure that the loan application has proper approval before entering facility limits into computer systems. Disbursement should be effected only after completion of covenants, and receipt of collateral holdings. In case of exceptions necessary approval should be obtained from competent authorities.

c. Credit monitoring. After the loan is approved and draw down allowed, the loan should be continuously watched over. These include keeping track of borrowers' compliance with credit terms, identifying early signs of irregularity, conducting periodic valuation of collateral and monitoring timely repayments.

d. Loan Repayment. The obligors should be communicated ahead of time as and when the principal/markup installment becomes due. Any exceptions such as non-payment or late payment should be tagged and communicated to the management. Proper records and updates should also be made after receipt.

e. Maintenance of Credit Files. Institutions should devise procedural guidelines and standards for maintenance of credit files. The credit files not only include all correspondence with the borrower but should also contain sufficient information necessary to assess financial health of the borrower and its repayment performance. It need not mention that information should be filed in organized way so that external / internal auditors or SBP inspector could review it easily.

f. Collateral and Security Documents. Institutions should ensure that all security documents are kept in a fireproof safe under dual control. Registers for documents should be maintained to keep track of their

movement. Procedures should also be established to track and review relevant insurance coverage for certain facilities/collateral. Physical checks on security documents should be conducted on a regular basis.

While in small Institutions it may not be cost effective to institute a separate credit administrative set-up, it is important that in such institutions individuals performing sensitive functions such as custody of key documents, wiring out funds, entering limits into system, etc., should report to managers who are independent of business origination and credit approval process.

Import & Export Documentation

Brief Perspective of Export Documentation

Now a day's export license is no more required to export. Only the following initial documents are required to export:

1) **NTN** National Tax Number Certificate, which is issued by the Income Tax Department on filing of application form accompanied with one attested copy of NIC.

2) Sales Tax Registration Commercial exporter is not required to register with Sales Tax

Department. But if you pay the sale tax on the goods from local market it will be better for you to get yourself registered with sales tax department so that you may claim your input tax deducting on your purchases. Once you are registered in sales tax department you will be obliged to the monthly sales tax return irrespective of the fact that you have been involved in any sales tax activity or not.

3) **Bank Account** Current Bank Account is required for export proceedings and documents.

4) **Chamber Membership Membership** certificate of Chamber of Commerce and Industries or any Relevant trade association is required.

5) Documents For Clearing Agent

Once the consignment, to be exported arrives at the port, usually a clearing agent services are sought. The following documents are required to provide to clearing agent to clear the consignment.

i) Packing List.

ii) Commercial Invoice.

iii) Letter of Credit (L/C).

iv) Certificate of Origin which is issued by Chamber of Commerce.

v) National Tax Number Certificate.

6) Form "E"

Form "E" (State bank form): All exports from Pakistan which are subject to Foreign Exchange Regulations are required to be declared on form „E which is in sets of four copies each. The exporter should submit the full set of Form „E to the bank after it has been completed and signed by the exporter himself or his authorized agent. While certifying Form „E, bank should ensure that exporters give only one address in Form „E. After the form is certified by the bank, it should be submitted to the Customs/Postal authorities at the time of shipment along with the shipping bill. The Customs authorities will detach the original copy and after filling in the portion relating to them and affixing their seal and signature thereon forward it to the State Bank. The Customs authorities will return the duplicate, triplicate and quadruplicate copies to the exporter or his authorized agent who will retain the quadruplicate for his own record and submit the duplicate and triplicate copies to the Authorized Dealer along with the shipping documents within 14 days from the date of shipment.

7) **Submission of Export Documents to the bank.** All shipping documents covering goods exported from Pakistan and declared on form „E must be passed through the medium of bank within 14 days from the date of shipment. The exporter must submit the duplicate (bearing Customs seal and signature of Customs Officials with Code number) and triplicate copies of form „E along with the shipping documents, invoices etc., to the

bank who had certified the form „E. An extra copy of the shipper's invoice must be attached to the triplicate copy of the form „E.

Brief Perspective of Import Documentation

Now a days import license is no MORE required to import into Pakistan. Only the following initial documents are required to import into Pakistan:

1) NTN National Tax Number Certificate, which is issued by the Income Tax Department on filing of application form accompanied with one attested copy of NIC.

2) Bank Account Current Bank Account is required for import proceedings and documents.

3) Sales Tax Registration Sales Tax Registration is required to import into Pakistan. For registration, Form ST-1is required to send to the local sales tax registration office via post with acknowledgment due (courier is preferable). The local registration office shall transmit filled up applications to the Central Registration Office based in CBR Islamabad. The previous requirements of furnishing supporting documents have been done away now there is no need to attach any document with the application. The Central Registration having on line access to database of NTN as well as of NADRA shall verify the particulars declared in the application with database. On verification, it shall generate and issue registration certificate to the applicant directly on his given address.

4) Chamber Membership ;Membership certificate of Chamber of Commerce and Industries or any relevant trade association of Pakistan.

SALES TAX ON IMPORT

Sales Tax Chargeable On Import into Pakistan.

Every importer is required to pay sales tax on taxable goods at the rate of 15% at the time of importation. "Taxable Goods" means all goods other than those which have been exempted from Sales Tax. The 6th Schedule of the Sales Tax Act, 1990 describes such goods on which Sales Tax is exempted. The Sales Tax in respect of goods imported into Pakistan shall be paid by the importer at the same time as making payment of customs duty.

The Sales Tax on imported goods is chargeable on assessed import value of the goods. "Assessed import value" means the value of imported goods determined under section 25 of the Customs Act, 1969 (IV of 1969), including the amount of customs duties and federal excise duty, if any, levied thereon;

Every importer is required to get himself registered with the sales tax department. For registration, Form ST-1 is required to send to the local sales tax registration office via post with acknowledgment due (courier is preferable). The local registration office shall transmit filled up applications to the Central Registration Office based in CBR Islamabad. The previous requirements of furnishing supporting documents have been done away now there is no need to attach any document with the application. The Central Registration having on line access to database of NTN as well as of NADRA shall verify the particulars declared in the application with database. On verification, it shall generate and issue registration certificateto the applicant directly on his given address.

In general, Sales Tax is chargeable at the rate of 15% but the section 4 of the Sales Tax Act, 1990 provide that the goods specified in the said section shall be charged to sales tax at the rate of zero per cent:(0%).

Every commercial importer shall pay Sales Tax in Value Addition Mode. "Commercial importer" means an importer who imports goods for the purpose of further supply to other persons and is registered as commercial importer whether exclusively or otherwise; "value addition" means the difference between the assessed import value of the goods and the value of supply for which the goods, in the same state, are supplied by the importer. A commercial importer shall pay sales tax on supplies of imported goods, at the rate of 15%, on a value addition of not less than ten per cent, through a challan in triplicate, at the same time as making payment of customs duty and sales tax in the Goods Declaration (GD) for such imported goods, calculated as shown in the Example below:

EXAMPLE: (a) Value of imported goods determined under section 25 of the Customs Act, 1969 (IV of 1969) = Rs. 100.00

(b) Customs duty e.g. (@20%) = Rs. 20.00

(c) Assessed import value (= a + b) = Rs. 120.00

(d) Sales tax (@15%) payable on bill of entry = Rs. 18.00

(e) Value of supplies, with value addition of 10% [= c + (c x 10 ¸100)] = Rs. 132.00

(f) Value addition on which sales tax is payable (= e - c) = Rs. 12.00

(g) Sales tax on value addition (= f x 15 ¸100)

(payable on treasury challan); = Rs. 1.80

5) Compliance Requirements of State Bank of Pakistan & Modern Trends in Banking

A. What Is Money Laundering?

Money laundering can be defined in a number of ways. Most countries subscribe to the definition adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention):

• The conversion or transfer of property, knowing that such property is derived from any [drug trafficking] offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

• The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses.

The Vienna Convention adds that money laundering also involves:

• The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses …or from an act of participation in such offense or offenses.

By its terms, the Vienna Convention limits predicate offenses (which is to say, the criminal activity whose illicit proceeds are laundered) to drug trafficking offenses. As a consequence, crimes unrelated to drug trafficking, such as tax evasion, fraud, kidnapping and theft, for example, are not defined as money laundering offenses under the Vienna Convention. Over the years, however, the international community has come to the view that predicate offenses for money laundering should go beyond drug trafficking. Thus, other international instruments have expanded the Vienna Convention's definition of predicate offenses to include other serious

crimes. For example, the United Nations Convention Against Transnational Organized Crime (2000) (Palermo Convention) requires all participant countries to apply that convention's money laundering offenses to "the widest range of predicate offenses."

The Financial Action Task Force on Money Laundering (FATF), which is recognized as the international standard setter for anti-money laundering (AML) efforts, defines the term money laundering succinctly as "the processing of…criminal proceeds to disguise their illegal origin" in order to "legitimize"the ill-gotten gains of crime.7 However, in its 40 recommendations for fighting money laundering (The Forty Recommendations), FATF specifically incorporates the Vienna Convention's technical and legal definition of money laundering and recommends expanding the predicate offenses of that definition to include all serious crimes.

B. What Is Terrorist Financing?

The United Nations (UN) has made numerous efforts, largely in the form of international treaties, to fight terrorism and the mechanisms used to finance it. Even before the September 11th attack on the United States, the UN had in place the International Convention for the Suppression of the Financing of Terrorism (1999), which provides:

1. Any person commits an offense within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or

(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

2. For an act to constitute an offense set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in paragraph 1, subparagraph (a) or (b).

The difficult issue for some countries is defining terrorism. Not all countries that have adopted the convention agree on what actions constitute terrorism. The meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country. FATF, which is also recognized as the international standard setter for efforts to combat the financing of terrorism (CFT), does not specifically define the term financing of terrorism in its eight Special Recommendations on Terrorist Financing (Special Recommendations) developed following the events of September 11, 2001. Nonetheless, FATF urges countries to ratify and implement the 1999 United Nations International Convention for Suppression of the Financing of Terrorism. Thus, the above definition is the one most countries have adopted for purposes of defining terrorist financing.

The Link between Money Laundering and Terrorist Financing

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

For these reasons, FATF has recommended that each country criminalize the financing of terrorism, terrorist acts and terrorist organizations, and designate such offenses as money laundering predicate offenses. Finally, FATF has stated that the eight Special Recommendations combined with The Forty Recommendations on money laundering constitute the basic framework for preventing, detecting and suppressing both money laundering and terrorist financing. Efforts to combat the financing of terrorism also require countries to consider expanding the scope of their AML framework to include non-profit organizations, particularly charities, to make sure such organizations are not used, directly or indirectly, to finance or support terrorism. CFT efforts also require examination of alternative money transmission or remittance systems, such as haw-alas. This effort includes consideration of what measures should be taken to preclude the use of such entities by money launderers and terrorists.

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations such as foundations or charities that in turn are utilized to support terrorist activities or terrorist organizations. Consequently, this difference requires special laws to deal with terrorist financing. However, to the extent that funds for financing terrorism are derived from illegal sources, such funds may already be covered by a country's AML framework, depending upon the scope of the predicate offenses for money laundering.

How is money laundered?

Proceeds of criminal acts can be laundered by a variety of methods and can range from buying and reselling high value items such as cars, jewellery, art etc. Criminal proceeds are also laundered through complex webs of legitimate businesses and company structures.

Whereas money can be laundered directly by purchasing high value goods such as cars or jewellery it can undergo a number of steps before it reaches the sales floor.

Typically, money laundering is a complex process involving a number of stages.

- **Placement;**
- **Layering**
- **Integration.**

Placement In the initial - or placement - stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

Layering After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

Integration Having successfully processed his/her criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

International initiatives For AML/CFT

What is "The Financial Action Task Force (FATF)" is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003 and most recently in 2012 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF's decision making body, the FATF Plenary, meets three times per year.

FATF 40 Recommendations

October 2003 (incorporating all subsequent amendments until October 2004)

INTRODUCTION

Money laundering methods and techniques change in response to developing counter-measures. Inrecent years, the Financial Action Task Force (FATF) has noted increasingly sophisticated combinations of techniques, such as the increased use of legal persons to disguise the true ownership and control of illegal proceeds, and an increased use of professionals to provide advice and assistance in laundering criminal funds. These factors, combined with the experience gained through the FATF's Non-Cooperative Countries and Territories process, and a number of national and international initiatives, led the FATF to review and revise the Forty Recommendations into a new comprehensive framework for combating money laundering and terrorist financing. The FATF now calls upon all countries to take the necessary steps to bring their national systems for combating money laundering and terrorist financing into compliance with the new FATF Recommendations, and to effectively implement these measures.

The review process for revising the Forty Recommendations was an extensive one, open to FATF members, non-members, observers, financial and other affected sectors and interested parties. This consultation process provided a wide range of input, all of which was considered in the review process.

The revised Forty Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the Eight Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing. The FATF recognises that countries have diverse legal and financial systems and so all cannot take identical measures to achieve the common objective, especially over matters of detail. The Recommendations therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional frameworks. The Recommendations cover all the measures that national systems should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and certain other businesses and professions; and international co-operation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering typologies. The 1996 Forty Recommendations have been endorsed by more than 130 countries and are the international antimony laundering standard.

In October 2001 the FATF expanded its mandate to deal with the issue of the financing of terrorism, and took the important step of creating the Eight Special Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organizations, and are complementary to the Forty Recommendations.

A key element in the fight against money laundering and the financing of terrorism is the need for countries systems to be monitored and evaluated, with respect to these international standards. The mutual evaluations conducted by the FATF and FATF-style regional bodies, as well as the assessments conducted by the IMF and World Bank, are a vital mechanism for ensuring that the FATF Recommendations are effectively implemented by all countries.

1 The FATF is an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering and terrorist financing. It currently has 36 members: 34 countries and governments and two international organizations; and more than 20 observers: five FATF-style regional bodies and more than 15 other international organizations or bodies. A list of all members and observers can be found on the FATF website at www.fatf-gafi.org.

2 The FATF Forty and Eight Special Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering and the financing of terrorism.

THE FORTY RECOMMENDATIONS

A. LEGAL SYSTEMS

Scope of the criminal offence of money laundering

1. Countries should criminalize money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year's imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences.

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

2. Countries should ensure that:

a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisional measures and confiscation

3. Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NONFINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

4. Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Customer due diligence and record-keeping

5.* Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customers due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

6.* Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.

4 Reliable, independent source documents, data or information will hereafter be referred to as "identification data".

**** Recommendations marked with an asterisk should be read in conjunction with their Interpretative Note.***

b) Obtain senior management approval for establishing business relationships with such customers.

c) Take reasonable measures to establish the source of wealth and source of funds.

d) Conduct enhanced ongoing monitoring of the business relationship.

7. Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

b) Assess the respondent institution's anti-money laundering and terrorist financing controls.

c) Obtain approval from senior management before establishing new correspondent relationships.

d) Document the respective responsibilities of each institution.

e) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

8. Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

9.* Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.

10.* Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

11.* Financial institutions should pay special attention to 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 such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

12.* The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance

13.* If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

14.* Financial institutions, their directors, officers and employees should be:

a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

15.* Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

b) An ongoing employee training programme.

c) An audit function to test the system.

16.* The requirements set out in Recommendations 13 to 15, and 21 apply to all designated nonfinancial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Other measures to deter money laundering and terrorist financing

17. Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

19. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

20. Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF

Recommendations

21. Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

22. Financial institutions should ensure that the principles applicable to financial institutions, whichare mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

Regulation and supervision

23.* Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

24. Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:

- casinos should be licensed;
- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino
- competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

25.* The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.

C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent authorities, their powers and resources

26.* Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

27.* Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialized in asset investigation and co-operative investigations with appropriate competent authorities in other countries.

28. When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

29. Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorized to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

30. Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staffs of those authorities are of high integrity.

31. Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with

each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

32. Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of legal persons and arrangements

33. Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures.

Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

34. Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

D. INTERNATIONAL CO-OPERATION

35. Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Mutual legal assistance and extradition

36. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

a) Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.

b) Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.

c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

37. Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalize the conduct underlying the offence.

38.* There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for coordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.

39. Countries should recognise money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other forms of co-operation

40.* Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

GLOSSARY

In these Recommendations the following abbreviations and references are used:

"**Beneficial owner**" refers to the natural person(s) who ultimately owns or controls a customer and/orthe person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

"**Core Principles**" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

"**Designated categories of offences**" means:

- participation in an organized criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- Insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

"**Designated non-financial businesses and professions**" means:

a) Casinos (which also includes internet casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

"**Designated threshold**" refers to the amount set out in the Interpretative Notes.

"**Financial institutions**" means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.
3. Financial leasing.
4. The transfer of money or value.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
(a) Money market instruments (cheques, bills, CDs, derivatives etc.);
(b) Foreign exchange;
(c) Exchange, interest rate and index instruments;
(d) Transferable securities;
(e) Commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.
13. Money and currency changing.

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

"**FIU**" means financial intelligence unit.

"**Legal arrangements**" refers to express trusts or other similar legal arrangements.

"**Legal persons**" refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

"**Payable-through accounts**" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

"**Politically Exposed Persons**" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign 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 reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

"**Shell bank**" means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

"**STR**" refers to suspicious transaction reports.

"**Supervisors**" refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

"**The FATF Recommendations**" refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing.

INTERPRETATIVE NOTES

General

1. Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions".

2. Recommendations 5-16 and 21-22 state that financial institutions or designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige financial institutions or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.

3. Where reference is made to a financial institution being satisfied as to a matter, that institution must be able to justify its assessment to competent authorities.

4. To comply with Recommendations 12 and 16, countries do not need to issue laws or regulations that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws or regulations covering the underlying activities.

5. The Interpretative Notes that apply to financial institutions are also relevant to designated nonfinancial businesses and professions, where applicable.

Recommendations 5, 12 and 16

The designated thresholds for transactions (under Recommendations 5 and 12) are as follows:

- Financial institutions (for occasional customers under Recommendation 5) - USD/EUR 15 000.
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3 000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15 000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Recommendation 5

Customer due diligence and tipping off

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

a) Normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.

b) Make a STR to the FIU in accordance with Recommendation 13.

2. Recommendation 14 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

CDD for legal persons and arrangements

4. When performing elements (a) and (b) of the CDD process in relation to legal persons or arrangements, financial institutions should:

a) Verify that any person purporting to act on behalf of the customer is so authorized, and identify that person.

b) Identify the customer and verify its identity - the types of measures that would be normally needed to satisfactorily perform this function would require obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the customer's name, the names of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.

c) Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons.The types of measures that would be normally needed to satisfactorily perform this function would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.

The relevant information or data may be obtained from a public register, from the customer or from other reliable sources.

Reliance on identification and verification already performed

5. The CDD measures set out in Recommendation 5 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile.

Timing of verification

6. Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at thetime the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
- Life insurance business. In relation to life insurance business, countries may permit the identification and verification of the beneficiary under the policy to take place after having established the business relationship with the policyholder. However, in all such cases, identification and verification should occur at or before the time of payout or the time where the beneficiary intends to exercise vested rights under the policy.

7. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. Financial institutions should refer to the Basel CDD paper (section 2.2.6.) for specific guidance on examples of risk management measures for non-face to face business.

Requirement to identify existing customers

8. The principles set out in the Basel CDD paper concerning the identification of existing customers should serve as guidance when applying customer due diligence processes to institutions engaged in banking activity, and could apply to other financial institutions where relevant.

Simplified or reduced CDD measures

9. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

10. Examples of customers where simplified or reduced CDD measures could apply are:

- financial institutions – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.
- Public companies that are subject to regulatory disclosure requirements.
- Government administrations or enterprises.

11. Simplified or reduced CDD measures could also apply to the beneficial owners of pooled accounts held by designated non financial businesses or professions provided that those businesses or professions are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring their compliance with those requirements. Banks should also refer to the Basel CDD paper (section 2.2.4.), which provides specific guidance concerning situations where an account holding institution may rely on a customer that is a professional financial intermediary to perform the customer due diligence on his or its own customers (i.e. the beneficial owners of the bank account). Where relevant, the CDD Paper could also provide guidance in relation to similar accounts held by other types of financial institutions.

12. Simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

- Life insurance policies where the annual premium is no more than USD/EUR 1 000 or a single premium of no more than USD/EUR 2 500.
- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.
- A pension, superannuation or similar scheme that provides retirement benefits toemployees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

13. Countries could also decide whether financial institutions could apply these simplified measures only to customers in its own jurisdiction or allow them to do for customers from any other jurisdiction that the original country is satisfied is in compliance with and has effectively implemented the FATF Recommendations.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

Recommendation 6

Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.

Recommendation 9

This Recommendation does not apply to outsourcing or agency relationships.

This Recommendation also does not apply to relationships, accounts or transactions between financial institutions for their clients. Those relationships are addressed by Recommendations 5 and 7.

Recommendations 10 and 11

In relation to insurance business, the word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits.

Recommendation 13

1. The reference to criminal activity in Recommendation 13 refers to:

a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or

b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

2. In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state inter alia that their transactions relate to tax matters.

Recommendation 14 (tipping off)

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.

Recommendation 15

The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.

Recommendation 16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.

Recommendation 23

Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view. Hence, where shareholder suitability (or “fit and proper”) tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Recommendation 25

When considering the feedback that should be provided, countries should have regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

Recommendation 26

Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

Recommendation 27

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

Recommendation 38

Countries should consider:

a) Establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

b) Taking such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Recommendation 40

1. For the purposes of this Recommendation:

- "Counterparts" refers to authorities that exercise similar responsibilities and functions.
- "Competent authority" refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

2. Depending on the type of competent authority involved and the nature and purpose of the cooperation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance of extradition.

3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

- Searching its own databases, which would include information related to suspicious transaction reports.
- Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information.

Basel Committee on Banking Supervision

Customer due diligence for banks

October 2001

Customer due diligence for banks

I. Introduction

1. 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 become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

2. In reviewing the findings of an internal survey of cross-border banking in 1999, the Basel Committee identified deficiencies in a large number of countries' know-your-customer (KYC) policies for banks. Judged from a supervisory perspective, KYC policies in some countries have significant gaps and in others they are non-existent. Even among countries with well-developed financial markets, the extent of KYC robustness varies. Consequently, the Basel Committee asked the Working Group on Cross-border Banking1 to examine the KYC procedures currently in place and to draw up recommended standards applicable to banks in all countries. The resulting paper was issued as a consultative document in January 2001. Following a review of the comments received, the Working Group has revised the paper and the Basel Committee is now distributing it worldwide in the expectation that the KYC framework presented here will become the benchmark for supervisors to establish national practices and for banks to design their own programmes. It is important to acknowledge that supervisory practices of some jurisdictions already meet or exceed the objective of this paper and, as a result, they may not need to implement any changes.

3. KYC is most closely associated with the fight against money-laundering, which is essentially the province of the Financial Action Task Force (FATF).2 It is not the Committee's intention to duplicate the efforts of the FATF. Instead, the Committee's interest is from a wider prudential perspective. Sound KYC policies and procedures are critical in protecting the safety and soundness of banks and the integrity of banking systems. The Basel Committee and the Offshore Group of Banking Supervisors (OGBS) continue to support strongly the adoption and implementation of the FATF recommendations, particularly those relating to banks, and intend the standards in this paper to be consistent with the FATF recommendations. The Committee and the OGBS will also consider the adoption of any higher standards introduced by the FATF as a result of its current review of the 40 Recommendations. Consequently, the Working Group has been and will remain in close contact with the FATF as it develops its thoughts.

4. The Basel Committee's approach to KYC is from a wider prudential, not just antimony laundering, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account

1 This is a joint group consisting of members of the Basel Committee and of the Offshore Group of Banking Supervisors.

2 The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. It has 29 member countries and two regional organizations . It works in close cooperation with other international bodies involved in this area such as the United Nations Office for Drug Control and Crime Prevention, the Council of Europe, the Asia-Pacific Group on Money Laundering and the Caribbean Financial Action Task Force. The FATF defines money laundering as the processing of criminal proceeds in order to disguise their illegal origin.

opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

5. The Basel Committee's interest in sound KYC standards originates from its concerns for market integrity and has been heightened by the direct and indirect losses incurred by banks due to their lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the banks' reputation significantly diminished had the banks maintained effective KYC programmes.

6. This paper reinforces the principles established in earlier Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation. In developing this guidance, the Working Group has drawn on practices in member countries and taken into account evolving supervisory developments. The essential elements presented in this paper are guidance as to minimum standards for worldwide implementation for all banks. These standards may need to be supplemented and/or strengthened, by additional measures tailored to the risks of particular institutions and risks in the banking system of individual countries. For example, enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers. In a number of specific sections in this paper, there are recommendations for higher standards of due diligence for higher risk areas within a bank, where applicable.

7. The need for rigorous customer due diligence standards is not restricted to banks. The Basel Committee believes similar guidance needs to be developed for all non-bank financial institutions and professional intermediaries of financial services such as lawyers and accountants.

II. Importance of KYC standards for supervisors and banks

8. The FATF and other international groupings have worked intensively on KYC issues, and the FATF's 40 Recommendations on combating money-laundering have international recognition and application. It is not the intention of this paper to duplicate that work.

9. At the same time, sound KYC procedures have particular relevance to the safety and soundness of banks, in that:

- they help to protect banks' reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
- They constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

10. The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

11. **Reputational risk** poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.

12. **Operational risk** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programmes, ineffective control procedures and failure to practice due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.

13. **Legal risk** is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

14. Supervisory concern about **concentration risk** mostly applies on the assets side of the balance sheet. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

15. On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analyzing deposit concentrations requires banks to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only

know but maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

16. Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis.

17. Both the Basel Committee and the Offshore Group of Banking Supervisors are fully convinced that effective KYC practices should be part of the risk management and internal control systems in all banks worldwide. National supervisors are responsible for ensuring that banks have minimum standards and internal controls that allow them to adequately know their customers. Voluntary codes of conduct4 issued by industry organizations or associations can be of considerable value in underpinning regulatory guidance, by giving practical advice to banks on operational matters. However, such codes cannot be regarded as a substitute for formal regulatory guidance.

III. Essential elements of KYC standards

18. The Basel Committee's guidance on KYC has been contained in the following three papers and they reflect the evolution of the supervisory thinking over time. The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering issued in 1988 stipulates the basic ethical principles and encourages banks to put in place effective procedures to identify customers, decline suspicious transactions and cooperate with law enforcement agencies. The 1997 Core Principles for Effective Banking Supervision states, in a broader discussion of internal controls, that banks should have adequate policies, practices and procedures in place, including strict "know-your-customer" rules; specifically, supervisors should encourage the adoption of the relevant recommendations of the FATF. These relate to customer identification and record-keeping, increased diligence by financial institutions in detecting and reporting suspicious transactions, and measures to deal with countries with inadequate anti-money laundering measures. The 1999 Core Principles Methodology further elaborates the Core Principles by listing a number of essential and additional criteria. (Annex 1 sets out the relevant extracts from the Core Principles and the Methodology.)

19. All banks should be required to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements".5 Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account.KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk.

1. Customer acceptance policy

20. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons (see section 2.2.3 below), should be taken exclusively at senior management level.

2. Customer identification

21. Customer identification is an essential element of KYC standards. For the purposes of this paper, a customer includes:

- the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);
- the beneficiaries of transactions conducted by professional intermediaries; and
- any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

22. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.

23. Banks should "document and enforce policies for identification of customers and those acting on their behalf". The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction.

24. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

25. Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

26. Banks should develop "clear standards on what records must be kept on customer identification and individual transactions and their retention period". Such a practice is essential to permit a bank to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution. As the starting point and natural follow-up of the identification process, banks should obtain customer identification papers and retain copies of them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

2.1 General identification requirements

27. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account. National supervisors are encouraged to provide guidance to assist banks in designing their own identification procedures. The Working Group intends to develop essential elements of customer identification requirements.

28. When an account has been opened, but problems of verification arise in the banking relationship which cannot be resolved, the bank should close the account and return the monies to the source from which they were received.

29. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer.

30. Banks should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.

2.2 Specific identification issues

31. There are a number of more detailed issues relating to customer identification which need to be addressed. Several of these are currently under consideration by the FATF as part of a general review of its 40 recommendations, and the Working Group recognises the need to be consistent with the FATF.

2.2.1 Trust, nominee and fiduciary accounts

32. Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. Banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlers/grantors and beneficiaries.

2.2.2 Corporate vehicles

33. Banks need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international business companies, may make proper identification of customers or beneficial owners difficult. A bank should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

34. Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies needs to be obtained. In the case of entities which have a significant proportion of capital in the form of bearer shares, extra vigilance is called for. A bank may be completely unaware that the bearer shares have changed hands. The onus is on banks to put in place satisfactory procedures to monitor the identity of material beneficial owners. This may require the bank to immobilize the shares, e.g. by holding the bearer shares in custody.

**** In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.**

**** Beneficiaries should be identified as far as possible when defined. It is recognised that it may not be possible to identify the beneficiaries of trusts precisely at the outset. For example, some beneficiaries may be unborn children and some may be conditional on the occurrence of specific events. In addition, beneficiaries being specific classes of individuals (e.g. employee pension funds) may be appropriately dealt with as pooled accounts as referred to in paragraphs 38-9.**

2.2.3 Introduced business

35. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries, it has therefore become customary for banks to rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way

remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

36. The Basel Committee recommends that banks that use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out in this paper. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:12

- it must comply with the minimum customer due diligence practices identified in this paper;
- the customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted itself for the customer;
- the bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- the bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the financial intelligence unit or equivalent enforcement agency, where appropriate legal authority has been obtained.

In addition, banks should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above.

2.2.4 Client accounts opened by professional intermediaries

37. When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

38. Banks often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Banks also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

39. Where the funds are co-mingled, the bank should look through to the beneficial owners. There can be circumstances where the bank may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as the bank. National supervisory guidance should clearly set out those circumstances in which banks need not look beyond the intermediary. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the bank should apply the criteria set out in paragraph 36 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

40. Where the intermediary is not empowered to furnish the required information on beneficiaries to the bank, for example, lawyers13 bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this paper or to the requirements of comprehensive anti-money laundering legislation, then the bank should not permit the intermediary to open an account.

2.2.5 Politically exposed persons

41. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

42. Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

43. Some countries have recently amended or are in the process of amending their laws and regulations to criminalise active corruption of foreign civil servants and public officers in The FATF is currently engaged in a review of KYC procedures governing accounts opened by lawyers on behalf of clients. accordance with the relevant international convention.14 In these jurisdictions foreign corruption becomes a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer, internal freeze of funds etc). But even in the absence of such an explicit legal basis in criminal law, it is clearly undesirable, unethical and incompatible with the fit and proper conduct of banking operations to accept or maintain a business relationship

if the bank knows or must assume that the funds derive from corruption or misuse of public assets. There is a compelling need for a bank considering a relationship with a person whom it suspects of being a PEP to identify that person fully, as well as people and companies that are clearly related to him/her.

44. Banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level.

2.2.6 Non-face-to-face customers

45. Banks are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview. One issue that has arisen in this connection is the possibility of independent verification by a reputable third party. This whole subject of nonface- to-face customer identification is being discussed by the FATF, and is also under review in the context of amending the 1991 EEC Directive.

46. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

47. Even though the same documentation can be provided by face-to-face and non face- to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers. With telephone and electronic banking, the verification problem is made even more difficult.

48. In accepting business from non-face-to-face customers:

- banks should apply equally effective customer identification procedures for nonface-to-face customers as for those available for interview; and
- there must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- certification of documents presented;
- requisition of additional documents to complement those which are required for face-to-face customers;

- independent contact with the customer by the bank;
- third party introduction, e.g. by an introducer subject to the criteria established in paragraph 36; or
- requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

2.2.7 Correspondent banking

49. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent banks have no physical presence. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this paper, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

50. Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country. Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

51. In particular, banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against anti-money laundering. Banks should establish that their respondent banks have due diligence standards as set out in this paper, and employ enhanced due diligence procedures with respect to transactions carried out though the correspondent accounts.

52. Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out in paragraph 36.

3. On-going monitoring of accounts and transactions

53. On-going monitoring is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities can be very helpful to banks and should be included as part of a jurisdiction's anti-money laundering procedures and/or guidance.

54. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.
- Senior management in charge of private banking business should know the personal circumstances of the bank's high risk customers and be alert to sources of third party information. Significant transactions by these customers should be approved by a senior manager.
- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

4. Risk management

55. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures are managed effectively and are, at a minimum, in accordance with local supervisory practice. The channels for reporting suspicious transactions should be clearly specified in writing, and communicated to all personnel. There should also be internal procedures for assessing whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement and and/or supervisory authorities.

56. Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

57. Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management should ensure that audit functions are staffed adequately with individuals who are well versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

58. All banks must have an ongoing employee-training programme so that bank staff are adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within banks that promotes such understanding is the key to successful implementation.

59. In many countries, external auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice.

IV. The role of supervisors

60. Based on existing international KYC standards, national supervisors are expected to set out supervisory practice governing banks' KYC programmes. The essential elements as presented in this paper should provide

clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice.

61. In addition to setting out the basic elements for banks to follow, supervisors have a responsibility to monitor that banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Supervisors should ensure that appropriate internal controls are in place and that banks are in compliance with supervisory and regulatory guidance. The supervisory process should include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts. Supervisors should always have the right to access all documentation related to accounts maintained in that jurisdiction, including any analysis the bank has made to detect unusual or suspicious transactions.

62. Supervisors have a duty not only to ensure their banks maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking system.17 Supervisors should make it clear that they will take appropriate action, which may be severe and public if the circumstances warrant, against banks and their officers who demonstrably fail to follow their own internal procedures and regulatory requirements. In addition, supervisors should ensure that banks are aware of and pay particular attention to transactions that involve jurisdictions where standards are considered inadequate. The FATF and some national authorities have listed a number of countries and jurisdictions that are considered to have legal and administrative arrangements that do not comply with international standards for combating money laundering. Such findings should be a component of a bank's KYC policies and procedures.

V. Implementation of KYC standards in a cross-border context

63. Supervisors around the world should seek, to the best of their efforts, to develop and implement their national KYC standards fully in line with international standards so as to avoid potential regulatory arbitrage and safeguard the integrity of domestic and international banking systems. The implementation and assessment of such standards put to the test the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a group wide basis. This is a challenging task for banks and supervisors alike.

64. Supervisors expect banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. The supervision of international banking can only be effectively carried out on a consolidated basis, and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Therefore, it is important that KYC documentation is properly filed and available for their inspection. As far as compliance checks are concerned, supervisors and external auditors should in most cases examine systems and controls and look at customer accounts and transactions monitoring as part of a sampling process.

65. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

66. Where the minimum KYC standards of the home and host countries differ, branches and subsidiaries in the host jurisdictions should apply the higher standard of the two. In general, there should be no impediment to prevent a bank from adopting standards that are higher than the minima required locally. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of home country KYC standards, where the latter are more stringent, host country supervisors should use their best endeavors to have the law and regulations changed. In the meantime, overseas branches and subsidiaries would have to comply with host country standards, but they should make sure the head office or parent bank and its home country supervisor are fully informed of the nature of the difference.

67. Criminal elements are likely to be drawn toward jurisdictions with such impediments. Hence, banks should be aware of the high reputational risk of conducting business in these jurisdictions. Parent banks should have a procedure for reviewing the vulnerability of the individual operating units and implement additional

safeguards where appropriate. In extreme cases, supervisors should consider placing additional controls on banks operating in those jurisdictions and ultimately perhaps encouraging their withdrawal.

68. During on-site inspections, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. This will require a review of customer files and some random sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. Where the home country supervisor requires consolidated reporting of deposit or borrower concentrations or notification of funds under management, there should be no impediments. In addition, with a view to monitoring deposit concentrations or the funding risk of the deposit being withdrawn, home supervisors may apply materiality tests and establish some thresholds so that if a customer's deposit exceeds a certain percentage of the balance sheet, banks should report it to the home supervisor. However, safeguards are needed to ensure that information regarding individual accounts is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner. A statement of mutual cooperation18 to facilitate information sharing between the two supervisors would be helpful in this regard.

69. In certain cases there may be a serious conflict between the KYC policies of a parent bank imposed by its home authority and what is permitted in a cross-border office. There may, for example, be local laws that prevent inspections by the parent banks' compliance officers, internal auditors or home country supervisors, or that enable bank customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are. In such cases, the home supervisor should communicate with the host supervisor in order to confirm whether there are indeed genuine legal impediments and whether they apply extraterritorially. If they prove to be Insurmountable, and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the bank may decide for itself, or be required by its home supervisor, to close down the operation in question. In the final analysis, any arrangements underpinning such on-site examinations should provide a mechanism that permits an assessment that is satisfactory to the home supervisor. Statements of cooperation or memoranda of understanding setting out the mechanics of the arrangements may be helpful. Access to information by home country supervisors should be as unrestricted as possible, and at a minimum they should have free access to the banks' general policies and procedures for customer due diligence and for dealing with suspicions.

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

BANKING POLICY & REGULATIONS DEPARTMENT

STATE BANK OF PAKISTAN

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 in line with Para 13 below;

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

CDD Measures for Establishing Business Relationship

Identification of Customers

2. Every customer shall be identified for establishing business relationship. For this purpose, 'Annexure–I' provides range of documents which shall be obtained for different types of customers.

3. 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;

(a) Full name as per identity document;

(b) CNIC/Passport/NICOP/POC/ARC number or where the customer is not natural person, the registration/ incorporation number or business registration number (as applicable);

(c) Existing residential address, registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable);

(d) Date of birth, incorporation or registration (as applicable);

(e) Nationality or place of birth, incorporation or registration (as applicable);

(f) Nature of business, geographies involved and expected type of counter-parties(as applicable);

(g) Purpose of account;

(h) Type of account;

(i) Source of earnings;

(j) Expected monthly credit turnover (amount and No. of transactions); and

(k) Normal or expected modes of transactions.

Verification of Identity;

4. The Bank/ DFI shall verify identity documents of the customers from relevant authorities/document issuing bodies and 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.

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

5. In relation to Para 4 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.

6. 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.

Identification and Verification of Identity of Beneficial Owners;

7. 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).

8. 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 Para 9 below and (ii) determine that the natural persons who ultimately own or control the customer.

Information on the Purpose and Intended Nature of Business Relations;

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

Timing of Verification;

10. 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.

11. 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.

12. In relation to Para 11 above, 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;

(a) 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.

(b) No debit will be allowed or cheque book is issued until positive verification is completed.

(c) 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.

CCD Measures for Occasional Customers/ Walk-in Customers;

13. Banks/DFIs shall;

(a) obtain copy of CNIC from occasional customers/walk-in customers conducting cash transactions above rupees 1.0 million whether carried out in a single operation or in multiple operations that appear to be linked;

(b) Obtain originator information along with copy of CNIC while carrying out online transactions (regardless of threshold) by occasional customers/walk-in customers or where such person is conducting transaction on behalf of an account holder;

(c) In relation to Para 13 (b) above, name and CNIC No. of originator shall be captured in system and made accessible along with transaction details at corresponding branch if (i) online transaction exceeds Rs. 100,000; and (ii) transaction is taking place between two branches of different cities.

(d) Obtain copy of CNIC from occasional customers/walk-in-customers who wish to purchase remittance instruments e.g. POs, DDs and MTs etc.

Where CDD Measures are Not Completed;

14. 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.

Ongoing Monitoring;

15. 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.

16. 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.

17. 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.

18. In relation to Para 17 above, in order to avoid the risk where front-end staff do not follow the desired procedures and update the KYC/CDD form of the customer based on their personal knowledge/perception rather than interviewing the customer, banks/DFIs shall obtain sign-off from the customer on every revision of KYC/CDD form.

Anonymous or Fictitious Account

19. 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

20. Banks/DFIs 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.

Joint Accounts

21. 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.

Government Accounts

22. 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.

23. 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.

Existing Customers

24. 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.

25. Banks/ DFIs shall not provide any banking services to proscribed entities and persons or to those who are associated 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.

26. 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.

Dormant accounts

27. 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 afresh attested copy of his/her CNIC and bank/DFI is satisfied with CDD of the customer.

28. In relation to Para 26 and 27 above, 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.

Prohibition of personal accounts for business purposes

29. 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.

Politically Exposed Persons (PEPs)

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

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP;

(b) 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;

(c) establish, by appropriate means, the sources of wealth or beneficial ownership of funds; including obtaining a self-declaration to this effect; and

(d) conduct during the course of business relations, enhanced monitoring of business relations with the customer.

NGOs/NPOs/ Charities' accounts

31. 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 are commensurate with the stated objectives and purposes.

32. 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.

33. 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.

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

35. 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.

REGULATION - 2

CORRESPONDENT BANKING

1. In addition to measures required under Regulation 1 (as necessary), banks/ DFIs shall take the following measures for providing correspondent banking services-

(a) assess the suitability of the respondent bank by taking the following steps:

(i) 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

- 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

(ii) 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

(iii) 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;

(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.

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 1 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 that third party and is willing and able to provide customer identification information to the correspondent bank/ DFI upon request.

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.

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.

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;

Responsibility of the Ordering Institution

2. 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.

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 wire transfer originator;

(b) the wire transfer originator's account number (or unique reference number assigned by the ordering institution where no account number exists);

(c) the wire transfer originator's address, CNIC/passport number, date or place of birth or where originator is a legal person, necessary details such as registration number, date and place of incorporation; and

(d) a System Track Audit Number (STAN)

Responsibility of the Beneficiary Institution

4. 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 as for possible, shall determine that cross border transactions on behalf of customers are in compliance with the regulations of other country (originator's country). 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.

Responsibility of Intermediary Institution

5. 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.

REGULATION - 4

REPORTING OF TRANSACTIONS (STRs/CTRs)

1. Banks/ DFIs shall comply with the provisions of AML Act, rules and regulations issued there under 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.

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 at 'Annexure-II'.

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 in real time, 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 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.

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. 2.5 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.

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.

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.

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.

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.

REGULATION - 6

INTERNAL CONTROLS, POLICIES, COMPLIANCE, AUDIT AND TRAINING

Bank/DFIs own AML/CFT policies, procedures & controls

1. 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.

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.

Foreign Branches and Subsidiaries

4. 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.

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.

Compliance

7. 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.

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.

Audit

9. 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.

Employee Due Diligence

10. 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.

Training

11. 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.

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. 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.

- Minimum Documents to be obtained from Various Types of Customers under AML/CFT Regulations for account opening Purpose;

(Annexure-I)

Sr. No	Type of Customers	Documents/papers 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
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.
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; (viii) For individual (natural person) shareholders holding 5% or above stake in company/corporation, photocopies of identity document as per S. No. 1 above; and (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. 1 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 (a) Certificate of Registration/Instrument of Trust (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 AML/CFT Regulations 20 Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.

7	NGOs/NPOs/Charities	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
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

Note:

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.

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 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired.

5. In case the CNIC does not contain a photograph, bank/DFI shall obtain following:

(i) A duly attested copy of either driving license, service card, Nikkah Nama, birth certificate, Educational degree/certificate, pension book, insurance certificate.

(ii) A photograph duly attested by gazetted officer/Nazim/Administrator/bank officer.

(iii) A copy of CNIC without photograph duly attested by the same person who attested the photograph.

6. 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.

7. 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.

Annexure–II

Examples or Characteristics of Suspicious Transactions (Red Alerts)

That May Be a Cause for Increased Scrutiny for AML/CFT Purposes

1. General Comments

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.

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;

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;

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;

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

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

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

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

xxii) 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;

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;

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);

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;

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;

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;

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;

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;

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;

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;

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);

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.

********HAPPY Learning**********