AML/CFT GUIDELINES ON RISK BASED APPROACH FOR BANKS & DFIs

(Updated up to March 31, 2015)

BANKING POLICY & REGULATIONS DEPARTMENT
STATE BANK OF PAKISTAN

AML/CFT Guidelines on Risk Based Approach

(A) PREAMBLE

1. The regulatory framework for combating money laundering and terrorist financing is applicable in the form of AML/CFT Regulations as amended from time to time. Keeping in view of growing sensitivities on domestic and international front, there is need to focus on the areas where related risks are relatively high in order to allocate resources in the most effective way. Accordingly, following guidelines are aimed at providing enabling environment for effective implementation of risk based approach considering banks' internal policies, procedures and risk parameters etc.

(B) GENERAL REQUIREMENTS

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

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

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

      (i) Customers: Identifying risk determinants while establishing relationships with customer;
      (ii) Products: Envisaging risk attributes resulting from customer's need for financial services and appropriate controls;

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

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

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

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

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

(C) RISK PROFILING OF CUSTOMERS

3. Banks/ DFIs should profile every new customer using their own judgment and information obtained through CDD/KYC process. A template of Customer Risk Profiling (CRP) is provided at '**Annexure-I**' for guidance of bank/DFIs in order to develop their own CRP formats considering their business activities, customer base and internal procedures etc.

(D) SPECIFIC HIGH RISK ELEMENTS AND RECOMMENDATIONS FOR EDD

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

S. no	Customers	Recommendations for EDD
a)	NPOs/NGOs/ Charities, Trusts, Clubs, Societies, and Associations etc	In relation to these customers, banks/DFIs may: (i) obtain a declaration from Governing Body/Board of Trustees/Executive Committee/sponsors on ultimate control, purpose and source of funds etc; (ii) obtain an undertaking from Governing

		Body/Board of Trustees/Executive Committee /sponsors to inform the bank/DFI about any change of control or ownership during operation of the account; and (iii) obtain a fresh Resolution of the Governing Body/Executive Committee of the entity in case of change in person(s) authorized to operate the account.
b)	Housewife accounts	In relation to housewife accounts, banks/DFIs may (i) obtain a self-declaration for source and beneficial ownership of funds; (ii) Update details of funds providers, if any along with customer's profile; and (iii) Identify and verify funds providers if monthly credit turnover exceeds an appropriate threshold to be decided by banks/DFIs.
c)	Proprietorships and self employed individuals/ professionals	In relation to these accounts, following measures may be taken by banks/DFIs: (i) The business transactions in personal accounts of proprietors may only be permitted by linking it with account/business turnover. For example, such customers having monthly credit turnover of Rs. 5 million or above may be required to open a separate account for business related transactions; and (ii) In order to verify the physical existence of business or self-employment status, banks/DFIs may conduct physical verification within 05 working days of the opening of account and document the results thereof on account opening form. In case of unsatisfactory verification, bank/DFI may consider reporting it to FMU and/or may change risk profile, as appropriate.
d)	Landlords	In relation to such customers, banks/DFIs may

		apply any recommend methods for assessment of source of funds/income e.g. Passbook of landholding records etc.
S. no	**Products & Services**	**Recommendations for EDD**
a)	Online transactions	In relation to online transactions, Banks/DFIs should pay special attention to geographical factors/locations for movement funds.
S. no	**Delivery Channels**	**Recommendations for EDD**
a)	Cash	In relation to cash transactions, Banks/DFIs may: (i) monitor cash transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and (ii) pay special attention on cash based transactions considering examples of Red Alerts given in Annexure-II to AML/CFT regulations.
b)	Wire transfers	In relation to wire transfers, banks/DFIs may: (i) monitor such transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and (ii) Ensure that funds transfers which are out of character/ inconsistent with the history, pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.

(E) GENERAL HIGH RISK SCENARIOS/ FACTORS

5. In addition, following high risk elements/factors should also be considered as per international standards.

Customers	Products and Delivery Channels	Geography or Locations
• Non-resident customers • Correspondent banks' accounts • Customers with links to	• Non-face-to-face business relationships or transactions	• The jurisdictions which have been identified for inadequate AML/CFT measures by FATF or called

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

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

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

(f) Obtaining additional information on the sources of funds or sources of wealth of the customer;
(g) Obtaining the approvals of senior management to commence or continue the business relationship;
(h) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
(i) A signatory who is neither a beneficial owner nor a key principal may also be verified if they were the principal contact with the bank/DFI acting on behalf of directors or owners with whom the bank/DFI had little or no direct contact; and
(j) Documentary evidence may be sought to support transaction where possible, e.g. purchase of property etc.

(F) GENERAL LOW RISK SCENARIOS/ FACTORS

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

Low risk factors for Customers	• A financial institution regulated/ supervised by the State Bank of Pakistan except exchange companies/ money remitters; • A Non-Bank Finance Company (NBFC) regulated/ supervised by Securities and Exchange Commission of Pakistan (SECP) unless an entity is notified for application of the requirements; • A government entity; • A foreign government entity; • Public administrations or enterprises; • An entity listed on any stock exchange in Pakistan; and • An entity listed on a stock exchange outside Pakistan that is subject to regulatory disclosure requirements and its information is publically available.
Low risk factors for Products and	• Basic Banking Accounts (BBA); • Low value accounts having monthly credit turnover up to Rs. 25,000; • Salary accounts of individuals subject to the condition that account

Transaction Channel	is not used for other than salary purposes; • Pension accounts for direct credit of pensions; • Remittance cards restricted to receive inward remittances only; and • Other financial products or services that provide appropriately defined and limited services to certain types of customers so as to increase access to financial services.
Low risk factors for Geography or Locations	• Country identified by credible sources such as mutual evaluation or detailed assessment reports, as adequately complying with and having effectively implemented the FATF Recommendations; and • Country identified by credible sources as having a low level of corruption, or other criminal activity.

8. In respect of general low risk elements mentioned at Para (7) above, Banks/ DFIs may perform such SDD measures as it considers adequate to effectively establish the identity of the customer, a natural person appointed to act on behalf of the customer and any beneficial owner. The SDD measures should be in accordance with pre-defined criteria within AML/CFT policy of a bank/DFI and should commensurate with the low risk factors e.g. the SDD measures could relate only to customer acceptance measures or to aspects of on-going monitoring. Examples of such SDD measures may include:

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

9. In relation to Para (7) & (8) above, SDD measures should not be considered in following situations:

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

(c) In case of certain high risk factors are identified by SBP, by bank/DFI in its own internal risk assessment or as per international standards viz-a-viz FATF Recommendations etc.

(d) In relation to customers that are from or in jurisdictions which have been identified for inadequate AML/CFT measures by FATF or identified by the bank itself having poor AML/CFT standards or otherwise identified by the State Bank of Pakistan.

Annexure-I

A Template of Customer Risk Profiling (CRP) Form

Risk Determinants	Risk Variables/ Determinants	Assigned Risk Weight
Customers	Exceptions in getting KYC related information from customer	**0**
	High net worth customer or high value transactions	**10**
	Politically exposed person, its close associate or family member	**0**
	Relatively complex control/ ownership structure	**0**
	Reliability of verification measures	**5**
	Unclear source of funds or income from undocumented sources	**10**
	Beneficial ownership of funds may not belong to customer	**5**
Product & Services	Use of products & services which entail non face-to-face conduct	**10**
	Customer seeks private banking or other riskier services	**0**
	Excessive use of funds remitting instruments	**10**
	Customer subscribes for International/ foreign products & services	**5**
Channels	Large wire-in/wire-out or inland online transfers	**10**
	Level of cash based transactions	**20**
	Element of anonymity in transactions	**5**
Locations	Customer is based or linked to High Risk Jurisdictions as per FATF	**0**
	Customer is based or linked to UN Sanctioned Countries	**0**
	Customer's link to offshore centers or tax heavens	**0**
	Name matches with databases i-e World Check, OFAC, EU lists etc.	**0**
Others	Transaction pattern matches with SBP's examples on Red Alerts or guidance provided by FMU on ML/FT typologies	**5**
	Any other risk factors etc	**--**
	Total Risk Score	**95**

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

****