



**AML/CFT GUIDELINES ON RISK BASED APPROACH (RBA)
FOR BANKs / DFIs / MFBs**

(Updated on December 30, 2019)

**BANKING POLICY & REGULATIONS DEPARTMENT
STATE BANK OF PAKISTAN**

Website Address: www.sbp.org.pk

AML/CFT Guidelines on Risk Based Approach

for SBP's Regulated Entities (SBP REs-Banks/DFIs/MFBs)

(A) PREAMBLE

- 1) Globally there has been an emphasis on application of Risk Based Approach (RBA) to ensure that measures to prevent or mitigate Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) are proportionate to the identified ML, TF and PF risks. In this regard expectations are that:
 - a) RBA should be an essential foundation for efficient allocation of resources across the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) regime and the implementation of risk-based measures.
 - b) There should be a National Risk Assessment (NRA) exercise which helps in identifying, assessing and understanding the ML and TF risks at country level.
 - c) The risks identified through NRA should be adequately addressed in AML/CFT regime implemented in the country. The areas where ML/TF/PF risks are identified as low, Regulated Entities (REs) may be allowed to take decision regarding application of simplified measures.
- 2) Meeting the above expectations requires an important and pivotal role by Regulators/Supervisors of Financial Institutions (FIs)/ REs for ensuring technical compliance and effectiveness on RBA. In this regard sharing of results of NRA and embedding those results in regulatory/ supervisory framework and REs policies/procedures/SOPs/compliance program/internal risk assessments and allocation of resources proportionate to the level of threats and vulnerabilities identified in NRAs is an essential element for achieving effective mitigation of ML/TF/PF risks.
- 3) In this perspective, Pakistan had completed NRA in 2017, NRA-TF in 2019 and updated NRA on ML/TF in 2019. SBP has not only actively participated in NRA exercises but also ensured involvement of its REs. SBP had shared results of NRA 2017 in Compliance Forum meetings and complete documents of NRA-TF 2019 and NRA on ML/TF 2019 with its REs. REs were not only instructed to ensure capacity building of their staff but also encouraged to undertake measures to enhance

outreach for raising customer awareness. REs were also instructed to use the results of NRAs for developing their understanding on ML/TF/PF risks and consider the findings while devising mitigation strategy and policy for ML/TF/PF risks. SBP also ensured extensive outreach/awareness on threats and vulnerabilities identified in NRAs to its supervisory staff through training sessions and REs through compliance forums.

- 4) SBP had issued its Risk Based Approach (RBA) Guidelines on AML/CFT in 2012. Subsequently, Pakistan committed an action plan with FATF in June 2018 and also undergone a Mutual Evaluation by Asia Pacific Group which was concluded in 2019. In the context, findings of NRAs and aforementioned developments, SBP is issuing following updated guidance to its REs for ensuring adoption of RBA in line with international standards and best practices in areas: identification, assessment and understanding of ML/TF/PF risks, devising AML/CFT controls and preventive measures recommended by FATF for mitigation of ML/TF/PF risk (including implementation of Targeted Financial Sanction (TFS) related to Terrorist Financing (TF) & Proliferation Financing (PF) , Suspicious Transaction Reporting (STR) and Currency Transaction Reporting (CTR)).

B) GENERAL REQUIREMENTS

- 1) Banks/DFIs/MFBs shall ensure an entity level internal risk assessment report covering ML/TF risks including Transnational TF, PF and other emerging risks to and from SBP's REs. The internal risk assessment report should help to identify, assess, and understand ML/TF/PF risks at entity level for customers, products, services, transactions, delivery channels and geographies. Internal risk assessment report should also assess major international /domestic financial crimes and terrorism incidents which have probability of posing ML/TF/PF risks to the entity, SBP REs and the Pakistan's financial sector.
- 2) The internal risk assessment report shall ensure the assessment of effectiveness of existing AML/CFT controls so as to arrive at residual ML/TF/PF risks about which banks/DFIs/MFBs have to take decisions.
- 3) Risk assessment would generally be based on perception, subjective judgment and experience of REs about ML/TF/PF risks posed to them. The REs may adopt any approach which is suitable to them depending upon the nature of their operations,

risk appetite and business strategy; and may incorporate the suggested factors mentioned in this guiding document.

4) Key Features of ML/ TF Risk Assessment Framework for Banks/ DFIs/ MFBs:

The ML/ TF/ PF risk assessment framework should provide an entity wide assessment of ML/TF/PF risks that RE is inherently exposed to without considering impact of effectiveness of controls (i.e. inherent risk), thereafter assess the impact of effectiveness of controls framework designed to mitigate these risks and in the end resulting exposure (i.e. residual risk).

5) Inherent Risk Assessment:

The inherent risk shall be measured on both external and internal ML/ TF/ PF risk factors without taking into consideration the efficacy of effectiveness of controls. While assessing inherent risk on external factors, the REs may consider referring to the various sources of information as enumerated in these guidelines.

6) Quantification of Risk through Risk Matrix:

A matrix which quantifies likelihood and impact/consequences on two dimensions may be developed thereby categorizing risks 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 on the overall inherent risk for the REs.

7) Controls Effectiveness:

After assessing the inherent risks, the effectiveness of REs AML/CFT control framework (preventive measures) implemented by REs including TFS related to TF & PF and STR/ CTR shall be assessed to ensure effectiveness of controls design, quality of implementation and performance.

8) Residual Risk/ Net Risk:

Residual risk/ net risk is an outcome of assessment of inherent risks and the effectiveness of internal control framework. The REs risk assessment framework should be able to quantify residual risks that would lead REs to devise appropriate controls specifically where weaknesses are found and the residual risk is exceeding REs approved risk appetite.

9) Risk Decision:

The process of identification and quantification of inherent risks, assessment of effectiveness of AML/CFT controls and residual risks would support risk taking decisions of REs such as:

- Decision for taking customer(s) on-board with required level of control(s).
 - Decisions for refusal of financial service(s).
 - Decision for launching of product/service/delivery channel.
 - Decision for selecting geographical location to operate.
 - Decisions for upgrade of systems and controls etc.
- 10)** REs shall ensure that their risk assessment process is dynamic and up-to-date. REs shall periodically update their entity's internal risk assessment and in any case when their circumstances change or relevant new threats emerge. Further, in case the NRA(s) is updated at national level, the REs should ensure update of their internal risk assessment document in light of the updated NRA(s). These requirements shall be clearly stated by the REs in their own AML/CFT policies duly approved by their Board of Directors (BODs).
- 11)** For identification and assessment of the ML/ TF/ PF risks to which REs are exposed and devising proportionate mitigating measures, SBP REs should consider a range of factors which may include but not limited to following factors. In this regard REs should ensure adequate coverage as per the requirements and relevance to their operational and business model/needs.
- The nature, scale, diversity and complexity of their business
 - Their target markets as per their approved risk appetite
 - The customers risk profile
 - The jurisdictions REs are exposed to, either through their own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient in term of AML/ CFT controls and listed by FATF
 - The distribution channels, including the extent to which the REs deals directly with the customer or the extent to which it relies
 - The internal audit and regulatory findings
 - The volume, size and complexity of its transactions, considering the usual activity of the banks/DFIs/MFBs and the profile of their customers etc.
- 12)** REs may complement the above with information/guidance obtained from relevant internal and external sources suitable for identification and mitigation of ML/ TF/ PF risks posed to their entities considering adequate coverage as per the requirements/relevance to their operational and business model/needs such as:

- Pakistan's NRA(s) (specially identified threats, vulnerabilities, inherent risks, effectiveness of controls and residual risks of the sectors relevant to REs business and operational model etc.).
- SBP's Regulations and Guidelines.
- SECP's applicable Regulations and Guidelines.
- Relevant guidance from FMU, NACTA, MOFA and other GoP authorities.
- FATF/FSRBs (FATF Style Regional Bodies) Standards and Guidance.
- World Bank NRA Methodology.
- Published AML/CFT Mutual Evaluation Report and follow-up reports by FATF or associated assessment bodies.
- Relevant typologies developed and disseminated by different sources and through REs own internal risk assessment processes.
- Guidance from Basel specially Basel AML Index and different recognized terrorism indices.
- Guidance from Wolfsburg, International Chamber of Commerce (ICC) and Banker's Association for Finance and Trade (BAFT) Trade Finance Principles.
- United Nations Office on Drugs and Crime (guidance on risk of money laundering) etc.
- Guidance from Joint Money Laundering Steering Group (JMLSG).
- Guidance from Federal Financial Institutions Examination Council (FFIEC) etc.

C) GOVERNANCE, OVERSIGHT, MONITORING OF ML/ TF/ PF RISKS

1. The responsibility of oversight of ML/ TF/ PF risks posed to the entity and ensuring that REs have implemented effective AML/CFT controls (preventive measures), including TFS related to TF & PF, STRs/CTRs, lies on the Board. The Board shall delegate oversight and monitoring functions to any of its sub-committee preferably Board Risk Management Committee (BRMC) or Board Audit Committee (BAC) and Compliance Committee of Management (CCM) which has been constituted in compliance of SBP guidance on Compliance Risk Management.
2. Further for the establishment of compliance function/ structure and its empowerment, REs shall refer to SBP's Regulations on AML/ CFT and SBP's Guidelines on Compliance Risk Management. With regard to compliance function/structure at overseas locations, REs shall refer, in addition to aforementioned documents, SBP Guidelines on Governance framework for banks overseas operations.

3. REs should ensure that policies, procedures, products and services etc. are compliant with applicable AML/ CFT laws and regulation and adopt best international practices to mitigate ML/ TF/ PF risk that suits their operational and business model/ needs. In this regard REs shall proactively monitor ML/ TF/ PF threats emanating from new technologies including digital financial products, virtual currencies and online (wire transfers) etc. and ensure commensurate control (preventive measures).
4. Further, in addition to Anti-Money Laundering Officer (AMLO) who as best practice is supposed to ensure AML controls (preventive measures), establishment of a dedicated Counter Terrorism Financing (CFT) desk within compliance function should also be ensured. CFT desk should be made responsible specifically for CFT controls (preventive measures). CFT desk head should ensure quality and coverage of STRs reporting in the areas of terrorism, TF, PF and TFS, if any.
5. CFT desk shall be responsible to ensure that REs internal risk assessment process for identification, assessment and understanding of TF risks including Transnational TF risk is adequate, effective and updated. In this regard, CFT desk shall analyze major terrorist incidents that occurs within the country or abroad for assessing the possibility of use of entity's product, services and delivery channels and consider reporting of STRs, if warranted.
6. Internal risk assessment report of entity shall be presented to Board/ relevant Board sub-committee (as per board delegation) for approval after review and recommendations of CCM. The recommendations with regard to internal risk assessment report by CCM should be in the form of time bound action plan, for developing mitigating measures on ML/ TF/ PF risks identified on weaknesses of controls observed. It will be the responsibility of CCM to monitor the implementation of time bound action plan developed for mitigation of governance, risks and control weaknesses identified in internal risk assessment report.
7. Further, the requirements with regard to "Compliance Program" in the SBP Guidelines on Compliance Risk Management should meticulously ensure inclusion of requirements such as: identification, assessment, and understanding of ML/ TF/ PF risk at entity level and implementation of effective AML/ CFT controls (preventive measures) including implementation of TFS related to TF & PF/ STR/ CTR.

8. REs should take steps to ensure that AML/ CFT controls (preventive measures) are adhered to and are effective. To this end, their AML/ CFT controls (preventive measures) should be monitored on an ongoing basis for ensuring timely remedial measures. In this regard, the entity's standardized report/MIS on the ML/ TF/ PF risks posed to the entity and the effectiveness of available AML/ CFT controls (preventive measures) is required to be submitted to the Board/ relevant Board sub-committee assigned by Board on periodical basis, preferably on quarterly basis. Significant internal control gaps and critical violations e.g. failure to timely freeze accounts of designated and proscribed entities & individuals, failure to take counter proliferation measures, delayed/non-reporting of STRs/CTRs etc. shall invariably be a part of the report. In this regard ensuring that MIS for Enterprise Risk Management (ERM) and Risk and Control Self-Assessment (RCSA) functions of entity should include parameters/factors pertaining to AML/CFT controls (preventive measures) including TFS related to TF & PF, STRs/ CTRs would facilitate the entity in submission of effective MIS/ Report. Standardized report/ MIS should include review and recommendations (for remedial measures) of CCM before submitting it to relevant Board sub-committee. CCM should be assigned monitoring on ensuring compliance on recommendations presented to Board sub-committee through the Standardized report/MIS.

D) MEASURES TO BE TAKEN BY BANKS/ DFIs/ MFBs FOR MITIGATION OF ML/ TF/ PF RISKS

- 1) Periodical internal risk assessment report should be comprehensive and must assess effectiveness of existing AML/CFT controls so as to guide towards ensuring measures for mitigation of ML/ TF/ PF risks including but not limited to:
 - a. Development or update of strategy including entity risk appetite & policy framework for identification, assessment and understanding of ML/ TF/ PF risks and proportionate AML/ CFT controls (preventive measures) approved by the Board.
 - b. Development or update of AML/ CFT compliance program/procedure manuals/ SOPs for ensuring AML/ CFT controls (preventive measures) including implementation of TFS related to TF & PF and reporting of STRs/ CTRs approved by the senior management.
 - c. Effective and empowered organizational structure for compliance function with clear and conflict free responsibilities and reporting lines. Refer SBP AML/ CFT

- Regulations, Guidelines on Compliance Risk Management and SBP Guidelines on Governance framework for Banks overseas operations.
- d. Ensuring the adequacy of resources (human resources and systems) for AML/CFT controls (preventive measures) including TFS related to TF & PF, STRs/CTRs.
- 2) Banks/ DFIs/ MFBs should check/screen/ensure that staff they employees have integrity and are adequately skilled and possess the knowledge and expertise necessary to carry out their functions, in particular where staff are responsible for implementing AML/ CFT controls.
- 3) Steps should be taken to manage potential conflicts of interest for staff assigned responsibilities of AML/CFT controls (preventive measures) at every level from top to down the line.
- 4) The effective application of AML/ CFT policies and procedures depends on qualified and skilled human resources within REs who not only understand/ skillful on the processes/ technology they are required to follow/ use but also the ML/ TF/ PF risks including Transnational TF risks. These policies, procedures, SOPs, and Regtechs are ensured to mitigate the possible consequences of those risks. It is therefore important that REs staff receive AML/ CFT trainings for development of their understanding and skills. The trainings should be:
- a. Of high quality, relevant to the REs ML/ TF/ PF risks, business activities and up to date with the latest legal and regulatory obligations, internal controls including preventive measures as guided in FATF Standards.
 - b. Obligatory, for all relevant staff.
 - c. Tailored, to particular lines of business within the REs, equipping staff with a sound understanding of specialized ML/TF/PF risks they are likely to face and their obligations in relation to those risks.
 - d. Effective, training should have the desired effect, and this can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the REs AML/ CFT controls/ preventive measures including implementation of TFS related to TF & PF / STRs/ CTRs and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected in area of AML/ CFT.
 - e. Ongoing, AML/ CFT training should be imparted to relevant staff and it shall not be a one-off exercise when they are hired.

- f. Complemented, by AML/ CFT information and updates that shall be disseminated to relevant staff, as appropriate.
 - g. Feedback, shall be obtained through a formal mechanism for improvement of understanding after capacity building/training sessions.
- 5) SBP's REs should implement adequate, reliable, efficient automated systems and technologies proportionate to ML/ TF/ PF risks posed to their business and operational models. They should ensure necessary Regtechs (Systems and Technologies for identification/ assessment of ML/ TF/ PF risks, compliance and control requirements in area of AML/ CFT including TFS for TF & PF / STRs/ CTRs). In this regard adequate, reliable, efficient and automated Regtechs for customer risk profiling, name filtering/screening, and transaction monitoring should be implemented by the REs.
- 6) The implementation of adequate, reliable, efficient and automated Regtechs for identification and assessment of ML/ TF/ PF risks posed from Trade Finance, Branchless Banking and other new technologies for digital payment systems are immediate challenges for which REs should ensure identification of suitable and adequate automated systems and their implementation on priority basis.
- 7) Further, REs are advised to ensure use of new technologies to minimize false positives and solving data integrity/ management issues which are posing not only ML/ TF/ PF risks but also financial crime risks to REs.
- 8) REs are required to have an independent audit function to test their AML/ CFT framework with a view to establish the effectiveness of their overall AML/ CFT policies and processes and the quality of its risk management across its operations both domestically and, where relevant, overseas operational locations. The audit function needs to give assurance/ recommendations to the Board and senior management on the adequacy of governance, risk, compliance and controls of REs AML/ CFT regime for mitigation of ML/ TF/ PF risks posed to entity.
- 9) REs should have an effective and judicious performance appraisal mechanism and transparent accountability mechanism to reward good performance and ensure accountability of delinquent officials of those who are assigned job of governance risk and control in area of AML/CFT.

E) RISK PROFILING

- 1) Banks/ DFIs/ MFBs should risk profile every new customer (depositors/ borrowers/ ADC user/ trade finance customer etc.) using their own judgment and information obtained through CDD/ KYC process. In this regard, it is advised to ensure automated systems and best practices to risk profile a customer while taking him on-board and ensure periodical update of the customers risk profile including legacy portfolio.
- 2) While ensuring risk profiling function and implementing risk profiling systems (Regtechs) appropriate weights should be given to elements/ factors/ parameters/ sectors probability of which for posing ML/ TF/ PF risks exists. Guidance with regard to elements/ factors/ parameters/ sectors which may have probability of posing ML/ TF/ PF risk is given at Annexure- A
- 3) Banks/ DFIs/ MFBs if on the basis of weights assigned to general high risk elements/ factors/ parameters/sectors mentioned at Annexure -A or any other identified by REs through their internal risk assessment process consider any customer or transaction as high risk then REs should ensure Enhanced Due Diligence (EDD) measures which are effective and proportionate to the level of identified risks. In particular, they may escalate level of approvals and 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. The EDD measures shall be in addition to CDD measures recommended in SBP AML/ CFT Regulations and may include but not be limited to one or more EDD measures recommended in SBP's AML/ CFT Regulations. Further, EDD measures should be proportionate and updated to high risk elements/ factors/ parameters/ sectors identified and documented in entity's updated internal risk assessment report.
- 4) There may be circumstances where the risk of ML/TF may be low, and provided that there has been an adequate analysis of the risk by the REs, Simplified Due Diligence (SDD) measures may be applied. In respect of general low risk elements REs may perform such SDD measures as they considers adequate to effectively establish the identity of the customers, 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 policies of REs and should be proportionate to the low risk factors identified and documented in internal risk assessment report. Further to facilitate REs, in area of SDD, SBP has issued separate guidelines on low risk bank accounts with SDD - Asaan Account and guidelines on Asaan remittance account.

**Guidance on Elements/Factors/Parameters to be
Considered for Risk profiling System/Function**

Customers	Products Services and Delivery Channels	Geographic Locations
<ul style="list-style-type: none"> • NPOs/NGOs/ Charities, Trusts, Clubs, Societies, and Associations etc., • Politically Exposed Persons, • Correspondent banking relationships, • Housewife, • Proprietorship and self-employed individuals/ professionals, landlords, • Non-resident customers, • Customers in whose accounts third party mandates are given, • Customers with links to offshore tax havens, • Customers conducting frequent online transactions from locations having tax amnesty to avoid taxes, • Customers dealing in high-value items etc., • Customers belonging to high risk sectors/ geographies as identified in NRAs, • High net worth customers where REs feeling difficulty in monitoring source and use of funds in an account, 	<ul style="list-style-type: none"> • Request by customers for use of products, services and delivery channels through cash intensive transactions, • Request by customers for frequent transactions from un-associated third parties, • Private banking relationships, • Online transaction and wire transfers, • FX remittances inward/ outward, • Products/delivery channels identified as high risk in NRAs. 	<ul style="list-style-type: none"> • The jurisdictions which have been identified for inadequate AML/ CFT measures by FATF or called for by FATF for taking counter-measures, • Countries identified by credible sources such as mutual evaluations or detailed assessment reports, as having inadequate AML/ CFT standards, • Countries subject to sanctions, embargos, for example, the United Nations, • Countries identified by credible sources as having significant levels of corruption, or other criminal activity, • Countries or geographic areas identified by credible sources as providing funding or support for terrorism activities, • Locations identified as high risk in NRAs.

<ul style="list-style-type: none">• Customers whose identification data with regard to source of income is difficult to verify,• Customer who have been refused banking facilities by another bank/ DFIs/MFBs,• Companies that have nominee shareholders or shares in bearer form,• Legal persons or arrangements that are personal asset holding vehicles,• Legal person and arrangement whose licenses/registration etc. have been expired not renewed or cancelled/de-registered,• Inactive Companies as disclosed by SECP on its website,• Legal person and arrangement where required necessary approvals for conducting financial transaction have been expired not renewed or cancelled.		
---	--	--