Approved by Order F018 dated 26.05.2015 issued by Director of the Financial Monitoring Service under the Central Bank of the Republic of Azerbaijan

METHODOLOGICAL GUIDANCE FOR THE RISK-BASED APPROACH TO COMBATING LEGALIZATION OF FUNDS AND THE FINANCING OF TERRORISM FOR CREDIT ORGANIZATIONS

OBJECTIVES OF THE METHODOLOGICAL GUIDANCE

1. The Risk-Based Approach (RBA) is of great importance for the effective implementation of applicable principles of the 2012 FATF International Standards on preventing legalization of funds, the financing of terrorism and proliferation of weapons of mass destruction and the Basel Committee on Banking Supervision.

2. The target group of this Methodological Guidance is the credit organizations operating in the territory of the Republic of Azerbaijan.

3. The purpose of this Methodological Guidance is as follows:

- To focus on principles related to RBA to combating money laundering and the financing of terrorism (AML/CFT);
- To render assistance to countries, authorities in charge and credit institutions in developing and implementing RBA to AML/CFT through general instructions on current practice and models;
- To support the effective implementation of national AML/CFT measures and control over them (by paying special attention to the risks and measures to mitigate them);
- To promote the target group's understanding of the nature of RBA to AML/CFT.

STATUS AND CONTENT OF THE METHODOLOGICAL GUIDANCE

4. The Methodological Guidance has been prepared in line with features of the legal and regulatory framework relating to the activities of credit institutions of the Republic of Azerbaijan and the sector's risk profile. The guidance specifies points that should draw attention during the development and implementation of RBA for the country-based credit institutions. The principles mentioned in this Methodological Guidance should be considered in the context of the operational features of the credit institutions.

5. The Methodological Guidance takes into account the international experience in this field, and is a methodological support tool to effectively implement requirements stemming from the FATF Recommendations for credit institutions.

THE RISK-BASED APPROACH (RBA) TO AML/CFT

A. WHAT IS THE RBA?

6. The RBA to AML/CFT implies that countries, competent authorities and financial institutions (including natural and legal persons) should identify, assess and understand ML/FT risks. In addition, they should take AML/CFT measures to effectively eliminate these risks.

7. During the ML/FT risk assessment process, credit institutions should analyze and understand the impact of these risks on them. Risk assessment should serve as the basis for ML/FT risk reduction measures.

8. RBA doesn't exempt credit institutions from taking measures aimed at reducing ML/FT risks that are considered to be low.

B. THE BASIS FOR A NEW APPROACH

9. In 2012, the FATF updated its recommendations. Novelties were introduced to provide countries with more powerful tools against financial crimes to strengthen international efforts and to ensure the reliability of the financial system.

10. One of the most important changes is aimed at increasing attention to RBA to AML/CFT. Special attention has been drawn to the preventive measures and supervision. If the Recommendations adopted in 2003 envisaged application of RBA only in some areas, the 2012 Recommendations indicate RBA as a basis of the AML/CFT system. This is a requirement applicable to the relevant FATF Recommendations.

11. RBA enables to apply a wider complex of measures aimed at using resources more efficiently and taking preventive measures (depending on the level of risk). This also creates conditions to carry out the AML/CFT efforts in the most effective way.

12. Thus, application of RBA should not be regarded as a binding condition but as a prerequisite for effective implementation of the FATF Standards.

C. APPLICATION OF THE RISK-BASED APPROACH

13. According to the national law, monitoring entities should apply the RBA.

14. Relevant AML/CFT supervisors should draw attention of a monitoring entity to measures aimed at assessing and mitigating its own risks and take into account results of its risk assessment during assessment of the sectoral risk.

15. Where the ML/FT risks are high, competent authorities and monitoring entities have to take enhanced measures to mitigate these risks. Thus, the range, degree, frequency and intensivity of control measures taken will match the level of risk. Where the ML/FT risk is lower, standard AML/CFT measures may be reduced. Thus, application of any required measure has to depend on the range, degree, frequency and intensivity of relevant risks.

ALLOCATING RESPONSIBILITY UNDER A RBA

16. An effective risk-based regime builds on and reflects Azerbaijan Republic's legal and regulatory framework, the nature, diversity and maturity of its financial sector, and the country's risk profile. When identifying and assessing their own ML/FT risks, credit institutions should take into account the country's risks (in accordance with FATF Recommendation 1), peculiarities of Azerbaijan Republic's legal and regulatory framework (including significant risks) and state policy in relevant areas. Where ML/FT risks are high, credit institutions should always enhance control and analysis (even when the national legal and regulatory framework and state policy do not prescribe exactly and unequivocally measures to mitigate these higher risks).

17. Credit institutions are able to make independent decisions on measures to be taken to address other risks. Those risks may be identified in the national risk assessment or by credit institutions themselves. During the development of a strategy to mitigate these risks, credit institutions should take into account Azerbaijan Republic's applicable legal and regulatory framework and state policy. When determining the extent to which credit institutions are able to make independent decisions, the country should consider, inter alia, the financial sector's potential to identify and manage ML/TF risks, the level of credit institutions' experience and resources.

IDENTIFYING ML/TF RISKS

18. Obtaining accurate, timely and unbiased information about ML/FT risks is a cornestone for an effective RBA. According to explanatory note 3 to FATF Recommendation 1, countries should have mechanisms to provide all monitoring participants with applicable information on the results obtained during the risk assessment. Credit institutions may face problems in correctly identifying, assessing and mitigating ML/FT risks in the following cases: (1) there is lack of accurate information, (2) competent authorities use inadequate information during the risk assessment, (3) competent authorities are unable to share important information on ML/FT risks and threats, (4) there are problems in obtaining applicable information.

ASSESSING ML/TF RISKS

19. ML/TF risk assessment means that credit institutions should assess an impact of relevant ML/FT risks. They should analyse the information obtained and explore the probability of these risks occurring and the extent to which these risks may affect them at both the micro and macro levels. As a result of a risk assessment, ML/FT risks are classified as low, medium and high (there can be also certain interim indicators: medium-high ora low-medium). The above-mentioned categories are used to understand ML/FT risks and to prioritise them. ML/TF risk assessment does not envisage a simple collection of quantitative and qualitative information: assessment forms the basis for effective mitigation of ML/TF risks and always echoes the real situation.

20. To assess risks and analyze results, credit institutions should have skilled, professional and reliable staff as well as applicable equipment and software.

MITIGATING ML/TF RISKS

21. The FATF Recommendations require that, when applying a RBA, credit institutions should decide on the most appropriate and effective way to mitigate the ML/TF risks related to them. They should take enhanced measures to manage and mitigate high ML/FT risks.

22. When the level of risks is low, simplified measures may be taken. In such cases, it should be proven that the level of relevant risks is really low and they are associated with a specific type of credit institution or activity, or that a credit institution provides financial services (excluding money transfer) rarely and to a limited extent.

23. Credit institutions seeking to take simplified measures should assess risks associated with the customer and service categories and define the lower level of these risks, the extent and intensity of the required AML/CFT measures. Explanatory notes to applicable Recommendations determine in more detail and accurately how those general principles apply to particular requirements.

ML/FT RISKS ASSOCIATED WITH CREDIT INSTITUTIONS

Credit institutions encompasses a wide range of financial products and services related to ML/. These include, but are not limited to:

- Retail banking, where credit institutions provide products and services directly to individuals and business customers (including legal institutions). Among these products and services are current accounts, loans (including mortgages) and savings;
- Corporate banking, where credit institutions provide corporate finance and corporate banking products and investment services to companies, government and institutions;
- Investment services (or asset management), where credit institutions provide products and services to manage their customers' wealth (sometimes referred to as private banking); and

- Correspondent services, where banking services are provided by one bank (a correspondent bank) to another bank (a respondent credit institution).

24. Examples of ML/TF risk associated with activities of credit institutions:

- Retail banking: percentage of cash transactions, volume of transactions, high-value transactions, diversity of services.
- Asset management: reliability culture, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, political figures, high-value transactions and numerous jurisdictions.
- Investment banking: differentiation and integration, transfer of assets between parties in exchange for cash or other assets.
- Correspondent banking: high value transactions, limited information about a remitter and source of funds, in particular, when a transaction executed by a credit institution in the area that does not comply or complies insufficiently with the FATF Recommendations.

RISK ASSESSMENT

25. The risk assessment forms the basis of a credit institution's RBA and helps credit institutions to understand how and to what extent they should grow and to determine their vulnerabilities. Often such an assessment will result in a classification of risks and help credit institutions to determine the level of AML/CFT resources required to mitigate each risk. The assessment results should always be duly documented, preserved and delivered to relevant staff within a credit institution.

26. A credit institution's risk assessment should not be complicated, but should be commensurable with the nature and volume of financial services provided by a credit institution. For small credit institutions that offer a limited range of services, a simple risk assessment may suffice. Conversely, where a credit institution offers more complex products and services, where its subsidiaries and branches provide a wide range of services and/or their customer base is more diverse, a more accurate risk assessment process is required.

27. When determining and assessing the ML/FT risks to which they are exposed, credit institutions should consider the following factors:

- The nature, scale, diversity and complexity of a buziness;
- Target markets they serve;
- The number of customers already identified as high risk;
- The area in which a credit institution is exposed to risks both through its own activities and activities of its customers, in particular areas with relatively high level of corruption or organized crime, and/or insufficient AML/CFT control and included in the FATF list.
- The extent to which a credit institution deals directly with customers or the extent to which reliance can be placed on the third party to conduct customer due diligence or the extent to which technologies are used in this;
- The internal audit and regulatory decisions;
- Types of products attractive for ML/FT purposes and the market share of these products;
- The volume and size of transactions, taking into account the usual activities of a credit institution and the profile of its customers.

28. A credit institution should be guided by this information, national risk assessment, lists and databases issued by international orhanizations and relevant government agencies, reports by FATF and associated assessment bodies as well as applicable typologies. In any case when they are modified or new threats emerge, they should revise their assessments.

29. A risk assessment should be approved by senior management after determining an acceptable level of a credit institution's risk, and form the basis for the development of policies

and procedures to mitigate ML/FT risks. It should be revised and updated on a regular basis. Policies, procedures, measures and controls aimed at mitigating ML/FT risks should be consistent with results of a risk assessment.

RISK MITIGATION

30. Credit institutions should develop and implement policies and procedures to mitigate ML/FT risks identified through a risk assessment. To help credit institutions understand who their customers are, customer due diligence (CDD) processes should be developed to gather information on what they do and why they require these services. The initial stage of the CDD process should be developed to help credit institutions assess ML/FT risks associated with business relations, determine the level of CDD that should be applied and prevent people from establishing business relationships to carry out illegal activities.

31. Credit institutions shoul prepare a customer risk analysis based on information obtained as a result of application of CDD measures. This analysis will determine the level and type of periodic monitoring and create the basis for a credit institution's decision to enter into, continue and terminate business relationships. A risk analysis can be applied at the individual customer level or, where a group of customers has similar characteristics (for example, customers with similar income level or carrying out a similar financial transaction), to this group. This approach is particularly important for retail banking customers.

32. The CDD process starts with the following:

- Identifying customers and, if possible, customers' beneficial owner;
- Verifying a customer's identity on the basis of reliable and independent information or documentation at least at the level required by the applicable legal and regulatory framework; and
- Understanding the purpose and nature of bsuiness relatioships and obtaining additional information in high risk situations.

33. In addition, credit institutions should take measures to meet the requirements of national and international requirements by checking a customer's and beneficial owner's names against the UN and othere relevant sanctions lists.

34. As a rule, CDD measures should be applied in all cases. The extent of these measures is being brought into line with regulatory requirements in accordance with a ML/FT risk (if any) associated with an individual business relationship. This means that the volume and type of information obtained and the extent to which this information is verified should be increased if the risk associated with business relationships is high. It may also be simplified if the risk the risk associated with business relationships is low. Therefore, credit institutions should draw up and periodically update customer risk profiles, which will help credit institutions apply the appropriate level of CDD.

35. Enhanced Due Diligence (EDD) may include the following but are not limited to them:

- obtaining additional information from various or more reliable sources and using the information to inform an individual customer about risk assessment;
- conducting additional searches (e.g. searches for verifiable news) that may be helpful in an risk assessment associated with an individual customer;
- submitting a report on a customer or beneficial owner to understand better the risk of a customer's or beneficial owner's involvement in criminal activity;
- verifying financial sources or wealth involved in the business relationship to prove that they do not constitute the profits derived from criminal activities;

- searching for additional information from a customer about the purpose and nature of bsuiness relatioships.

36. Simplified Due Diligence (SDD) envisages obtaining less information (e.g. information on a potential customer's address or place of residence is not required) and/or more simple verification of a customer's identity and the purpose and nature of business relationships, as well as postponing verification of a customer's identity.

37. If credit institutions cannot apply the appropriate level of CDD, they are banned from entering into business relationships or such relationships should be terminated.

ONGOING CDD/MONITORING

38. Ongoing monitoring means the control over transactions to determine whether these transactions are consistent with a credit institution's knowledge of a customer and the nature and purpose of its product and business relationships. Monitoring also implies identifying changes made to a customer's profile (e.g. their behavior, using of products and an amount of money attracted) and maintaining them at the necessary level, which may require the application of new or additional CDD measures. Monitoring transactions is an important component in identifying potentially suspicious transactions.

39. Monitoring should be conducted on a continuous basis and launched because of specific transactions. It could be also used to compare a customer's activity with that of a similar group. It does not require electronic systems but automated systems may be the only real method of monitoring transactions for some types of bank activities implying large volumes of transactions on a regular basis. However, when using automated systems a bank should understand their operating rules, verify regularly their integrity and addressing identified ML/FT risks.

40. Credit institutions should adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring may be required for high risk situations, while credit institutions may reduce the frequency and intensity of monitoring where risks are low. The adequacy of monitoring systems and the factors causing credit institutions to adjust the monitoring level should be reviewed regularly to comply continuously with credit institutions' AML/CFT program.

41. Credit institutions should document and state clearly criteria and parameters used for customer segmentation and allocation of a risk level for each cluster of customers. Criteria for a decision on the frequency and intensity of monitoring of various customer segments should be also transparent.

42. Examples of monitoring in high/low risk situations include the following but are not limited to them:

- Monitoring in high risk situations: daily transaction monitoring, manual transaction monitoring, frequent information analysis, considering the destination of funds, creation of indicators based on a typological report, reporting on monitoring results to senior management, etc.

43. Monitoring in low risk situations: thresholds, low frequency, automated systems determined by supervisory authorities and credit institutions to ensure adequacy of the monitoring system. Credit institutions should properly document, maintain and notify personnel in charge of the results of monitoring as well as any questions raised and resolved.

REPORTING

44. If a credit institution suspects or has grounds to suspect that funds are associated with ML/FT, it should immediately report its suspicions to the FMO. Credit institutions should have

the ability to mark unusual movement of funds or unusual transactions for further analysis. Credit institutions should ensure that such funds or transactions are taken under control in a timely manner and determination made as to whether the funds or transaction are suspicious.

45. Even if the policy and procedures leading a credit institution to form a suspicion are applied in line with the RBA, it must report to FMO after identifying a ML/FT suspicion.

INTERNAL CONTROL MECHANISMS

46. Applicable internal control mechanisms are a prerequisite for effective implementation of policies and processes to mitigate ML/FT risks. Internal control includes relevant governmental requirements clearly stating responsibility for AML/CFT, regulations to ensure monitoring of the integrity of staff, compliance with national legislation, especially in sutiations with international transactions and during national risk assessment, compliance to verify the effectiveness of a credit institution's policies and prosedures enabling to identify, asess and monitor risk.

GOVERNANCE

47. The successful implementation and effective operation of a RBA in the AML/CFT field depends on senior management support, development process and control over its implementation.

48. Senior management should consider various ways to support AML/CFT initiatives:

- To promote AML/CFT as a key value of a credit institution by stating openly and clearly that it will not enter or maintain business relationships associated with excessive ML/FT risks which cannot be effectively mitigated. Senior management together with the governing body is responsible for risk management and control mechanisms applied in a bank and a risk policy adopted by the bank;
- To implement appropriate mechanisms of internal communication related to existing or potential ML/FT risks faced by a credit institution. These mechanisms should link the board of directors, an AML/CFT senior officer, any relevant or specialized committees within a bank (e.g. risk or ethic committees), IT divisions and all business areas;
- To decide on measures required to mitigate ML/FT risks identified and on the extent of risk that a credit institution is prepared to accept;
- To provide a credit institution's AML/CFT unit with adequate resources.

49. Senior management should not only know about ML/FT risks to which a credit institution is exposed but also understand how to mitigate these risks within the AML/CFT system. This may require that senior management,

- obtains comprehensive, regular and objective information to get an accurate view of an ML/FT risk to which a credit institution is exposed through its activities and individual business relationships;
- obtains comprehensive and objective information to understand whether a credit institution's AML/CFT control mechanisms are effective;
- and these processes are aimed at enhancing important decisions on these processes that directly affect the ability of a credit institution to address and control risks.

50. It is important that responsibility for the consistency and efficiency of AML/CFT control mechanisms be clearly assigned to a credit institution's governing body because top management shoud be informed about the importance of ML/FT risk management and compliance, and they should always remain focused on ML/FT issues. This includes but is not limited to the appointment of a skilled employee at management level.

RBA AND ORGANIZATIONAL STRUCTURE

51. An RBA provides for the availability of 3 protection levels within credit institutions. The first level is comprised of employees providing services directly to customers (credit experts and operators). Those employees are in charge of customer identification and suspicious transaction detection. The compliance division's staff headed by a senior AML/CFT officer form a second level. Those employees ensure the overall coordination and performing the continous monitoring function to identify suspicious schemes in transactions. The third level consists of a credit institution's internal auditors. They assess the adequacy of a credit institution's internal rules and procedures and verify compliance of its activity with these rules and procedures. Moreover, the assistance of external auditors may be advisable.

ENSURING AND MONITORING COMPLIANCE

52. A credit institution's internal control environment should be favourable to ensure the integrity, competence and compliance with applicable policies and procedures. The measures relevant to AML/CFT control mechanisms should possess a wide set of control mechanisms capable to address business, financial and operational risks in general.

RECRUİTMENT ISSUES

53. Credit institutions should verify that staff they employ, in particular those are liable for implementing AML/CFT control mechanisms, have integrity and adequately skilled and possess the knowledge and expertise needed to perform their duties.

54. The level of staff inspection procedures should reflect ML/FT risks to which staff are exposed and not focus only on senior management duties. Steps should be taken to manage a potential conflict of interest for staff with AML/CFT responsibilities.

TRAINING AND AWARENESS

55. The effective application of AML/CFT policies and procedures depends on a credit institution's staff understanding not only the processes they should to implement but also the risks that these processes mitigate, as well as possible consequences of those risks. Therefore, it is important that bank staff participate in AML/CFT trainings which should be as follows:

- Trainings should be of high quality: relevant to a credit institution's ML/FT risks, business activities and up-to-date legal and regulatory obligations and internal control mechanisms;
- Mandatory for all relevant staff;
- Adapted: should ensure that staff understand specail PL/FT risks they face and their duties with regard to those risks;
- Effective: a training should have the necessary effect; this can be reached, for example, by requiring staff to pass exams or by checking staff's ability or inability to demonstrate the expected level of knowledge during monitoring levels of compliance with a credit institution's AML/CFT control mechanisms;
- Continuous: AML/CFT trainings should be held on a regular basis and at a time most convenient to staff;
- Complemented with AML/CFT information and updates that are disseminated to relevant staff.

56. In general, a training should also build a business behavior where compliance requirements are reflected in activities and decisions of all credit institution's staff.

ASSESSMENT OF CONTROL

57. Credit institutions should take measures to make sure that their AML/CFT policies and control mechanisms are adhered to and effective. To this end, their control mechanisms should be monitored on a regular basis by a credit institution's officer in charge. In addition, the adequacy of and compliance with credit institutions' AML/CFT control mechanisms should be reviewed by an auditor.

58. FATF Recommendation 18 requires credit institutions to appoint an officer at the management level. In addition to advising staff on how to fulfill their obligations, their role should include monitoring and assessment of ML/FT risks as well as the adequacy and effectiveness of the measures taken by a credit institution to mitigate risks. Officers in charge should therefore have the independence, authority, superiority, resources and expertise as well as the ability to obtain all relevant internal information (including through business lines and foreign branches and subsidiaries) to perform these functions effectively.

59. FATF Recommendation 18 also requires credit institutions to have an independent audit inspection to test a AML/CFT program with a view to ensure efficiency of a credit institution's all AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries (both domestically and abroad, where appropriate). Results of an audit inspection will form top management's view of the development and implementation of a credit institution's AML/CFT framework. The audit inspection should examine the adequacy of all risks and therefore not focus merely on high risks.

60. During the assessment process, both the compliance and audit should be guided by all applicable information including, where reasonable and appropriate, information obtained confidentially through relevant internal mechanisms or hotlines. Other sources of information may include training pass rates, compliance failures and analysis of questions raised by staff.

61. Examples of control mechanisms aimed at ensuring complaince with AML/CFT requirements include the following but are not limited to them:

■ Facilitating reporting on suspicious transactions:

- to organize trainings on mechanisms to detect unusual transactions;
- to identify channels enabling staff to report unusual transactions to an officer in charge;
- to ensure confidentiality to staff reporting suspicious transactions;

■ Allowing staff to report on unclear/useless/inefficient policies and control mechanisms:

- to establish regular consultation channels for staff dealing with AML/CFT issues;
- to ensure regularity of responses to questions raised by staff with regard to AML/CFT issues;
- to conduct AML/CFT activities in a way that is understandable to all staff to ensure both the quality of banking services provided to clients and the integrity of a credit institution.