

Approved
by the decision of the
Management Board of
the Central Bank of the Republic of
Azerbaijan dated 4 April 2025
Protocol №_07_

Methodological Guidelines

for institutional risk assessment on the legalization of criminally obtained property, the financing of terrorism, proliferation, and the financing of proliferation of weapons of mass destruction

1. General provisions

1.1. These Methodological Guidelines have been developed in line with international best practices and in consideration of the requirements of the legislation and provide recommendations for financial institutions on assessing institutional risks associated with the legalization of criminally obtained property, the financing of terrorism, proliferation, and financing of proliferation of weapons of mass destruction (ML/TF/PF) (hereinafter – IRA). These Guidelines also outline a simplified approach to the IRA.

1.2. According to Article 21.7 of the Law of the Republic of Azerbaijan ‘on Prevention of the legalization of criminally obtained property and the financing of terrorism’, financial institutions are required to identify, assess, document and report to supervisory authorities institutional ML/TF/PF risks and take actions to manage, eliminate or mitigate risks under internal rules and procedures approved by the management.

1.3. Financial institutions, considering the requirements specified in Item 2.9 of the ‘Minimum requirements to be met by internal control programs of reporting entities’ (hereinafter – the Requirements), should conduct an institutional ML/TF/PF risk assessment at least annually.

1.4. According to ‘Corporate governance standards in banks’, ‘Corporate governance standards in insurers’ and ‘Corporate governance standards in investment companies’, banks, insurers, and investment companies should approve risk appetite statements. The statements specify aggregate risk limits the said institutions can assume to reach their business goals. The document also provides for limits on non-financial risks, including

ML/TF/PF risks along with the limits on financial risks. Other financial institutions are also recommended to approve a similar document along with the banks, insurers, and investment companies.

1.5. Each financial institution, taking into account the nature of its activities, types of its operations, and the structure and size of its customer base, may develop and implement its own IRA methodology in a simplified or more comprehensive form based on these Methodological Guidelines.

1.6. The overall approach to the IRA is based on quantitative and qualitative data and consists of evaluating specific risks (arising from the financial institution's activities and to which it is exposed in the absence of internal control mechanisms) and assessing the adequacy of the internal AML/CFT control program.

1.7. The IRA is a periodic process, and financial institutions should regularly identify, assess, and manage risks, as risks are not static and may respond to internal and external factors. For example, the expansion of financial institution's operations, changes in its business direction, the emergence of new global trends, or amendments to legislation can increase or decrease of risks.

2. Preparation to IRA

2.1. Before initiating the IRA, the financial institution prepares an activity map. The map outlines its areas and types of business activity, size, markets in which it operates (economic sectors to which it offers services and products), etc., essentially inventorying its operations. Financial institutions that have branches, representative offices, and/or other structural units, as well as subsidiaries, also inventory the activities of those structural units and subsidiaries.

2.2. The activity map includes the following quantitative indicators related to the financial institution's high-risk customers, products/services, operations, delivery channels, and geographical locations, along with information about the internal control program:

2.2.1. regarding customers - types and number of customers, the number and value of transactions conducted, or contracts concluded by them.

2.2.2. regarding products/services/delivery channels - their types, the number of customers using them, the number and value of transactions/contracts.

2.2.3. regarding geographical location - the number and value of transfers made to and from other countries (territories), as well as the number and value of contracts connected to these countries (territories).

2.2.4. the internal control program components.

2.3. Once the activity map has been developed, the process of identifying and assessing risks begins.

2.4. After the IRA identifies the inherent risk and the adequacy level of the internal control program, residual risks are calculated using the following formula:

$$\text{Residual risk} = \text{Inherent risks} - \text{Adequacy of the internal control program}$$

3. Identification and assessment of inherent risks

3.1. Consisting of four main categories (customer risk, product/service/transaction risk, delivery channel risk, and geographic location risk), inherent risks are the risks arising from financial institution’s activities, identified without considering internal control measures. These Methodological Guidelines use a risk scoring scale and weighting factors, when calculating inherent risks.

3.1.1. The risk scoring scale is one of the main tools used by financial institutions to identify and assess risks related to their activities. These scores are individually determined by each financial institution, taking into account their specific areas of activity, customer base, specifics of products and services, geographical areas of operation, and delivery channels used. Accurate determination of scoring plays a critical role in the effective management of risks and in minimizing residual risks. For this purpose, financial institutions familiarize themselves with the publications of the Financial Action Task Force (FATF), the European Union, the International Monetary Fund, the World Bank, as well as national and international supervisory and financial monitoring authorities, including the most recent National Risk Assessment and Sectoral Risk Assessment reports.

For example, a higher risk score may be assigned to customers, transactions, products/services, or delivery channels characterized by features such as anonymity, difficulties in determining the source of funds, or political influence (remotely delivered services and transactions, politically exposed persons, individuals connected with high-risk zones, and their transactions, among others).

Example 1¹:

Scores	Scoring level	Risk factors (For instance, customer categories)
1	Low risk	Local individuals
2	Low-medium risk	Local legal entities
3	Medium risk	Foreign legal entities

¹ Examples and illustrations provided in this Methodological Guideline are presented to give an understanding of the methodology for conducting the IRA.

4	Medium-high	Non-regulated virtual asset service providers
5	High risk	Politically exposed persons

Explanation of the example: In this example, risk scoring is determined using a 5-point scale (the scale range is individually defined by the financial institution) based on the nature of different customer types. Customer categories that, by their nature, pose a high ML/TF/PF risk are assigned a high-risk score. A similar approach is applied to determine scores for products/services, delivery channels, and geographic locations.

3.1.2. Weights reflect the significance of risk factors in the context of financial institution's operations. Each financial institution individually determines its weights based on its specific activities and risk profile. This approach plays a critical role in systematically and effectively assessing the risk level associated with the institution's business lines, customer base, products and services offered, delivery channels, transactions conducted, and the geographical areas with which it is connected.

The weight can be calculated with the below formula:

$$\text{Weight} = (\text{Share in the portfolio} + \text{Share in operations}) / 2$$

Example 2:

Risk factors (e.g., customer categories)	Share in the portfolio (e.g., share of the respective customer category in total number of customers) (%)	Share in operations (e.g., share of the number/value of transactions conducted by the respective customer category in total number/value of transactions conducted by all customers) (%)	Weight (%)
Politically exposed persons (PEPs)	10	15	12.5
Virtual Asset Service Providers	20	25	22.5
Foreign legal entities	15	20	17.5
Local legal entities	25	20	22.5

Explanation of the example: PEPs constitute 10% of the financial institution's customer portfolio, and their transactions account for 15% of the total transaction volume. Consequently, their weighting factor is calculated as $(10 + 15) / 2 = 12.5\%$. This rule also applies to other categories.

3.2. Calculation of the customer risk

Customer risks arise from the nature of the customer, his/her legal status, and the nature of his/her transactions. The level of this risk varies depending on whether the customer belongs to a high-risk group. Customer risk can be calculated based on various factors that influence the risk level, as well as the criteria specified in sub-item 2.9.3.6 of the Requirements, as follows:

$$\text{Customer risk} = \sum (\text{Risk factor scores} \times \text{Weight})$$

Example 3:

Risk factors (Customer categories)	Scores (1-5)	Weight	Risk
Politically exposed persons	5	40	2.0
High-risk area citizens	4	30	1.2
Citizens of other foreign countries, excluding those from high-risk areas	3	20	0.6
Resident individuals	2	10	0.2
Total			4.0

Explanation of the example: Risk is determined based on the assigned scoring (1–5) for each risk factor and the corresponding weight (%) in the portfolio. PEPs are classified as a high-risk group and scored 5. Considering their 40% weight in the portfolio, the risk is calculated as $5 \times 0.4 = 2.0$. Similarly, citizens from high-risk areas are classified as a medium-high risk group and assigned a score of 4. With a 30% weight in the portfolio, their risk is calculated as $4 \times 0.3 = 1.2$. The total of the calculated risk factors determines the final customer risk of the financial institution. In this example, the final customer risk stands at 4.0.

3.3. Calculation of product/service/transaction risks

The risk level of products/services/transactions can be calculated as follows, considering various factors affecting the risk level and the criteria specified in sub-items 2.9.3.3 and 2.9.3.4 of the Requirements:

$$\text{Product risk} = \sum (\text{Risk factor scores} \times \text{Weight})$$

Example 4:

Risk factors (Product/service/transaction categories)	Score (1-5)	Weight (%)	Risk
Private banking	5	50	2.5
Electronic commerce	4	30	1.2
Consumer loan	3	20	0.6
Total			4.3

Explanation of the example: Private banking is classified as a high-risk group and scored 5. Since this product holds a 50% weight in the portfolio, the risk is calculated as $5 \times 0.5 = 2.5$. Similarly, e-commerce is classified as a medium-high risk group (score of 4), and with a 30% portfolio weight, its risk is calculated as $4 \times 0.3 = 1.2$. Consumer loans are classified as a medium-risk group (score of 3), and with a 20% portfolio weight, their risk is calculated as $3 \times 0.2 = 0.6$. The total of the calculated risk factors determines the financial institution's overall product/service/transaction risk. In this example, the product risk stands at 4.3.

3.4. Calculation of the delivery channel risk

The delivery channel risk can be calculated as follows, considering various factors affecting the risk level and the criteria specified in sub-item 2.9.3.5 of the Requirements:

$$\text{Delivery channel risk} = \sum (\text{Delivery channel factor scores} \times \text{Weight})$$

Example 5:

Risk factors (Delivery channel categories)	Score (1-5)	Weight (%)	Risk
Mobile banking	5	50	2.5
Payment terminals	5	30	1.5
Cash counter	1	20	0.2
Total			4.2

Explanation of the example: Mobile banking and payment terminals are classified as high-risk groups and scored 5. Based on their respective portfolio weights, the risk is calculated as $5 \times 0.5 = 2.5$ for mobile banking (50% weight) and $5 \times 0.3 = 1.5$ for payment terminals (30% weight). Cash office transactions are classified as a low-risk group and scored 1. With a 20% weight in the portfolio, the risk is calculated as $1 \times 0.2 = 0.2$. The total of the calculated risk factors determines the financial institution's overall delivery channel risk. In this example, the final delivery channel risk stands at 4.2.

3.5. Calculation of the geographical risk

Geographical risks can be calculated as follows, considering various factors affecting the risk level and the criteria specified in sub-item 2.9.3.7 of the Requirements:

$$\text{Geographical risk} = \sum (\text{Geographical factor scores} \times \text{Weight})$$

Example 6:

Risk factors (Country/area)	Score (1-5)	Weight (%)	Risk
Countries in the FATF's 'blacklist'	5	40	2.0
Countries in the FATF's 'grey list'	4	30	1.2
Other countries	1	30	0.3
Total			3.5

Explanation of the example: Countries on the FATF 'blacklist' are classified as a high-risk group and scored 5. With a 40% weight, the risk is calculated as $5 \times 0.4 = 2.0$. Countries on the FATF 'grey list' are classified as a medium-high risk group (score of 4), and with a 30% weight, the risk is calculated as $4 \times 0.3 = 1.2$. Other countries are classified as a low-risk group and scored 1. With a 30% weight, the risk is calculated as $1 \times 0.3 = 0.3$. The total of the calculated risk factors determines the financial institution's overall geographical risk. In this example, the final geographical risk stands at 3.5.

3.6. Calculation of the inherent risk rate

After identifying the risks for each of the four categories, the final inherent risk rate is calculated with the below formula.

$$\text{Inherent risk} = \text{Total of risk rates} / \text{Number of risk rates}$$

As is seen in the above formula, the final inherent risk level is calculated as the mean of the risk rates assessed for the main risk categories faced by the financial institution (customer, product/service, delivery channel, and geographic risks); i.e. based on the above examples, as the customer risk is 4.0, product risk is 4.3, delivery channel risk is 4.2, and geographic risk is 3.5 – the final inherent risk rate is calculated as $4.0 + 4.3 + 4.2 + 3.5 / 4 = 4.0$.

As a result, the inherent risk level is determined to be 4.0. The higher this calculated figure, the greater the corresponding risk level.

4. Assessment of the adequacy of the Internal Control Program

4.1. The Internal Control Program (ICP) is a set of policies, procedures, and control mechanisms implemented in financial institutions to manage ML/TF/PF risks. The ICP ensures the compliance of the operations of financial institutions with legislative requirements and the minimization of ML/TF/PF risks.

4.2. The ICP is developed in accordance with the operational structure of the financial institution and is regularly assessed. This assessment helps determine how effective the ICP is and whether it complies with legislative requirements.

4.3. The adequacy of the ICP is measured by assessing the quality indicators of its various components. A 5-point scale (or alternative scales) may be used in this process. Each component (e.g., "compliance officer, customer due diligence measures, etc.) is evaluated based on specific criteria (e.g., the expertise and knowledge level of the "compliance officer). The criteria may be scored in terms of significance. Each financial institution may define its components and evaluation criteria individually, based on the nature of its operations. Provisions in the Requirements should be considered during this process. The final adequacy score is calculated as the arithmetic mean of adequacy scores of individual components.

The results of the assessment by the components of the ICP can be as follows:

Example 7:

Components	Score (1-5)
Compliance officer (expertise, knowledge, and functional effectiveness of the AML/CTF responsible person)	3.1
Reporting (timely delivery and high quality of reports on suspicious operations)	2.5
Ongoing monitoring (real-time monitoring of operations and detection of potential suspicious operations)	2.9
CDD (obtaining customer information, identification of risks and updating information)	3
Staff training (increasing AML/CFT/CPF knowledge of the staff and effective organization of trainings)	3
Final ICP adequacy rate	2.9

Explanation of the example: The arithmetic mean of the mentioned components, i.e., the final ICP adequacy level, is evaluated as 2.9, which indicates that the adequacy is at an acceptable level, as shown in the following example.

Example 8 – ICP Assessment Scale:

Scores	Assessment	Description
1 – 2	Weak	The ICP has serious non-conformities (legal requirements are not complied with).
2 – 3	Acceptable	There are non-conformities in the ICP (legal requirements are partially followed), but a certain level of effectiveness is ensured.
3 – 4	Medium	The ICP is effective (legal requirements are followed in full), but all ICP areas need to be improved.
4 – 5	Good	The ICP is effective (legal requirements are followed in full), but certain ICP areas need to be improved.
5	Excellent	The ICP is effective and fully compliant with the AML/CFT requirements.

5. identification and assessment of the residual risk

5.1. The residual risk represents the level of risk remaining after considering the adequacy of internal control mechanisms and is calculated with the formula.

$$\text{Residual risk} = \text{Inherent risk} - \text{ICP adequacy}$$

This formula allows assessing how effectively a financial institution can reduce its inherent risks (risks before supervisory measures are imposed) through its internal control measures. When internal controls are effective, the residual risk will be minimal. Otherwise, due to gaps or deficiencies in the internal control program, the residual risk will remain high. The risk assessment considers the criteria specified in sub-item 2.9.3 of the Requirements.

5.2. This approach allows measuring the level of residual risk, taking into consideration the effectiveness of the financial institution's internal control mechanisms. The residual risk can never be zero or negative, as certain risks will always exist regardless of how effective internal control mechanisms are. These risks mainly arise from human error, changing circumstances (legislative changes, technological advancements, etc.), and external factors (international sanctions, political and economic changes). These factors indicate that it is impossible for financial institutions to eliminate all risks entirely, and that a certain level

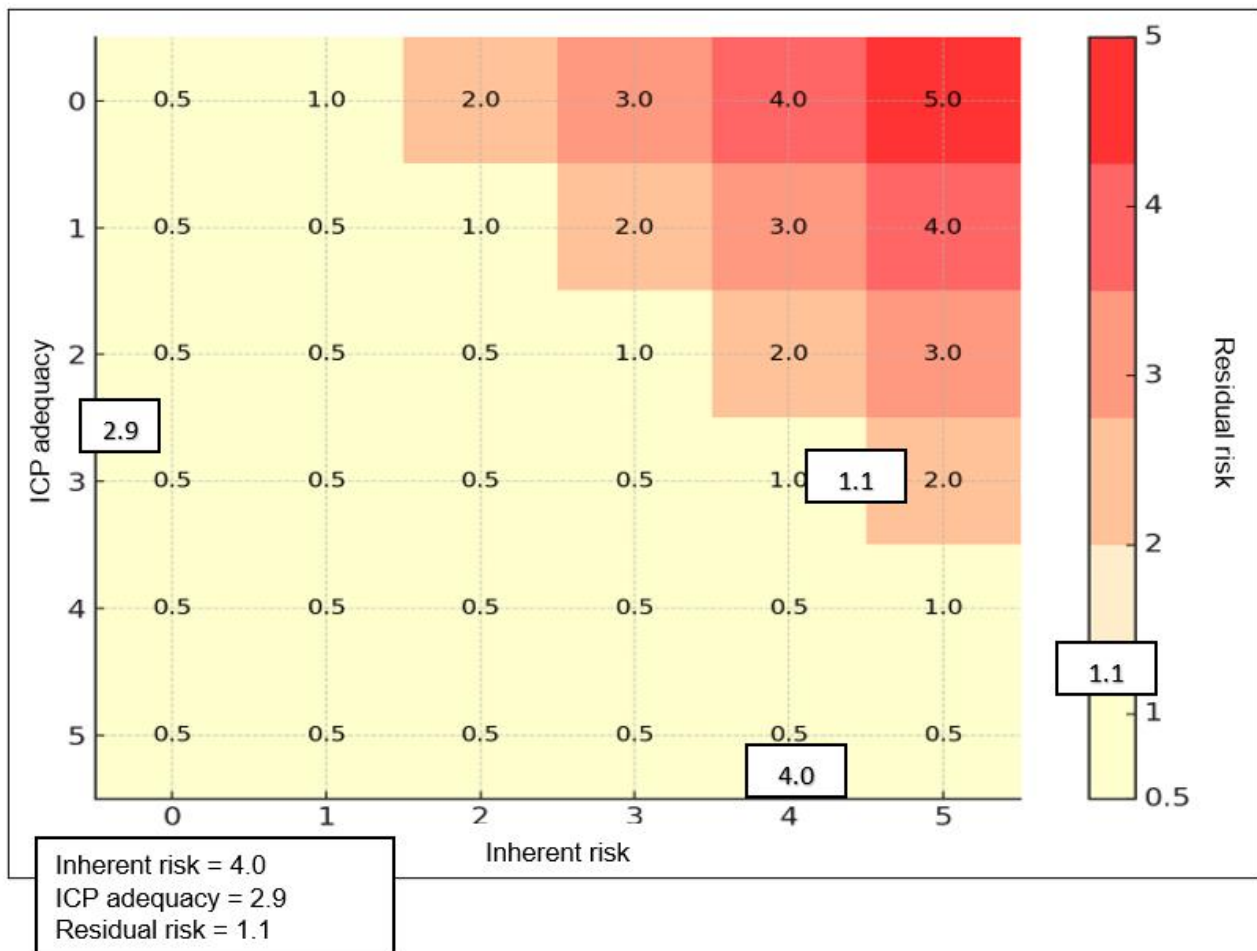
of residual risk will always remain. Therefore, a minimum residual risk value is recommended to be accepted as 0.5 (equivalent to 10%). Using the examples provided above, *the residual risk level is calculated as 4.0 – 2.9 = 1.1 and, according to the scale provided in Example 9, is evaluated as Low risk.*

Example 9 – Residual risk assessment scale:

Risk rate	Residual risk
Low	0 – 1
Medium low	1 – 2
Medium	2 – 3
Medium-high	3 – 4
High	4 – 5

5.3. Results can be illustrated in the Heatmap provided in Example 10.

Example 10 – Heatmap:



5.4. Residual risk levels also allow comparing results from previous years and help determine the overall risk trend. If financial institution's residual risks exceed the limits defined in its risk appetite statement, the institution implements appropriate regulatory and supervisory measures.

6. Use of IRA results

6.1. Results act as an important facility for effectively assessing and managing risk levels in financial institution's operations. They also form a basis for making critical decisions to ensure compliance with legislative requirements. Upon completion of the IRA, financial institutions are expected to take the following actions according to the results:

6.1.1. Development of an action plan – Financial institutions prepare an action plan for implementing measures to reduce identified risks and manage residual risks resulting from these measures. The plan is submitted to management for approval and includes at least:

6.1.1.1. Specific measures for high risks: introduction of stricter control mechanisms for high-risk customers, products/services, and delivery channels.

6.1.1.2. Resource allocation: effective management of financial, human, and other resources according to risk levels.

6.1.1.3. Improvement activities: actions to eliminate gaps in internal control mechanisms.

6.1.1.4. Awareness: ensuring relevant staff are informed about the action plan.

6.1.2. Annual reporting to the supervisory authority – Financial institutions submit annual reports to the Central Bank of the Republic of Azerbaijan detailing risk assessment results and measures taken:

6.1.2.1. Risk assessment report: detailed information on identified risk levels for each category of inherent risks, internal control mechanisms, and residual risks.