Report on the results of the national risk assessment covering the years 2022–2024 regarding the anti-money laundering and combating the financing of terrorism in the Republic of Azerbaijan

The Methodology for assessing effectiveness and technical compliance with the Financial Action Task Force (FATF) Recommendations—in the context of combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction and its financing—was published in a revised edition in February 2022. Countries that are members of the FATF or FATF-style regional bodies undergo mutual evaluations based on this Methodology on a periodic basis.

In accordance with the assessment criteria for FATF Recommendation 1, the risks of money laundering and terrorist financing within the country must be identified and assessed. A mechanism or a responsible body must be established to organize the coordination of assessment activities. The results of risk assessments must be kept up to date, and a mechanism must be established to ensure that relevant persons and entities are informed accordingly. Based on a risk-based approach, countries should allocate their resources and implement countermeasures—proportional to the risks identified through the assessment—to combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction and its financing.

These requirements are reflected in the national legislation within Articles 20–21 of the Law of the Republic of Azerbaijan "Anti-Money Laundering and Combating the Financing of Terrorism" (hereinafter – the Law). Based on the results of sectoral and institutional assessments, a national risk assessment is conducted at least once every three years by the Coordination Council on Anti-Money Laundering and Combating the Financing of Terrorism and the Proliferation and Financing of the Proliferation of Weapons of Mass Destruction (hereinafter – the Coordination Council). This process involves relevant supervisory and other state bodies (institutions), reporting entities, providing auditing services, religious institutions, non-governmental organizations and representatives from related sectors.

At its meeting held on February 13, 2024, the Coordination Council established the methodology for conducting the national risk assessment; it also approved the working groups—including their leadership and composition—as well as a Roadmap for the assessment process. The working groups established for assessment purposes and their composition are as follows:

№	Working group name	Working group leading body	Working group member bodies
1	National vulnerability assessment group on money laundering	Prosecutor General's Office	Ministry of Internal Affairs, Ministry of Justice, State Customs Service, State Security Service, State Statistics Committee, Supreme Court, Central Bank, Financial Monitoring Service, State Tax Service, Chamber of Auditors, Bar Association

2	National threat Assessment Group on money laundering	Financial Monitoring Service	Prosecutor General's Office, Ministry of Internal Affairs, Ministry of Justice, State Customs Service, Supreme Court, Central Bank, State Tax Service , Chamber of Auditors, Bar Association
3	National Vulnerability Assessment Group for designated nonfinancial businesses and professions	National Vulnerability Assessment for real estate agencies, legal, accounting and tax advisory services: State Tax Service	State Border Service,State Committee on Affairs with Religious Associations, Financial Monitoring Service
		National Vulnerability Assessment for notaries: Ministry of Justice	
		National Vulnerability Assessment for lawyers: Bar Association	
4	National vulnerability assessment on financial institutions assessment group	Central Bank	Prosecutor General's Office, Ministry of Internal Affairs, State Security Service, Financial Monitoring Service, State Tax Service, Azerbaijan Banks Association, Azerbaijan Insurers Association, Azerbaijan Capital Markets Association
5	National Threats and Vulnerabilities Assessment Group on Financing of Terrorism and Proliferation and Financing of Weapons of Mass Destruction	State Security Service	Prosecutor General's Office, Ministry of Internal Affairs, Ministry of Justice, State Tax Service, State Customs Committee, State Border Service, Foreign Intelligence Service, State Committee on Affairs with Religious Associations, Supreme Court, Financial Monitoring Service, Central Bank

Within the framework of the national risk assessment, working groups developed the necessary questionnaires, collected and analyzed data from relevant institutions and open sources, and conducted various thematic analyses. Furthermore, through discussions and working meetings with relevant state authorities, existing and potential money laundering risks were assessed at the macro level and across various sectors.

Consistent with previous assessments, this national risk assessment was conducted based on the World Bank’s methodology for national money laundering risk assessment.

To broaden the scope of the analyses and leverage international best practices, cooperation between the Financial Monitoring Service and the Council of Europe was

continued. In this context, training on conducting strategic analyses for the national risk assessment was organized for the state institutions participating in the aforementioned working groups. Additionally, the initial national risk assessment report was reviewed by an expert from the Council of Europe and subsequently refined based on the expert's feedback.

NATIONAL THREATS REGARDING THE MONEY LAUNDERİNG

During the assessment of threats related to the laundering of proceeds of crime, 21 categories of offenses—as defined by the Financial Action Task Force (FATF)—were analyzed. Based on criteria such as the frequency of offenses and the extent of damage caused, the following were identified as crimes posing a threat of money laundering: theft and fraud committed using electronic data storage media and information technologies; the misappropriation of state funds; the illicit trafficking and smuggling of narcotic substances; and tax evasion.

A. Current trends and methods

- The rapid spread of virtual assets and digital payment platforms has led to a significant increase in the share of cybercrime among the predicate offenses that generate illicit proceeds;
- The emergence of new potential threats—particularly the application of artificial intelligence and various deceptive identification/authentication technologies within new technological environments—increases the risk of manipulation financial institutions and their customers.
- Shell companies remain one of the tools widely used for money laundering purposes during this period.

B. Money laundering typologies and sectors subject to abuse

- The withdrawal of funds in cash, transfers to bank accounts in foreign countries, and conversion into real estate—following numerous transfers between the accounts of individuals and shell companies—are the most prevalent methods of money laundering.
- Financial institutions (as the sector) and banks or payment organizations (as reporting entities) have been frequently utilized for money laundering. Specific products and services exploited include: card deposits via payment terminals, card-to-card transfers, cash withdrawals, transfers between the accounts of individuals and legal entities, and transfers to bank accounts located abroad.
- The virtual asset service provider sector, along with financial services involving the use of virtual assets, has emerged as a new trend.

NATIONAL VULNERABILITIES REGARDING MONEY LAUNDERING

The assessment examines various aspects of the country's anti-money laundering system across 11 input variables, including reforms implemented between 2022 and 2024, as well as the effectiveness of legislative and institutional mechanisms. The key vulnerabilities and shortcomings identified through this analysis are as follows:

- The need to align legislation with the updated requirements of Recommendation 4 of the Financial Action Task Force (FATF);
- The lack of regulation concerning virtual assets and related activities;
- The absence of systematic feedback mechanisms with foreign partners;
- A low level of awareness regarding the requirement to disclose beneficial ownership information, given that this is a new obligation.

SECTORAL WEAKNESSES

- Violations were identified, including: the failure to use the unified system intended for the verification of beneficial owners (due to its lack of accessibility), the failure to identify beneficial owners or determine whether they are foreign politically exposed persons (PEPs), the failure to terminate business relationships with clients whose beneficial owners have not been identified, the failure to apply enhanced due diligence measures for high-risk clients, and the failure to update identification data;
- The sanctions provided for under Article 598 of the Code of Administrative Offenses are not considered effective, proportionate, or dissuasive in terms of their nature and amount (according to the MONEYVAL assessment).
- Common weaknesses among reporting entities (primarily designated non-financial bodies and professionals, excluding notaries) appear in the absence of an internal control program—either in its entirety or in specific components—and the failure to implement customer due diligence measures. Consequently, this leads to a failure to detect suspicious transactions in a timely manner and a failure to report them to the Financial Monitoring Service. The extent of these weaknesses varies across different sectors. Among reporting entities that have already established an anti-money laundering and counter-terrorist financing (AML/CFT) system (mainly non-bank financial institutions), the primary weakness lies in the quality of reports on suspicious transactions and their suitability for analysis.