Approved by the Supervisory Board of "ABB" OJSC
Protocol No. 5; Decision No. 5;
Date: 07.04.2025
"ABB" OJSC
Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)

POLICY

Contents

1. General Provisions

1.1. The Anti-Money Laundering and Combating the Financing of Terrorism Policy (hereinafter – the Policy) of "ABB" OJSC (hereinafter – the Bank) defines the Bank's internal control program for AML/CFT, outlines the necessary activity areas in this field, and identifies other necessary control mechanisms.

1.2. This Policy is based on the Law of the Republic of Azerbaijan "On the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism," normative legal acts of the Financial Monitoring Service of the Republic of Azerbaijan, the recommendations of the Financial Action Task Force (FATF), principles of the Basel Committee on Banking Supervision, and the widely adopted Wolfsberg Principles in banking practice.

1.3. This Policy reflects the minimum requirements for AML/CFT and applies to the Bank's management, all structural divisions, and customer service units.

2. Key Definitions

2.1. The following terms used in this Policy shall have the meanings ascribed below:
2.1.1. AML/CFT – Anti-Money Laundering and Combating the Financing of Terrorism;
2.1.2. AML/CFT (in Azerbaijani: ƏL/TMM) – the fight against the legalization of criminally obtained property and the financing of terrorism;
2.1.3. Legalization of criminally obtained property – a crime as defined in Article 193-1 of the Criminal Code of the Republic of Azerbaijan;
2.1.4. Financing of terrorism – a crime as defined in Article 214-1 of the Criminal Code of the Republic of Azerbaijan;
2.1.5. Responsible structural unit – the structural unit of the Bank responsible for activities in the field of financial monitoring;
2.1.6. Responsible person – the person in the Bank responsible for overseeing the implementation of AML/CFT legislation, internal rules and procedures, for conducting information exchange with the financial monitoring authority, and for preparing and submitting relevant reports on transactions subject to monitoring.

2.1.7. Politically Exposed Persons (PEPs) – individuals who currently hold or have previously held significant political or public functions in any state (territory) or international organization (e.g., heads of state and government, heads of state bodies (institutions) and their deputies, members of legislative bodies, members of political party management bodies, judges of supreme and constitutional courts, members of supreme audit and supervisory bodies and central bank management bodies, ambassadors extraordinary and plenipotentiary, chargés d'affaires, senior military and high-ranking officials with special titles, members of state-owned enterprise management bodies, heads and deputy heads of international organizations, and members of their governing bodies).

2.1.8. Beneficial Owner – a natural person (or persons) who ultimately exercises control over the customer or who is the real owner of a legal entity or foreign legal arrangement that is a customer, and/or for whose benefit a transaction is carried out and/or agreements are made, as well as a person who ultimately exercises effective control over a legal entity or foreign legal arrangement.

2.1.9. Unusual Transactions – transactions that are atypical, complex, considered large under current circumstances, lacking rational economic substance, or accompanied by suspicious behavior, and which are not in line with the customer's usual business practices or relationships.

2.1.10. Sanctions Lists – lists of individuals as determined by the Law of the Republic of Azerbaijan "On Targeted Financial Sanctions" and published on relevant official web resources, including persons listed by the European Union (EU), the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), and the United Kingdom Sanctions List.

2.2. The definitions provided in this section are used solely for the purposes of this Policy.
2.3. Other terms used in this Policy shall have the meanings as defined in the applicable legislative acts of the Republic of Azerbaijan.

3. Purpose and Principles of the Policy

3.1. The objectives and principles of this Policy are as follows:

3.1.1. The purposes of the AML/CFT Policy are:
– To prevent misuse of the Bank's products and services for money laundering and terrorism financing by establishing an appropriate control environment;
– To instruct Bank employees to identify and prevent suspicious money laundering or terrorism financing activities;
– To protect the Bank from any financial losses, administrative or criminal liability that may arise from non-compliance with AML/CFT requirements;
– To safeguard the Bank's name and sound business reputation from AML/CFT-related risks.

3.1.2. The Bank's AML/CFT activities are based on the following principles:

3.1.2.1. Principle of Legality:
– Compliance with the legislation of the Republic of Azerbaijan in the field of AML/CFT and the requirements set out in international treaties to which the Republic of Azerbaijan is a party.

3.1.2.2. Know Your Customer (KYC) Principle:
– Implementation of customer due diligence measures, formation of customer profiles, identification of customer profile risks, and taking measures to minimize the Bank's involvement in suspicious, complex, large-scale, and unusual financial transaction schemes.

3.1.2.3. Restrictions and Zero Tolerance[1]
– In all cases where there is suspicion of money laundering or terrorism financing, and in relation to individuals and transactions connected with high-risk zones, restrictions are applied in accordance with internal rules. Furthermore, zero tolerance is demonstrated toward customers and transactions involving individuals listed in the "Sanctioned Persons" lists.

4. AML/CFT Responsibilities and Obligations

4.1. The Bank's management ensures that the rights and responsibilities related to AML/CFT are clearly detailed in the job descriptions of employees according to the nature of their job functions, and that a specialized approach is applied to each position based on its functional duties. The AML/CFT responsibilities and obligations of the Bank's supervisory and executive bodies, as well as its structural units, are defined as follows:

*(1)In international terminology, **"Zero tolerance"***

4.1.1. Supervisory Board:
– Forms the Bank's internal structure in accordance with effective AML/CFT control and accountability mechanisms;
– Approves the Bank's AML/CFT policy and internal regulations and oversees general compliance with them;
– Establishes an AML/CFT organizational structure that is adequate to the Bank's operations.

– Appoints or dismisses the **Responsible Person** who has independent decision-making authority within the Bank.

4.1.2. Management Board:
– Ensures the implementation of the AML/CFT policy within the Bank and its communication to employees;
– Ensures the Bank's AML/CFT system complies with legislation and internal Bank documents;
– Oversees the institutional risk assessment process related to AML/CFT within the Bank.

4.1.3. Responsible Person:
– Monitors the compliance of the Bank's employees with AML/CFT legislation, as well as internal rules, procedures, and control mechanisms;
– Conducts daily monitoring of transactions, applies ongoing customer due diligence measures, ensures that reports on current and suspicious transactions are prepared and submitted to the financial monitoring authority, and ensures that incoming inquiries are responded to;
– Organizes regular AML/CFT training sessions for employees involved in related activities;
– Takes measures to resolve issues that may arise in connection with the suspension of transactions;
– Informs the management, within the timeframes established by legislation, about high-risk transactions, potential AML risks the Bank may face, results of institutional risk assessments, and reports submitted to the financial monitoring authority;
– Notifies management about any violations of AML/CFT legislation requirements committed by Bank employees;
– Carries out other duties stipulated by legislation in the AML/CFT field.

4.1.4. Internal Audit Department:
– Conducts audit inspections within the timeframes established by legislation;
– Based on the results of the audits, reviews the software, systems, and processes that support AML/CFT compliance, and provides recommendations.

– Analyzes the compliance of the internal control program with AML/CFT legislation, identified risks, and the scale and characteristics of the Bank's operations;
– Communicates any issues identified during the audit with the audit subject and Bank management, and submits the final audit results to the Audit Committee after the audit is completed.

4.1.5. Employees of other structural units:
– Must be aware of, comply with, and participate in relevant training on AML/CFT legislation and internal Bank regulations;

– Upon identifying suspicious activity related to AML/CFT, must immediately inform the responsible structural unit without disclosing any information to the customer.

5. Internal Control Program on AML/CFT

5.1. The AML/CFT control program includes:
5.1.1. Approval of internal rules and procedures, control mechanisms, and their development plans;
5.1.2. Establishment of screening procedures and continuous training for staff to ensure high professionalism and civil integrity during the recruitment process;
5.1.3. Organization of an independent and effective compliance system at the management level through a designated responsible person to fulfill anti-money laundering and counter-terrorism financing requirements;
5.1.4. Establishment of an independent audit mechanism to assess the effectiveness of the existing AML/CFT control system based on internal audit standards.

6. Customer Due Diligence (CDD) Measures

6.1. Within the framework of customer due diligence measures, identification data of customers is collected, and the purpose and nature of business relationships are determined to create a customer profile.
Identification and verification measures are carried out based on documents obtained from reliable sources.
Depending on the level[2] of risk, the Bank applies standard, simplified, enhanced, or ongoing due diligence measures.
If the Bank is unable to fully implement these due diligence measures, it does not establish or continue any business relationship and informs the financial monitoring authority accordingly.

6.2. As part of customer due diligence measures, appropriate actions are taken to identify the beneficial owner of the customer.
The identification of the beneficial owner continues until full certainty of their identity is established and is verified using information and documents obtained from reliable and independent sources.
If a legal entity has no identifiable beneficial owner, the individual(s) in senior management positions authorized to represent the legal entity are considered the beneficial owner(s).

(2) *Currently, in accordance with the "Rules on Determining Customer Risk Levels in the Field of Combating the Legalization of Criminally Obtained Property and the Financing of Terrorism" at "ABB" OJSC:*

7. Risk-Based Approach

7.1. The Bank adopts a risk-based approach and continuously identifies, assesses, and takes appropriate measures in accordance with the level of exposure to AML/CFT risks.
Accordingly, enhanced customer due diligence measures are implemented in higher-risk cases, while simplified measures are applied in lower-risk situations.
In applying the risk-based approach, relevant actions are taken based on FATF recommendations, national legislation, general risks identified by competent authorities, and the characteristics of customers and products.

7.2. When a new product or service is developed and before it is launched, an AML/CFT risk assessment is conducted. If the risk is deemed high, measures are identified to eliminate or mitigate it.

7.3. The Bank determines customer risk levels based on their profile data, transactions, and behavioral patterns. These indicators are compared, and the highest indicator is accepted as the customer's risk level. The process of determining customer risk levels, categorizing them, and conducting subsequent monitoring is regulated by internal bank procedures.

8. Sanctions Lists and Politically Exposed Persons (PEPs)

8.1. Appropriate measures are implemented in accordance with current legislation, international standards, and best practices concerning sanctions lists. When establishing or continuing a business relationship, customers, beneficial owners, and other related parties—as well as transaction counterparties—are regularly screened against relevant sanctions lists.
The Bank freezes the assets of individuals and entities subject to sanctions, without delay and without prior notification, as soon as international or domestic sanctions lists are published. The Bank immediately notifies the relevant executive authority and the financial monitoring authority about such actions.

8.2. The status of Politically Exposed Persons (PEPs) is determined based on information provided by the customer, by cross-checking with relevant lists, and through external sources. If the customer themselves, their beneficial owner, or their authorized representatives are identified as a PEP, or a close relative or close associate of a PEP, the customer is classified as a high-risk customer. In such cases, the establishment of a business relationship is subject to management approval and confirmation by the Compliance Officer, and enhanced due diligence measures are continuously applied.

9. Correspondent Relationships

9.1. To mitigate risks, the AML/CFT responsible unit evaluates resident and non-resident banks with which correspondent relationships are intended to be established, within the AML/CFT framework. Business relationships are established only if the results of the assessment are

satisfactory. Correspondent banking relationships are formed with the approval of the Management Board. The identification data provided by correspondent banks must be reviewed at least once a year. Under no circumstances are correspondent relationships established or transactions conducted with shell banks—banks that lack a physical presence in their country of incorporation and are not regulated or supervised by competent authorities.

10. Transactions Subject to Monitoring

10.1. The Bank conducts ongoing monitoring of customer transactions to ensure they align with the customer's profile and the nature of the business relationship. Monitoring is carried out using criteria[3] (special indicators) defined by legislation and internal policies for detecting transactions subject to monitoring. Transactions that raise suspicion are identified and analyzed through scenarios built into specialized software used for customer and transaction monitoring. Monitoring and control measures are carried out with consideration of at least the following:

10.1.1. Customers, transactions, and countries classified as high risk;

10.1.2. Complex and unusual transactions;

10.1.3. The alignment of the transactions conducted by the customer with their profile (including information about their business, risk level, financial sources, etc.);

10.1.4. Transactions related to a new product or service that is classified as high risk, conducted at least one (1) year after its introduction.

11. Application of New Technologies

11.1. The bank considers transactions conducted through new and emerging technologies as high-risk transactions and takes appropriate measures to assess and mitigate AML/CFT risks during their execution. When transactions are conducted through new technologies, data and documents are obtained in electronic form using appropriate authentication methods in compliance with legal requirements, and customer due diligence measures are implemented. If new technologies do not allow the application of customer due diligence measures, the use of the new technology is declined.

11.2. When business relationships are established and transactions are conducted through new technologies without direct communication with the customer, the bank takes one or more of the following measures, depending on the type and nature of the transaction, for document verification and identity verification of the customer:

(3)Currently, Methodological Guidelines for the identification and analysis of unusual transactions in the field of legalization of property obtained through criminal means and financing of terrorism at "ABB" OJSC

11.2.1. Request the customer's request to be verified with their enhanced electronic signature;

11.2.2. Perform enhanced customer authentication;

11.2.3. Obtain the documents provided by the customer from a reliable third party or government agency, with the customer's consent, upon request.

11.2.4. Request the customer to use the security codes, electronic signatures, tokens, and other similar identity verification passwords provided by the bank;

11.2.5. Conduct identity verification of the customer through real-time video calls or video recordings;

11.2.6. Implement other verification and control measures as specified by internal procedures.

12. Recruitment Process and Training Program

12.1. Based on the Labor Code of the Republic of Azerbaijan, other normative legal acts, and advanced international practices, high professionalism and impeccable citizenship requirements are applied during the recruitment process for employees related to the AML/CFT field.

12.2. In the recruitment procedures, the following measures are implemented to ensure that only individuals who meet the high professionalism and impeccable citizenship requirements are hired, and that individuals related to AML/CFT are not employed:

12.2.1. Verification of knowledge level in the field of AML/CFT;

12.2.2. Verification of the accuracy of the provided information and documents;

12.2.3. Obtaining information regarding criminal records, as well as personal and professional qualifications.

12.3. To ensure that bank employees acquire the necessary knowledge in the field of AML/CFT, planned training sessions or ad-hoc training sessions are held each calendar year in accordance with the training program approved by the management. The training program is determined based on the employee's position, qualification level, as well as the requirements for the form, frequency, and duration of the training. The training program is periodically reviewed and updated whenever there are additions or changes to the applicable legislation in the field of AML/CFT, international standards, or internal rules, procedures, and control mechanisms.

13. Requirements for the Responsible Person

13.1. The Responsible Person is appointed or dismissed by the Supervisory Board, registered in the financial monitoring authority's information system for the period specified in the legislation, and

this information is provided to the regulatory authority. The Responsible Person cannot be an employee of the internal audit service or the customer service department. The activities of the Responsible Person are not dependent on other structural units and are directly subordinate to and report only to the Supervisory Board.

14. Independent Audit Mechanism

14.1. The bank has an independent audit mechanism that evaluates the effectiveness of the implementation of internal rules, procedures, and control mechanisms adopted under the legislative requirements and internal control program. The bank's management is responsible for ensuring regular audits to verify the effectiveness of the implementation of legislative requirements. Audit inspections are carried out with the frequency provided by the legislation in accordance with the sectoral laws.

15. Reporting

15.1. The Responsible Person prepares an AML/CFT activity report at least every 6 (six) months and submits it to the Supervisory Board.

15.2. The report includes at least the following information:

15.2.1. The work and analyses carried out during the reporting period;
15.2.2. Identified non-compliance with the requirements of legislation and internal regulatory documents;
15.2.3. Potential risks to which the bank may be exposed in relation to AML/CFT;
15.2.4. Results of the risk assessment based on the characteristics of customers, products, services, operations, delivery channels, and geographical locations;
15.2.5. Statistics of reports submitted to the financial monitoring authority;
15.2.6. Training sessions held for the bank's employees.

16. Document Retention and Confidentiality Protection

16.1. All documents obtained within the scope of customer due diligence, results of analyses, account files, and business correspondence are retained in accordance with the conditions and timeframes set by legislation. The rights and duties of employees responsible for recording, retaining, and ensuring the confidentiality of information and documents are determined, and access to confidential information is restricted.

17. Final Provisions

17.1. The internal rules, procedures, and control mechanisms in the field of AML/CFT are reviewed once a year, and if necessary, measures are taken to update them.
17.2. All employees of the bank are directly responsible for ensuring the proper implementation of the requirements of this Policy.

17.3. This Policy enters into force after being approved by the bank's Supervisory Board.
17.4. Any additions or changes to this Policy may be made by the decision of the Supervisory Board.