BANK 3/4

APPROVED
by Supervisory Board
JSC «BANK 3/4»
Protocol No. 12
of 31 August 2022

POLICY

of Preventing and Counteracting to Legalization (Laundering) of the Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction

JSC «BANK 3/4»

(new edition)

Kyiv - 2022

CONTENT

1. GENERAL PROVISIONS

1.1. The Policy of Preventing and Counteracting to Legalization (Laundering) of the Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction of JSC «BANK 3/4» (hereinafter referred to as the Policy) has been drawn up with purpose to prevent the use of JSC BANK 3/4's services (hereinafter referred to as the Bank) for legalization (laundering) of the proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction (hereinafter referred to as ML/FT) and countering any other activities preceding or promoting the ML/FT.

The Policy defines the general principles and standards that the Bank is guided by when complying with the requirements of the Ukrainian legislation on preventing and countering ML/FT (hereinafter referred to as AML/CFT).

1.2. The Bank considers the legalization (laundering) of proceeds from crime, financing of terrorism and financing of the proliferation of weapons of mass destruction as inadmissible phenomena in its activities, which are under complete and unconditional prohibition. The Bank performs operations in such a way that the accepted ML/FT risks are identified, evaluated and are at the lowest possible and acceptable level for the Bank. With this, because, as a rule, it is impossible to completely exclude the identified risks, their acceptance at the approved level does not mean that the Bank considers ML/FT as acceptable. The Bank takes whatever action is required and introduces an internal control system to minimize ML/FT risks.

The Bank declares zero tolerance to all attempts to conduct operations through the Bank for the purpose of legalizing criminal proceeds, committing acts of corruption, other illegal acts, financing terrorism and financing the proliferation of weapons of mass destruction.

1.3. When implementing AML/CFT measures, the Bank takes into account that:

1) the legalization (laundering) of criminal proceeds includes any activity associated with the financial transaction or transactions with the proceeds of crime, as well as actions aimed at concealing or masking the illicit origin of such proceeds or ownership of them, rights to such income, sources of their origin, location, movement, changing of their form (transformation), as well as the acquisition, possession or use of proceeds of crime;

2) financing of terrorism is the provision or collection directly or indirectly of any assets with purpose of their use or with the awareness that they may be used in whole or in part :

- for any purpose by an individual terrorist or a terrorist group (organization);
- for the organization, preparation or commission of a terrorist act, involvement (recruitment) to commit a terrorist act, training persons to commit a terrorist act, printing handouts urging to commit a terrorist act, public calls to commit a terrorist act, creating a terrorist group (organization), facilitating the commission of a terrorist act, training terrorists, exit from Ukraine and entry to Ukraine with a terrorist intention, the exercise of any other terrorist activities, as well as attempts to commit such acts;

3) financing the proliferation of weapons of mass destruction is the provision, collection or use of any assets for proliferation of weapons of mass destruction for which international sanctions are provided;

1.4.The Policy has been developed in compliance with:

- the Law of Ukraine 'On Banks and Banking' (hereinafter referred to as the Law on Banks);
- the Law of Ukraine 'On Preventing and Counteracting to Legalization (Laundering) of the Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction' (hereinafter referred to as the Law);
- Regulation on financial monitoring by banks, approved by the Resolution of the Board of the National Bank of Ukraine No. 65 of 19.05.2020 (hereinafter referred to as the legislative act on financial monitoring);
- International standards (FATF Recommendations, Directives of the European Parliament and the Council of Europe, the Basel Committee on Banking Supervision, the OFAC sanctions programs, etc.);
- other legislative and regulatory acts of Ukraine,

– the Bank's Charter, the Bank's Corporate Ethics Code, the Bank's internal documents.

1.5. This Policy applies to all structural divisions, employees and managers of the Bank who, in compliance with their official duties, are involved in the internal banking system of AML/CFT, as well as customers who conduct financial transactions through the Bank.

1.6. The Policy is brought by the Bank's Supervisory Board (hereinafter referred to as the Bank's Board) to the attention of the Bank's Management Board and the Bank's Compliance Officer responsible for AML in charge of conducting financial monitoring in order to form a clear understanding of the expectations of the Bank's Board on:

- the proper organization and functioning of the internal banking system of AML/CFT and conducting primary financial monitoring, functioning of a proper ML/FT risk management system;
- the Bank's risk appetite in AML/CFT (including, if applicable, established prohibitions/restrictions on the implementation of certain types of activities and/or attracting certain types of customers for service);
- volume of Bank’s internal documents on AML/CFT issues required for the development and approval;
- requirements for the construction of three lines of defence in AML/CFT and the allocation of duties and responsibilities among the Bank's employees;
- functioning of internal control over AML/CFT issues;
- ensuring of training sessions concerning AML/CFT issues.

1.7. The Bank's Management Board and the Compliance Officer responsible for AML ensure introduction of employees involved in AML/CFT with the Policy . The Bank's Management Board is obliged to ensure that employees' job descriptions define the responsibilities and powers of employees concerning AML/CFT.

1.8.The Policy is not a restricted access document.

2. DEFINITION OF TERMS AND ABBREVIATIONS

2.1. The Policy applies the following terms and abbreviations:

FATF is Financial Action Task Force on Money Laundering;

PEP (PEPs (plural)) is an individual who is politically exposed person, his/her family member or a person related to politically exposed person or other person, whose ultimate beneficial owner is a politically exposed person, his/her family member or a person related to politically exposed person;

Banking Group is the banking group within the Bank, MICROCREDIT LLC and «KAPOWAI UKRAYINA» LLC;

Compliance Officer responsible for AML is the Bank’s responsible employee for conducting financial monitoring;

ML/FT is legalization (laundering) of the proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction;

USR is the Unified State Register of legal entities, individual entrepreneurs and public formations;

UBO is an ultimate beneficial owner;

USREOU code is an identification code in the Unified State Register of enterprises and organizations of Ukraine;

National Bank is the National Bank of Ukraine;

CDD is customer due diligence;

AML/CFT is preventing and counteracting to legalization (laundering) of the proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction;

List of terrorists a list of persons associated with the implementation of terrorist activities or subject to international sanctions, developed in accordance with the procedure established by the Cabinet of Ministers of Ukraine, and published on the official website of a specially authorized body;

The Bank’s Board is the Supervisory Board of JSC «BANK 3/4»;

reputation risk is an existing or potential risk to revenue and capital that arises from an unfavourable perception of the Bank's image by customers, counterparties, potential investors or supervisory authorities, which affects the Bank's ability to establish new relationships with counterparties, provide new services or maintain existing relationships, and may result in financial losses to the Bank (or its managers), or a reduction in the customer base, administrative, civil or criminal liability;

legal risk is an existing or potential risk to the Bank's income or capital that arises from the Bank's violation or non-compliance with the requirements of the laws of Ukraine, regulatory legislative acts and may lead the Bank to financial losses, abuse, bringing the Bank and/or its managers to administrative, civil or criminal liability;

Risk-appetite (risk propensity) of the Bank in AML/CFT is the size of ML/FT risk, that are determined in advance and within the acceptable level of ML/FT risk, in respect of which the Bank has decided whether it is appropriate /necessary to retain it in order to achieve its strategic goals and implement the business plan;

RNTRC is a registration number of the taxpayer's registration card;

AS is SR Bank automation system;

SSU is the Security Service of Ukraine;

RE is a reporting entity;

DA is a designated authority - the Central Executive Body responsible for the implementation of the state AML/CFT policy;

2.2. Interpretation of terms not defined by the Policy is made in accordance with the legislation of Ukraine, regulations of the National Bank of Ukraine and internal documents of the Bank.

3. KEY TARGETS OF THE INTERNAL AML/CFT BANK SYSTEM

3.1. In order to achieve the efficiency of internal financial monitoring system functioning under the current legislation of Ukraine and approved internal Bank's AML documents, the Bank is entrusted with fulfillment of following major tasks:

1) performing due diligence measures of new customers as well as existing customers;
2) ensuring the functioning of an appropriate risk management system, applying a risk-based approach in its activities on a permanent basis, and taking appropriate measures to minimize risks;
3) ensuring monitoring of the customer's financial transactions (including those that are carried out in the interests of customers) for compliance of such financial transactions with the Bank's information about the customers, their activities and risk, including, if necessary, information about the source of funds related to the financial transaction(s));
4) ensuring the identification of financial transactions subject to financial monitoring before, during, on the day of suspicion, after they are conducted or when they are attempted, or after the customer refuses to conduct them;
5) ensuring registration of financial transactions subject to financial monitoring, including the use of automation tools and DA notifications on:
   a) threshold and suspicious financial transactions (activities) or attempts to conduct them, regardless of the amount for which they are conducted;
   b) discrepancies between data about the customer's UBO in the USR, and information about the ultimate beneficial owners obtained as a result of CDD;
   c) at the DA's request, etc.;
6) assistance, under the legislation , to the DA's employees in conducting the analysis of financial transactions;
7) taking measures to prevent disclosure of information provided to the DA and other information on financial monitoring issues (including the fact of submission of such information or the fact of receipt of a request, decision or order from the DA and their implementation), except for cases specified by Law;

8) recording of measures taken to meet the requirements of legislation in AML/CFT by creating (maintaining) appropriate documents (including electronic ones), and records;
9) storage of documents (including electronic ones), their copies, records, data, information regarding measures in AML/CFT, in particular concerning the implementation of CCD (including identification and verification of customers' representatives, definition of their authority, as well as persons to whom the Bank refused to establish business relations and/or conduct financial transactions) , as well as all documents relating to the business relationship (carrying out of financial transaction) with a customer, not less than five years after termination of business relations with a customer or completing a one-time financial transaction without establishing business relations with customer;
10) providing access to documents (or information contained therein) on AML/CFT issues to the National Bank and at reasonable requests from law enforcement agencies, in accordance with the procedure and to the extent established by the Law on Banks;
11) suspending of fulfillment or ensuring monitoring of the financial transaction of a relevant person in accordance with the procedure established by legislation , by DA's order, provided with purpose to fulfill the request of the foreign state's authority;
12) suspension of carrying out of expenditure financial transactions or ensuring of monitoring of the financial transaction (financial transactions) of a relevant person in accordance with the procedure established by legislation , in accordance with the DA's decision;
13) conducting internal audits of its activities in accordance with the established procedure for compliance with the requirements of legislation in AML/CFT;
14) taking measures in compliance with the legislation to ensure that the Compliance Officer responsible for AML completes training in AML/CFT within three months from the date of his/her appointment, as well as upgrading the skills of the Compliance Officer responsible for AML by completing training at least once every three years at the respective educational institution that belongs to the DA's management sphere, and in other educational institutions coordinated with the DA;
15) taking ongoing measures to train staff to properly comply with the requirements of this Law, in particular through educational and practical activities;
16) managing risks associated with the introduction or use of new and existing information products, business practices, or technologies, including those that enable financial transactions to be conducted without direct contact with the customer;
17) ensuring the compliance with the requirements of the National Bank for the implementation (elimination of violations) in the field of AML / CFT on the basis of, within the powers and in order, foreseen by legislation ;
18) establishing procedures for employees to notify the Chairman of the Management Board and/or the Compliance Officer responsible for AML of violations of the legislation's requirements in AML/CFT , including without authorship (anonymously), with the provision of appropriate ways ;
19) ensuring of protection of employees in connection with the notifying of the Chairman of the Management Board and/or the Compliance Officer responsible for AML, the National Bank of violations of requirements of legislation in AML/CFT;
20) non-admission to the management, membership in the Bank's Board , the Bank's Management Board or to the fulfillment of control over the Bank of individuals that have outstanding or unexpunged conviction for acquisitive criminal offences or terrorism, and their accomplices in these criminal offences;
21) non-admission of formation of the Bank's authorized capital at the expense of funds whose sources of origin cannot be confirmed;
22) ensuring the continuity of the functioning of the intra-bank financial monitoring system and interaction with the DA, National Bank of Ukraine and other state bodies in the event of emergency events;
23) adoption of other specific measures in AML/CFT.

4. ORGANIZATION OF THE AML/CFT INTRABANK SYSTEM AND ITS GOALS

4.1. The Bank is a reporting entity of the national financial monitoring system and takes appropriate measures for prevention and counteracting to legalization (laundering) of proceeds from crime, financing of terrorism and financing of the proliferation of weapons of mass destruction.

4.2. Distribution of powers, duties and responsibilities for the functioning of the AML/CFT system between the Bank's Board, the Management Board, the Chairman of the Management Board, the Internal Audit Service, the Compliance Officer responsible for AML and the employees of the Financial Monitoring Department is following:

-

Name of the division/ management body	Functions and duties for managing the AML/CFT system	Responsibility
The Bank's Board	1) appoints the Bank's Compliance Officer responsible for AML in the manner specified by the Bank's Charter and Ukrainian legislation, and monitors the compliance of the Compliance Officer responsible for AML with regulatory requirements; 2) creates the separate structural unit for AML/CFT, headed by the Compliance Officer responsible for AML; provides sufficient resources for the functioning of the intrabank system of AML/CFT (including the separate structural unit for AML/CFT); 3) approves the Bank's Policy on AML/CFT issues, brings it to the attention of the Management Board and monitors its implementation, compliance and timely updating; 4) provides the control over efficiency of the ML/FT risk management system; 5) approves the list of limits (restrictions) and other instruments that restrict the use of a particular service/product [in particular, regarding the volume of activities, amounts of financial transactions, states (jurisdictions), and counterparties]; 6) distributes AML/CFT functions between the three lines of defence by defining the organizational structure. 7) introduces and continually improves internal control of AML/CFT issues, in particular, ensures timely identification of problematic issues and signs of an inadequate ML/FT risk management system by the internal audit; 8) annually reviews the report of Compliance Officer responsible for AML on the results of the assessment of the Bank's risk profile, problematic issues related to the development of a proper organization of the internal AML/CFT banking system and conduct of the initial financial monitoring, problematic issues related to ensuring a proper ML/FT risk management system and, following the results of consideration, approves the	The Bank's Board is responsible for creating a comprehensive, proper and effective system for managing ML/FT risks the Bank is exposed to in its operations.

Name of the division/ management body	Functions and duties for managing the AML/CFT system	Responsibility
	relevant decision and brings it to the attention of the Management Board and the Bank's Compliance Officer responsible for AML for its further execution. 9) reviews and approves the report of Internal Audit Service on the results of auditing the Bank's observance of the legislative requirements in AML/CFT, reviews the audit report of the external auditor, results of the Bank's audits by regulatory authorities as for the Bank's compliance with the legislative requirements in AML/CFT 10) sets requirements for ensuring the continuity of functioning of the intrabank financial monitoring system.	
The Bank's Management Board	1) participates in the development and approves internal Bank documents on AML/CFT issues, in compliance with the requirements of this Policy; 2) grants permission to establish business relations in the cases specified in subparagraph 9 of clause 5.8. of this Policy; 3) takes measures on AML/CFT within its competence; 4) performs the functions of a collegial body that considers the following AML/CFT issues at least once a quarter: • results of monitoring of business relations with customers, followed by the discovery of their suspicious activity, and suggestions for taking the appropriate steps in relation to such customers in order to minimize ML/FT risks; • issues related to offers to refuse to continue business relations with customers (including in the case of establishing an unacceptably high level of risk to the customer); • problematic issues that arise when conducting CDD measures in the Bank; • changes in the Ukrainian legislation in respect of AML/CFT issues and taking by Bank the required measures related to these amendments (in particular, updating the Bank's internal documents on AML/CFT issues), indicating the time frame for taking such measures ; • results of new banking products/services' evaluation and their inherent ML/FT risks; • problematic issues related to conducting training sessions for Bank employees, and Bank agents (their employees);	Members of the Management Board are liable for improper execution of tasks and decisions of the Bank's Board on the functioning of the ML/FT risk management system.

Name of the division/ management body	Functions and duties for managing the AML/CFT system	Responsibility
	• problematic issues related to establishing business relationships with PEPs and/or their servicing; • other issues regarding the Bank's compliance with the requirements of the Ukrainian legislation in AML/CFT that need to be considered. 5) approves the limits for each type of ML/FT risks in accordance with the list of limits (restrictions) determined by the Bank's Board); 6) ensures verification of impeccable business reputation for all Bank's employees involved in conducting initial financial monitoring; 7) ensures timely preparation of reliable reports on the AML/CFT system's functioning	
Chairman of the Management Board	1) manages the work of the Management Board, 2) grants permission to establish business relations with a PEP, and with foreign financial institutions, 3) grants permission to establish relations with agents and third parties on issues related to CDD (subject to the Management Board's decision to allow the use of the relevant services), 4) reviews reports of violations in AML/CFT, 5) approves AML/CFT training schedule, 6) provides protection for employees who have reported violations in AML/CFT, 7) organizes the proper storage of the documents	The Chairman of the Management Board and the Compliance Officer responsible for AML are liable for the improper organization of the internal AML/CFT banking system and fulfillment of primary financial monitoring
Internal audit service	1) Providing the Bank's Board, the Management Board with independent objective judgments, conclusions and assessments regarding the adequacy and effectiveness of the ML/FT risk management system; 2) Assessment of the Financial Monitoring Department's activities and the quality of ML/FT risk reports provided to the Bank's Board and the Management Board	Head and employees of the division are liable for violations /improper performance of the functions assigned to the division
Compliance Officer responsible for AML	1) ensuring the notification of DA of financial transactions subject to financial monitoring; 2) ensuring notification of DA of discrepancies between information about the customer's UBO in USR and information about UBO obtained by the Bank as a result of customer's CDD; 3) conducting audits of the activities of any division of the Bank and its employees on their compliance with internal documents on financial monitoring;	The Compliance Officer responsible for AML is liable for improper organization of the internal AML/CFT banking system and fulfillment of primary financial monitoring

Name of the division/ management body	Functions and duties for managing the AML/CFT system	Responsibility
	4) involvement of the Bank's employees in conducting primary financial monitoring and audits on these issues; 5) organization of development, submission for approval, ensuring continuous updating, as well as monitoring the implementation of internal documents on financial monitoring issues; 6) receives explanations on financial monitoring issues from the Bank's employees, regardless of their positions; 7) assistance in conducting audits of the Bank's activities on compliance with legislation in AML/CFT by authorized representatives of the National Bank of Ukraine; 8) deciding on submitting information on financial monitoring issues at the DA's requests and relevant law enforcement agencies; 9) performing other functions in accordance with the legislation and internal documents on financial monitoring; 10) drafting and submitting reports on ML/FT risks to the Bank's Board at least once a year, and to the Bank's Management Board at least once a quarter; 11) ensuring sufficient awareness and knowledge of the Chairman, members of the Bank's Board and the Management Board concerning their duties in AML/CFT, and ML/FT risks inherent to the Bank's risk profile; 12) ensuring of informing the Bank's managers on the importance of fulfilling the requirements of the Ukrainian legislation on AML/CFT issues to ensure proper risk management system, the need to adopt effective measures to efficiently prevent the use of the Bank's services with the aim of ML/FT and understanding of the consequences the Bank would face in case of default of requirements of the Ukrainian legislation on AML/CFT issues. 13) in case of emergency events, coordinates the actions of the personnel in order to ensure the continuity of the functioning of the intrabank financial monitoring system; 14) provides instructions to the responsible persons of the Bank regarding the immediate implementation of certain procedures, actions, refraining from actions in case of a change in legislation and/or with the aim of taking immediate	

Name of the division/ management body	Functions and duties for managing the AML/CFT system	Responsibility
	preventive measures to prevent the use of the Bank for ML/CFT purposes.	
The Financial Monitoring Department	1) provides the functioning of the ML/FT risk management system; 2) develops internal documents of the Bank on the AML/CFT issues to the extent necessary for the effective functioning of the internal AML/CFT banking system and the Bank's employees' understanding of their responsibilities and powers in AML/CFT; 3) studies new products/services, including new sales channels, the use or development of new technologies for existing or new products in order to properly assess their inherent ML/FT risks and properly control of ML/FT risks for existing products/services; 4) provides ongoing training sessions for Bank employees and Bank agents (their employees) for them to understand their responsibilities and procedures; 5) establishes and provides the functioning of an effective and timely system for escalating suspicions and problematic issues in AML/CFT and the procedure for their consideration, including reporting information/facts related to cases of violation or possible violation of the legislation of Ukraine in AML/CFT, in accordance with the procedure provided for in the Bank's internal documents; 6) introduces the AS, which ensures timely and comprehensive fulfillment of the Bank's RE obligations (in particular, the identification of financial transactions subject to financial monitoring, freezing assets related to terrorism and/or its financing, the proliferation of weapons of mass destruction and/or its financing, the impossibility to carry out operations by persons from the list of terrorists); 7) ensures timely identification of financial transactions subject to financial monitoring and proper information exchange with DA; 8) develops and carries out CDD measures aiming at the understanding of the customer's activity, purpose and intended nature of the business relationship with it that enables the Bank to be sure that the customer's financial transactions conform to the Bank's information about it, its business, risk profile, including, if necessary, the sources of origin of its	Members of the Financial Monitoring Department are liable for violation /improper performance of the functions assigned to the division

Name of the division/ management body	Functions and duties for managing the AML/CFT system	Responsibility
	funds/means, the identification of UBO for rapid detection of unusual behaviour and suspicious financial transactions (activities); 9) properly records the actions of the Bank's employees and events related to the Bank's performance of RE's duties; 10) stores all documents, data, and information (including relevant reports, orders, and files) related to the Bank's performance of RE's obligations for the period specified by the legislation of Ukraine; 11) promptly and fully provides the necessary documents/information/clarifications/arguments at the National Bank's requests, duly confirming the Bank's compliance with the requirements of the Ukrainian legislation in AML/CFT issues; 12) takes steps to continuously improve the internal AML/CFT banking system.	

4.3. The purpose of creating a proper organization of the internal bank AML/CFT system and conducting primary financial monitoring of the Bank is:

- compliance with the requirements of the Ukrainian legislation in AML/CFT ;
- minimization of ML/FT risks;
- the possibility of proper identification of threshold and suspicious financial transactions (activities) and reporting them to DA;
- preventing the use of the Bank's services and products for customers to conduct financial transactions for ML/FT purposes.

4.4. The Chairman of the Bank's Management Board, and the Compliance Officer responsible for AML shall be liable for improper organization and conduct of primary financial monitoring.

4.5. All Bank employees are involved in the internal financial monitoring system. The list of divisions and employees is defined in the Bank's internal regulatory documents on financial monitoring, taking into account the Bank's organizational structure.

4.6. To prevent violations of laws in AML/CFT, the Bank identifies in its internal documents the workers who make decisions at different stages of control in accordance with their functions, ensuring the principle that 'the higher position means more power and responsibility' and sets out a clear allocation of responsibilities and powers among the Bank’s Board, the Chairman of the Management Board, the Management Board/ members of the Management Board, Compliance Officer responsible for AML, other employees and structural divisions of the Bank.

4.7. Distribution of duties, responsibility of employees involved in the process of the Bank activities in AML/CFT is defined in their job descriptions and/or contracts, and internal documents of the Bank regulating the activity of employees, departments, including internal regulations on financial monitoring. Employees are to get acquainted with such documents against the signature (including an electronic signature).

4.8. The Chairman of the Management Board and other Bank employees are obliged to facilitate the fulfillment by Compliance Officer responsible for AML's of his/her functions.

5. DETERMINATION OF THE BANK'S RISK APPETITE IN AML/CFT. MAJOR PROHIBITIONS AND RESTRICTIONS

5.1.The Bank applies in its activities a risk-based approach, taking into account respective risk criteria, in particular those related to the customers, geographical location of the state of customer's registration or the institution through which the transfer (receipt) of assets, type of goods and services that the customer receives from the Bank is conducted, method of provision (receipt) of services proportionate to the nature and scale of its activities.

5.2. The Bank's risk-based approach is based on a two-stage risk assessment and includes an assessment of the Bank's risk profile (including determining the Bank's risk appetite in AML/CFT (acceptable level of ML/FT risk for the Bank) and an assessment of the customer's risk profile. The Bank's Board reviews the results of the Bank's risk profile assessment, approves the relevant decision based on the results of such review, and informs the Management Board and the Compliance Officer responsible for AML of the Bank for its further implementation.

5.3. By applying a risk-oriented approach, the Bank refrains from unreasonable application of de-risk, which contradicts the risk-oriented approach and does not promote financial inclusion.

5.4. To assess ML/FT risks, the Bank applies a 4-level scale that identifies the following risk levels:

1) low
2) medium
3) high
4) unacceptably high.

Methods for assessment of the Bank's risk profile, assessment of customers risk profile, the procedure for determination (identification) and assessment of the customers' risks are defined in the Bank's financial monitoring risk management program.

5.5. The Bank's risk appetite is the basis for further setting of risk limits.

5.6. The calculation algorithm and specific values of the acceptable level of risk and risk appetite are determined by the Bank annually in the Risk Appetite Statement (RAS), which is approved by the Bank's Board.

5.7. Risk Appetite Statement is an internal Bank document in which the Bank's Board determines the total size of risk appetite, the types of risks that the Bank may accept or must avoid in order to achieve its business goals, and the level of risk appetite for each of them (individual level) .

5.8. Taking its activity the Bank sets the certain prohibitions/restrictions in its activities in part of establishing business relations, fulfilling of certain transactions, taking into account their unacceptable risk for the Bank, in particular:

1) it does not open or maintain anonymous (numbered) accounts;
2) it does not establish correspondent relations with shell banks, as well as with banks and other non-resident financial institutions known to maintain correspondent relations with shell banks;
3) it does not perform customer and interbank financial transactions of other banks with which the correspondent has established correspondent relations through a correspondent account opened with the Bank;
4) it does not establish business relationships (except in cases stipulated by UN Security Council resolutions), does not conduct expenditure financial transactions, does not provide services directly or indirectly to customers who are:

- individuals and/or organizations included in the list of persons associated with terrorist activities or that are subject to international sanctions;
- persons and/or organizations acting on behalf of persons and/or organizations included in the list of persons associated with terrorist activities or that are subject to international sanctions;
- persons and/or organizations that are directly or indirectly owned or whose ultimate beneficial owners are persons and/or organizations included in the list of persons associated with the implementation of terrorist activities or that are subject to international sanctions;
- a counterparty of a financial transaction or financial institution that provides a financial transaction is a person who belongs to persons specified in this clause, and the Bank has become aware of it during the provision of services/execution of operations;

5) it refuses to establish (maintain) business relations/refuses to open an account (or to service) to the customer, including by terminating the business relationship, closing the account/refusing to conduct a financial transaction in case of:

- if identification and/or verification of customer, as well as establishment of data that allows identify the ultimate beneficial owners, is impossible, or if the Bank has doubts about the fact that the person acts on his/her own behalf;
- establishing an unacceptably high risk to the customer or failure by the customer to provide the necessary documents or information for proper verification of the customer;
- submission of false information to the Bank by the customer or its representative or submission of information for the purpose of deluding the Bank;
- detection of the fact that a bank or other financial institution with which a correspondent relationship has been established is a shell bank and/or such bank or financial institution maintains a correspondent relationship with a shell bank;
- if identification of person on whose behalf or in whose interests the financial transaction is being conducted and identification of its ultimate beneficial owner or beneficiary for the financial transaction is impossible;

6) it does not carry out a payment transaction in the absence of mandatory information which must be accompanied the payment transaction or transfer of virtual assets;

7) the Bank's directors, the Compliance Officer responsible for AML, other Bank employees involved in primary financial monitoring, and the ultimate beneficial owners of the Bank shall not use their powers and related opportunities or refrain from using them for the purpose of ML/FT or assisting other persons in performing such actions;

8) does not establish/maintain business relations with customers and does not fulfill financial transactions of Bank’s clients if at least one of the parties participating in the financial transaction has the appropriate registration, place of residence or location (the residency) in the state/self-proclaimed territory, or for fulfillment of transactions use an account opened with financial institution registered in the state/self-proclaimed territory, or use documents issued in its name by the state/self-proclaimed territory that is on the list of territories or countries that:

- support terrorism;
- conduct military operations;
- do not comply or do not properly comply with the guidelines of international and intergovernmental organizations working in ML/FT;
- are self-proclaimed;
- not recognized by Ukraine.

The list of territories or countries mentioned above includes, but is not limited to:

No.	**Country code**	**Character code of the country**	**Name**
1	364	IRN	Iran, Islamic Republic
2	408	PRK	Democratic People's Republic of Korea
3	643	RUS	Russian federation
4	112	BLR	Republic of belarus
5	728	SSD	Southern Sudan
6	760	SYR	Syrian Arab Republic
7	-	-	Pridnestrovien Moldavian Republic
8	-	-	Nagorno-Karabakh Republic
9	-	-	Somaliland
10	-	-	Republic of Kosovo
11	-	-	Sudan (North)
12	-	-	Republic of Abkhazia
13	-	-	South Ossetia
14	-	-	Donetsk People's Republic
15	-	-	Luhansk People's Republic

16	-	-	Crimea (a ban on business entities, as well as on persons whose residence in the territory of Crimea and Sevastopol is confirmed by a document issued not by Ukraine)

The list of territories may be expanded by order of the Chairman of the Management Board on the recommendation of the Compliance Officer responsible for AML for the purpose of operational ML/FT risk management.

The Bank's Management Board is entitled to determine the list of countries with residents of which the Bank establishes business relations only with the permission of the Chairman of the Management Board.

9) the Bank does not establish/maintain business relations with customers who conduct operations/whose business activity is aimed at the production of narcotic drugs (except for institutions that have a state license), marijuana, or adult entertainment services.

By decision of the Management Board of Bank business relations are established with customers who:

- provide employment services abroad;
- trade in military weapons (it does not apply to hunting weapons);
- hold lotteries and/or gambling;
- carry out activities in nuclear energy;
- collect and trade of agricultural products;
- collect and trade scrap metal
- provide / participate in the circulation of virtual assets.

Business relations with charitable organizations are established with the approval of the Compliance Officer responsible for AML and the permission of the Chairman of the Management Board.

Business relations with a PEP and foreign financial institutions are established with the permission of the Chairman of the Management Board.

5.9. Following the analysis's results, the Bank's Management Board sets forth (if needed) in its internal documents on AML/CFT issues additional prohibitions/restrictions in its activities (certain types of activities and/or attracting certain types of customers).

5.10. All other risks of ML/FT can be accepted by the Bank, including after taking steps to manage risks (minimize them). When taking appropriate risks, the Bank takes into account the availability of effective measures to manage them, in particular, the availability of required resources.

5.11. The Bank during the establishment of business relations, conducting a one-time financial transaction in the amount equal to or exceeding UAH 400 000,00 or equal to or exceeding the amount in foreign currency, banking metals, other assets, equivalent at the official exchange rate of UAH to foreign currencies and banking metals UAH 400 000,00 at the time of the financial transaction, as well as in other cases established in the internal documents, establishes at least the following identification data:

1) for an individual - surname, first name and patronymic (if any), date of birth, number (and series, if any) of passport (or other document proving the identity and which according to the laws of Ukraine may be used in Ukraine for conclusion of transactions), date of issue and issuing authority, citizenship, information about the place of residence or place of temporary stay in Ukraine, unique entry number in the Unified State Demographic Register (if any). If, according to the customs of the national minority to which the person belongs, the surname or patronymic are not constituents of the name, only the constituents of the name shall be indicated;

2) for a legal entity – full name, location; details of bank with which the account was opened, bank account number; information about executive body (management authorities);

identification data of persons who have the right to manage accounts and/or property. During verification Bank is provided with a copy of legalized extract from the trade, bank or court register or a notarized registration certificate of the competent authority of a foreign state on registration of the legal entity in question;

3) for trusts and other similar legal arrangements that are not legal entities – full name, purpose and objectives of the activity, management objects belonging to a nonresident in respect of which identification and verification is conducted, a country of establishment, location; details of a bank in which an account was opened, bank account number; identification number (if any) used by a non-resident when submitting tax declarations and other tax documents to tax authorities in its country of residence. During verification Bank is provided with a certified copy of the document on establishment (foundation) of a trust or other similar legal arrangement.

5.12. Information obtained during identification, verification, and study of the customer is properly documented and stored for the entire duration of the business relationship, and for at least 5 years after its termination or completion of a one-time financial transaction without establishing a business relationship with the customer.

5.13. During the establishment of business relations, and during the execution of any financial transactions of the Bank's customers, operations performed in favour of the Bank's customers, as well as its own operations, the Bank checks whether a participant or beneficiary of the transaction is included in the list of persons subject to sanctions. The relevant checks are carried out by means of the AS (as far as it is possible), and include at least the following lists:

1) List of persons involved in terrorist activities;
2) National sanctions lists established by the National Security and Defence Council of Ukraine and approved by Presidential decrees and other legislative acts
3) Office of Foreign Assets Control (OFAC) lists
4) European Union (EU) lists
5) United Nations (UN) lists
6) Black list of the Bank.

5.14. The Bank takes steps to identify a PEP and enter information about PEP to the AS as far as possible to ensure further control of operations involving PEP based on a risk-based approach. The Bank uses public official registers, information published on industry-specific Internet resources, and information obtained in the course of customer's study . The Bank recognizes that the verification of the customer's membership in the PEP category is partially performed by means of automation, partially by manual means, therefore, the identification procedures are subject to periodic reviewing and continuous upgrading.

6 . COMPLIANCE CONTROL.

6.1. The Bank’s internal control system should provide sufficient assurance to the Bank’s Board and Management Board regarding the Bank's proper fulfillment of the RE's responsibilities and prevention of using the Bank for ML/FT.

6.2. Bank creates and implements an internal control system based on the distribution of responsibilities between the Bank's divisions.

This distribution is based on the application of the model of three lines of defence, namely:

• first line of defence - employees, divisions of the Bank that conduct / ensure the conduct of operations or provision of services;

• second line of defence - employees of the Financial Monitoring Department, Compliance Officer responsible for AML;

• third line of defence - the Bank's Internal Audit Service.

6.3.Internal compliance control measures are determined by the Bank's Management Board, second and third defence line divisions in accordance with their powers, taking into account the following:

1) The Bank implements automated control measures as much as possible.
2) Internal control is to be at least double ('two sets of eyes' principle).
3) In order to improve the ML/FT risk management system, the Bank implements preventive (aimed at preventing violations and risks), proactive (aimed at identifying risks) and corrective (aimed at avoiding/minimising realized risks) measures.
4) Despite the internal audit function, the Bank fulfills further control at the first and second line of defence.

6.4. Regardless of the applied control procedures, the Bank, in order to implement internal control, shall conduct periodic further monitoring of financial transactions in the manner prescribed in internal documents of the Bank on AML/CFT, with the purpose of revealing financial transactions subject to financial monitoring, but which for certain reasons have not been timely identified.

7.PROVISION OF TRAINING ACTIVITIES ON AML/CFT ISSUES

7.1. In order to properly comply with requirements of the legislation in AML/CFT Bank engages competent persons to perform functions and duties, ensures the maintenance of an appropriate level of employees' qualification, including by conducting training activities in AML/CFT issues.

The Compliance Officer responsible for AML is to continually keep his/her level of knowledge in AML/CFT issues at the appropriate level, including through AML/CFT training, and upgrade training. .

The Bank's training sessions are to take into account the specific features of employees' job duties, their powers and responsibilities, as well as the level of knowledge and qualifications required for such employees in order to properly perform their duties in AML/CFT.

7.2. The Compliance Officer responsible for AML ensures awareness of the Management Board and the Bank employees involved in the AML/CFT procedures of the amendments to legislation, guidelines of world organizations in AML/CFT and changes in the Bank's internal documents concerning AML/CFT issues.

7.3. Measures to organize training and professional development of employees are taken by the Bank on an ongoing basis. 7.4. The purpose of staff training is to ensure the appropriate level of their professional training for a deep understanding of their responsibilities and procedures, for timely identification of transactions subject to financial monitoring, and to prevent attempts to use the Bank's system for ML / FT.

7.5. Training activities, if necessary, end with a knowledge test with subsequent evaluation of the results of inspections by management.7.6.Description of the internal bank financial monitoring system, in particular, effective risk-oriented procedures that are sufficient for the proper organization and functioning of the AML/CFT system and conducting primary financial monitoring is defined in the internal documents on financial monitoring. The key principles for developing internal regulatory documents on financial monitoring and their requirements are defined in section 8 of the Policy.

8.INTERNAL BANK'S REGULATORY DOCUMENTS CONCERNING AML/CFT ISSUES

8.1. In compliance with the requirements of this Policy and the requirements of current legislation, the Bank develops and approves, including but not limited to, following internal documents in order to comply with the requirements of legislation in AML/CFT:

- Bank's financial monitoring rules;
- Program for fulfilment of due diligence measures for the Bank's customers;
- Bank's financial monitoring risk management program ;
- Training and advanced training program for the Bank's employees on preventing the legalization (laundering) of proceeds from crime, financing of terrorism, financing of the proliferation of weapons of mass destruction;

- Procedure for providing necessary information for payment transactions or transfer of virtual assets.

These documents and this Policy are internal regulatory documents of the Bank on financial monitoring.

The Bank's Management Board is entitled to develop and approve other documents on AML/CFT issues in order to improve the Bank's AML/CFT system.

The Chairman of the Management Board is entitled to approve methods, temporary procedures, distribution of powers between employees of divisions of the 1st line of defence, job descriptions of employees in order to resolve practical issues of implementation of internal Bank documents on AML/CFT issues.

The Compliance Officer responsible for AML develops guidelines, clarifications, and other documents to ensure that employees correctly apply internal Bank documents on AML/CFT issues and that the Bank properly fulfills its responsibilities as a primary financial monitoring entity.

8.2. The basic principles of development and implementation of internal documents on AML/CFT issues are:

- proper organization and functioning of the internal AML/CFT banking system and conducting primary financial monitoring, functioning of proper ML/FT risk management system, ensuring the functioning of an effective intrabank AML/CFT system;
- the introduction of a risk-based approach in the implementation of AML/CFT procedures;
- fulfilling of all obligations in AML/CFT by the Bank stipulated by the legislation;
- accounting for all types and activities of the Bank;
- introduction of AML/CFT culture in the Bank and ensuring the direct participation of each employee (within his/her competence) in the implementation of AML/CFT procedures;
- clear allocation of duties and powers among the Bank's Board, the Chairman of the Management Board, members of the Management Board, the Compliance Officer responsible for AML, other employees and structural divisions of the Bank to prevent the Bank violations of the law in AML/CFT;
- proper internal control (for different types of services/products, types of customers, the level of customer risks, the amount of financial transactions) and identification of Bank employees who make decisions at different stages of control in accordance with their functions, ensuring the principle of 'the higher position means more power and responsibility';
- establishing a detailed and clearly understandable procedure for the Bank's employees when performing AML/CFT procedures;
- ensuring the secrecy of financial monitoring and confidentiality of information about information exchange with the DA, including the fact of transmitting information about the customer's financial transaction to the DA;
- ensuring confidentiality of information about internal documents concerning AML/CFT issues;
- ensuring the confidentiality of information about customers, their accounts and financial transactions, as well as other information that constitutes Bank secrecy;
- prevention of the Bank employees' involvement in the ML/FT.

8.3. The Bank's internal documents on AML/CFT issues are to contain:

- identification of the Bank's division(s) and/or Bank employees in charge of the implementing the CDD measures and allocation of responsibilities among them;
- the procedure that ensures the implementation of all measures for the CDD (in particular, measures for identification and verification, identification of an UBO, monitoring business relations and financial transactions, updating customer's data);
- PEPs' identification procedure and procedure for taking required supplementary steps;
- the procedure for evaluating/revaluing the Bank's risk profile and customer's risk profile and taking steps to minimize ML/FT risks;
- the procedure for identifying ML/FT risk criteria and indicators of suspicious financial transactions;

- the procedure for taking necessary extra steps to establish correspondent relations with a foreign financial institution;
- the procedure for keeping an electronic questionnaire, which will ensure the timeliness, completeness and reliability of the information entered in the customer's electronic questionnaire;
- the procedure for the Bank's refusal to establish (maintain) a business relationship/open an account (servicing), including by terminating a business relationship, closing an account/refusing to conduct a financial transaction in cases stipulated by the law on AML/CFT;
- the procedure for the Bank to identify discrepancies between the information about the UBO contained in the USR and the information received by the Bank as a result of CDD;
- the procedure for using the reliance tool (if the Bank decides to use this tool);
- the procedure for involving agents by the Bank, conducting training activities for them (their employees) and monitoring their activities (if the Bank decides to involve agents);
- the procedure for entering relevant information in the notification registers;
- the procedure for using the AS;
- the procedure for information exchange with the DA and implementation of relevant DA's decisions/instructions;
- the procedure for freezing assets related to terrorism and its financing, proliferation of weapons of mass destruction and its financing;
- the procedure for suspension of operations by the Bank in cases defined by Law;
- the procedure for Bank's support of payment transactions or transfer of virtual assets with relevant information in accordance with the requirements established by Law;
- the procedure for controlling the relevant limits in case the Bank applies simplified methods of identification and verification of the customer (customer's representative);
- the procedure for ensuring the secrecy of financial monitoring and confidentiality of other information;
- the procedure for informing the Security Service of Ukraine in cases stipulated by the legislation in AML/CFT;
- the procedure for conducting training activities for the Bank employees;
- the procedure for familiarising the Bank's employees with the Bank's internal documents on AML/CFT issues;
- the procedure for storing all documents/information on the Bank's compliance with the requirements of legislation in AML/CFT.

8.4. The Bank's internal documents on financial monitoring take into account the Bank's specific features and activities, the characteristics of different types of customers, as well as the Bank's implementation of a risk-based approach.

8.5. If necessary, other documents not provided for in this Policy may also be developed for the purpose of ensuring the proper organization of the Bank's AML/CFT system. The Bank's internal regulatory documents on financial monitoring are to be approved by the Bank's Management Board.

8.6. The Financial Monitoring Department ensures that internal documents on AML/CFT issues are continually updated, taking into account the amendments to legislation in AML/CFT and events that may affect the Bank's ML/FT risks.

8.7. In case of changes in the legislation, detection of schemes, typologies of operations that carry increased ML/CFT risks before updating internal bank documents and in order to prevent the Bank from violating legislation or involving the Bank in ML/CFT, the Compliance Officer responsible for AML has the right to issue orders regarding changes in certain operating procedures the AML/CFT system in terms of strengthening controls, banning certain operations, refraining from actions, etc.

9. FINAL PROVISIONS

9.1. The Policy is open-ended, it comes into force after its approval by the Bank's Board and is valid until its cancellation or approval by the Bank's Board of a new Policy, with the entry into force of which the previous one becomes invalid.

9.2. With the entry into force of this Policy, the Policy on Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction of JSC BANK 3/4, approved by the Supervisory Board decision from 29.01.2021 (Protocol № 2), shall cease to be valid.

9.3. The Policy is to be reviewed if necessary, but at least once a year. Following the reviewing, the Bank’s Board is entitled to decide not to make amendments to the Policy. Amendments to this Policy are to be made provided they are approved by the Bank's Board in accordance with the established procedure.

9.4. If any part of this Policy does not comply with the current legislation of Ukraine and regulations of National Bank, including in connection with the adoption of new legislative acts or changes of existing ones, this Policy shall apply to the extent that it does not contradict the legislation and regulations of the National Bank. Prior to making appropriate changes to this Policy, the Bank's employees must be guided by the norms of the current legislation of Ukraine in their work.