



JOINT-STOCK COMPANY  
“FIRST UKRAINIAN INTERNATIONAL BANK”  
(JSC “FUIB”)

Kyiv

APPROVED BY  
the Supervisory Board of JSC “FUIB”  
Minutes No. 433 dated 19.12.2024  
AGREED BY  
the Board of JSC “FUIB”  
Minutes No. 1035 dated 16.12.2024  
Chairman of the Board


\_\_\_\_\_ Serhii CHERNENKO

**RISK MANAGEMENT**

**POLICY of JSC “FUIB”**


All rights to this document belong to JSC “FUIB”.

This document may not be used or reproduced in whole or in part without the written permission of the copyright holder.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

## CONTENTS

1. INTRODUCTION.....	3
2. PURPOSE .....	4
3. SCOPE OF APPLICATION .....	5
4. TERMS, DEFINITIONS, AND ABBREVIATIONS .....	5
5. RISK MANAGEMENT PRINCIPLES.....	6
6. RISK MANAGEMENT ORGANIZATIONAL STRUCTURE.....	8
7. ROLES, POWERS AND RESPONSIBILITIES OF PARTICIPANTS .....	10
8. MAIN PART .....	17
9. CREDIT RISK .....	24
10. LIQUIDITY RISK .....	27
11. INTEREST RISK IN THE BANKING BOOK .....	28
12. MARKET RISK .....	29
13. OPERATIONAL RISK .....	29
14. COMPLIANCE RISK .....	36
15. PAYMENT SYSTEM PARTICIPANT RISK (PSP RISK) .....	41
16. PROCESS OF ASSESSMENT AND MANAGEMENT OF RISKS OF CHANGES IN PROCESSES AND PRODUCTS DURING BUSINESS INITIATIVES IMPLEMENTATION	43
17. LEVELS OF CONTROL (LINES OF DEFENCE) OF THE BANK’S ICS .....	46
18. CORPORATE RISK MANAGEMENT CULTURE.....	47
19. REPORTING.....	47
20. CONTROL WITHIN THE INTERNAL CONTROL SYSTEM OF FUIB .....	49
21. DOCUMENT REVIEW PROCEDURE .....	50

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	<b>JSC “FUIB” Risk Management Policy</b>	

## 1. INTRODUCTION

1.1. JSC “FUIB” consistently implements its business development strategy as a leading universal financial institution with Ukrainian capital, serving all categories of clients.

1.2. The key areas of its activities are:

- Private banking (including banking for wealthy retail clients – VIP-banking) – providing banking services to clients, opening and maintaining card accounts, attracting deposits; processing credit and debit cards; providing consumer loans, documentary operations (letters of credit and guarantees); safe deposit services; conducting cash and currency exchange operations; providing services using RSS (Remote Service Systems).

- Wholesale banking – opening and maintaining current and deposit accounts, providing lending services (including overdrafts), encashment services; clearing and settlement; financial leasing, trade finance and documentary business.

- Depository activities of a depository institution (according to the licensed type of activity);

- Activities in the capital markets for financial instruments trading (according to the Bank’s licensed type of activity); trading in foreign currency and bank metals on the interbank foreign exchange market of Ukraine and on international foreign exchange markets; repurchase agreements without transfer of securities ownership; structured financing; attraction and placement of interbank loans and deposits; opening and maintaining correspondent accounts of resident and non-resident banks, cash transactions, provision of processing centre services, provision of guarantees and confirmation of letters of credit.

1.3. When determining its business objective, the Bank takes into account requirements of the “Risk Management Strategy of JSC “FUIB” approved by the Supervisory Board of the Bank.

1.4. The main objectives of the Bank’s risk management system are:

- ensuring the sustainable development of the Bank in accordance with its business development strategy;

- ensuring and protecting the interests of shareholders, depositors, creditors, clients, and other stakeholders in the sustainable operation of the Bank, while mitigating risks that could threaten its existence;

- strengthening the Bank’s competitive advantage through strategic planning that considers level of risk accepted, enhancing risk management effectiveness, and increasing Bank’s market value while maintaining its reliability and expanding product offerings;

- increasing investor confidence through a transparent risk management system and establishing Corporate Governance System, subject to constant supervision of the NBU and other relevant state bodies.


1.5. An effective risk management system ensures that the Bank achieves its tactical and strategic objectives while strictly adhering to internal and external regulations, including capital adequacy requirements, under both normal and crisis conditions.

1.6. Capital adequacy is monitored by dedicated units (Financial Controlling Department, General Banking Risk Department)

1.7. and officers, as well as by the Supervisory Board, the Board, the Chairman of the Board, and relevant committees of Management/Supervisory Board.

1.8. The main instruments of capital adequacy control are:

- formalized approaches to calculating capital adequacy, assessment of their actual values and forecasting, stress tests;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- exposure to risks: determination of target levels of capital adequacy and internal minimum limits for risk metrics;

- capital adequacy reporting and making management decisions based on it.

1.9. The Bank regularly (annually) prepares and approves a Risk Exposure Declaration. The Risk Exposure Declaration is approved by the Supervisory Board and is based on the following risk categories:

- **Risk capacity** is the maximum risk that the Bank is able to accept for all types of risks, taking into account the level of its capital; the ability to adequately and effectively manage risks, as well as taking into account regulatory restrictions.

- **Risk appetite** is the aggregate level of risk appetite and types of risks that the bank intends to take and hold to achieve its business goals and implement the business plan.

- **Risk limits** is a quantitative restriction established by the Bank to control the amount of risks that the Bank faces within its activities.

- **Risk profile** is an assessment of the Bank’s exposure to risks (before risk minimization measures) or residual exposure to risk (after risk minimization measures) in aggregate and for each type of risk, conducted as of a certain date based on current or forecast assumptions.

a. Due to the fact that the largest volume of JSC “FUIB” operations is related to banking activities, the following types of risks are potentially material:

- credit risk (the largest exposure) taking into account the impact of climate change risks;

- liquidity risk;

- interest risk in the banking book;

- market risk, including: currency risk and price risk, as an estimate of losses in the event of conversion of the hryvnia portfolio of OVDPs into primary liquidity and price risk of Sovereign bonds G7;

- operational risk taking into account the impact of climate change risks (including legal, ICT and information security risk, including cyber risk);

- compliance risk (including money laundering/terrorism financing risk – the Bank’s ML/TF risk).


b. The risk profile is defined in the Risk Management Strategy approved by the Supervisory Board.

## 2. PURPOSE

2.1. The Risk Management Policy of the JSC “FUIB” is aimed to organise a clear process of effective risk management by setting restrictions, and thresholds for each type of risk, which aims to implement a systematic process of identifying, calculating, monitoring, controlling, reporting and mitigating all types of risks at all organisational levels of the Bank. In the context of a trend of decreasing profitability of most financial instruments and, as a result, earnings dilution, risk control is one of the main sources of maintaining the Bank’s profitability.

2.2. An effective way to minimize risks is to regulate them by setting limits. In accordance with the risk appetite, the Bank sets the main risk limits, and all major decisions on asset and liability management are analysed for possible violation of the established limits.

2.3. Most business indicators are approved as limits to accurately reflect the Bank’s strategy in the risk profile. The limit setting system is mainly designed to ensure the formation of the Bank’s asset and liability structure in accordance with the nature and scale of its business.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

2.4. Every quarter, the Bank’s risk profile as of the reporting date is correlated with the risk appetite approved for the year by type of risk.

### 3. SCOPE OF APPLICATION

3.1. This Policy applies to all employees of the Bank, all processes, the entire organizational structure and management levels.

### 4. TERMS, DEFINITIONS, AND ABBREVIATIONS

**Bank** is JSC “FUIB”, JOINT STOCK COMPANY “FIRST UKRAINIAN INTERNATIONAL BANK.”

**Basel II/III** is a document of the Basel Committee on Banking Supervision (BCBS) “Basel III: A global regulatory framework for more resilient banks and banking systems”.

**Internal Capital Adequacy Assessment Procedures (ICAAP)** are the process of Bank’s assessment of the capital adequacy at its disposal, i.e. internal capital to cover accepted and potential risks. ICAAP also includes capital planning procedures based on the established development strategy of the Bank, business growth guidelines and the results of a comprehensive current assessment of the specified risks, stress testing of the credit institution’s resilience to internal and external risk factors. ICAAP is part of the Bank’s corporate culture.

**ML/FT** means (laundering) of proceeds from crime funds, financing of terrorism and/or financing of proliferation of weapons of mass destruction;

**CCO** means the Bank’s chief compliance officer, performing the functions of the chief compliance manager and the function of the employee responsible for Bank’s financial monitoring.

**Deputy Chairman of the Board for Risk Management (CRO)** means the Bank’s chief risk officer, performing the functions of the Bank’s chief risk manager (hereinafter referred to as the “CRO”).

**Available internal capital** means the Bank’s financial resources that can be used to cover any unforeseen losses from the materialization of significant risks.

**CBRD** – Corporate Business Risks Department.

**RRD** – Retail Risks Department.

**GBRD** – General Banking Risk Department

**Stakeholders/parties** – entities (individuals and legal entities) interested in the financial and other results of the Bank’s activities, such as: shareholders, creditors, employees, clients (counterparties) including depositors, supervisory authorities.

**Significant/Material risks** – risks whose materialization may significantly affect the efficiency of the Bank’s work, including the adequacy of the Bank’s capital with the established level of materiality (for each of the risks)


**Risk matrix** means Bank’s report, which includes a two-dimensional table, the axes of which reflect the impact and probability of risk materialization. This report becomes the basis for Bank’s determination of material risks.

**ALMC**- Asset and Liability Management Committee.

**Residual risk** is the risk remaining after the Bank’s actions to reduce the inherent risk.

**Potentially material risks** – inherent/potential risks, which are annually determined by the Bank and, subsequently, are used to determine significant risks.

**Inherent risk** is a risk assessed without taking into account any actions of the Bank to change the probability of risk materialization or its impact.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

**Capital allocation** means the process of distributing the Bank’s available financial resources (available internal capital) and other sources of capital by types of risks, activities, transactions, etc.

**Regulatory authority** – the National Bank of Ukraine (NBU).

**Regulatory capital requirements** – minimum capital requirements necessary to cover significant risks (H1 and H2).

**Bank’s managers, Management** – Chairman, his deputies and members of the Supervisory Board of the Bank, Chairman, his deputies and members of the Board of the Bank, chief accountant.

**Structural unit (unit)** – an administratively separated organizational element in the Bank’s structure with subordination relations, which performs a definite set of interrelated tasks and functions on an ongoing basis.

**The subjects of the Bank’s risk management system:**

- 1) Supervisory Board;
  - Risk Management Committee of the Supervisory Board
  - Audit Committee of the Supervisory Board
  - Remuneration and Nomination Committee of the Supervisory Board
- 2) Board of the Bank;
- 3) Credit Council;
- 4) Non-Performing Assets Management Committee (KNPA)
- 5) Asset and Liability Management Committee (ALMC);
- 6) Operational Risk Management Committee (ORMC);
- 7) Ethics and Business Conduct Committee;
- 8) Financial Monitoring Committee;
- 9) Internal Audit Department;
- 10) CRO and risk management units (CBRD, RRD, SBRMD, GBRD, CMB, MRB);
- 11) CCO and compliance management units (including AML/CFT risk) (CCB, FMD, FCSCFCOSP and MTPAC);
- 12) Business units, including the non-performing assets management unit (NPA, workout unit) and support units (the first level of control (line of defence) of the ICS).

**Risk management units** – Corporate Business Risks Department (CBRD), Small Business Risk Management Department (SBRMD), Retail Risks Department (RRD), General Banking Risk Department (GBRD), Collateral Management Body (CMB), Microcredit Risk Body (MRB).

**Compliance management units (including ML/TF risk)** (CCB, FMD, FCSCFCOSP and MTPAC) (**Vertical Compliance Management Relationship**) – Compliance Control Body (CCB), Financial Monitoring Department (FMD), Foreign Currency Surveillance and Clients Foreign Currency Operations Support Department (FCSCFCOSP), Methodology, Transformation and Processes Automation Centre (MTPAC).


**RMS** – Risk Management System

**ICS** – Internal Control System.

## 5. RISK MANAGEMENT PRINCIPLES


5.1. Risk management is based on the following principles:

- **sufficiency and effectiveness of minimising measures** – financing of measures to minimise risks, economic incentives for their reduction;
- **clarity** – understandable, clarity of policies and mechanisms of risk management, assignment of responsibilities and duties of all subjects/participants of the RMS;

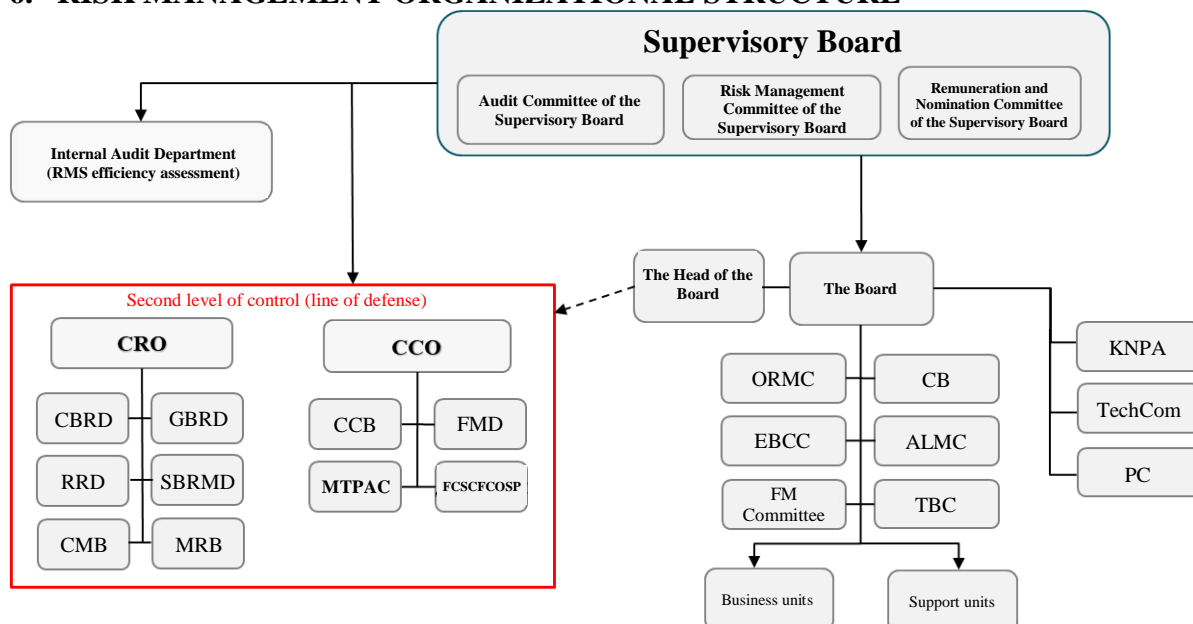
	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- **risk awareness:** when making a decision to carry out a transaction, it is mandatory to analyse potential risks, and after the transaction is carried out, to correctly account for the associated risks and their subsequent regular monitoring;
- **independence of the risk management function:** in order to prevent conflicts of interest, the Bank applies the principle of independence of any decision to accept a risk from risk assessment and control;
- **control of the risk level:** the Bank’s management and collegial bodies receive information on the accepted risk levels and facts of violations of the established risk management procedures, limits and restrictions on a regular basis;
- **ensuring 3 levels of protection and control:** in the process of carrying out risk management activities, the involvement of all structural units of the Bank in the assessment, acceptance and control of risks is ensured;
- **management of the Bank’s activities with due regard to the risk accepted:** the Bank shall monitor capital adequacy and perform capital planning based on the Bank’s Development Strategy;
- **limiting the level of accepted risks:** determination of the risk appetite by the Board and its transfer to the system of limits and restrictions allows to ensure the accepted level of risks for aggregated positions, transparent distribution of the total risk limit by the Bank’s business lines. The RMS ensures control over compliance with the Bank’s risk appetite and limits;
- **improvement of the risk management system:** the Bank’s risk management system is in line with the level of development of the Bank’s operations, as well as external conditions and innovations in the global risk management practice;
- **efficiency:** ensuring an objective assessment of the size of risks and completeness of risk management measures with optimal use of financial resources, personnel and risk management information systems;
- **timeliness:** ensuring timely (at an early stage) identification, measurement, calculation, monitoring, control, reporting and mitigation of all types of risks at all organisational levels;
- **structuredness:** a clear division of functions, duties and powers in risk management among all structural units and employees of the Bank, and their responsibility in accordance with such unit;
- **segregation of duties** (separation of the control function from the performance of the Bank’s operations) – avoiding a situation where the same person performs the Bank’s operations and performs control functions;
- **comprehensiveness and complexity:** coverage of all types of the Bank’s activities at all organisational levels and in all its structural units, assessment of the mutual impact of risks;
- **proportionality:** compliance of the risk management system with the Bank’s business model, its systemic importance, and the level of complexity of the Bank’s operations;
- **independence** means lack of dependence on the circumstances threatening the impartial performance of the functions by the risk management unit and the compliance control unit;
- **confidentiality:** restriction of access to information that shall be protected from unauthorised access;
- **transparency:** disclosure of information on the risk management system and risk profile by the Bank.



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

## 6. RISK MANAGEMENT ORGANIZATIONAL STRUCTURE



**Straight arrow** – functional direct subordination

**Dotted arrow** – administrative subordination

**ORMC** – Operational Risk Management Committee

**TechCom** – Technology Committee

**TBC** – Tariff and Business Committee

**ALMC** – Asset and Liability Management Committee

**CB** – Credit Board

**FM Committee** – Financial Monitoring Committee

**EBCC** – Ethics and Business Conduct Committee

The functionality of these collegial bodies is described in separate regulatory documents, the Regulation on Collegial Bodies.

**KNPA** – Non-Performing Assets Management Committee.


**PC** – Project Committee

### 6.1. Independence of risk management and compliance management units.

The independence of risk management and compliance units is ensured by the Supervisory Board by:

- 1) subordination of the risk management unit to the CRO, CRO – to the Bank’s SB, subordination of the compliance control unit to the CCO, CCO – to the Bank’s SB;
- 2) reporting of the CRO and CCO to the SB/RMC of the Bank;
- 3) providing the CRO/risk management units, CCO/compliance management units (including AML/CFT risk) with a direct and unlimited opportunity to discuss risk issues directly with the SB without the need (obligation) to inform the members of the Bank’s Board;



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	


- 4) organizational and functional separation of CRO/risk management units and CCO/compliance management units (including AML/CFT risk) from the units (heads of units) of the first and third levels of control (lines of defence);
- 5) ensuring a sufficient number of employees for these units and the level of their qualifications to achieve the goals and objectives set for them;
- 6) accounting for a sufficient amount of financial support for these units in the Bank’s budget. The remuneration of employees of these units should not depend on the results of the work of business units under control, and should contribute to staffing these units with qualified employees. The performance of employees in these units shall be assessed based on the achievement of their goals while ensuring their independence is not unduly restricted;
- 7) ensuring access of CRO/employees of risk management units and CCO/employees of compliance management units (including AML/CFT risk) to information necessary for their effective work. The Bank’s managers and staff should facilitate the provision of such information;
- 8) preventing CRO/employees of risk management units and CCO/employees of compliance management units (including AML/CFT risk) from exercising control functions over operations for which they were previously directly responsible or for which they previously made decisions at the first level of control (line of defence), in order to prevent any conflict of interest.

## **6.2. Veto right of CRO and CCO.**

The main principle of independence is implemented as follows: risk management must be independent of the business, have the opportunity to express its position, which is a mandatory part of the description of the draft decision. Risk management must have sufficient authority to defend its position. It is important to ensure that any non-standard or large transaction cannot be carried out without the approval of the 2nd level of control (line of defence). The features for classifying a transaction as non-standard and/or large, as well as the procedure for their approval by the units of the second level of control (line of defence), are established by a separate internal regulatory act of the Bank.

CRO/CCO have the right of veto. Veto (from the Latin veto – “forbid”) is a right that means the authority of an official (CRO/CCO) to unilaterally block the adoption of a particular decision by the Board/Collegial body established by the Bank’s Board. (hereinafter referred to as the “Collegiate Body of the Board”), if the implementation of such decisions will lead to a violation of the established risk appetite and/or approved risk limits, as well as in cases established by the Supervisory Board of the Bank, by:

- In case the CRO/CCO is a direct member of the collegiate body: as a Member of the Board/Collegiate Body of the Board directly by voting during the discussion of issues (vetoing is clearly recorded in the Minutes of the Board/Collegiate Body of the Board not as a vote “against”, but as the right of veto) on one specific issue.
- If a member of the Board/Collegial Body of the Board is a representative of any risk management unit (CBRD, RRD, SBRMD, GBRD, CMB, MRB) or compliance management units (including AML/CFT risk) (subordinate to the CRO/CCO) not the CRO/CCO: such employee is obliged to inform the CRO/CCO about the need to exercise the veto right. The veto right is exercised in the form of a CRO/CCO Memorandum to the Head of the Collegial Body of the Board (copy to the secretary) with information about vetoing of a specific decision.
- If the CRO/CCO/representative of the 2nd level of control (line of defence) is not a member of the Board/Collegial Body of the Board, the secretary of the Board/Collegial Body of the

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

Board is obliged to send the agenda of the meeting of the Board/Collegial Body of the Board in order to the CRO/CCO/representative of the 2nd level of control (line of defence) could independently determine the need to attend the meeting. In case of participation in the meeting, the right of veto is exercised by reflecting such decision in the minutes of the collegial body. If the CRO/CCO/representative did not participate in the meeting of the collegial body, then he has the right to request the minutes of the collegial body meeting in order to familiarize with the issue. Vetoing of the adopted decisions (the need for which was discovered later) can be carried out no later than 2 (two) business days from the date of receipt of the minutes in the form of a memorandum from the CRO/CCO to the Chairman of the Collegial Body of the Board (with a copy to the Secretary) with information about the veto of a specific decision.

- During the period of absence of the CRO/CCO for any reasons (illness, vacation, business trip, etc.), the veto right is entrusted to an employee of the risk management/compliance management units (including AML/CFT risk), appointed as the acting CRO/CCO in accordance with the procedure regulated by the provisions of the labour legislation of Ukraine and the internal regulatory and administrative documents of the Bank.


**IMPORTANT! In case of exercising the veto right:**

- 1) CRO/CCO must inform the SB justifying the veto reasons for further decision-making on the discussed/agreed issue. Such informing is carried out by sending the Memorandum to the SB secretary, who is obliged to immediately carry out centralized informing of the SB members;
- 2) The SB considers issues/decisions of the Bank's Board, committees and other collegial bodies established by the Bank's Board, banned (vetoed) by the CRO and/or CCO. The Bank's Supervisory Board may override a ban (veto) of the decisions of the Bank's Board, committees and other collegial bodies established by the Bank's Board imposed by the CRO and/or CCO. The decision of the Bank's Supervisory Board to override the veto must be based on an adequate assessment of the Bank's risk profile. The Bank's Supervisory Board must understand the reasons that led to the CRO's and/or CCO's vetoing and the consequences of overriding it. The presence of the person who exercised the veto right at meetings of the Supervisory Board considering this veto override is mandatory.

## **7. ROLES, POWERS AND RESPONSIBILITIES OF PARTICIPANTS**

### **7.1. The Supervisory Board (SB) shall:**

- be fully responsible for functioning of a comprehensive, adequate and effective system of risk management to which the Bank is exposed in its activities;
- define and monitor adherence to the Bank's corporate values, based on conducting business in a legal and ethical manner, and consistently maintain a high risk management culture;
- devote sufficient time, effort, and resources to participate in the Bank's risk management and control comprehensiveness, adequacy, and effectiveness of the risk management system;
- maintain an appropriate level of risk management organizational structure, information system, and internal controls supporting effective risk management;
- ensure that the Bank's remuneration policy aligns with and promotes effective risk management, without incentivizing excessive risk-taking;
- define cases of the CRO and the CCO vetoing the decisions of the Board, committees and other collegial bodies of the Bank's Board;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	


- promote the creation of Bank’s regular and transparent communication mechanisms.
- ensure functioning and control over the effectiveness of the risk management system;
- approve internal risk management documents and monitor their implementation, compliance and timely updates;
- approve a list of limits (restrictions) for each type of risk and procedures for escalating violations of the risk limits;
- make decisions on introducing significant changes in the Bank’s activities;
- approve the Recovery Plan and ensure the performance of functions to restore the Bank’s activities;
- approve the appointment and termination of powers (dismissal) of CRO and CCO;
- approve the financial support (budget) of the risk management and compliance control units, set the amount of remuneration for CRO, CCO and monitor their implementation/compliance;
- determine the nature, form and scope of information on risks, consider management reporting on risks and, if the Bank’s risk profile does not correspond to the approved risk appetite, immediately make a decision on implementing adequate mitigation measures;
- take measures to prevent any conflict of interest in the Bank, promote their settlement and inform the NBU of any conflicts of interest in the Bank;
- ensure an appropriate level of documentation of discussions and decisions taken, which should include a brief overview of the issues considered, recommendations made, decisions taken by roll call voting and special opinions (if any).

#### **7.2. Risk Management Committee shall:**

- provide Bank’s SB with recommendations, consultations, and proposals on risk management issues for further decision-making;
- monitor Bank’s compliance with the established aggregate risk appetite level and the risk appetite level for each type of risk;
- monitor the implementation of the risk management strategy and policy;
- monitor the performance of the functions assigned to CRO, CCO, risk management units, and compliance management units (including ML/TF risk);
- participate in the development of internal bank documents;
- control the implementation of measures for the operational elimination of deficiencies in the functioning of the risk management system (including ML/FT risks), implementation of recommendations and comments of the internal audit unit, external auditors, the National Bank and other supervisory authorities;
- monitor that pricing/tariff setting for banking products takes into account the Bank’s business model and risk management strategy. If prices/tariffs do not cover the bank’s risks, the risk management committee develops measures and submits them for Bank’s Supervisory Board consideration;
- submit reports on the performance of its functions to the Bank’s Supervisory Board at least once a quarter;
- ensure the performance of other functions and powers related to risk management issues assigned to the Bank’s SB.

#### **7.3. Board of the Bank shall**

- ensure and participate in the development and approval of internal bank documents;


	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- ensure the preparation and submission of management reporting on the risks to which the Bank is exposed to the SB, including information on new types of products or significant changes in the Bank’s activities;
- ensure the preparation and submission of proposals on changes to the risk management strategy and policy to the SB;
- provide control over informing the Bank’s relevant structural units and employees on any changes in the Bank’s Risk Management Strategy and other internal risk management documents;
- develop measures for the prompt elimination of deficiencies in the functioning of the risk management system, the implementation of the recommendations and comments based on the results of risks assessment, inspections conducted by the internal audit unit, external auditors and supervisory authorities;
- approve the limits for each type of risk according to the list of limits (restrictions) set by the SB;
- provide CRO, CCO, risk management units and compliance management units (including ML/FT risk) with administrative support (ensure the organization of their workflow, issue administrative documents for the implementation of SB decisions).

7.3.1. The Board of the Bank shall ensure the fulfilment of tasks, decisions of the SB on the implementation of the risk management system, including the risk management strategy and policy, risk management culture, procedures, methods and other measures of effective risk management. The Board of the Bank recognises and complies with the requirements for the independent performance of duties by the risk management and compliance management units (including ML/TF risk) and does not interfere with the performance of their duties.

#### **7.4. Risk management units (CBRD, RRD, SBRMD, GBRD, CMB, MRB) shall:**

- ensure timely identification, measurement, monitoring, control, mitigation and reporting of significant risks;
- participate in the development of a distressed assets management strategy and operational plan and monitor their implementation;
- ensure monitoring and prevention of violations of risk appetite indicators and risk limits, monitor the approach of risk indicators (key risk indicators) to the established risk appetite and risk limits, and initiate measures to prevent their violations;
- prepare risk reports;
- carry out a constant analysis of the risks to which the Bank is exposed during its activities, in order to prepare proposals for making timely and adequate management decisions to mitigate risks;
- exercise control over property valuation, namely:
  - exercise control over the replacement (rotation) of the valuator after his two consecutive valuations of the same property;
  - verify property value on a regular basis;
  - carry out back-testing of property value.
- develop and maintain up-to-date methodologies, tools and models used by the Bank to analyse the impact of various risk factors on Bank's financial condition, capital and liquidity;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- carry out credit risk assessment;
- carry out stress testing;
- calculate the Bank’s risk profile;
- prepare conclusions on risks inherent in new products and significant changes in the activities of the Bank, until their introduction for management decisions;
- prepare conclusions regarding the risks inherent in both new loans and amendments of existing loans, for making management decisions on granting new loans or amending existing loan agreements;
- develop, implement and monitor an early response system;
- prepare conclusions for management decisions on settling debtors/counterparties’ debts
- participate in and develop internal banking documents.

Deputy Chairman of the Board for Risk Management (CRO) shall be responsible for the activities of risk management units, shall have the right to attend meetings of the Board of the Bank, committees and other collegial bodies established by the Board of the Bank and to impose a ban (veto) on decisions of these bodies, if the implementation of such decisions leads to violations of the established risk appetite and/or approved risk limits (leads to deterioration of the Bank’s risk profile), as well as in other cases established by the SB or the RMC, and promptly inform the SB of such decisions. The Deputy Chairman of the Board for Risk Management (CRO) shall perform the following functions:


- 1) submit risk reports to the Supervisory Board, the Board;
- 2) inform the Supervisory Board, the Board of any excessive risks to which the Bank may be exposed;
- 3) ensure the coordination of work on risk management issues between the Bank’s structural units as well as on developing internal control system;
- 4) provide Supervisory Board and the Board with proposals on necessary measures to mitigate the impact of risks (regarding each type of risk) on the financial condition, capital and liquidity of the Bank, including initiating the establishment of risk limits and/or revising their values;
- 5) develop and participate in the development of the internal banking documents on risk management.

#### **7.5. Compliance management units (including ML/TF risk) (CCB, FMD, FCSCFCOSP and MTPAC):**


##### **CCB shall:**

- 1) provide control over Bank’s compliance with the norms of legislation, regulatory internal banking documents and relevant standards of professional associations applicable to the Bank;
- 2) ensure monitoring of changes in legislation and relevant standards of professional associations which may affect the Bank, and assess their impact on Bank’s processes and procedures, record the facts of notification and the terms of implementation of such changes in the Bank’s processes and documents in accordance with the term specified by the process/document owner within the requirements of the current legislation of Ukraine; ensure control over the timely and proper introduction of relevant changes to internal bank documents, as well as coordination of the Bank’s internal regulatory and administrative documents from the point of view of compliance risk;



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	<b>JSC “FUIB” Risk Management Policy</b>	

- 3) provide control over compliance risk arising in the Bank's relations with clients and counterparties in order to prevent participation and/or use of the Bank in any illegal transactions;
- 4) provide the management of the risks associated with a conflict of interests that may arise at all levels of the Bank's organizational structure, transparency of the Bank's processes implementation, and in case of revealing any facts indicating the existence of any conflict of interests in the bank, inform the CCO;
- 5) ensure organization of control over Bank's compliance with the rules on timeliness and reliability of financial and statistical reporting;
- 6) ensure control over the Bank's compliance with the norms for determining the list of persons related to the Bank to ensure the integrity and completeness of the process of identifying persons related to the Bank and control over their transactions;
- 7) ensure organization of control over the protection of personal data in accordance with the legislation of Ukraine;
- 8) ensure organization of control over the compliance of the processes related to distressed assets management to the legislation of Ukraine and the internal banking documents;
- 9) monitor the compliance of Bank's compensation and indemnity system, as well as procedures for bringing to disciplinary responsibility of the bank employees, with the requirements of the legislation;
- 10) process reports of violations/unacceptable behaviour received through the SCM trust line (reporting mechanism for unacceptable behaviour);
- 11) ensure management of compliance risks related to conflicts of interest that may arise at all levels of the Bank's organizational structure, transparency of the implementation of the Bank's processes, including control of procedures for mandatory declaration of personnel external activities, presentation and receipt of gifts and invitations, consideration of appeals regarding situations of joint work of relatives and inform the CCO in case of detection of any fact indicating the presence of a conflict of interest in the Bank;
- 12) regularly monitor the absence of a conflict of interest between the bank's managers and the subject of assessment activities;
- 13) ensure control over compliance with requirements during working with sensitive information;
- 14) maintain a database of compliance risk events (incidents) in the general database of operational and compliance risk events;
- 15) provide explanations to the Bank's management on their request regarding control over Bank's compliance with the legislation of Ukraine and relevant standards of professional associations, applicable to the Bank;
- 16) provide training and awareness of the Bank's employees regarding the compliance with the legislation, relevant standards of professional associations applicable to the Bank, and risk management culture, taking into account the code of conduct (ethics);
- 17) ensure the functioning of the risk management system by timely identifying, measuring, monitoring, controlling, reporting and providing recommendations on mitigation of compliance risk;
- 18) take all possible measures to prevent decisions that may impose the Bank to significant compliance risk, and properly inform the Bank's management;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- 19) prepare conclusions on compliance risk that is inherent in new products and significant changes in the activities of the Bank, until their introduction for timely adequate management decisions;
- 20) prepare conclusions on compliance risk for making credit decisions on loans to persons related to the Bank (except for loans to individuals for which decisions are made by an automated system, taking into account that the system applies standard product price parameters and there is no conflict of interest);
- 21) prepare compliance risk reports;
- 22) calculate the compliance risk profile;
- 23) develop and participate in the development of internal banking documents that regulate risk management issues, and monitor their compliance;
- 24) participate in the investigation of internal and external fraud.


**FMD shall:**

- 1) ensure proper organisation of internal bank system for prevention and counteraction to legalisation (laundering) of proceeds of crime, terrorist financing and financing of proliferation of weapons of mass destruction;
- 2) ensure organisation of the Bank's compliance with the requirements of Ukrainian legislation regarding prevention and counteraction to legalisation (laundering) of proceeds of crime, terrorist financing and financing of proliferation of weapons of mass destruction;
- 3) manage the risks of money laundering/terrorist financing in order to reduce them to an acceptable level;
- 4) ensure the identification of risky financial transactions of Clients, determine the presence or absence of signs that the Clients' financial transactions are aimed at using the Bank's services for the purpose of ML/TF, take appropriate actions regarding transactions that contain signs of risk;
- 5) perform second-level controls over the implementation of AML/CTF requirements at the first level of control (line of defence);
- 6) is involved in the identification, assessment and reduction of ML/TF risks in accordance with the Bank's risk-based approach;
- 7) participate in the development of internal banking documents regulating risk management issues in accordance with AML/CFT requirements;
- 8) prepare conclusions on the possibility of establishing/extending business relationships with certain categories of Bank's Clients who carry the risk of ML/TF;
- 9) participate in the preparation of materials for training the Bank's employees involved in AML/CTF processes in accordance with their job responsibilities;
- 10) identify areas of activity at the first level of control (line of defence) that may carry increased ML/TF risks, ensure training activities to raise the awareness of the Bank's employees involved in the relevant activities;
- 11) ensure the escalation of cases that carry an increased ML/TF risk or cause suspicion to the CCO level;
- 12) prepare reports on the main indicators of the department's activities for corporate governance bodies.

**FCSCFCOSP shall:**

- 1) monitor preventing of violations of legislation in the field of currency surveillance and financial monitoring in the Bank's operations (within its competence);




	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- 2) ensure organisation of the Bank’s compliance with the requirements of Ukrainian legislation regarding prevention and counteraction to legalisation (laundering) of proceeds of crime, terrorist financing and financing of proliferation of weapons of mass destruction during exchange transactions/ servicing currency contracts;
- 3) manage the risks of money laundering/terrorist financing in the field of currency surveillance and financial monitoring in order to reduce them to an acceptable level;
- 4) ensure the identification of risky exchange transactions of Clients, determine the presence or absence of signs that the Clients’ exchange transactions are aimed at using the Bank’s services for the purpose of ML/TF, take appropriate actions regarding exchange transactions that contain signs of risk;
- 5) perform second-level controls over the implementation of AML/CTF requirements at the first level of control (line of defence) when conducting exchange transactions/maintaining exchange contracts;
- 6) participate in the development of internal banking documents regulating risk management issues in accordance with AML/CTF requirements and relate to currency surveillance;
- 7) participate in the preparation of materials regarding AML/CTF requirements in the field of currency legislation for training the Bank’s employees involved in AML/CTF processes in accordance with their job responsibilities;
- 8) prepare conclusions on the possibility of exchange transactions/maintaining exchange contracts taking into account ML/TF risks;
- 9) ensure the escalation of cases that carry an increased ML/TF risk or cause suspicion to the CCO level;
- 12) prepare reports on the main indicators of the department’s activities for corporate governance bodies.

**MTPAC shall:**

- 1) establish standards (rules, measures) on ML/TF risk management;
- 2) coordinate and provide methodological support to ensure the Bank’s compliance with the requirements of the legislation on AML/CTF and ML/TF risk management;
- 3) identify areas of Bank’s activity that may carry increased ML/TF risks, conduct training activities to raise the awareness of the Bank’s employees involved in the relevant activities;
- 4) provide expert support to the Bank’s processes (projects) related to ML/TF, which contribute to improving the identification and response to relevant risks;
- 5) be involved in monitoring of the regulatory framework on risk assessment and customer due diligence, assess the impact on the Bank’s activities;
- 6) coordinate changes in the Bank’s processes caused by ML/TF legislation changes;
- 7) assess and search ways to reduce ML/TF risks when implementing new products/services and initiatives, changes to existing ones;
- 8) be involved in automation and change management of AML/CTF process automation systems, which may positively affect ML/TF risk management processes;
- 9) ensure the escalation of cases that carry an increased ML/TF risk or cause suspicion to the CCO level;
- 10) prepare reports on the main indicators of the MTPAC’s activities for further presentation to corporate governance bodies.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

CCO shall be responsible for the activities of compliance management units (including ML/TF risk), shall have the right to attend meetings of the Board of the Bank, committees and other collegial bodies established by the Board, and to impose a ban (veto) on decisions of these bodies if implementation of such decisions leads to violation of the requirements of the legislation, relevant standards of professional associations applicable to the Bank, conflict of interest, as well as in other cases established by the SB, and promptly inform the SB of such decisions.

The CCO shall perform the following functions:

1) submit compliance risk reports to the Supervisory Board of the Bank, the Risk Management Committee and the Board of the Bank;

2) ensure the coordination of work on compliance risk-management issues between the Bank's structural units;

3) inform the Supervisory Board of the Bank, the Risk Management Committee, the Board of the Bank about excessive risks to which the bank may be exposed;

4) inform the National Bank of confirmed facts of inappropriate behaviour in the Bank/violations in the Bank's activities and conflicts of interests arising in the Bank, if the SB has not taken measures to eliminate them.

5) ensure and participate in the development of the internal risk management documents;

6) ensure organisation of an appropriate ML/TF risk management internal bank system;


7) report to the Supervisory Board on the results of the assessment of the bank's risk profile and on problematic issues related to ensuring an adequate ML/TF risk management system, at least once a year.

## 8. MAIN PART

### 8.1. Risk management goals.

#### Strategic goals:

- ensuring the sustainable development of the Bank within the framework of its business development strategy;
- ensuring and protecting the interests of shareholders, depositors, creditors, clients, and other stakeholders in the sustainable operation of the Bank, so that risks accepted by the Bank would not threaten its existence;
- strengthening the Bank's competitive advantage through strategic planning that considers risk tolerance, enhancing risk management effectiveness, and increasing Bank's market value while maintaining its reliability and expanding product offerings;
- increasing investor confidence through a transparent risk management system and establishing Corporate Governance System, subject to constant supervision of the NBU and other state supervisory authorities;
- supporting all areas of the Bank's Business and other units in achieving the goals and objectives by:
  - ✓ minimizing the volatility of income (including from the materialization of credit risks);
  - ✓ increasing the diversification of asset and liability portfolios;
  - ✓ monitoring the compliance of the Bank's risk profile, approved by the SB, with the level of risk appetite;
  - ✓ creating and maintaining a high risk management culture;
  - ✓ minimise the losses of the operational risk event;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- ✓ ensuring compliance with the requirements of the legislation of Ukraine and internal regulatory and administrative documents;
- ✓ preventing conflicts of interest.

**Operational objectives:** ensuring timely (at an early stage) identification, measurement, monitoring, control, reporting and mitigation of all types of risks at all organisational levels of the Bank.

**Information objectives:** ensuring the integrity, completeness and reliability of risk management information used to make management decisions; creating information flows both vertical and horizontal within the Bank’s organizational structure; providing management and stakeholders with reliable financial and statistical reporting.

**Compliance objectives:** compliance with the requirements of the legislation of Ukraine, regulations of the National Bank of Ukraine, internal banking documents, standards of professional associations applicable to the Bank.

8.2. The Bank’s risk management strategy is directed/aimed at fulfilling the principle of a stable level of return on capital from the JSC “FUIB” activities by ensuring an optimal balance between the fulfilment of the main tasks of the business plan, profitability of the Bank’s main activities and the level of risks accepted.

8.3. The Bank implements a strategy of both preventive and subsequent impact on risks, using the full range of available risk reduction tools, both at the portfolio level and at the level of individual transactions/processes. Particular attention shall be paid to improving the risk management system, capital adequacy and liquidity as a risk management mechanism (RMS) and potential sources of loss coverage.

#### 8.4.MAIN TYPES OF BANK’S RISKS

8.4.1. The Bank identifies the following significant types of risks and conducts their self-assessment annually:


- 1) credit risk taking into account the impact of climate change risks;
- 2) liquidity risk;
- 3) interest risk in the banking book;
- 4) market risks (currency risk, price risk of OVDs, price risk of Sovereign bonds G7)
- 5) operational risk taking into account the impact of climate change risks;
- 6) compliance risk (including money laundering/terrorism financing risk – the Bank’s ML/TF risk);
- 7) payment system participant risk.

#### 8.4.2. The approach to identifying significant types of risks is based on:

- Annual identification of the total set of risks significant to the Bank (1st stage of Self-Assessment).
- Expert assessment on a three-point scale (1 – low, 2 – medium, 3 – high)
- Risks ranking (TOP-5 for each type of risk is determined by the highest sum of points received from experts)
- Supervisory Board’s annual approval of the Action Plan on minimizing TOP-5 banking risks.


#### 8.4.3. The following types of risks are defined as (definition):

- **Credit risk** is a probability of occurrence of losses or additional losses, or the revenue deficit caused by the debtor/counterparty’s failure to fulfil the obligations assumed under

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

the terms and conditions of the agreement. Credit risk arises from all active banking operations, with the exception of debt securities and other financial instruments in the Bank’s trading book.

- **Liquidity risk** means a probability of losses or additional losses, or a shortfall in the planned revenues as a result of the Bank’s inability to finance the growth of its assets and/or fulfil its obligations in due time.
- **Interest risk in the banking book** is a probability of occurrence of losses or additional losses, or a shortfall in the planned revenues due to the effect of unfavourable changes in the interest rates in the bank book. The interest risk in the banking book affects the economic value of a Bank’s capital and its net interest income.
- **Market risks, the most significant of which are:**
  - Price risk of UAH OVDPs is the risk of losses when selling the entire OVDP portfolio on the secondary market in the event of the need to convert the secondary liquidity cushion into primary liquidity.
  - Price risk of G7 sovereign bonds is the risk of possible losses in the event of changes in market interest rates due to the revaluation of G7 bonds in the Bank’s portfolio, or in the event of the sale of G7 bonds on the open market.
  - Currency risk is a probability of occurrence of losses or additional losses, or a shortfall in the planned revenues due to the result of unfavourable changes in the foreign currency.
- **Operational risk** is a probability of occurrence of losses or additional losses, or a shortfall in the planned revenues due to defects or mistakes in the organization of internal processes, or intentional or unintentional actions of the Bank’s employees or other persons, failures in the work of the Bank’s information systems or as a result of external factors. Operational risk includes legal risk, but should exclude reputation risk and strategic risk. **Components of operational risk:**
  - **Legal risk** (component of operational risk) – the probability of losses or additional losses, or failure to receive planned income due to unexpected application of legal norms as they may possibly be interpreted ambiguously or result in invalidation of contract terms due to their non-compliance with the requirements of the legislation of Ukraine
  - **Information and communication technology risk (ICT risk)** (component of operational risk) – the probability of losses or additional losses, or failure to receive planned income due to malfunction or non-compliance of information and communication technologies with the business needs of the Bank, which may lead to disruption of their sustainable functioning, or shortcomings in the organization of management of such technologies.
  - **Information security risk (a component of operational risk)** – the probability of losses or additional losses, or failure to receive planned income due to violation of the confidentiality, integrity, availability of data in the Bank’s information systems, shortcomings or errors in the organization of internal processes or any external events, including cyberattacks or inadequate physical security. Information security risk includes cyber risk (the risk of losses and/or additional losses due to materialization of cyber threats).

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- **Compliance risk** (including money laundering/terrorist financing risk – ML/TF risk of the Bank) is a probability of occurrence of losses/sanctions, additional losses or a shortfall in the planned revenues or loss of reputation due to failure of the bank to comply with the requirements of the legislation, regulations, market standards, rules of fair competition, rules of corporate ethics, the emergence of a conflict of interest, as well as the internal bank documents.
- **Payment system participant risk (PSP risk).**

8.4.4. The second-level of control units (lines of defence) develop separate Risk Management Policies for each block of significant risks, which are reviewed at least once a year:


- Corporate Business Credit Risk Management Policy is a component of the Credit Policy of JSC “FUIB” for corporate business (is developed by CBRD);
- Small Business Credit Risk Management Policy (is developed by SBRMD);
- Retail Credit Risk Management Policy (is developed by RRD);
- Financial Institutions (Banks) Credit Risk Management Policy (is developed by GBRD);
- Liquidity Risk Management Policy (is developed by GBRD);
- Interest Risk in the Banking Book Management Policy (is developed by GBRD);
- Market Risk Management Policy (is developed by GBRD);
- Operational Risk Management Policy (is developed by GBRD);
- Compliance Risk Management Policy (is developed by CCB);
- Risk Management Policy of the Payment System Participant of JSC “FUIB” (is developed by GBRD);
- Policy of JSC “FUIB” on compliance with the requirements of legislation regarding prevention and counteraction to legalisation (laundering) of proceeds of crime, terrorist financing and financing of proliferation of weapons of mass destruction (is developed by CCO).

#### 8.4.5. All Risk Management Policies must include:

- purpose, objectives and principles of categories risk management;
- the organizational structure of the risk management process taking into account three levels of control (lines of defence);
- types of risks included in this risk category;
- approaches to identifying, calculating, monitoring, controlling, reporting in order to minimize risks;
- criteria for determining significant risks;
- insurance/risk transfer policy (if the risk management strategy provides for such approach);
- risk limits for this risk category;
- risk appetite for this risk category (without detailed calculation methodology, which is described in a separate regulatory document);
- approaches to stress testing of risks (without detailed methodology);
- list, frequency, submission deadlines and form (information content) of management reporting for this risk category.

#### 8.4.6. The compliance risk management policy (including ML/TF) should contain:

- purpose, objectives and principles of compliance risk management;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- the organizational structure of the compliance risk management process, taking into account the distribution of the functionality of the process participants, their powers, responsibilities and interaction procedure;
- approaches to identifying, calculating, monitoring, controlling, reporting and minimization of compliance risk;
- the list, form of management reporting forms on compliance risk, the procedure, frequency and terms of its provision to the risk management system subjects.

**8.4.7. Policy of JSC “FUIB” on compliance with the requirements of legislation regarding prevention and counteraction to legalisation (laundering) of proceeds of crime, terrorist financing and financing of proliferation of weapons of mass destruction shall contain:**

- purpose, objectives and principles of ML/TF risk management;
- the organizational structure of the ML/TF risk management process, taking into account the distribution of the functionality of the process participants, their powers, responsibilities and interaction procedure;
- approaches to identifying, calculating, monitoring, controlling, reporting and minimization of the ML/FT risk;
- the list, form of management reporting forms regarding ML/TF risk, the procedure, frequency and terms of its provision to the risk management system subjects.
- requirements for establishing three lines of defence in the field of AML/CTF and the distribution of duties and responsibilities among bank employees
- the bank’s risk appetite regarding AML/CTF (including established prohibitions/restrictions for certain types of activities and/or attracting certain types of clients)
- the functioning of internal control on AML/CFT issues
- the procedure for conducting training events on AML/CFT issues
- the volume of the Bank’s AML/CFT internal documents to be developed and approved.

**8.5. General escalation process of credit/market/operational and liquidity risk events requiring immediate notification of the Bank’s Supervisory Board**

8.5.1. Risk management units (CBRD, RRD, SBRMD, GBRD, MRB, CMB) monitor risk limits and no later than the next business day after detecting a risk limit violation, inform the Bank’s CRO via corporate email, and the Bank’s CRO further notifies:

- Supervisory Board;
- The Bank’s Board and its profile committees (Credit risks – CB/CC, market risks – ALMC, operational risks – ORMC).


Subject of the letter: “Overlimit *“risk category”* – name of the limit as of XX.XX.20XX.

Content of the letter:

1. Fact of overlimit
2. Date of overlimit
3. Reason for overlimit
4. Recommendation for responding to overlimit (action plan to eliminate limit violations).

Sender: Deputy Chairman of the Board for Risk Management (CRO) or other appointed official.



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

8.5.2. The Supervisory Board may delegate the authority to approve transactions that lead to an increase in risk limits (authorized overlimits) to the Bank’s collegial bodies. Detailed procedures for monitoring compliance with delegated authorities are described in the Risk Management Policies by area. Such control procedure should regulate:

- types of risks where overlimits is authorized;
- maximum volume of authorized overlimit;
- requirements for documenting the overlimit decision;
- procedure for informing the Supervisory Board on the decision on authorized overlimits for the quarter (regular reporting).

8.5.3. Risk management units accumulate information on all authorized overlimits (and dates of collegial bodies decisions within the scope of delegated powers) and all unauthorized overlimits.

8.5.4. The Supervisory Board conducts an extraordinary review of limits in case overlimits (authorized and unauthorized) have become frequent (once a week) or permanent (once a day).

8.5.5. As a result of such review Supervisory Board may decide to:

- review the existing limits (increase the limit);
- review the powers of the Bank’s collegial body on the volume of authorized overlimit (if its reason is objective);
- leave the limit value unchanged and approve an action plan to prevent overlimit in the future (timelines and units/persons responsible for eliminating the causes of risk overlimits).

## **8.6. General escalation process for compliance risk events (including ML/TF risk) requiring immediate notification of the Bank’s Supervisory Board:**

8.6.1. Compliance management units (including ML/TF risk) (CCB, FMD, FCSCFCOSP and MTPAC) ensure monitoring of facts indicating the materialization of compliance risk events (including ML/TF risk).

In the event of significant compliance risk events (including ML/TF risk) (which lead/may lead to a high level of compliance risk), the CCO informs the Head of the Risk Management Committee of the Supervisory Board via corporate e-mail no later than the next business day after detection.

## **8.7. The general process of SB’s approval of the risk appetite for the next year:**


8.7.1. At the beginning of the year, the responsible risk management units (CBRD, SBRMD, RRD, GBRD) determine the risk appetite indicators as a list of key risk indicators for various types of risks (credit risk, interest risk in the banking book, market risk, liquidity risk, operational risk) proposed for monitoring in the current year and provide them for GBRD’s consolidation.

8.7.2. The CCO calculates the compliance risk profile (including ML/TF risk), forms a minimum list of quantitative and qualitative risk appetite indicators for each type of controlled compliance risks (including ML/TF risk).

8.7.3. An employee of the Risk Management unit, assigned by the CRO, forms a consolidated file-report “Risk-appetite dashboard\_TARGET” and the CCO forms a file-report on compliance risks (including ML/TF risk) and submits these indicators with threshold values for Board’s consideration and Supervisory Board’s approval.

8.7.4. The decision adopted by the Supervisory Board to establish risk appetite indicators and their threshold values for the current year is accepted for control by the relevant collegial bodies (Board/CB/ALMC/ORMC) and the Bank’s units.



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

8.7.5. Each risk appetite indicator (from the list of key risk indicators) as of the date of report drawing has its own value, which correlates with indicator thresholds:

- “Green zone”;
- “Yellow zone”;
- “Orange zone”;
- “Red zone”.

8.7.6. The units of the 2nd level of control (line of defence) of the ICS (CBRD, SBRMD, RRD, GBRD, CMB, MRB, CCB, FMD, FCSCFCOSP, MTPAC) calculate risk appetite indicators (in accordance with the list of risk indicators approved by the SB) based on the results of quarterly monitoring of the Bank’s current risk level to compare the actual and established risk level at the beginning of the year (comparison of current values of key risk indicators with established risk appetite values).

8.7.7. Quarterly consolidated file-report “Risk-appetite dashboard” and report of risk-appetite indicators for compliance risks (including ML/TF risk) are submitted to the Bank’s Board, the RMC and the Supervisory Board for consideration.

**IMPORTANT!** Such report shall contain actual risk-appetite indicators for significant risks, calculated as of the reporting date compared to the established target thresholds for these risks at the beginning of the year.

8.7.8. Decisions of the management based on the results of consideration of the Bank’s risk-appetite reports are recorded in the minutes of meetings of the relevant collegial bodies (Board/RMC/Supervisory Board).

## 8.8. Methodology for determining significant risks

8.8.1. The Bank annually determines significant risks, which allows comprehensive consideration of the Bank’s risk profile.


8.8.2. During risk identification and assessment (including stress testing to determine potential consequences), the Bank takes into account the following negative factors:

- Bank’s actual losses;
- potential losses (expected and unexpected);
- non-financial (reputational loss);
- amount of open exposure to risk.

Significant risks are assessed by the 2nd line of defence of the ICS during separate assessment methods for each type of risk and are approved by the and the Supervisory Board.

8.8.3. A significant risk is defined as risk that has or may have a significant impact on the capital adequacy (Risk Capacity) and financial stability of JSC “FUIB”. The impact may be non-financial, for example, causing reputational damage to the Bank, or criticism from the Regulator, or financial, or non-financial and financial at the same time, for example, a possible failure of information systems may have financial and/or reputational consequences. To assess the materiality of financial consequences, a minimum threshold of “materiality” has been set at 1% of the Bank’s Authorized Capital (as of 01.01.2025 – UAH 47.8 million), however, this should not prevent the identification of other risks that have financial consequences below the specified threshold.

8.8.4. The business strategy for the current year takes into account the impact on the financial stability of all material risks for the Bank listed in the Risk Exposure Declaration for the current year.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

## 9. CREDIT RISK

9.1. Credit risk – the uncertainty of the final result of the Bank, due to possible losses caused by the ability of the Bank’s debtors (individuals and legal entities, including banks) to repay the principal outstanding and interest accrued within the terms stipulated in the credit agreements on credit transactions.

9.2. Credit risk is the dominant element of the hierarchical system of banking risks in JSC “FUIB” and an integral part of the overall banking risk. Credit risk refers to significant risks (according to clause 11 of Section 2 of the Resolution of the NBU Board No. 64 dated 11.08.2018)

9.3. Organizational structure of credit risk management:

1st level of control (line of defence): Bank business lines and the Distressed Assets Management Vertical, units supporting the Bank’s lending activities,

2nd level of control (line of defence): Corporate Business Risks Department, Small Business Risk Management Department, Retail Risks Department, GBRD (in terms of risks of financial institutions-banks), Collateral Management Body, Microcredit risk Body, Compliance Management Units (including ML/TF risk).

3rd level of control (line of defence): Internal Audit Department

9.4. Credit risk management is carried out by analysis of the level of the aggregate credit portfolio (by type of borrower), individual borrower, product, operations, lending segment. Such management is carried out systematically and comprehensively with other types of risks (market risks, liquidity risks, interest risk in the banking book, operational risk, compliance risk).

9.5. The Bank’s credit risk management process implements the following principles:


- integrity (consideration of credit risk elements as an aggregate integral system);
- openness (interconnection with other types of risks);
- structure (the process has a clear structure, with of the unity of clear interactions between its elements as its main criterion, as well as the laws of these relationships);
- efficiency (ensuring a strategic risk/return ratio);
- regulation (all credit risk management processes must be regulated);
- coherence (the credit risk management strategy is consistent with the general bank business development strategy);
- awareness (the credit risk management process is accompanied by the availability of objective, reliable and relevant information, relevant reports).

9.6. The credit risk management system is a process that has the following sequence of stages:

- risk identification;
- assessment of the risk occurrence consequences;
- risk management (selection of decisions on management impact to mitigate or avoid credit risk);
- control (monitoring and accounting, reporting, responsibility)

9.7. Identification

9.7.1. Identification of credit risk is a basic stage of the process of credit risk system management. Identification of credit risk means its detection, forecasting of opportunities and features of materialization, change in risk over time, the degree of interconnection with other risks, fixation of factors affecting the identified credit risk. At this stage, the degree of compliance of the risk position with its planned characteristics is determined.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

9.7.2. The main goal of identification is to create conditions for the third stage of credit risk management, which provides for the direct selection of decisions on management actions.

#### 9.8. Assessment

9.8.1. Credit risks determined at the identification stage are assessed in the following time limits:

- Data of previous periods. Collection of statistical data which allows assessing the consequences of the occurrence of credit risks and drawing conclusions about the statistical nature of events related to the manifestations of these risks.
- Present moment. Collection of data which allows adjusting estimates based on historical data for their use in the present time, since such information makes allows to take into account temporary changes in the Bank’s operating environment.
- Forecasting future positions. Collection of data necessary for forecasting, as well as information allowing taking into account future changes affecting the characteristics of the operating environment.

9.8.2. The Bank distinguishes the following credit risk factors:

- 1) Individual credit risk factors.
- 2) Aggregate credit risk factors.

9.8.3. Such division was introduced due to the possibility of analysing credit risk both at the level of a specific borrower and at the level of a specific credit portfolio.

Factors affecting the credit risk


Individual risk	Collective risk
Instability of the economic situation	
Change in the borrower’s financial status	Change in the monetary policy of the NBU (reserve requirements)
Borrower’s credit history	Change in the Bank’s credit policy
Loan security quality change	Macroeconomic factor
Quality of borrowing enterprise management	
Amendment of the loan agreement	
Defaults of major suppliers/buyers	

#### 9.9. Risk management

9.9.1. The main objectives of credit risk management are:

- Risk prevention can be achieved by eliminating the prerequisites for the emergence of credit risk.
- Maintaining risk at a certain level.
- Minimizing risk.

Method	Nature of risk impact	Contents
Risk prevention	Indirect influence	Selection and assessment of credit specialists Optimization of the credit process Personnel development Study of the potential client Continuous client monitoring

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	<b>JSC “FUIB” Risk Management Policy</b>	

Risk assessment and calculation	Indirect influence	Borrower creditworthiness assessment Evaluation of the quality of the Bank’s credit portfolio Credit risk measurement Predicting credit risk trends
Credit risks avoidance	Direct influence	Refusal of lending to an unreliable client
Risk minimization	Direct influence	Loan diversification Funds reservation Loan structuring
Risk insurance	Indirect influence	Reassignment of responsibilities for credit loss compensation to an insurance organization
Risk containment	Indirect influence	Creation of structural units for nonperforming loans Suspension of lending activities in high-risk industries Search for new sectors of the credit market and development of new credit products

9.10. To classify credit operations by risk level, the Bank uses an internal credit risk assessment system. In particular, the Bank uses expert rating models (internal rating assessments). The rating is set depending on the financial stability of the borrower and depicts an expert assessment of the relative probability of its default, in accordance with the methods developed by the Bank. For standardized credit products, the Bank uses automated assessment tools – scoring models.

9.11. The Bank uses an internal credit risk assessment system and compares the results of its assessment with the amount of credit risk calculated in accordance with the requirements of the Regulation “On determining the amount of credit risk by Ukrainian banks under active banking transactions” approved by NBU Board Resolution No. 351 dated 30.06.2016, and analyses the reasons for deviations


9.12. The assessment of borrowers’ credit risk is carried out in accordance with internal regulatory documents. In order to reduce the risks of financing clients with a negative reputation, the Bank has implemented a system of client data verification.

9.13. The results of credit risk identification and assessment shall be basis for a decision on credit risk management. JSC “FUIB” distinguishes the following credit risk management strategies:

- The avoidance strategy is applied if the cost of risk event materialization exceeds the estimated cost of the object exposed to the risk, in the absence of a critical need for this object.
- The acceptance and ignoring strategy is applied if the cost of managing a risk position exceeds the cost of risk event materialization, and avoidance is impossible.
- The acceptance and management strategy is applied if it is not possible to apply the strategies listed above, by using special banking risk management tools.

9.14. The Bank adopts one of 3 decisions:

- refuse to issue (avoidance);
- accept and manage (issue a loan);
- accept with minimization measures (setting additional requirements for the borrower, loan, collateral, partial satisfaction of the requested loan parameters).

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	<b>JSC “FUIB” Risk Management Policy</b>	

#### 9.15. Control

9.15.1. The credit risk management process continues after adoption of decision to conduct a credit transaction until full repayment of all obligations of the debtor client to the Bank.

9.15.2. The level of credit risk control before changes is carried out by monitoring risk indicators (quality of debt service, financial condition of the borrower, fulfilment of the terms of the loan agreement, lien condition, etc.), their dynamics for timely management response in case of sudden deviations of the risk position values from planned/budget values.

9.15.3. To reduce the control over nonperforming loans, control the volume and dynamics of overdue liabilities, the Bank has designed application scoring models for retail business products and a behavioural scoring model for collecting debts from individuals.

9.15.4. The following processes are automated:

- decision making;
- interaction with three Credit Histories Bureaus: (Ukrainian Bureau of Credit Histories LLC (UBCB), International Credit Histories Bureau PJSC (ICHB), First All-Ukrainian Credit Histories Bureau PJSC (FACHB)).

9.16. As noted above, the function of current credit risk management is carried out by the Bank's business line as a subject of the RMS, initiating a credit transaction, maintains contact with the client on behalf of the Bank throughout the entire term of the credit agreement, and ensures timely repayment of the debt by the client. Risk management units monitor the activities of the business line units within the limits of assigned functions as the second level of control (line of defence) of the Bank in the process of lending. This approach allows to promptly monitor and respond to changes in the amount of credit risk on both a portfolio and individual basis. The Bank's Credit Council shall be responsible for operational monitoring of compliance with the Bank's credit policy.

9.17. The credit risk control reporting system also includes information on compliance with established credit risk limits, identified facts of overlimiting (taking into account their preliminary analysis), taking into account the relevant powers of the Bank's credit body.

9.18. Strategic control over the Bank's compliance with credit risk management requirements is carried out by the Supervisory Board by quarterly analysis of specialized reporting, which includes a credit portfolio quality report, information on overlimiting (including authorized overlimits).

### 10. LIQUIDITY RISK

10.1. Liquidity risk means a probability of losses or additional losses, or a shortfall in the planned revenues as a result of the Bank's inability to finance the growth of its assets and/or fulfil its obligations in due time.


10.2. The main goal of the Bank's liquidity risk management is to ensure a sufficient level of balance liquidity in ordinary and stress situations to meet the indicators specified in the Bank's strategy and budget.

10.3. The organizational structure of the liquidity risk management process has 3 levels of control (lines of defence):

- 1st level of control (line of defence). Business units of the Bank.
- 2nd level of control (line of defence). Risk management and compliance management unit.
- 3rd level of control (line of defence). Internal Audit Department.

10.4 The Bank has a developed separate document – the Liquidity Risk Management Policy, which defines:

1) goals, task and principles of liquidity risk management;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- 2) the organizational structure of the liquidity risk management process, taking into account the distribution of the functionality of the process participants, their powers, responsibilities and interaction procedure;
- 3) a list of limits for liquidity risk control and the procedure for their setting;
- 4) approaches to identification, measurement, monitoring, control and mitigation of the liquidity risk;
- 5) procedures for determining, approving and reviewing assumptions used to measure liquidity risk;
- 6) principles of assets and sources of financing diversification from the point of view of their impact on liquidity risk;
- 7) methodological approaches to liquidity stress testing;
- 8) a list and form (information content) of liquidity risk management reporting forms, the procedure and frequency/terms of their provision to risk management system entities.

## 11. INTEREST RISK IN THE BANKING BOOK

11.1 Interest risk in the banking book is a probability of occurrence of losses or additional losses, or a shortfall in the planned revenues due to the effect of unfavourable changes in the interest rates in the bank book. The interest risk in the banking book affects the economic value of a Bank's capital and its net interest income.

11.2 The interest risk in the banking book includes the following risks:

- 1) The risk of gaps that arises due to the difference in maturity (for instruments with a fixed interest rate) or changes in the value of the interest rate index (for instruments with a floating interest rate) of assets, liabilities and off-balance sheet positions in the banking book.
- 2) The basis risk that arises from the fact that there is not a sufficiently close connection between the adjustment of rates received and paid for various instruments, all other characteristics of which are the same for revaluation.
- 3) Option risk arising from the Bank's operations with options (automatic option risk) or the presence of embedded options in the Bank's standard products (option behavioural risk).


11.3. The organizational structure of the interest risk in the banking book management process has 3 levels of control (3-x lines of defence):

- 1st level of control (line of defence). Business units of the Bank.
- 2nd level of control (line of defence). Risk management and compliance management unit.
- 3rd level of control (line of defence). Internal Audit Department.

11.4 The Bank has a developed separate document – the Interest Rate Risk Management Policy, which defines:

- 1) goals, tasks and principles of the interest risk in the banking book management;
- 2) the organizational structure of the interest risk in the banking book management process, taking into account the distribution of job functions between the process participants, as well as their powers, responsibilities and interaction procedure;
- 3) a list of limits for controlling interest risk in the banking book and the procedure for their setting;
- 4) approaches to identification, measurement, monitoring, control and mitigation of the interest risk in the banking book;
- 5) procedures for determining, approving and reviewing assumptions used in measuring interest risk in the banking book;
- 6) methodological approaches to stress testing of the interest risk in the banking book;



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

7) a list and form (information content) of interest risk management reporting forms, the procedure and frequency/terms of their provision to risk management system entities.

## 12. MARKET RISK

12.1 Market risk is a probability of occurrence of losses or additional losses or a shortfall in the planned revenues as a result of unfavourable changes in the foreign exchange rates, interest rates, cost of financial instruments.

12.2 The Bank identifies the 3 most significant market risks:

- 1) Currency risk arising from adverse fluctuations in foreign exchange rates affecting assets, liabilities and off-balance sheet items contained in the Bank’s trading and bank books;
- 2) Price risk of OVDPs is the risk of losses when selling the entire OVDP portfolio on the secondary market in the event of the need to convert the secondary liquidity cushion into primary liquidity. Such risk arises from adverse changes in market interest rates that affect the value of debt securities or other financial instruments whose trade on and off organized capital markets is characterized by market behaviour;
- 3) Price risk of G7 sovereign bonds (as part of the market risk) is the risk of possible losses in the event of changes in market interest rates due to the revaluation of G7 bonds in the Bank’s portfolio, or in the event of the sale of G7 bonds on the open market. G7 countries have large and developed economies, therefore bonds issued by these governments are considered investments with a very low level of risk and reliable protection.

12.3. The organizational structure of the market risk management process consists of 3 levels (3 lines of defence):

- 1st level of control (line of defence). Business units of the Bank.
- 2nd level of control (line of defence). Risk management and compliance management unit.
- 3rd level of control (line of defence). Internal Audit Department.

12.3. The Bank has a developed separate document – Market Risk Management Policy. This document defines:


- 1) goals, task and principles of market risk management;
- 2) the organizational structure of the market risks management process, taking into account the distribution of the functionality of the process participants, their powers, responsibilities and interaction procedure;
- 3) a list of limits for market risks control and the procedure for their setting;
- 4) approaches to identification, measurement, monitoring, control and mitigation of the market risks;
- 5) procedures for determining, approving and reviewing assumptions used in measuring market risks;
- 6) approaches to market risks stress testing;
- 7) a list and form (information content) of market risk management reporting forms, the procedure and frequency/terms of their provision to risk management system entities.

## 13. OPERATIONAL RISK

13.1. JSC “FUIB” has an effective operational risk management system, which is fully integrated into the overall Risk Management System. Operational risk is assessed taking into account its interconnection and impact on other risk categories inherent in banking activities.

13.2. The Supervisory Board annually approves the size of the risk appetite for operational risk (for the next 12 months).



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

13.3. The Bank has ensured the operational risk management process, adhering to a single ICS model in terms of three levels of control (lines of defence):

- 1) at the first level of control (line of defence) – Owners of all operational risks that arise in their area of responsibility: business units and supporting units. ORMS Risk Officers (responsible for operational risks internal control) are appointed in these units, or the Heads of these structural units are ORMS Risk Officers by default;
- 2) at the second level of control (line of defence) – the General Banking Risk Department;
- 3) at the third level of control (line of defence) – the Internal Audit Department.

13.4. Operational risk management process:

- Identification;
- Calculation (assessment);
- Reporting;
- Management;
- Monitoring;
- Control.

13.5. The SB/Board of the Bank has delegated the authority to manage operational risk to the Operational Risk Management Committee (ORMC) and its Subcommittees, and has also created an independent unit in the risk management vertical – the General Banking Risk Department (GBRD), which coordinates effective functioning of the Operational Risk Management System (ORMS), consolidating all operational risk incidents and reporting on the level of operational risk control.

13.6. Reporting:

**The GBRD shall prepare the following regular reports:**


- To the Supervisory Board – quarterly
- To the Board/ORMC – quarterly.

**IMPORTANT!** The Bank ensures timely detection of significant operational risk events and immediate notification of such events to the GBRD, namely: information on a significant/resonant operational risk event shall be provided to the Supervisory Board and the Board/ORMC no later than the next business day from the date of receipt of the notification of the incident.

**13.7. The minimum list of mandatory quarterly ORMS reporting to the Supervisory Board:**

- Consolidated data on all operational risk events for the period (dynamics, management results) – quarterly;
- Significant operational risk events as well as their causes and measures to minimize them in the future – quarterly;
- Significant external events and their potential consequences for the Bank – quarterly;
- Report on monitoring of KRIs (thresholds, KRI values as of the reporting date and their dynamics) – annually;
- Operational risk self-assessment results – annually;
- Stress testing results – annually.

13.8. Since 2011, the Bank has maintained an internal database of operational risk events which is analysed and used as the source information for reporting to Management. The classification of business lines is defined in the “FUIB” process catalogue, and the list of operational risk events is defined in the ORMS General Banking Classifier.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

The list of rows of operational risk events internal database is regulated by the Operational Risk Management and Control Policy.

**Note!** Incidents identified by the IAD during scheduled audits of banking processes, which are registered in accordance with the requirements for ORMS Risk Officers, are entered into the operational risk events database.

#### 13.9. Bank’s approaches to operational risk identification and assessment:

- Maintaining an operational risk events internal database.
- Maintaining an operational risk events external database (External Data Collection and Analysis);
- Determination and quarterly monitoring of Key Risk Indicators (KRIs);
- Annual operational risk self-assessment by heads of structural units of the Bank (Risk Self Assessments);
- Business Process Mapping analysis: analysis of process stages to identify operational risks inherent in a specific process/process stage;
- Scenario analysis during annual operational risk stress testing (Scenario Analysis). The Bank conducts scenario analysis based on the judgments of employees of the first level of control units (line of defence) and employees of risk management units in case of:
  - 1) a probable increase in the frequency (number) of events and/or the volume of operational losses compared to statistics in the internal operational risk event database;
  - 2) the emergence of new operational risk events result of the introduction of new or significant changes in effective processes;
  - 3) the emergence of operational risk events with a significant level of losses and a low probability of occurrence.


The stress testing methodology is described in detail in a separate internal regulatory document of the GBRD.

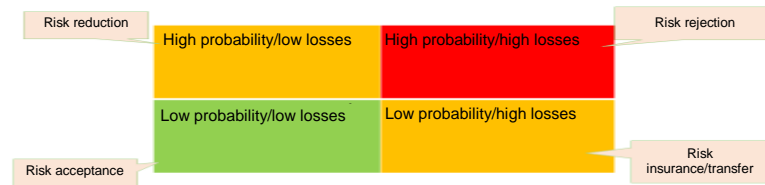
**IMPORTANT!** The Bank performs operational risk stress-testing on an annual basis for various short-term and long-term stress scenarios that can materialize both for the Bank and for the market as a whole, in order to identify the causes of possible losses through the implementation of operational risk and assess the relevance of stress-testing results to a certain level of risk appetite for operational risk. The result of the operational risk stress testing shall be presented as the amount of possible losses. Comparative Analysis is a tool for comparing the results of different tools in order to objectively assess (measure) the Bank’s operational risk.

#### 13.10. The Bank approves the procedure for classifying significant operational risk events:

- 1) criteria for classifying operational risk events as significant: the amount of actual losses is greater than or equal to 5,000 USD (equivalent), or events with zero tolerance (internal fraud);
- 2) the procedure for creating a working group – the Commission for Operational Risk Incidents Investigation (CORII), which investigates operational risk events is set out in a separate regulatory document – CORII Regulations;
- 3) the procedure for escalating the results of the investigation and approving measures to minimize the consequences of events and prevent occurrence of similar events in the future is described in the Operational Risk Management Policy.

#### 13.11. The Bank divides possible operational risk events according to the following criteria:

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	



13.12. Depending on the defined operational risk category, the Bank is entitled to use the following methods of operational risk management:

- 1) **Acceptance of risk**, which implies the continuation of the activity without changes in the case of the possibility of incurring minor losses with a low probability of occurrence;
- 2) **Transfer of risk**, involving insurance of risks with potentially substantial losses with a low probability of occurrence or risks that are under the Bank’s limited control;
- 3) **Risk mitigation**, which involves the adjustment of certain processes and the introduction of additional controls in case of minor losses with a high probability of occurrence;
- 4) **Avoiding the risk** that provides the interruption of risky activity which results in significant losses with a high probability of occurrence.

13.13. Risk categories for calculating the level of operational risk:

**13.13.1. Risk capacity** is the maximum level of risk that the Bank is able to accept based on the operational risk stress testing. The stress testing methodology is regulated by a separate internal regulatory document.

**13.13.2. Risk appetite** is the total amount and types of risks that the Bank is willing to accept in accordance with its business model and strategic goals.

*IMPORTANT! The indicator takes into account the strategic goals of business lines development and is exclusively an analytical/management value.*

**Thresholds values demonstrating exceeding of the operational risk appetite:**

“**Green zone**”: no more than 100% of the risk appetite approved by the SB.

“**Yellow zone**”: from 100 to 130% of the risk appetite approved by the SB.

“**Orange zone**”: from 130% to risk capacity.

“**Red zone**”: exceeding risk capacity.

**13.13.3. Risk limits** are quantitative restrictions to control the amount of risks that the Bank faces in the course of its activities in a certain category of operational risk.

Limits are approved by operational risk categories and monitored for overlimiting daily by the GBRD.


**Thresholds values demonstrating exceeding of the operational risk limits:**

“**Green zone**”: no more than 100% of the risk limit approved by the SB.

“**Yellow zone**”: from 100 to 120% of the risk limit approved by the SB – is an authorized overlimit, approved by the decision of the ORMC.

“**Red zone**”: exceeding the risk limit approved by the SB by more than 120% is unauthorized and requires immediate notification of the SB and the Board.

The process for escalating operational risk limits violations is described herein.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

#### **13.14. Business Continuity Management System (BCMS).**

To ensure continuous operations and minimize losses, the Bank has a Recovery Plan and the Business Continuity Plan (BCP) developed and approved by the SB of JSC “FUIB”. During Plan development “critical” stress scenarios of OR events are considered, which will help identify critical processes, systems and key positions. Practical testing of the BCP for the HO and analysis of the impact of negative factors on the Bank’s processes (Business Impact Analysis) are carried out annually in case of the Bank’s normal operation mode, as well as annual training of Bank employees in the requirements of the BCMS.

#### **13.15. Third-party risk management system (including outsourcing risks).**


13.15.1. In its activities, the Bank manages third-party risks (including pure outsourcing risks) associated with the transfer of certain Bank functions to third parties. A group of “critical” (providing the Bank with highly critical services even during an emergency and the Company has the necessary competencies, resources, experience, etc.) Counterparties (including outsourcers) for the continuity and efficiency of business operations is identified. One of the main tasks of the Operational Risk Management System is determination of the degree of dependence on the quality and timeliness of the Counterparty’s performance of contractual obligations and operational management of potential threats. These third-party risks are also part of the single Bank’s ORMS Classifier, and all the stages of the management process from detection to control are similar to the JSC “FUIB’s” RMS concept.

13.15.2. Counterparty reliability risk management is aimed at managing the following risks:

- Fraud risk.
- Risk of cooperation with Counterparties involved in money laundering/terrorism financing.
- Risk of cooperation with Counterparties subjects of economic sanctions.
- Risk of cooperation with potential subjects of corruption.

13.16. Depending on the defined operational risk category, the Bank may use the following **methods of operational risk management:**

- Testing existing products/processes/resources (including IT resources) for their sensitivity to the negative impact of operational risk factors and implemented/strategic processes/products/resources;
- Finding the best management solutions (best practices). Due to the insufficient development of quantitative risk assessment, qualitative approaches allow identification of bottlenecks in the processes and implement better optimization or control methods (for example, “two pairs of eyes”);
- Approval of risks by a Collegiate Body (for example, the ORMC/ORMC Subcommittee);
- Risk limitation. Setting risk thresholds, as well as approving liability limits for decision-making;
- Risk insurance;
- Risk transfer, risk processes outsourcing;
- Formation of reserves to compensate for unforeseen losses from operational risks;
- Avoiding risk by cancelling risky operations, processes, products, systems or refusing to enter into a Contract with an unreliable counterparty;
- Monitoring the quality and timeliness of third party’s performance of contractual obligations, strengthening its contractual obligations or finding alternative Counterparties (if the Counterpart is not a monopolist).

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- Regular internal control and audit. Internal control is a preventive tool, it is not aimed at simple ascertaining the facts of past events.

13.17. Direct control is applied under the following conditions:

- The responsibility of each employee is clearly defined and understood.
- Access (physical and system) is controlled by Competent Units.
- Adequate self-control and post-control by the manager or by the next unit in the process chain.
- Authorisation of transactions.
- Transactions recording.
- Mandatory documenting of policies, procedures.
- Provision of continuous training of new and advanced training of existing personnel
- Analysis of processes for the adequacy/reasonableness of the division of responsibilities (avoidance of duplication of functions).
- Regular inventory: recorded assets are compared with available.
- Verification of the business reputation of counterparties, including verification of the presence of international economic sanctions against them.

### **13.18. ICT AND INFORMATION SECURITY RISK MANAGEMENT (AS A COMPONENT OF OPERATIONAL RISK)**

13.18.1. JSC “FUIB” has effective mechanisms for managing ICT risk and information security risk (including cyber risk), which are an integral part of the Bank’s operational risk management, taking into account its impact on other risks inherent to the Bank.

13.18.2. When managing operational risk (including ICT risk, information security risk (including cyber risk)), the Bank adheres to the “3 levels of control (lines of defence)” model:

- 1st level of control (line of defence): all Bank’s structural units which must ensure compliance with the requirements of the policy, procedures and use of operational risk management tools, including the identification and assessment of ICT risks, information security risks (including cyber risks), taking management measures and reporting on such risks, including information security requirements in general. Responsible persons/units of the 1st level of control (lines of defence): Information Technology Department (ICT risk) and Information Security Department (information security risk (including cyber risk)).


- 2nd level of control (line of defence): General Banking and Operational Risk Body (GBORB)

- 3rd level of control (line of defence): IAD.

13.18.3. The purpose, objectives and principles of ICT and information security risk management (including cyber risk) are the same as operational risk management (Section 5 of this Policy).

13.18.4. The Bank’s objectives regarding ICT and information security risk management (including cyber risk) are: taking measures for minimizing the occurrence of losses or additional losses or failure to receive the planned revenues due to the occurrence of internal and external events regarding the Bank’s information systems and other information resources used to achieve the Bank’s objectives, lack of internal control or inadequate or erroneous internal processes of the Bank in the field of information and communication technologies.

13.18.3.5. ICT and information security risks (including cyber risk) can have a significant impact on the Bank’s:

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- strategic goals: level of automation and digitalization, growth in business volumes and compliance of IT capacity with this growth;
- operational objectives: IT systems must guarantee the speed, security, and timeliness of processing of the Bank’s transactions and ensure the functionality of processes through their automation;
- compliance objectives: compliance of IT architecture and IT services with the requirements of the legislation of Ukraine;
- information objectives: ensuring information protection and clear access mediation depending on the level and type of user;
- objectives related to preparation of financial and statistical reporting: ensuring the preparation of complete and correct/reliable reporting and its timely submission/publication.

13.18.6. The organizational structure of ICT and information security risk management (including cyber risk) is similar to operational risk management.

13.18.7. Approaches to ICT and information security risk management (including cyber risk) correspond to general risk management approaches: avoidance, transfer, minimization, and rejection of risk.

13.18.8. The methodology for assessing ICT and information security risks (including cyber risk), indicators and the procedure for their application are determined during ORMS with the same periodicity and based on single approaches and metrics.

13.18.9. The Operational Risk Classifier highlights these risks with a separate markers “ISMS” (for information security risks) and D – “Systems” (for information and communication technology risk (ICT risk)).

13.18.10. Assessment, escalation of information and reporting are carried out only within the ORMS framework.

13.18.11. The Bank creates and maintains a database of ICT and information security risks (including cyber risk) incidents, as well as analyses the information gathered at the 1st level of control (line of defence). At the same time, all registered events that fall under the operational risk criteria for ORMS reporting are entered into the operational risk events database, under responsibility of GBORB.


### **13.19. LEGAL RISK MANAGEMENT (AS A COMPONENT OF OPERATIONAL RISK)**

13.19.1. When managing legal risk, the Bank adheres to the “3 levels of control (line of defence)” model:

- 1st level of control (line of defence): all Bank’s structural units which must ensure compliance with the requirements of the policy, procedures and use of operational risk management tools, including the identification and assessment of legal risks, taking management measures and reporting on such risk. Responsible persons/units of the 1st level of control (lines of defence): Legal Department.
- 2nd level of control (line of defence): GBORB of the GBRD
- 3rd level of control (line of defence): IAD.

13.19.2. The purpose, objectives and principles of legal risk management are the same as for operational risk management (Section 5 of this Policy).



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

13.19.3. At the first level of ICS control (line of defence) the Legal Department assesses the probability of legal risk materialization and consequences in processes and products that may have a potential legal risk. Risks are registered by Risk Officers according to the ORMS classifier.

13.19.4. The Bank monitors legal risk by studying:

- fines and restrictions on activities as a result of studying court decisions/inspection reports;
- lawsuits against the Bank from clients/counterparties;
- lawsuits against the Bank by clients/counterparties/contractors;
- other facts related to legal risk when analysing/creating model contracts, etc.

## 14. COMPLIANCE RISK

14.1. The internal control system for compliance risk management covers all Bank’s structural units and employees based on the following distribution:

1 level of control (line of defence): Business lines and Support units;

2nd level of control (line of defence): Compliance management vertical;

3rd level of control (line of defence): Internal Audit Department.

14.2. Bank’s Compliance Risk Management System is a component of the JSC “FUIB’s Risk Management System.

14.3. The Bank’s objectives in implementing the compliance risk management system are:

- prevention of losses/sanctions, additional losses or a shortfall in the planned revenues or loss of reputation due to failure of the bank to comply with the requirements of the legislation, regulations, market standards, rules of fair competition or minimization of these negative factors impact on the Bank;
- ensuring compliance with the requirements of the Bank’s internal regulatory and administrative documents;
- ensuring proper management of conflict of interest cases: preventing abuse of such situations, minimizing their consequences;
- ensuring compliance with corporate ethics requirements, including proper informing of owners (shareholders) and their authorized persons about the key areas of the Bank’s activity, fair treatment of clients and ensuring a diligent approach to consulting;


14.4. The functioning of the compliance risk management system is ensured by:

- The Supervisory Board of the Bank ensures strategic management of the compliance risk system, establishment of an independent compliance control unit (compliance).
- The Board of the Bank ensures the implementation of tasks and decisions of the Supervisory Board of the Bank related to the compliance risk management system.
- The IAD assesses the compliance risk management system. The CCB ensures the implementation of control functions by performing:
- Regulatory control – control of the Bank’s compliance with the requirements of the legislation, regulatory legal acts, market standards, as well as internal documents of the Bank;
- Deontology – control of compliance with the requirements of corporate ethics, conflict of interest management.

Business units and support units of the first level of control (line of defence), as owners of compliance risks, implement a set of measures managing compliance risks within the limits of their powers and in accordance with the approaches and procedures implemented in the Bank.

14.5. To achieve the objectives of the compliance risk management system, the Bank:




	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	<b>JSC “FUIB” Risk Management Policy</b>	

- provides control over Bank’s compliance with the norms of legislation, regulatory internal banking documents and relevant standards of professional associations applicable to the Bank;
- monitors changes of the legislation and relevant professional associations standards, assessing the impact of such changes on Bank’s processes and procedures, monitoring the implementation of relevant changes in internal bank documents;
- provides control over compliance risk arising in the Bank’s relations with clients and counterparties in order to prevent participation and/or use of the Bank in any illegal transactions;
- manages risks associated with conflicts of interest (including conflicts of interest between the Bank’s managers and the subject of assessment activities);
- ensures control over observing the rules on timeliness and reliability of financial and statistical reporting;
- controls compliance with requirements for personal data protection according to legislation of Ukraine;
- provides explanations to the Bank’s management on their request regarding control over Bank’s compliance with the legislation of Ukraine and relevant standards of professional associations, applicable to the Bank;
- provides training of the Bank’s employees regarding the compliance with the legislation, relevant standards of professional associations applicable to the Bank, and risk management culture, taking into account the code of conduct (ethics);
- carries out compliance risk identification, measurement, monitoring, control, reporting, mitigating;
- controls over the compliance of the processes related to distressed assets management to the legislation of Ukraine and the internal banking documents;
- prepares conclusions on compliance risks inherent in new products and significant changes in the Bank’s activities;
- prepares conclusions on compliance risk for making credit decisions on loans to persons related to the Bank (except for loans to individuals for which decisions are made by an automated system taking into account that the system applies standard product price parameters and there is no conflict of interest);
- controls the compliance of the compensation and indemnity systems introduced in the Bank, as well as procedures for bringing to disciplinary responsibility of the Bank employees, according to the requirements of the legislation of Ukraine;
- controls the Bank’s compliance with the norms for determining the list of persons related to the Bank to ensure the integrity and completeness of the process of identifying persons related to the Bank and control over their transactions;
- calculates the compliance risk profile.

#### 14.6. Identification of compliance risks:

- 14.6.1. The Bank shall ensure timely identification, analysis and assessment of compliance risks in order to choose an appropriate and relevant way to manage them. For these purposes the CCB uses information on unacceptable behaviour (from the Bank’s employees within the framework of the confidential reporting mechanism)/on violations in

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

the Bank’s activities (from the operational and compliance risk event database which is explored by the GBRD);

- from customer complaints;
- from personal appeals of the Bank’s employees or third parties to the CCB;
- from reports, from the results of IAD audits or from audits performed by external auditors;
- from regulatory and supervisory authorities (results of on-site inspections, surveillance, fines imposed, identified violations of Ukrainian legislation);
- from other sources of information received by CCB employees in the course of their activities.

14.6.2. The information received is accumulated and systematized by the CCB in the manner determined by the Bank’s internal regulatory documents for its analysis in order to manage compliance risks.

14.7. Assessment of the compliance risk level

14.7.1. When measuring the compliance risk level, the Bank assesses the impact of the following indicators:


- Financial impact;
- Impact on the Bank’s activities;
- Impact on the Bank’s reputation;
- Probability of compliance risk materialization;
- Assessment of control measures effectiveness;
- In order to implement effective compliance risk management, the level of compliance risk control in the Bank is subject to regular assessment. Risk assessment includes the identification and analysis of compliance risks to determine measures to manage them. The assessment is carried out in accordance with the Regulations “On the Assessment of Compliance Risks of JSC “FUIB”” and the Regulations “On Monitoring Compliance Risk Indicators of JSC “FUIB””.

14.7.2. The following criteria are assessed to determine the overall level of compliance risk:

- **Low risk** – compliance risk may lead to a minor impact on the reputation and disruption of the activities of individual internal/non-critical processes of the Bank. The ability to perform planned tasks and functions is not affected by compliance risk, financial losses do not exceed 0.01% of the authorized capital.
- **Medium risk** – the identified compliance risk is considered as partially affecting the Bank’s activities, reputation and lead to financial losses (0.01% – 0.1% of the authorized capital).
- **High risk** – the identified compliance risk may significantly affect the Bank’s activities and negatively affect the Bank’s reputation. The Bank’s ability to perform planned tasks and functions is subject to very high compliance risk (may lead to the Bank’s inability to perform some functions), significant financial losses are possible (exceeding 0.1% of the authorized capital).

14.7.3. Compliance risk assessment is a regular compliance risk management tool. In the Bank compliance risk assessment is carried out in accordance with the methods and procedures specified by the Bank's internal regulatory documents on compliance risk management and ML/TF risks of the Bank.

14.7.4. The CCB assesses the compliance risk level of the Bank as a whole. The results are submitted to the Risk Management Committee of the Supervisory Board, the Supervisory

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

Board, and the Board of the Bank for consideration as part of the information escalation and reporting procedure.

14.8. Compliance risk reporting:

14.8.1. To ensure proper and timely informing of the Board, the Risk Management Committee of the SB and the SB, the Bank generates a “Compliance Risk Assessment Report” containing the following information:

- a general assessment of Bank’s compliance risk with a breakdown by components;
- products, activities, processes that expose the Bank to significant compliance risk and affect the Bank in the event of its materialization, as well as proposals for avoiding or mitigating this risk,
- significant changes in legislation and their potential consequences for the Bank;
- external information regarding compliance risk (fines imposed on other banks, events that led to a deterioration in the reputation of other banks);
- cases of conflict of interest;
- training of the Bank’s employees on compliance issues;
- cases of unreliable reporting to regulatory and supervisory authorities, as well as sanctions imposed to the Bank;
- cases of violation of the code of conduct (ethics) by the Bank’s employees;
- cases of violation of the requirements of the current legislation of Ukraine and internal banking documents, as well as sanctions imposed to the Bank or other negative consequences of such violations.

14.8.2. The compliance risk assessment report includes aggregated data and information, significant events and key changes. Detailed information on events, dynamics of indicators, detailing/decoding of data can be included as annexes (if necessary). The structure of the report and the minimum requirements for filling its sections are defined in Annex 1 to the Compliance Risk Management Policy of JSC “FUIB”.

14.8.3. The report is prepared using information received from other units within interaction procedures during performance of compliance functions and summarized/aggregated information of the CCB received during performance of the functions assigned.

## **14.9. ML/TF RISKS MANAGEMENT (AS A COMPONENT OF COMPLIANCE RISK)**


14.9.1. When managing ML/TF risk, the Bank adheres to the “3-level control (lines of defence)” model:

- 1st level of control (line of defence): all business lines and support units.
- 2nd level of control (line of defence): Compliance management vertical (including ML/TF risk);
- 3rd level of control (line of defence): Internal Audit Department.

14.9.2. The Bank’s objectives in implementing ML/TF risk management are the same as for compliance risk management (clause 14.3. of this Policy).

14.9.3. To achieve the objectives of ML/TF risk management, the Bank:

- monitors compliance with legislation and internal banking documents related to AML/CTF;

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	<b>JSC “FUIB” Risk Management Policy</b>	

- monitors changes of the legislation, assessing the impact of such changes on Bank’s processes and procedures, monitoring the implementation of relevant changes in internal bank documents related to AML/CTF;
- provides control over ML/TF risk arising in the Bank’s relations with clients and counterparties in order to prevent participation and/or use of the Bank in any illegal transactions;
- provides explanations and consultations on AML/CTF issues for the Bank’s managers on their request;
- conducts training for employees on compliance with the requirements of the legislation in the field of financial monitoring;
- carries out ML/TF risk identification, measurement, monitoring, control, reporting;
- controls over the compliance of the processes related to ML/TF risks management to the legislation of Ukraine and the internal banking documents;
- prepares conclusions on ML/TF risk inherent in new products and significant changes in the Bank’s activities;
- calculates the ML/TF risk profile.

#### 14.9.4. Assessing the ML/TF risk level.

In order to implement effective ML/TF risk management, the level of ML/TF risk control in the Bank is subject to regular assessment.

Risk assessment includes the identification and analysis for further determining of measures to manage them.


The AML/CFT risk appetite targets are calculated quarterly, and the results are submitted for the Supervisory Board’s consideration (the list of target indicators and their threshold values are specified in the Risk Appetite Statement of JSC “FUIB”)

The Bank’s risk profile regarding AML/CFT is assessed at least once a year. The assessment is carried out in accordance with the Bank’s risk profile calculation methodology, set out in Policy of JSC “FUIB” on compliance with the requirements of legislation regarding prevention and counteraction to legalisation (laundering) of proceeds of crime, terrorist financing and financing of proliferation of weapons of mass destruction. The results of the Bank’s risk profile assessment are submitted to the Supervisory Board for consideration and approval.

#### 14.9.5. Reporting on ML/TF risk:

To ensure proper and timely informing of the Board, the Risk Management Committee of the SB and the SB on ML/TF risk assessment, the CCO generates a report containing the following information:


- a general assessment of ML/TF risk with a detailed assessment of components;
- significant changes in legislation field of ML/TF and their potential consequences for the Bank;
- training of the Bank’s employees on financial monitoring issues;
- cases of unreliable reporting to regulatory and supervisory authorities, as well as sanctions imposed to the Bank;
- cases of violation of the requirements of the current legislation of Ukraine and internal banking documents, as well as sanctions imposed to the Bank or other negative consequences of such violations.

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

## 15. PAYMENT SYSTEM PARTICIPANT RISK (PSP RISK)

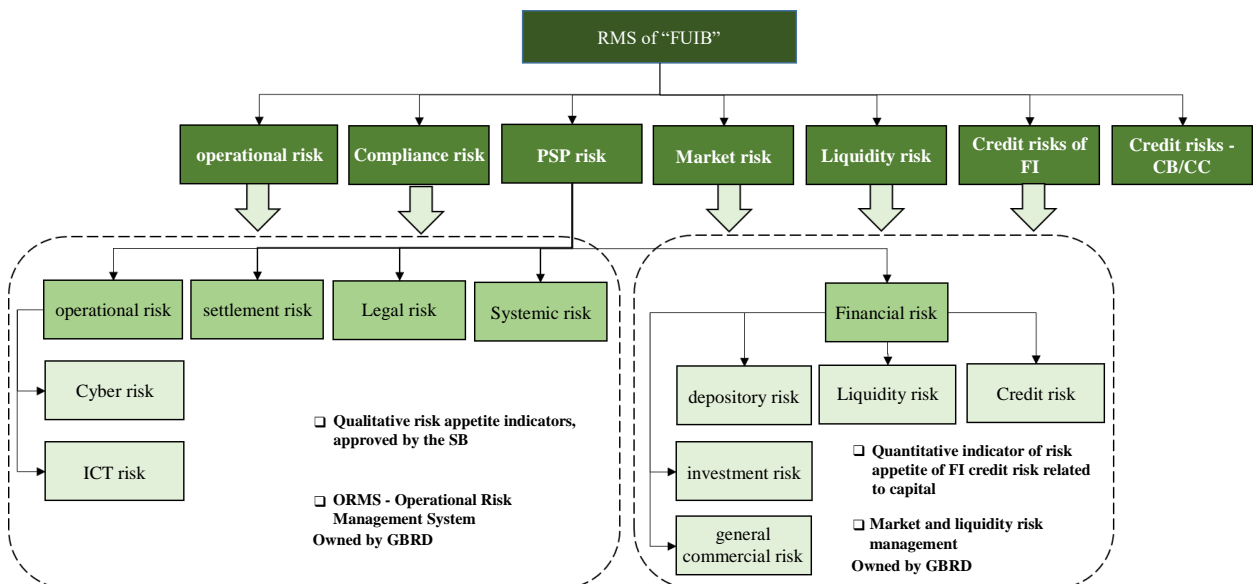
15.1 Payment system participant risk (PSP risk) – the probability of losses or additional losses or failure to receive planned income as a result of the materialization of any/some of the subtypes of PSP risk. In particular:

Subtypes of significant PSP risk	Risk definition
Legal risk	<b>Legal risk</b> – the risk of lack of legal regulation, change or unforeseen application of the provisions of the legislation of Ukraine, which may lead to losses for the oversight object.
Financial risk	<p>Financial risk is a quantitative risk including:</p> <ul style="list-style-type: none"> <li>• <b>Credit risk</b> – the risk that the oversight object will not be able to fulfil its financial obligations at a given or any other moment of time. The oversight object may have current credit risk and/or potential future credit risk;</li> <li>• <b>Liquidity risk</b> – the risk that the oversight object will not have sufficient funds to fulfil its financial obligations at a given period, but it will be able to fulfil them in the future;</li> <li>• <b>general commercial risk</b> – the risk of deterioration in the financial condition of the oversight object as a result of a decrease in its income or an increase in expenses which result in the situation where expenses exceed income and lead to losses, which are covered by capital. General commercial risk does not include risks associated with the failure to fulfil obligations by a payment system participant, payment service provider, electronic money issuer or other person having financial obligations to the oversight object;</li> <li>• <b>depository risk</b> – the risk of loss of financial assets of the oversight object;</li> <li>• <b>investment risk</b> – the risk of loss or unavailability of the Bank’s financial assets arising from their investment;</li> <li>• <b>market risk</b> – the probability of incurring losses or additional losses or not receiving planned income on both balance sheet and off-balance sheet items due to changes in market prices.</li> </ul>
Settlement risk	<b>settlement risk</b> – the risk that settlements in a payment system/scheme will not be carried out properly
Operational risk	<ul style="list-style-type: none"> <li>• <b>operational risk</b> – the risk of reduction, deterioration or suspension of the provision of services by the oversight object due to deficiencies in information systems or internal processes, human errors, operational failures (processing errors or delays, system outages (ICT risk), cyber incidents, insufficient bandwidth), loss or leakage of information, fraud or management violations due to external events;</li> <li>• <b>cyber risk</b> (a component of information security risk within operational risk management) – the risk of information resources</li> </ul>

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

	<p>and/or information infrastructure cyber threats materialization, as well as the consequences of such events;</p> <ul style="list-style-type: none"> <li>• <b>Information and communication technology risk (ICT risk)</b> (component of operational risk) – the probability of losses or additional losses, or failure to receive planned income due to malfunction or non-compliance of information and communication technologies with the business needs of the Bank, which may lead to disruption of their sustainable functioning, or shortcomings in the organization of management of such technologies;</li> </ul>
Systemic risk	<b>systemic risk</b> – the risk that the inability of one of the participants of the payment system and/or the technological operator to fulfil its obligations or disruption of the continuity of the payment system will lead to disruption of the activities of the payment system participants, other institutions or the functioning of the financial system as a whole

15.2. The management of PSP risk is integrated into the overall Risk Management System and the Bank’s Internal Control System, and operates under the uniform principles and levels of control. Currently no additional internal documents, methods, policies, etc. are developed, because management is carried out according to the methods of JSC “FUIB” under the scheme:




15.3. The organizational structure of the PSP risk management process consists of 3 levels (3 lines of defence):

1st level of control (line of defence): ITDD, ISD, ITD, OSC and other units of the ICS first line of defence within their competence.

2nd level of control (line of defence): General Banking Risk Department

3rd level of control (line of defence): Internal Audit Department.



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

15.4. The Bank has a separate document – the Risk Management Policy of the JSC “FUIB” as Payment System Participant. This document defines the main steps of implementation, the roles of employees and units, the limits of their responsibilities, approaches to managing and controlling PSP risk.

15.5. The process of PSP risk management:

- **identification:** depending on the source of the risk subtype, an event/materialization of the PSP risk may be detected and the head of the first level of control (line of defence) is obliged to notify the GBRD for implementation of mitigating measures to eliminate the negative consequences of the incidents;
- **assessment/measurement:** methodologies vary depending on the subtype of the PSP risk;
- **reporting:** consolidated data on all PSP risk events for the period (dynamics, management results) are generated quarterly;
- **management:** classical PSP risk management methods are used: risk acceptance, risk transfer, risk mitigation, risk avoidance;
- **monitoring:** to monitor PSP risk, the Bank has determined qualitative and quantitative risk appetite indicators and tolerance to their overlimits, which are specified in the JSC “FUIB” Risk Exposure Declaration. These indicators are included in the quarterly report for the Board’s and the Supervisory Board’s consideration, and are set by the Supervisory Board once a year.
- **control** is implemented by risk analysis and identification of the causes of their occurrence. Risk data is managed according to the principles and methods of the Bank’s general Risk Management System.

## 16. PROCESS OF ASSESSMENT AND MANAGEMENT OF RISKS OF CHANGES IN PROCESSES AND PRODUCTS DURING BUSINESS INITIATIVES IMPLEMENTATION

16.1. The Bank considers the process and risk management when implementing business initiatives in two areas:

- optimization/improvement of existing services, expansion of the line of existing banking products and services;
- introduction of new products and significant changes in the Bank’s activities.


16.2. Optimization/improvement of existing services, expansion of the line of existing banking products and services.

16.2.1. OR Competence Centre of the Bank (involving representatives of GBORB of the GBRD) was established to consider and implement initiatives.

If necessary, the OR Competence Centre engage representatives of the Compliance Management Vertical for control of financial monitoring risks (ML/TF risk) and compliance risks in potential risks identification and assessment.

If necessary, the OR Competence Centre engages any specific risk control unit representative of the 1st level of control (line of defence) of the ICS in identifying and assessing potential risks:

- Security Department (SD) – physical security risks and fraud risks (internal and external),
- Transaction Monitoring Centre (TMC) – control of transaction risks,
- Legal Department (LD) – control of legal risks,
- Information Security Department (ISD) – control of information security risks,


	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- Financial Accounting and Tax Reporting Department (FATRD),
- Operational Support Centre (OSC),
- and other controlling units within their competences.

16.2.2. When considering and implementing initiatives, the OR Competence Centre analyses the initiatives planned for implementation and determines/identifies potential risks of their implementation. The OR Competence Centre lists all identified risks and assesses them by the level of their potential negative consequences according to the ORMS (Operational Risk Management System) methodology.

16.2.3. After assessing the level of operational risk with the initiative owner, risk management representatives and competent units, the following solutions may apply:

Operational risk level	Description of consequences	Test	Pilot	Scaling
<b>Feature</b>		A small focus group (enables prompt correction/elimination of negative consequences of risks).	Clearly defined terms and scope of operations (control of operations and the ability to test hypotheses).	A full, expanded process that generates additional risks and increases the scale of negative consequences.
<b>Low</b>	Potential damages or losses up to 0.01% of the Bank's Authorized Capital on the date of risk calculation	Can be implemented if the OR Competence Centre has conducted a risk assessment	Can be implemented if the OR Competence Centre has conducted a risk assessment	Approval of the Supervisor + CRO (CS or Order) or ORMC Subcommittees
<b>Medium</b>	Potential damages or losses from 0.01% to 0.1% of the Bank's Authorized	Can be implemented if the OR Competence Centre	Approval of the Supervisor + CRO (CS or Order) or	Acceptance of risks by the ORMC

	TRADE SECRET		Version 9.0.
	4. Risk management and internal control		
	JSC “FUIB” Risk Management Policy		

	Capital on the date of risk calculation	has conducted a risk assessment	ORMC Subcommittees	
<b>High</b>	Potential damages or losses exceed 0.1% of the Bank's Authorized Capital on the date of risk calculation	Approval of the Supervisor + CRO (CS or Order)  or ORMC Subcommittees	Acceptance of risks by the ORMC	The Bank refuses to accept the risk (risk avoidance)/by decision of ORMC

In case of compliance risk detection (including ML/TF risk), decisions are made as follows:

Residual risk “low”	CCO and the Supervisor/Member of the Board of the relevant business vertical
Residual risk “medium”	Financial Monitoring Committee and/or the Board
Residual risk “high”	SB

### 16.3. Creation and introduction of new products and significant changes in the Bank's activities

16.3.1. Initiation, analysis, approval and implementation of new products and significant changes in the Bank's activities are carried out in accordance with the procedures established by the Bank and in accordance with the legislation of Ukraine and internal documents: Policy for the introduction of new products


and significant changes in the activities of JSC “FUIB” (hereinafter referred to as the “NPSC Policy”) and Procedure for the introduction of new products and significant changes in the activities of JSC “FUIB”.

16.3.2. Procedure for the introduction of new products and significant changes in the Bank consists of the following stages: analysis of the need and feasibility; initiation; agreement and approval of implementation in the Bank; development; implementation; monitoring.

16.3.3. The process of preparing documents for making a decision on the introduction of NPSC in the Bank's activities involves all competent units for analysing and providing relevant conclusions on potential risks of the proposed product.

The competent units include:

- Compliance Control Body (CCB),

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- General Banking and Operational Risks Body of the General Banking Risk Department (GBORB of the GBRD),
- Financial Controlling Department (FCD),
- Financial Monitoring Department (always for NP introduction);
- Methodology, Transformation and Processes Automation Centre (always for NP introduction);

Foreign Currency Surveillance and Clients Foreign Currency Operations Support Department (if necessary);

- credit risk management units in the event of the introduction/change of credit products;
- Financial Accounting and Tax Reporting Department (FATRD; always, if the changes relate to significant changes of the “Business Model” segment);
- Legal Department (LD; exclusively in case of need to obtain opinions on individual issues regarding compliance with legal requirements);
- Operational Support Centre (OSC; if necessary).
- Other structural units of the Bank within the scope of their competence (if necessary).

The decision on the implementation of a new product/type of activity or a significant change in types of activity is made on the basis of a package of documents with the opinions of all competent units and in accordance with the checklist.

Issues regarding the implementation of a new product and/or a significant change that meet the characteristics of new products and significant changes are regulated by a separate NPSC Policy.


## **17. LEVELS OF CONTROL (LINES OF DEFENCE) OF THE BANK’S ICS**

17.1. The Bank ensures risk management by adhering to the three-level model (lines of defence):

- The first level of control (line of defence) involves the Business Units and Support Units of the Bank. They are the owners of all risks arising in their area of responsibility (especially operational risk and compliance risk). These units are responsible for identifying and assessing risks, the possibility of applying management measures and reporting on such risks.
- The second level of control (line of defence) involves the risk management units (CBRD, RRD, SBRMD, GBRD, CMB, MRB) and compliance management units (including ML/TF risk) (CCB, FMD, FCSCFCOSP and MTPAC).
- the third level of control (line of defence) includes the Internal Audit Department, assesses the effectiveness of the risk management system of the units of the first and second levels, including evaluation of the effectiveness of the internal control system.

17.2. **3 levels of control (lines of defence) ensure:**

- Acceptance of risks and implementation of their current management (1st level of control (line of defence)): the Bank’s structural units (business units and support units) preparing and carrying out banking operations are involved in the process of identifying, assessing and monitoring risks, comply with the requirements of internal risk management regulatory documents, and take into account the level of risk control during preparation of transactions;
- Risk management (2nd level of control (line of defence)): Risk management (CBRD, SBRMD, RRD, GBRD, CMB, MRB) and compliance management (including ML/TF risk) ( CCB,

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

FMD, FCSCFCOSP and MTPAC) are responsible for risk management and develop risk management mechanisms, methodology, assess and monitor the level of risk control, prepare risk reporting, aggregate risks, calculate the amount of total capital requirements;

- Internal audit (3rd level of control (line of defence)): conducts an independent assessment of the quality of existing risk management processes, identifies violations and makes proposals for improving the risk management system.

## 18. CORPORATE RISK MANAGEMENT CULTURE

18.1. In order to ensure the sustainable and effective functioning of the entire risk management system, the Bank is implementing measures to develop a risk management culture focusing mainly on:

- providing the Bank’s employees with knowledge and skills in the field of risk management by their systematic (regular, distance) training;
- correct application of risk management tools by managers and employees in their everyday activities;
- developing employees’ skills for the correct and timely use of risk management tools;
- open and active communication regarding the values and principles of the risk management culture.


18.2. To ensure that both the Bank’s managers and other employees adhere to the risk management culture, the management of JSC “FUIB” creates the specific atmosphere (tone at the top) by:

- defining and adhering to corporate values, as well as monitoring compliance with such values (approval of the Code of Corporate Ethics and monitoring its compliance by all employees);
- ensuring that both the Bank’s managers and other employees understand their role in risk management to achieve the Bank’s objectives, as well as responsibility for violating the established level of risk appetite (training and testing RMS and ICS knowledge);
- promoting risk awareness by ensuring systematic informing of all units of the Bank about the risk management strategy, policy, and procedures and encouraging free exchange of information and critical assessment of the Bank’s risk acceptance (publication of information on RMS and its results on the internal corporate portal);
- obtaining confirmation that managers and other employees of the Bank are informed about disciplinary sanctions or other actions that will be applied in case of unacceptable behaviour/violations in the Bank’s activities (confirmation of familiarization with regulatory documents using EDM means/signature).

## 19. REPORTING

19.1. To implement the principles of implementing RMS in practice, JSC “FUIB” has approved a list of reporting based on the following principles:

- **Rationale:** when generating reporting, the Bank focuses on maximizing the efficiency of the reporting system, ensuring the availability of all necessary information that meets the requirements of the regulator and allows making management decisions.
- **Clarity:** reporting must be understandable to the target audience in terms of the level of detail and the volume of information.
- **Transparency:** risk reporting must have correct and accurate comparable data.


	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	

- **Completeness:** reporting must contain information on all significant risks, sources of capital to cover risks, as well as information on compliance with regulatory requirements. Reports should include a comparison of the amounts of accepted risk with the available financial resources to cover the accepted risks.
- **Comparability:** the reporting form should allow for the aggregation of information on different types of significant risks by business units to ensure the completeness of the presentation and risk structure at the Group level.
- **Unity of terminology:** the organization of the reporting system should allow switching to the prompt provision of data on actual and target levels and risk structure in crisis situations for timely adoption of management measures.
- **Integrity:** reporting should be provided with a given frequency and in a structured form.

19.2. The Supervisory Board/Board Committees determine the following reporting to inform about the Bank's risk level:

No.	Report	Supervisory Board	Board/Committees of the Board
1	Risk appetite for the reporting period	annually	annually
2	Risk appetite level fulfilment	quarterly	quarterly
3	Capital size and results of capital adequacy assessment	quarterly	quarterly
4	Results of significant types of risks stress-testing	quarterly	quarterly
5	Report on fulfilment of mandatory standards and violation of established risk limits	quarterly	monthly
6	Report on the structure and quality of the credit portfolio of KB and RB (which includes information on concentration risks, overdue, non-performing assets, written-off credits, levels of formed reserves according to IFRS standards, formed credit risk as provided for by Regulations No. 351 of the NBU and other information)	quarterly	monthly
7	Report on significant risks (results of annual banking risks self-assessment)	annually	annually
8	Reports on violations of the Bank's established risk appetites, or on the materialization of resonant events of significant risks (namely: credit, market, liquidity, operational, compliance risk)	upon occurrence (no later than the next business day)	upon occurrence



	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	JSC “FUIB” Risk Management Policy	


9	Report on compliance risk management (including AML/CFT risk)	quarterly	quarterly
10	Report on the results of the assessment of the Bank’s AML/CFT risk profile	annually	annually
11	Report on problematic issues related to the creation of a proper organization of the intra-bank AML/CTF system and conducting primary financial monitoring, as well as on problematic issues related to ensuring a proper ML/TF risk management system	quarterly	quarterly
12	Report on the assessment of ML/TF risk (as part of the report on the results of the assessment of the Bank’s AML/CTF risk profile)	annually	annually
13	Report of the IAD on the assessment of the effectiveness of the Internal Control System.	annually	annually

18.3. The form (sections) and deadlines for submitting these reports are agreed separately by the relevant decisions of the bodies provided with these reports (Supervisory Board, Board/Board Committees)

## 20. CONTROL WITHIN THE INTERNAL CONTROL SYSTEM OF FUIB

In accordance with the “Policy on Organisation of the Internal Control System of JSC “FUIB”, the Bank implemented a three-level control of the banking risk:

ICS levels	Controller	Supreme Supervisory Authority
Self-control/Current control/Follow-up control	Employees assigned with control functions within the processes in accordance with the Bank’s internal documents, Heads of structural units, Members of the Board	Board/ALMC/ORMC/Credit Board/EBCC
Risk management and compliance control	CRO and risk management units (CBRD, SBRMD, RRD, GBRD, CMB, MRB)  CCO and compliance management units (including ML/TF risk) (CCB, FMD, FCSCFCOSP and MTPAC)	Supervisory Board of the Bank/Risk Management Committee
Internal audit	Internal Audit Department	Supervisory Board of the Bank/Audit Committee

	TRADE SECRET	Version 9.0.
	4. Risk management and internal control	
	<b>JSC “FUIB” Risk Management Policy</b>	

## 21. DOCUMENT REVIEW PROCEDURE

This Policy shall be updated at least once a year.