



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

POLICY

on Organisation of the Internal Control System 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.

ПУМБ	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

CONTENTS

1. INTRODUCTION.....	3
2. PURPOSE	3
3. SCOPE OF APPLICATION	5
4. TERMS, DEFINITIONS, AND ABBREVIATIONS.....	5
5. MAIN PART	10
5.1 STRUCTURE OF INTERNAL CONTROL SYSTEM OF JSC “FUIB”	10
5.2 PRINCIPLES AND ORGANIZATIONAL STRUCTURE OF THE ICS	17
5.3 ROLES, POWERS AND RESPONSIBILITIES OF PARTICIPANTS	22
5.4 MAIN COMPONENTS OF INTERNAL CONTROL SYSTEM.....	35
5.5 IMPLEMENTATION OF INTERNAL CONTROL SYSTEM OF JSC “FUIB”	41
6. CONTROL WITHIN THE INTERNAL CONTROL SYSTEM OF FUIB.....	42
7. DOCUMENT REVIEW PROCEDURE.....	43

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

1. INTRODUCTION

1.1. Given the rapid development of the banking system and the emergence of new high-tech products requiring a certain level of knowledge, experience and qualifications, as well as the need to achieve strategic goals, the Bank’s management understands the importance of implementing a number of recommendations of the Basel Committee and the National Bank of Ukraine, which regulate the implementation of an effective internal control system for the Bank’s activities as a whole, and guarantees prevention of events that negatively affect the continuity and quality of work of any banking organization.

1.2. At the same time, the management is aware of the importance of providing timely, complete and correct/reliable reporting to state supervisory authorities, and takes into account the negative experience of foreign and Ukrainian banks, as well as the catastrophic consequences for profit and profitability of the impact of internal and external fraud, the dependence of Ukrainian banks on the performance of systems and technologies, and possible penalties for failure to comply with the requirements of Ukrainian legislation.

1.3. The Bank’s strategic objectives in terms of creating an internal control system are:

- transition to banking process management;
- creation of a system that ensures and controls the process of compiling and providing reliable, complete, timely financial, statistical and other reporting;
- ensuring fraud prevention;
- compliance with legislative and regulatory acts, standards and internal documents of the Bank;
- creation of an internal control system in accordance with the COSO principles.


1.4. The JOINT-STOCK COMPANY “FIRST UKRAINIAN INTERNATIONAL BANK” Internal Control System Policy (hereinafter referred to as the “Policy”) was created to ensure the stability and security of the Bank, improve the processes of conducting banking operations and control procedures.

2. PURPOSE

2.1. The main purpose of the Internal Control System (ICS) is to provide the Bank’s management with a reasonable guarantee of achieving the Bank’s general goals and objectives, increase the level of internal control organization, the effectiveness of internal control functioning and improve the effectiveness of the tasks performed and ensure the stability, security and effectiveness of the Bank’s operations and processes.

2.2. Objectives of implementing the Internal Control System in JSC “FUIB” (ICS):

- ensuring the efficiency of operations, protection against potential errors, violations, losses, damages of the Bank’s activities;
- ensuring the functioning of a comprehensive, adequate and effective risk management system;
- providing adequate, comprehensive, complete, reliable, accessible, timely information to users (interested units) for appropriate management decisions;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- reliability, completeness, objectivity and timeliness of preparation and provision of financial, statistical and other reporting to internal users, shareholders, Clients, counterparties and/or state supervisory authorities;
- timeliness and reliability of accounting treatment of the Bank’s operations;
- compliance (monitoring the Bank’s compliance (fulfilment) of the requirements of the legislation, regulatory legal acts, market standards, rules of fair competition, rules of corporate ethics, internal banking documents, as well as procedures for resolving conflicts of interest;
- effective personnel management;
- implementation of processes targeted operational models with a sufficient level of automation and the presence of the necessary number of control preventing and/or minimizing the materialization of potential risks identified by the Bank as significant;
- preventing the Bank from engaging in illegal financial transactions, including preventing the Bank’s Clients (residents and non-residents) from conducting illegal currency transactions, preventing and detecting financial transactions related to the legalization of proceeds from crime and the financing of terrorism;
- preventing the materialization of all significant risks inherent in the Bank’s products/services by identifying, analysing and assessing them in accordance with the Risk Management Policy of the JSC “FUIB” and establishing appropriate control within the scope of the ICS in two main areas:
 - optimization/refinement of existing services, expansion of the line of existing banking products/services, new channels for their sale, assessment of their intended use, target segment for their sale and other ML/TF risks;
 - introduction of new products and significant changes in accordance with the Policy for the introduction of new products and significant changes in the activities of JSC “FUIB”.


2.3. The internal control system of JSC “FUIB” ensures the achievement of operational, information and compliance activity objectives.

- ***Operational objectives:***

- ensuring that control procedures are focused on the effectiveness of managing the Bank’s assets, liabilities and off-balance sheet items in order to achieve profitability of Bank’s activities, avoiding or limiting losses occurred as a result of negative internal and external factors;
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 of the Bank’s activities:***

ensuring the integrity, completeness and reliability of financial, management and other information used to make management decisions and create information flows both vertically and horizontally within the Bank’s organizational structure. Such information includes the Bank’s reporting on financial and non-financial issues provided to external and internal users.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- ***Compliance objectives of the Bank’s activities:***

compliance of the activities of JSC “FUIB” with the requirements of the legislation of Ukraine, regulations of the NBU, internal banking documents, standards of professional associations applicable to the Bank.

3. SCOPE OF APPLICATION

3.1. This Policy applies to all structural units, all employees and all processes of the Bank.

4. TERMS, DEFINITIONS, AND ABBREVIATIONS

Bank is JSC “FUIB”, JOINT STOCK COMPANY “FIRST UKRAINIAN INTERNATIONAL BANK” (hereinafter referred to as the “Bank”).

Business units (units of Business Lines: Retail Business, Corporate Business, Financial Leasing, Investment Business and Treasury Operations, Processing Centre, Collection and Transportation of Valuables, Depository Institution, etc.) – structural units of the Bank:


- initiating and carrying out current control of a banking transactions with one of the categories of Clients: corporate clients, individuals, small and medium-sized businesses, financial organizations, as well as companies operating in financial markets (for example, organizations engaged in treasury, depository operations, securities trading, etc.);
- providing services to Partner Banks regarding optimization and servicing of operations related to electronic payment instruments;
- carrying out cash collection and currency assets transportation activities.

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

The Bank’s internal regulatory documents are divided into 2 groups: normative (policies, regulations, procedures, instructions) and regulatory (orders, instructions), which regulate the Bank’s activities, including the procedure for implementing Bank’s internal control. In the document also referred to as the abbreviation – “BIRD”.

Internal audit is an independent, objective activity providing assurance and consulting services by the assessment of the Bank’s systems and processes, which should benefit the Bank and improve its activities. Internal audit is an integral part of the Bank’s internal control system and is introduced by the Bank’s Supervisory Board aimed at assessing and improving the Bank’s internal control system, providing the Supervisory Board and the Board with the necessary support (assistance) in the performance of their duties to achieve the Bank’s goals.

Internal control – processes (sets of measures) of the Bank, integrated into all its processes and corporate governance, aimed at achieving operational, informational, compliance goals of the Bank’s activities, including ensuring the efficiency and effectiveness of the Bank’s operations, the efficiency of asset and liability management, banking risks, ensuring the reliability, completeness and timeliness of the preparation and submission of financial, statistical and other reporting, fraud prevention, compliance with legislative and regulatory legal acts, standards and internal documents, and professional ethics requirements.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

Additional control is carried out by responsible employees during preliminary and current control (if necessary) if such control can minimize the materialization of the most undesirable operational risks (mainly – internal fraud). The list of operations subject to additional control, a description of the rules/procedures and features of its implementation for each type of operation is set in the Bank’s internal documents. The employee who carried out the additional control signs a record document (in paper and/or electronic form) confirming the fact of such control.

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).


Information resource is information and resources related to its processing that are valuable to the Bank. The Bank’s information resources include information, software, computer and telecommunications equipment, removable mediums, and services.

Information security is a set of Bank’s organizational measures, software and technological means that operate at all organizational levels of the Bank and ensure the protection of information from any accidental and/or intentional threats, which may result in a violation of the availability, integrity, and confidentiality of information on the activities of the Bank or its clients.

IT system is a set of methods, production, software and technological means combined into a technological chain that ensures the collection, storage, processing, output, and distribution of information.

Support units – structural non-business units of the Bank, which, within the scope of their powers, influence/are able to directly influence sources of risk at the first level of control (line of defence), participate in the implementation of business processes by introducing additional control mechanisms and/or measuring control results.

- 1) The Financial Accounting and Tax Reporting Department headed by the Chief Accountant of the Bank, performs accounting control over the correctness of the banking transactions accounting, checks other units compliance with the requirements established by the Accounting Policy of the Bank for accounting for the results of operations and the preparation of financial and statistical reporting;
- 2) The Financial Controlling Department – ensures monitoring and control of compliance with the strategic course and target parameters of business development (including costs, profitability and efficiency of business);
- 3) The Security Department – is the owner of:

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- Fraud Risk Management System (FRMS), ensures insider threat management (participation in personnel administration), fraud risk management, which is subsystem of the Operational Risk Management System (ORMS);

- Physical Security Management System (PSMS), which is subsystem of the Operational Risk Management System (ORMS), ensuring security and management of access to the Bank's facilities and premises;

4) Information Security Department is the owner of the Information Security Management System (ISMS), develops it according to the risk-oriented approach provided for by international standards and requirements of the NBU, manages information security risk (including cyber risk) and ensures the information security of the Bank, including the protection of banking and commercial secrets, which is a subsystem of the Operational Risk Management System (ORMS);

5) Operational Support Centre – identifies errors of the Bank's units during the implementation/support of banking operations and ensuring the functioning of a unified internal control system for the correct accounting treatment of banking operations with clients in the accounting system; the OSC also checks the effectiveness of employees of departments / sectors of control and operational activities of the RC and branches, as well as deputy managers of departments for control and operational activities (DCOA), assesses their effectiveness and introduces measures to eliminate systemic shortcomings and improve the Bank's business processes at the regional network level;

6) Collection and Money Circulation Department carries out on-site scheduled and unannounced inspections of cash discipline and cashiers and employees of collection units compliance with established requirements for transactions and their documenting;

7) Marketing Department (under the competence of the CMB of the MD) monitors compliance of front office employees with customer service standards, organizes the process of considering customer and other persons' requests, customer wishes and complaints, and assesses the main systemic shortcomings that arise during customer service;


8) Legal Department – monitors employees' compliance with the requirements of the legislation and the Bank's internal requirements;

9) Transaction Monitoring Centre monitors and controls transactions on the Bank's clients' accounts, including using the BPC, partner banks and financial companies;

10) Information Technology Department – monitors and controls the serviceability and compliance of information and communication technologies with the business needs of the bank, as well as controls their sustainable functioning, manages the information and communication technologies risk.

The main task of the Support Units is to support operations/functionality, ensure proper control over the efficiency of both the Business Units and the Support Units, and counteract the materialization of risks.

Operational Risk Management Committee (ORMC – Collegial body for operational risk management) is a management body of the Bank, established to consider the most resonant operational risk events, make unified management decisions to minimize the consequences and

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

prevent future events, promote a culture of operational risk management and control in the Bank, approve risk appetites, take preventive measures based on management reporting, determine priorities in operational risk management and control, assess the effectiveness of measures taken by the Subcommittees and assess the effectiveness of the Internal Control System (within the powers delegated by the Board).

Compliance is the Bank’s activity aimed at identifying, assessing, preventing and eliminating 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.


The Bank’s operational activities are a set of technological processes related to documenting information on the Bank’s operations (hereinafter referred to as “operations”), their registration in the relevant registers, verification and control over operational risks.

The operational process model is a target process model with a sufficient level of automation, based on the principles of an effective three-level internal control system and meeting the requirement that one Bank employee cannot simultaneously initiate, control and record banking operations.

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”) in accordance with the legislation of Ukraine.

Risk Management Units (Risk Management Vertical) – units headed by heads of units and subordinate to CRO, ensuring the performance of risk management functions defined by the legislation of Ukraine:

- General Banking Risk Department (GBRD) – a unit responsible for consolidating all operational risk events of the Bank and preparing regular reporting for the ORMC and for managing market risks and interest risks in the banking book, and also preparing reports for the ALMC.
- Corporate Business Risks Department (CBRD) – a unit that ensures the management of credit risks to which the Bank is exposed during lending to large and medium-sized corporate businesses, as well as the control of these risks within the Bank’s internal control system.
- Small Business Risk Management Department (SBRMD) – a unit that ensures the management of credit risks to which the Bank is exposed during lending to small-sized corporate businesses, as well as the control of these risks within the Bank’s internal control system.
- Retail Risks Department (RRD) – a unit that ensures the management of credit risks to which the Bank is exposed during lending to retail businesses, as well as the control of these risks within the Bank’s internal control system.
- Microcredit Risk Department (MRD) – a unit that ensures the management of credit risks to which the Bank is exposed during lending to Microcredit clients, as well as the control of these risks within the Bank’s internal control system.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- Collateral Management Body (CMB) – a unit that ensures the management of collateral risks to which the Bank is exposed in the process of lending to corporate and retail clients, as well as the control of these risks within the Bank’s internal control system

Professional ethics – a system of moral and ethical norms and rules, based on the principles of honesty and integrity, determining the minimum behaviour requirements of a Bank employee for the specific activity and specific situations.

COSO Principles (Committee of Sponsoring Organization) – Internal Control Concept principles in accordance with the best international practice.

The Bank’s **Internal Control System (ICS)** is a set of the Bank’s organisational structure, procedures and internal control measures aimed at:

- achieving the Bank’s goals, including the fulfilment of its planned performance indicators, ensuring the efficiency and effectiveness of the Bank’s operations, and preservation of its assets;
- ensuring the effectiveness of corporate governance in the Bank through the functioning of a comprehensive, efficient and adequate risk management system; ensuring the completeness, timeliness and reliability of financial, statistical, management and other reporting; compliance of the Bank’s activities with the legislation of Ukraine, regulations of the National Bank of Ukraine, standards of professional associations applicable to the Bank and internal documents.

Risk management system is a set of duly documented and approved policies, methods and procedures for risk management, which determine the procedure of actions aimed at implementing the systematic process of identification, measurement, monitoring, control, reporting and mitigation of all types of risks at all organizational levels.


Risk is a probability of occurrence of losses or additional losses, or a revenue shortfall, or a party’s failure to fulfil its obligations due to the influence of negative internal and external factors.

Risk avoidance – refusal to carry out certain transactions or termination of business relationships that expose the Bank to risk.

Member of the Board (CCO) means the Bank’s chief compliance officer, performing the functions of the chief compliance manager (hereinafter referred to as the “CCO”) and the function of the employee responsible for Bank’s financial monitoring.

Compliance management units (including ML/TF risk) (Vertical compliance management (including ML/TF risk)) – units headed by their respective heads and subordinate to the CCO, which monitor compliance with the norms (compliance) and identify facts of legalization (laundering) of proceeds from crime funds, financing of terrorism, facts of violation of the legislation of Ukraine within its competence set by the legislation of Ukraine:

- **Compliance Control Body (CCB)** – a compliance control unit that ensures the performance of compliance risk management functions, determined by the legislation of Ukraine.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- Financial Monitoring Department (FMD) – a unit that ensures control over the implementation of ML/TF risk management functions and the requirements of Ukrainian legislation in the field of combating money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.
- Foreign Currency Surveillance and Clients Foreign Currency Operations Support Department (FCSCFCOSP) – a unit that ensures control over the implementation of risk management functions in the field of currency supervision and ensures compliance with the requirements of Ukrainian legislation for currency control.
- Methodology, Transformation and Processes Automation Centre (MTPAC) is a unit that provides methodological expertise, process automation, expert support, management of transformation processes and projects related to the functions of compliance management units.

Risk management is a systematic process of identifying, assessing, minimizing/eliminating, monitoring and controlling potential events or situations to provide sufficient confidence in achieving the Bank’s goals.

Functional control is a control activity carried out by the Bank’s employees responsible for implementing regular internal control over the compliance of job functions performed by the Bank’s employees with their job descriptions.

SB – Supervisory Board


5. MAIN PART

5.1 STRUCTURE OF INTERNAL CONTROL SYSTEM OF JSC “FUIB”

5.1.1. The Policy regulates the main steps of implementing the internal control system (hereinafter referred to as the “ICS”), the roles and areas of responsibility of all structural units of the Bank involved in establishing, implementing and performing internal control. The Bank’s ICS is based on the principles developed by COSO.

5.1.2. This Policy has been developed taking into account the requirements of:

- The Law of Ukraine “On the National Bank of Ukraine”;
- Law of Ukraine “On Banks and banking activity”;
- The document of the Basel Committee on Banking Supervision “Principles for the Assessment of Internal Control Systems”, taking into account generally accepted international principles and standards;
- Regulation “On Organization of Risk Management System in Banks and Bank Groups of Ukraine” approved by the NBU Board Resolution No. 64 dated 11.06.2018);
- Regulation “On the Organization of Accounting, Accounting Control during Implementation of Operating Activities in Banks of Ukraine” (Resolution of the NBU No. 75 dated 04.07.2018);
- Regulation “On Organization of internal control in Banks and Bank Groups of Ukraine” (NBU Board Resolution No. 88 dated 02.07.2019);

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- Regulation “On Organization of internal audit in Banks Ukraine” (NBU Board Resolution No. 311 dated 10.05.2016);
- Regulation “On Financial Monitoring Carried out by Banks” (NBU Board Resolution No. 65 dated 19.05.2020);
- The recommendations of the Basel Committee on Banking Supervision on risk management, contained in the current convention (Basel II, June 2006);
- The COSO’s internal control concept (Internal Control Framework), as amended in 2013;
- recommendations of Basel Committee on Banking Supervision: “Compliance and compliance function in banks” (April, 2005)
- JSC “FUIB” Risk Management Policy.

5.1.3. The Internal Control System of JSC “FUIB” has the following structure:


- control environment,
- management of risks inherent in the Bank’s activities,
- control activities in the Bank,
- control over information flows and communications of the Bank,
- monitoring the effectiveness of the Bank’s ICS.

5.1.4. The ICS shall be implemented at each of the Bank’s organisational levels:

- **Control environment** – a set of subjects of the Bank’s internal control system, procedures, policies for each separate activity of the Bank as well as other internal control banking documents, and control culture. Internal control culture – employees’ compliance with the Bank’s principles, rules, norms aimed at informing Bank employees about the functioning of the internal control system and the role of each employee in this activity.
- **Risk management** includes the identification and analysis of significant risks for further determination of risk management measures. The assessment is carried out in accordance with the Bank’s approved Risk Management Policy, regulations, procedures, instructions for each type of risk.
- **Control activities** consist of policies and procedures that can guarantee the implementation of instructions and risk minimization measures. Control measures must be developed for all levels of the internal control system and for any functions of Bank employees.
- **Information and communication** (control of information flows) – information about identified risks must be documented and timely provided to the units responsible for minimizing risks and implementing control.
- **Monitoring of the ICS effectiveness**: The Supervisory Board of the Bank ensures regular control (at least once a quarter) over the effectiveness of the internal control system and ensures the functioning and control over the effectiveness of the risk management system.

5.1.5. The Board of the Bank ensures the implementation of tasks and decisions of the Supervisory Board of the Bank on the implementation of the risk management system, on the ICS and carries out constant monitoring of the effectiveness of the ICS.

5.1.6. The Bank ensures the functioning of the internal control system by:

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- ✓ management control over compliance with legislation of Ukraine and internal documents of the Bank;
- ✓ management of conflict of interest situations;
- ✓ allocating responsibilities within the Bank’s activities;
- ✓ implementation, ensuring the functioning and control over the effectiveness of the risk management system (including when considering business initiatives to create/optimize/improve products and services);
- ✓ controlling information security and information exchange;
- ✓ introduction of internal control procedures;
- ✓ conducting regular monitoring of the internal control system;
- ✓ introduction of internal audit procedures.

5.1.7. The subjects of the Bank’s internal control system are:

- the Supervisory Board and its committees (Risk Management Committee, Audit Committee and Remuneration and Nomination Committee, etc.);
- Board;
- Collegiate bodies of the Board of the Bank (ORMC, ALMC, etc.).
- Internal Audit Department;
- CRO and risk management units (CBRD, RRD, SBRMD, GBRD, CMB, MRB);
- CCO and compliance management units (including AML/CFT risk) (CCB, FMD, FCSCFCOSP and MTPAC);
- Business units and support units and their managers, as well as all employees carrying out internal control in accordance with the powers defined by the Bank’s internal documents and job descriptions.

5.1.8. The Bank ensures a clear allocation of responsibilities, powers and duties between all subjects of the internal control system.

5.1.9. According to the “Regulation On Organization of Internal Control System in Ukrainian Banks and Banking Groups” approved by NBU Board Resolution No. 88 dated 2.07.2019 and the Law of Ukraine “On Banks and Banking Activities” the Internal Control System and Risk Management System of FUIB provide for three levels of control (three lines of defence):


1. Bank’s business units and supporting units;
2. Risk management units and compliance management units (including ML/TF risk);
3. Internal Audit Department.

Namely:

- **The first level of control (line of defence) includes business units and support units.**

They are the owners of all risks (especially operational, compliance risks and ML/TF risk) that arise in their field of activity. These units perform current risk management and are responsible for identifying and assessing risks, taking management actions and reporting on such risks.

IMPORTANT! At the first level of control (line of defence), the Bank appoints employees of the units responsible for internal control of operational risk – risk officers within the framework of the

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

Operational Risk Management System (ORMS), which perform additional functions in terms of operational and compliance risk management (including ML/TF risk) (identify events, ensure their recording, informing units of the second level of control (line of defence), etc.).

The risk management functions of the first level of control (line of defence) include:


- development of process maps (technological cards) owned by units that are also used to organize the implementation of these processes, as well as for development and implementation of an effective internal control system;
- interaction with Risk Management Units, Compliance Management Units (including ML/TF risk) to resolve identified risks and implement measures to minimize their consequences, as well as to prevent them in further activities;
- current and further control over compliance with the requirements of legislation, regulatory legal acts, market standards, rules of fair competition, rules of corporate ethics, the conflicts of interest, as well as internal risk management documents within business processes;
- conducting training and ensuring awareness of employees of related units on issues of their competence, including the requirements of internal risk management documents;
- complete and timely collection and entry of information on the facts of risk materialization;
- facilitating and ensuring the implementation of constant monitoring and reporting to the Risk Management Units and Compliance Management Units (including ML/TF risk) on the dynamics of their values in the unit;
- participate as experts in the creation of scenarios for scenario analysis of risks and ensure the involvement of experts of the unit in scenario analysis and stress tests;
- ensure unit’s identification and assessment of the risks inherent in new products / significant changes in the Bank’s operations;
- conducting self-assessment of banking risks on the basis of methodological principles introduced by the Risk Management Units and Compliance Management Units (including ML/TF risk);
- ensure the compilation of management reporting on risks.

During their activities all structural units of the Bank are responsible for compliance with the requirements of the Bank’s internal risk management documents.

- **The second level includes the Risk Management Units and Compliance Management Units (including ML/TF risk).**

The risk management functions of the second level control include:

- development, implementation and continuous modernization of a system for managing individual types of risks;
- ensuring timely identification, measurement, monitoring, control, mitigation and reporting on significant risks;
- assessment of the value of the Bank’s risks, including assessment based on the information provided by the employees of first-level units;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- advising the Bank’s structural units on risk management issues;
- training and rising awareness of the Bank’s employees on risk management;
- 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;
- generating consolidated reports on the results of risk management and their submission to the Supervisory Board of the Bank at least once a quarter, to the Board of the Bank – at least once a month/quarter, and in the event of identifying situations requiring urgent notification – to the Supervisory Board of the Bank no later than the next business;
- influencing the adoption of decisions that expose the Bank to significant risks, and, if necessary, taking all possible measures to properly inform the Supervisory Board of the Bank, the Board of the Bank in order to prevent the adoption of such decisions;
- control of the implementation of measures to avoid, transfer and mitigate risk;
- participation in the development of process maps;
- planning and conducting scenario analysis and stress testing;
- coordination or control over the development of a business continuity plan depending on the chosen process management model;
- coordinating and conducting analysis of the results of the banking risk self-assessment;
- providing expert opinions, coordinating the results of analysis and assessment of risks inherent in new products / significant changes in the Bank’s activities carried out by the units of the first control level (line of defence);
- analysis of outsourced risks inherent in the Bank’s activities;
- forming proposals on the Bank’s risk insurance policy.

○ **The third level of control (line of defence) includes the Internal Audit Department**

The functions of the Internal Audit Department include:

- review and assessment of processes that ensure the Bank’s activities, including those that carry potential risk and the implementation of which is ensured by involving legal entities and individuals on a contractual basis (outsourcing);
- assessment of the effectiveness and adequacy of the Bank’s corporate governance, internal control system, including risk management system, Bank management processes, their compliance with the Bank size, complexity, volumes, types, nature of operations carried out by the Bank, organizational structure and risk profile of the Bank, taking into account the specifics of the Bank’s activities as systemically important and/or the activities of the banking group to which the Bank belongs, organization of the internal system for preventing and combating ML/TF, ML/TF risk management system;
- review the Bank’s management processes, the capital and liquidity adequacy assessment process, and means of ensuring the preservation of assets, taking into account the Bank’s risks;

ПУМБ	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- verification of the correctness and reliability of Bank’s accounting, information, financial and other reporting, their completeness and timeliness of submission, including to the NBU, state authorities and management bodies supervising the Bank’s activities;
- independent assessment of the control system implemented by the Bank’s management, in particular:
 - compliance of Bank’s managers and employees involved in the provision of banking and other financial services with the requirements of the legislation of Ukraine, including regulatory legal acts of the NBU, and internal regulations of the Bank, their fulfilment of professional duties and rules established by the Bank’s Articles of Association and internal documents of the Bank, including on compliance and risk management issues;
 - identifying and analysing facts of Bank employees’ violations of the requirements of the legislation of Ukraine, professional standards, and internal regulations that regulate the Bank’s activities;
 - timeliness of elimination of deficiencies identified by the NBU and other state authorities and management bodies supervising the Bank’s activities;
- independent assessment of the reliability, effectiveness and integrity of the Bank’s information systems and processes management (including relevance, accuracy, completeness, availability, confidentiality and comprehensiveness of data);
- inspection of financial and business activities of the Bank;
- assessing the effectiveness and adequacy of the Bank’s recovery plan;
- assessing the activities of the Risk Management Units, Compliance Management Units (including ML/TF risk), and committees established by the Bank, and the quality of risk reports provided to the Supervisory Board and the Board of the Bank;
- identifying and examining abuses of powers by the Bank’s officials and conflicts of interest in the Bank;
- provision of consulting services within the Bank and in the absence of a threat to independence, performance of other functions related to supervision of the Bank’s activities, stipulated by the legislation of Ukraine.

The assessment of the effectiveness of the internal control system is provided by internal audit directly to the Supervisory Board and the Board based on the results of the inspections, taking into account the approved procedures for internal audits.

5.1.10. JSC “FUIB” has a three-level of internal controls within the ICS which is defined by the BIRD in the mandatory section “Control within the ICS of FUIB”.

5.1.11. The Bank has the following types of controls:

- depending on the time of control:
 - **preliminary** – precedes any actions or operations;
 - **current** – is carried out during an action or operation;
 - **subsequent** – is carried out after an action or operation and is aimed at identifying deficiencies, correcting mistakes;

ПУМБ	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- **Additional control** is carried out by responsible employees during preliminary and current control (if necessary) if such control can minimize the materialization of the most undesirable operational risks (mainly – internal fraud).

Example of additional control: As of the end of the last business day of the reporting period the following account balances which are assessed as having a high probability of operational risk materialization are subject to mandatory verification: transit accounts; accounts receivable and accounts payable, transactions with clients, counterparties of the Bank and intra-bank transactions; balances and amounts transferred on loro, nostro accounts; balances of dormant accounts.

The results of the analysis of the verified records enable determination of the nature, amounts and reasons for discrepancies. In case of discrepancies entries in the accounting registers are made in accordance with the primary documents and/or available assets.

The Bank ensures a consistent combination of preliminary, current and subsequent controls to increase the effectiveness and efficiency of control.

- depending on the purpose of control:
 - **preventive** is aimed at preventing violations and risks (including risk control when considering business initiatives to create/optimize/improve products and services);
 - **detective** is aimed at identifying risks;
 - **corrective** is aimed at avoiding/mitigating materialized risks;
- depending on the subject of control:
 - **independent control** is carried out by the employee independently;
 - **double control** is carried out by two (or more) employees (the principle of “two pairs of eyes”);
 - **collegial control** is exercised by the collegiate body;
 - **automated control** is carried out by an automated system;
- depending on the frequency:
 - **functional (permanent)** is carried out on a regular basis;
 - **periodic** is carried out in accordance with the frequency established by internal banking documents;
- depending on the scope of control:
 - **full** – covers the entire scope of the relevant Bank process;
 - **portfolio** covers certain group of functions, operations, contracts;
 - **selective** – covers selected elements of the relevant Bank process.

5.1.12. The main areas of the Bank’s internal control include:

- control over achieving the objectives of the Bank’s activities, including the objectives set out in the Bank’s strategy and business plan;
- control over ensuring the efficiency of the Bank’s financial and business activities in the course of banking and other operations;

ПУМБ	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	


- control over the efficiency of asset and liability management;
- control over the safety of the Bank's assets;
- control over the effectiveness of the risk management system;
- control over 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;
- control over the accuracy, completeness, objectivity and timeliness of accounting, preparation and disclosure of financial and other reports for external and internal users;
- management of information flows, including receiving and transmitting information, ensuring the functioning of the information security management system.

5.1.13. For the proper functioning of the ICS the Bank ensures the availability of appropriate employees, equipment, software, and premises that meet the requirements established by the National Bank of Ukraine.

5.2 PRINCIPLES AND ORGANIZATIONAL STRUCTURE OF THE ICS

The Bank creates a comprehensive, effective and adequate internal control system (ICS) complying with the following principles:

- comprehensiveness and complexity – implies that the Bank has implemented each of the five components of the internal control system in its activities and ensures their implementation in an inter-integrated manner, i.e. the results of the implementation of such component shall be used in the implementation of other components of the internal control system; internal control procedures are incorporated into the Bank's processes at all organisational levels;
- effectiveness – i.e., internal control measures are efficient and ensure achievement of the set objectives of the Bank's activities and reasonable assurance that:
 - ✓ transactions are efficient and reflected correctly in information systems of the Bank/accounting systems;
 - ✓ financial, statistical, management, tax and other reports are reliable;
 - ✓ The Bank complies with the requirements of the legislation of Ukraine, regulations of the National Bank of Ukraine, and internal documents;
 - ✓ The Bank's employees have the necessary information on the components of the internal control system and ensure the implementation of these components within the competence and authority defined by their job descriptions;
 - ✓ The Bank shall ensure identification and assessment of deficiencies in the internal control system and take timely, adequate and sufficient corrective measures to correct such deficiencies;
- adequacy – implies that the internal control system meets the specifics its activities, including the size, business model, scope of activities, types, complexity of operations, risk profile;
- prudence – ensuring sufficient confidence of the managers in achieving the objectives of the Bank's activities based on conservative assumptions and considering a certain probability of erroneous judgements or decisions of the Bank's managers and/or employees;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- risk-based orientation – the Bank shall ensure the organisation and functioning of the internal control system based on the risk-based approach, which provides for the application of more in-depth and frequent control measures to those areas of activity that are subject to greater risks
- integrity – implies that control procedures shall be an integral part of all processes of the Bank’s activities and corporate governance;
- timeliness – implies that the internal control system shall be capable of detecting potential threats of negative impact on the Bank’s activities before such threats actually occur;
- independence – stipulates that the Bank shall avoid circumstances that may pose a threat to the impartial performance of its internal control system by the subjects of its internal control functions;
- continuity – stipulates that the Bank’s internal control activities allow for the prevention, detection and elimination of internal control system deficiencies on an ongoing basis and in a timely manner;
- confidentiality – stipulates that the Bank shall not disclose information to persons who are not authorised to receive it

Internal Control System of the JSC “FUIB” is based on 5 main pillars (components) and, accordingly, the COSO principles:

1. Control environment:


- 1.1. Demonstration of a commitment to ethical values (Corporate Code and development of corporate culture);
- 1.2. Responsibility for the implementation of control functions (definition of control functions in job descriptions, regulatory documents, administrative documents of the Bank);
- 1.3. Clearly defined organizational structure, powers and responsibilities (component of Corporate Governance);
- 1.4. Responsibilities are distributed according to competence;
- 1.5. Responsibility for results is fixed at the level of the entire Bank.

2. Risk management:

- 2.1. Risk identification and monitoring;
- 2.2. Risk identification, recording and assessment;
- 2.3. Fraud risk assessment in processes;
- 2.4. Significant change identification and assessment.

3. Control activities:

- 3.1. Control processes are clearly defined and selected for implementation;
- 3.2. Clearly defined general controls over technologies (within the framework of the ISMS, the FRMS);

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

3.3. Control activities are formalized in procedures (according to the mandatory section of any regulatory document of the Bank – **“CONTROL WITHIN THE INTERNAL CONTROL SYSTEM OF FUIB”**)

4. Information and communication:

- 4.1. Preparation of reporting on control quality;
- 4.2. Formalized transfer of information within the Bank;
- 4.3. Reporting outside the Bank only after management’s approval.

5. Monitoring:

- 5.1. Current and periodic controls and assessments (1st and 2nd levels of control within the scope of the ICS);
- 5.2. Assessment and further consideration of reports on identified deficiencies (3rd level of the ICS).


The FUIB’s Internal Control System is based on a clear division of powers of the Supervisory Board and the Board of the Bank, other collegial bodies, as well as structural units and/or employees of the Bank in order to prevent duplication of functions.

Effective control is ensured by:

- process integration (implementation of control into the process);
- regular risk assessment;
- development and implementation of risks minimization measures with subsequent assessment of their effectiveness.

The Internal Control System (ICS) provides:

- 1) double control ensured by the “two pairs of eyes” principle during the Bank’s operations, and according to which the implementation and control of operations cannot be performed by one person;
- 2) clear division of duties, powers and responsibilities between the Bank’s management bodies, its structural units, employees to avoid their duplication;
- 3) a thorough and comprehensive preliminary analysis of the Bank’s operations for promptly preventing illegal (incorrect or unauthorized) operations;
- 4) further analysis of the Bank’s operations in order to:
 - ensure proper recording of legal operations;
 - ensure prevention of any illegal operations in the future;
- 5) ensure timely and reliable accounting treatment of the Bank’s operations;
- 6) fulfil requirements for organizing information protection in hardware and software suites in accordance with the regulatory legal acts of the National Bank of Ukraine;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- 7) implementation and functioning of the information security management system in accordance with the standards of the National Bank of Ukraine, international standards and requirements of state bodies exercising control in the field of information security;
- 8) protection against personnel deliberate actions harmful for the Bank, as well as personnel errors, their prevention and control;
- 9) personnel training based on an analysis of the qualifications of the existing staff, compliance with experience and knowledge of the process and existing software requirements, as well as statistics of mass errors (source – human factor) for the Bank as a whole;
- 10) Bank’s compliance with legislative norms and other mandatory requirements;
- 11) prevention of conflict of interest and their resolution;
- 12) protection of the image and reputation of the Bank.

Principles of control:


- **strategic orientation** (control must support the general priorities of the Bank);
- **commitment to results** (measuring and announcing changes is important only as a means of achieving goals or for their timely correction);
- **compliance with actions** (identification of important aspects of the controlled activity);
- **control timeliness** (the time interval between measurements and evaluation of results must adequately correspond to the controlled event);
- **adaptability of control** (control, as well as plans, must promptly adapt to the changes);
- **control simplicity** (the most effective control is rather simple from the point of view of its goals);
- **economic feasibility of control** (the total costs of the control system must be less than the benefits that it provides).

FUIB distinguishes 3 main types of control which are base for the analysis of processes (in terms of their adequacy):

- 1) self-control (activities to prevent, identify and correct problems and errors are carried out by the employee on his initiative).
- 2) automated control (control is performed by the software/AS using a built-in algorithm).
- 3) control by another employee (control is performed by an employee of the next/other stage of the process, which is assigned to him by a role model or through job duties).

The internal control system covers all stages of the Bank’s activities and includes:

- 1) preliminary control, which is carried out before the actual implementation of operations and is provided by:
 - recruitment of personnel – a thorough analysis of the business and professional qualities of candidates for vacant positions, improving the professional level and qualifications of employees;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- attraction and placement of funds – a preliminary analysis of the riskiness and effectiveness of the Bank’s operations, determining the optimal means and methods for their implementation in order to avoid or minimize possible losses and risks;
- material resources – an analysis of the quality and level of provision of the Bank with the necessary technical means, equipment, banking automation systems with modern information technologies that correspond to the volume and complexity of its operations;
- selection of suppliers of goods, works and services – a thorough analysis of the business reputation and level of employees expertise, adherence to the principle of diversification of suppliers and preventing the concentration of order volumes to one supplier;
- development and implementation of new products through a preliminary analysis of the risk and effectiveness of the product/service to be introduced.

2) current control, which is carried out during the Bank’s operations and includes control over compliance with legislative acts and internal documents of the Bank, the procedure for making decisions on their implementation, control over the completeness, timeliness and reliability of data in accounting and reporting, control over the preservation of the Bank’s property;

3) subsequent control, which is carried out after the Bank’s operations and consists in checking the validity and correctness of the operations, the compliance of documents with the established forms and requirements, the compliance of the duties performed by employees with their job descriptions.

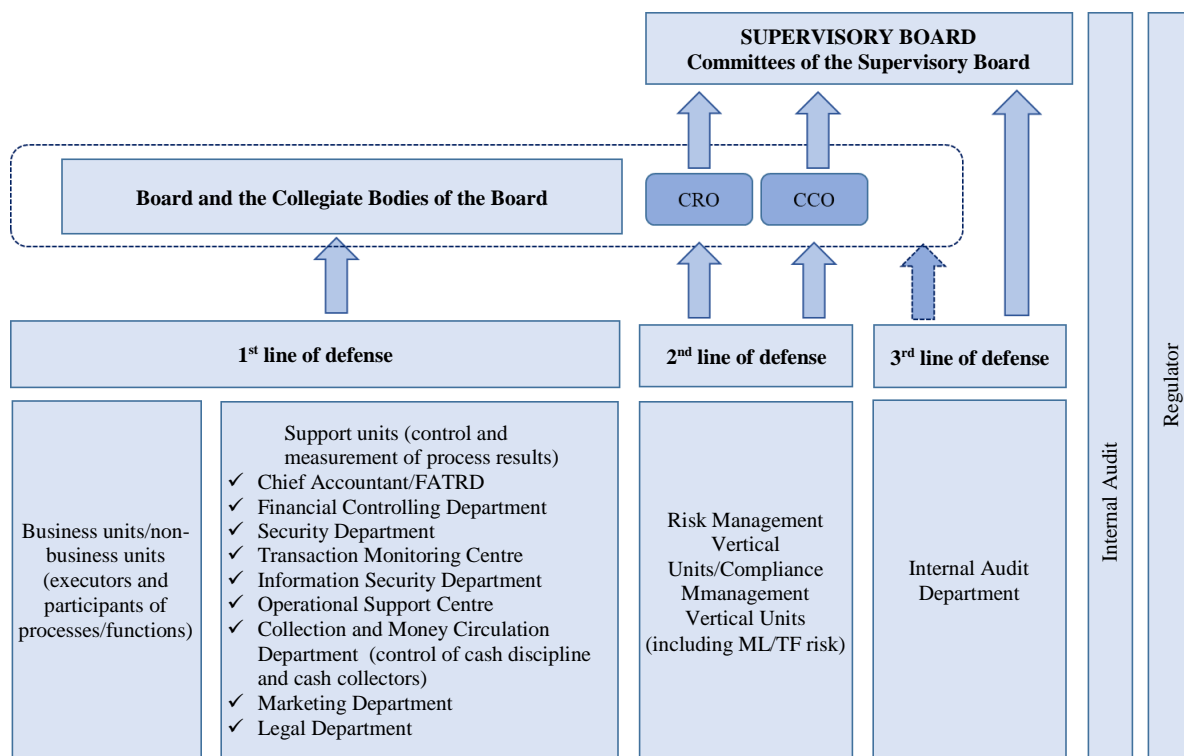
The Bank ensures the implementation of internal control procedures for current activities on a daily basis.

Organizational structure of the internal control system (ICS):

3rd level of control (line of defence) of the ICS	Internal Audit Department	Reports to the Supervisory Board and the Audit Committee of the SB
Second level of control (line of defence) of the ICS	Risk Management Vertical: CRO and CBRD, SBRMD, RRD, GBRD, CMB, MRB;	Report to the Supervisory Board and the Audit Committee of the SB and the Risk Management Committee
	Compliance Management Vertical (including ML/TF risk): CCO and CCB, FMD, FCSCFCOSP and MTPAC.	Report to the Supervisory Board and the Audit Committee of the SB and the Risk Management Committee Inform the Board and the Collegiate Bodies of the Board

ПУМБ	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	


1st level of control (line of defence) of the ICS	Business units/non-business units and support units (all Bank employees)	Report to the Board and collegial bodies of the Board
---	--	---



5.3 ROLES, POWERS AND RESPONSIBILITIES OF PARTICIPANTS

To ensure the effectiveness of the internal control system, the **Supervisory Board of the Bank** shall:

- approve the Bank's strategy and business plan and monitors their implementation;
- create and ensure the functioning of an adequate and effective internal control system corresponding to the size of the Bank, complexity, types, volumes, nature of the operations carried out by the Bank, its organizational structure and risk profile;
- provide regular control (at least once a quarter) over the effectiveness of the internal control system;
- monitor the effectiveness of the internal control system;
- ensure functioning and control over the effectiveness of the risk management system;
- consider the managerial risk reporting and makes decisions on the application of adequate risks mitigation measures;
- take measures to prevent conflicts of interest, promotes their settlement, as well informs the National Bank of Ukraine of conflicts of interest arising in the Bank;
- approve the Bank's internal documents on the organization of the internal control and risk management system;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- distribute the responsibilities and powers between the members of the Supervisory Board, as well as persons responsible for internal control, heads of the risk management and the compliance control units;
- consider the comments and recommendations of the National Bank of Ukraine, other state authorities and management bodies supervising the activities of the Bank, the Internal Audit Department, external auditors on the organization of the internal control system, and monitor the elimination of identified deficiencies;
- monitor the Bank’s Board prompt response and elimination of deficiencies of the internal control system;
- approve the Bank’s risk management policies;
- determine the operation procedure of the risk management and the compliance control unit and monitor their activities;
- appoint and dismiss the CRO, CCO;
- appoint and dismiss the Director of the Internal Audit Department;
- supervise the activities of the Bank’s Internal Audit Department;
- approve the general organizational structure of the Bank, in particular, the organizational structure of the Bank’s internal control system, including the structures of risk management units, compliance management units (including ML/TF risk) and the Internal Audit Department;
- ensure the organization of effective corporate governance in accordance with the corporate governance principles (code) approved by the general meeting of shareholders of the Bank;
- determine the remuneration policy of the Bank in accordance with the requirements of the National Bank of Ukraine, and monitor its implementation.

The Supervisory Board of the Bank has established committees from among its members for preliminary study and preparation for consideration of issues falling within their competence at the meeting of the Bank’s SB:

- Risk Management Committee of the Supervisory Board
- Audit Committee of the Supervisory Board
- Remuneration and Nomination Committee of the Supervisory Board


The Supervisory Board Committees are permanent advisory and consultative bodies.

The functions of the SB Committees are described in the regulations on respective committees.

The SB of the Bank remains responsible for overall risk management and ensures control over the performance of the committees’ functions.


Board of the Bank shall:

- be responsible for implementing the Bank’s strategy on establishing the Internal Control System of the Bank, approved by the Supervisory Board;
- ensure the fulfilment of tasks, decisions of the Supervisory Board of the Bank 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

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

management. The Board of the Bank recognises and complies with the requirements for the independent performance of duties by the CRO, CCO, risk management and compliance management units (including ML/FT risk) and does not interfere with the performance of their duties;

- ensure the organization of the internal control system;
- ensure the current management of the subordinate entities of the Bank’s internal control system;
- be entitled to delegate part of the functions on organization of the internal control system to permanent committees (namely, the ORMC), heads of the Bank’s structural units. In this case, the Bank’s Board shall remain responsible for the performance of the functions delegated by it;
- implement the principles of corporate governance, professional standards and codes of conduct of employees determined by the Supervisory Board in order to increase the efficiency of the Internal Control System;
- ensure the distribution of functions, powers, duties and responsibilities on the implementation of internal control between the collegial bodies of the Bank’s Board, units and employees of the Bank, excluding any conflicts of interest and the conditions for their occurrence, as well as any possibilities of committing crimes or any other illegal actions during the Bank’s operations;
- regulate the establishment of an organizational structure that complies with the principles of the Internal Control System;
- provide clear division of responsibilities for the Bank’s structural units, their managers and employees;
- ensure the functioning of the Bank’s information systems responsible for accumulation, processing of necessary information and its provision to users;
- approve the Policy on the organization of the Internal Control System of JSC “FUIB”, which is implemented at the level of all structural units, products, operations, processes and systems of the Bank;
- consider the results of current monitoring of the Internal Control System;
- take immediate and necessary measures to eliminate violations or shortcomings of the internal control system;
- provide reports on the results of the internal control system and proposals to the Supervisory Board on improving the efficiency of the internal control system;
- submit reports to the Supervisory Board of the Bank on the implementation of its decisions on improving the efficiency of the internal control system, taking into account changes and external factors affecting Bank’s activities;
- ensure the preparation and submission of proposals on changes to the risk management strategy and policy to the Supervisory Board;
- be responsible for the strategic development of the Bank’s principles regarding the implementation/establishment of bank risk management and control culture, and create an

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

environment for staff's understanding of the importance and role of internal control of the Bank's activities;

- constantly improve the Bank's risk management system, ensure the implementation of procedures for risks identification, measuring, controlling, minimizing and monitoring;
- ensure the preparation and provision of the Supervisory Board of the Bank with management reporting on the risks to which the Bank is exposed, including information on new types of products or significant changes in the Bank's activities;
- 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 Department, external auditors and supervisory authorities;
- monitor the compliance of the qualification of the Bank's employees with their job functions, and ensure their advance training;
- form the organizational structure of the Bank (including the responsibilities, powers, subordination and accountability of the Board committees to the Supervisory Board and the Board of the Bank);
- delegate the authority to carry out current control over the assessment of the effectiveness of the Internal Control System (ICS) to the Operational Risk Management Committee, which consists of representatives of the Business Units (generating operational risk) and units (support units) supporting business continuity (responding/managing/minimizing operational risk events within the limits of their powers). The Board shall be responsible for the quality of the performance of the functions delegated by it;
- consider a report on the effectiveness of the Internal Control System on an annual basis and, if necessary, makes strategic adjustments of the banking risks control process;
- ensure the development and approval of internal bank documents stipulated by the Policy on the development, coordination, approval, placement, updating, cancellation of internal regulatory documents and familiarization of JSC “FUIB's” employees with them;
- provide CRO, CCO, risk management units, 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).

The Bank's Board shall not allow:

- ineffective distribution of duties;
- any encouragement of Bank employees to poorly perform their job functions (excessive insistence on achieving short-term results without taking into account long-term goals, etc.);
- any compensation schemes that are excessively dependent on short-term performance;
- any ineffective disciplinary sanctions (insignificant or excessively severe sanctions for unacceptable behaviour).

The Bank's Board shall distribute the duties ensuring the avoidance of:

ПУМБ	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	


- 1) any conflicts of interest as well as conditions for their occurrence;
- 2) any possibility of committing crimes and other illegal actions within the Bank’s operations;
- 3) any possibility of performing by one unit or employee (except for operations carried out using appropriate software with an appropriate level of control and subject to subsequent control);
 - Bank operations and their registration and/or accounting treatment;
 - documenting cash transactions, carrying out their actual execution and timely accounting treatment;
 - transactions on the accounts of the Bank’s clients and accounts reflecting the financial and economic activities of the Bank;
 - assessment of the reliability and completeness of documents provided by the client when obtaining a loan, and borrower monitoring after granting the loan;
 - actions in any other areas subjects to a conflict of interest.

The Bank’s Board ensures constant monitoring of the internal control system effectiveness.

The Internal Audit Department (IAD) conducts an annual independent assessment of the Internal Control System and submits it to the Supervisory Board for consideration.

The Chief Accountant heads the Financial Accounting and Tax Reporting Department (FATRD) and shall be:

- responsible for organizing the Bank’s reporting system (financial, tax, statistical);
- responsible for organizing an effective accounting control system and its operation;
- responsible for generating reliable financial statements (including those in accordance with IFRS standards);
- ensure compliance with the Bank’s established unified accounting methodology principles, preparation and submission of financial statements within the established deadlines;
- organize control over the accounting treatment of all transactions carried out by the Bank;
- provide constant control over the correctness and legality of the accounting treatment of all banking transactions;
- participate in the preparation of materials related to shortages and compensation for losses from shortages, theft and damage to the Bank’s assets;
- ensure verification of the accounting in separate units of the Bank;
- organize the process of signing the daily balance list/balance sheet;
- monitor the correctness of recordkeeping of open accounts;
- ensure inspections of the Bank’s accounting status;
- depending on the volume of operations in the Bank, determine the employees to be involved in further control/inspections;
- ensure Bank’s compliance with tax legislation and the Bank’s Accounting Policy as a whole;
- ensure timely submission of correct reporting to state supervisory authorities.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	


The Chief Accountant shall have the right to require separate units of the Bank to:

- 1) ensure the organization of accounting and accounting control;
- 2) submit the documents necessary for the registration of transactions;
- 3) observe the established procedure for accepting, posting, storing and spending cash, material and other valuables;
- 4) have the right to require any unit of the Bank to provide explanations, and if necessary, directly intervene in its working procedures if the data obtained from them raises doubts.

The Chief Accountant, performing organizational and control functions, cannot be assigned the duties of the Head of the Bank in his temporary absence, as well as the duties for the direct execution of accounting transactions.

Risk management units (CBRD, SBRMD, RRD, GBRD, CMB, MRB), subordinate to CRO shall:

- 1) ensure timely identification, measurement, monitoring, control, mitigation and reporting of material risks by types (credit, market, interest risk in the banking book, operational risk and liquidity risk);
- 2) conduct control at the second level of control (line of defence) of the Bank's ICS;
- 3) ensure monitoring and prevention of any violations of risk appetite indicators and risk limits, monitor the approach of risk indicators to the risk appetite and limits and initiate measures to prevent their violations;
- 4) participate in the development of a distressed assets management strategy and operational plan and monitor their implementation;
- 5) prepare risk reports for the Supervisory Board at least once a quarter, for the Bank's Board – at least once a month, and in the event of identifying situations requiring urgent notification of the Bank's Supervisory Board – no later than the next business day;
- 6) 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;
- 7) 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;
- 8) prepare conclusions on risks inherent in new products and significant changes in the activities of the Bank, until their introduction for management decisions within their competence;
- 9) prepare conclusions regarding the risks that may inherent in both new loans and amendments for existing loans, for making management decisions regarding granting new loans or amending existing loan agreements;
- 10) exercise control over property evaluation;
- 11) carry out credit risk assessment;
- 12) develop, implement and monitor an early response system;
- 13) prepare conclusions for management decisions on settling debtors/counterparties' debts;
- 14) develop, participate in the development of internal risk management and internal control documents;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

15) The GBRD coordinates all internal regulatory documents.

The Deputy Chairman of the Board for Risk Management (CRO) is the supervisor of the Risk Management Units and is responsible for the activities of these units, has the right to attend meetings of the Board (even if the **CRO** is not a member of the Board), Board committees and other collegial bodies established by the Board, and ban (veto) the decisions of these bodies if they will lead to a violation of the established risk appetite and/or approved risk limits, as well as in other cases established by the Supervisory Board, and immediately notifies the Supervisory Board about 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 the risk management 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.

Compliance management vertical units (including ML/TF risk) (CCB, FMD, FCSCFCOSP and MTPAC), subordinate to CCO:

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) provide monitoring of changes in the legislation and relevant standards of professional associations, applicable to the Bank, and evaluates the impact of such changes on the processes and procedures implemented in the Bank, as well as provide control over relevant amendments of the Bank's documents;
- 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 the organization of control over observing the rules on timeliness and reliability of financial and statistical reporting by the Bank;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- 6) regularly monitor the absence of a conflict of interest between the Bank's managers and the subject of assessment activities;
- 7) ensure organization of control over the protection of personal data in accordance with the legislation of Ukraine;
- 8) 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;
- 9) 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);
- 10) ensure the functioning of compliance risks management system by timely identifying, measuring, monitoring, controlling, reporting and providing recommendations on compliance risk mitigation;
- 11) 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;
- 12) 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
- 13) prepare conclusions on compliance risk (including ML/TF risk) that is inherent in new products and significant changes in the activities of the bank until their introduction to timely take adequate management decisions (with the involvement of other vertical units if necessary);
- 14) prepare conclusions on compliance risk to take decisions on loans to the bank's associated persons;
- 15) monitor the compliance of the compensation and indemnity system introduced in the Bank, as well as procedures for bringing bank employees to disciplinary responsibility according to the requirements of the legislation of Ukraine;
- 16) prepare compliance risk reports for the Supervisory Board, the Board at least once a quarter, and in the event of identifying situations requiring urgent notification of the Bank's Supervisory Board – no later than the next business day;
- 17) participate in the development and approval of internal banking documents.

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;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- 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, 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);
- 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;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- 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;

The **CCO**, is the supervisor of the Compliance Management Verticals (including ML/TF) and shall be responsible for their activities, 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 Supervisory Board of the Bank, and promptly inform the Supervisory Board of such decisions.

The CCO shall perform the following functions:


- 1) submit compliance risk and ML/TF risk (as part of compliance risk) reports to the Supervisory Board and the Board of the Bank;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- 2) ensure the coordination of work on compliance risk-management issues between the Bank's structural units as well as on internal control issues;
- 3) inform the Supervisory Board, the Board of any 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 Bank's Supervisory Board has not taken measures to eliminate them. Information on confirmed facts of unacceptable behaviour in the Bank/violations in the Bank's activities and on conflicts of interest is provided to the structural unit of the National Bank carrying out on-site supervision of banks;
- 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.

The Supervisory Board ensures independence of Risk Management Units and Compliance Management Units (including ML/TF risk) by:

- 1) risk management units subordinate to CRO, CRO – to the Supervisory Board, compliance management units (including ML/TF risk) subordinate to CCO, CCO – to the Supervisory Board;
- 2) reporting of the CRO and CCO to the Supervisory Board;
- 3) providing the CRO/risk management units, CCO/compliance management Unit (including AML/CFT risk) with a direct and unlimited opportunity to discuss risk issues directly with the Supervisory Board without the need (obligation) to inform the members of the Bank's Board;
- 4) organizational and functional separation of CRO/risk management units, CCO/compliance management Unit (including ML/TF 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) inclusion of a sufficient amount of financial provision/remuneration for CRO/employees of risk management units, CCO/employees of compliance management units (including ML/TF risk) in the Bank's budget. The remuneration of CRO/risk management units, CCO/compliance management units (including ML/TF risk) should not depend on the results of the work of business units under their control, and should contribute to staffing these units with qualified employees. The variable part of the remuneration should be provided based mainly on the achieved results of their activities;
- 7) ensuring access of CRO/risk management units, CCO/compliance management units (including ML/TF risk) to information necessary for their effective work. The Bank's managers and staff should facilitate the provision of such information.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

Within the powers delegated by the Bank’s Board to carry out control of the functioning of the Internal Control System (ICS) the Operational Risk Management Committee (ORMC) shall:

- tactically ensure the implementation of the strategy on the implementation and development of the Internal Control System;
- approve measures for the implementation/establishment of a internal control corporate culture (at the first and second levels of control (line of defence));
- consider issues on the implementation of control procedures taking into account the Bank’s risk matrix (within the annual self-assessment of the Bank’s risk level);
- quarterly monitor the effectiveness of the Bank’s internal control as a whole according to the key control indicators;
- annually report on the functioning of the Internal Control System to the Bank’s Board.


The functions of the Bank's collegial bodies are described in the Regulations on these collegial bodies.

Support units shall:

- be responsible for current and subsequent control within their powers, for the consistent accumulation and provision of statistics on events/incidents/problems identified during control of operations and/or activities of the Bank’s business units;
- be responsible for risk assessment of processes owned or controlled by them;
- be responsible for identifying, assessing, monitoring and controlling (minimizing) risks arising at different stages of the process which fall within their functional responsibility or control;
- participate in investigating the causes of banking risks materialization and, within their powers, develop and implement measures to minimize their negative consequences;
- participate in assessing the effectiveness of measures implemented to minimize/eliminate the consequences of banking risks materialization.

Heads of business units shall:


- provide current control/self-control over the provision of high-quality and timely services to Clients, and in case of detection of any problems related to the failure to perform a banking transaction/service in a timely manner, organize and control the process of their eliminating/solving.
- in case of failure to independently apply effective measures to solve the specified problems, ensure timely informing of support units about the cause and consequences for further development of measures to eliminate the existing problem, as well as to accumulate practical experience in solving it. In addition to the above, it is aimed at preventing the emergence of similar problems in the future and/or minimizing the frequency of their occurrence;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- be responsible for high level of communication with representatives of support units and other business units;
- complete the annual questionnaire “Risk Level Self-assessment” by type of risk to assess the effectiveness of controls built into the process;
- be responsible for risk assessment of the process owned by them or in which they participate.

Heads of all structural units (support and business units) shall:

- ensure control over the performance of job functions of employees subordinate to them, increase their efficiency, taking into account the Bank’s development strategy and business plans;
- ensure clarity, logic and compliance with job functions of tasks assigned to their subordinates, and ensure control over subordinates’ performance of duties stipulated in job descriptions;
- contribute to the implementation of a banking risk management and control corporate culture for their subordinates;
- contribute to and supervise the implementation of effective risk management and control system in reporting units;
- be responsible for high-quality communications of the reporting unit with representatives of other units;
- be responsible for development of a motivation system for subordinates to improve the effectiveness of risk management;
- conduct preliminary, current and subsequent quality/efficiency control of subordinates’ work for errors and motivate high level of employees’ self-control;
- execute orders and recommendations of the Operational Risk Management Committee and the Risk Factor Management Subcommittees, and also help implement specific minimization and control measures to prevent risk, and also help assess the effectiveness of the measures taken;
- each head of a structural unit is obliged to inform his current/new employees about the implementation of the internal control system in the Bank and the need to register operational risk events, and familiarize his subordinates with this Policy;
- participate in identifying and resolving conflict of interest situations according to the procedure established in the Bank;
- inform the CCB of all facts of violation of fair competition standards, legal norms and other mandatory requirements, the emergence and resolution of conflict of interest situations;
- contribute to the implementation and maintenance of an appropriate level of professional ethics of the Bank’s employees, which contributes to minimizing risks;
- contribute to minimization of the risk of reputational losses;
- if necessary, participate in working groups on additional risk assessment when implementing a new product/service.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

Employees of all structural units of the Bank shall:

- know their job functions;
- ensure the implementation of internal control procedures within the their job functions;
- ensure high-quality, timely, error-free performance of their job functions, as well as conduct self-monitoring of the work performed and, in case of error detection, report it to their immediate supervisor;
- inform their immediate supervisor/risk officer of any operational events that affected the speed, quality and timeliness of the performance of their job functions for their entering into the database for further development of measures preventing such problems in the future or minimizing their frequency by experts of support units;
- understand the meaning of the term “banking risk”, be aware of the probability of its occurrence in their work and the need to implement an Internal Control System in the Bank;
- participate in identification of conflict of interest within the procedure established in the Bank.

5.4 MAIN COMPONENTS OF INTERNAL CONTROL SYSTEM

5.4.1 Control environment


Control environment – a set of subjects of the Bank’s internal control system, procedures, policies for each separate activity of the Bank as well as other internal control banking documents, and control culture. Internal control culture – employees’ compliance with the Bank’s principles, rules, norms aimed at informing Bank employees about the functioning of the internal control system and the role of each employee in this activity.

5.4.2. Management of risks inherent in the Bank’s activities. The internal control system ensures the availability of the Bank’s risk management system and constant monitoring of its development and functioning.

The Bank creates a risk management system that ensures the identification, measurement (assessment), monitoring, reporting, control and mitigation of all significant risks of the Bank at all organizational levels, taking into account the specifics of the Bank.

Risk management is divided into 4 large groups:

1. **Credit risk management** – Credit Council (control is carried out by the Corporate Business Risks Department, the Small Business Risk Management Department and the Microcredit Risk Department – over transactions with corporate clients and the Retail Risks Department – over transactions with retail clients and the Market and Interbank Risks Body of the GBRD – over transactions with banks);
2. **Market risk management** – Asset and Liability Management Committee (control is carried out by the Market and Interbank Risks Body of the GBRD over interest risk in the banking book, market risks and liquidity risk);

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	


3. **Operational risk management** – Operational Risk Management Committee (control is carried out by the General Banking and Operational Risks Body of the GBRD over operational risk: factor “Personnel”, factor “Processes”, factor “Systems and Technologies”, factor “External Factors”);
 - 3.1. *ICT risk and information security risk management (including cyber risk)* – Operational Risk Management Committee (control is carried out by the GBRD and ISD within the scope of the ISMS and ITD regarding ICT risk);
 - 3.2. *Fraud risk management* – Operational Risk Management Committee (control is carried out by the GBRD and SD within the scope of the FRMS);
 - 3.3. *Physical security risk management* – Operational Risk Management Committee (control is carried out by the GBRD and SD within the scope of the PSMS);
 - 3.4. *Third-party risk management* – ORMC and semi-annual reporting to the Tender Commission on the effectiveness of cooperation with counterparties (control is carried out by the GBRD and SD within the scope of the TPRMS) and semi-annual reporting to the ORMC.
4. **Compliance risk management** – Ethics and Business Conduct Committee (EBCC), Supervisory Board of the Bank (control is carried out by the CCB).
 - 4.1. **ML/TF risk management (as part of compliance risk)** – Financial Monitoring Committee (control of regulatory compliance risks is carried out by the Compliance Management Vertical (including ML/TF risk) within the scope of ML/TF risk management).

The Bank has established a risk management system that ensures:

- a) assessment of external factors (changes in economic conditions, changes related to a particular type of economic activity, technological changes, etc.);
- b) consideration of internal factors (complexity of the Bank’s organizational structure, specifics of the Bank’s activities, level of personnel qualification, organizational changes, introduction of new products, etc.);
- c) assessment of measurable and non-measurable risks;
- d) identification of risks out of Bank’s control. The Bank may make decisions on acceptance of risks that are out of Bank’s control, taking into account the possibility of their negative impact on the achievement of the Bank’s goals;
- e) control over the ratio of the risk management and control systems cost with benefits of their application.

The objectives of the Internal Control System regarding control of banking risk management systems are achieved by:

- a) verification of the use of the granted accesses and permissions;
- b) control over the frequency, completeness and quality of inspections of compliance with limits, mandatory conditions, indicators, etc., as well as their monitoring;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- c) verification of the actual updating internal risk management documents;
- d) verification of the sequence of process stages and, if necessary, optimizing/updating the banking risk management process.

5.4.3. Internal control procedures and distribution of responsibilities within Bank’s operations.

The Bank ensures that its activities are covered by internal control procedures on a daily basis.

Bank employees ensure fulfilment of all requirements of internal control procedures within their job functions.

The internal control system provides for the creation and operation of:

- development of internal control policies and procedures;
- verification of compliance with internal control procedures;
- monitoring the effectiveness of internal control procedures.


The Bank implements internal control procedures with:

- 1) reporting to the Supervisory Board and the Board. In accordance with the distribution of job functions, Bank managers constantly receive and analyse reports on the implementation of goals to determine correspondence of actual financial results with planned indicators;
- 2) multi-level control over the Bank’s activities (3 levels of control (lines of defence) of JSC “FUIB”):

- control performed by heads of structural units over the employees’ performance of their job functions and control performed by Support Units over the results of business processes within the limits of their responsibility, determined by the Bank’s internal documents;
- control performed by the Risk Management Units and the Compliance Control Body over the work (results of activities) of the Bank’s structural units;
- control performed by the Bank’s Supervisory Board through the introduction of internal audit.

The internal control system **excludes** any possibility of one unit or employee (except for operations carried out using appropriate software with an appropriate level of control and subject to subsequent control) performing:

- Bank operations and their registration and/or accounting treatment;
- documentation of cash transactions and their actual execution;
- transactions on the accounts of Bank’s clients and on accounts stating the financial and economic activities of the Bank;
- assessment of the reliability and completeness of documents provided by the borrower when granting a loan, and monitoring of the borrower’s financial condition;

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

- servicing of personal transactions or transactions of close relatives, except for cases permitted by the Bank;
- any other actions that entail any conflict of interest situations, except for cases permitted by the Bank.

5.4.4. Control over information security management and information exchange.

The internal control system regulates the description of the Information Security Management System (ISMS) in accordance with the standards of the National Bank of Ukraine on information security management in the banking system of Ukraine.

The Information Security Department organizes control over information exchange by ensuring the integrity, confidentiality and availability of internal financial, operational and statistical information, information on compliance with the requirements of legislation and regulatory legal acts, internal regulations, other mandatory requirements, external market information necessary for decision-making and performance of official duties.

JSC “FUIB” has established the following information exchange flows, namely:

- a) “splash back” – the Supervisory Board and the Board of the Bank know and are aware of the risks to which the Bank is exposed and control the work of the Bank;
- b) “downward communication” – information about the Bank’s strategies and policies is communicated to all management levels and other employees to the extent that allows them to understand the direction, goals, mission and planned indicators of the Bank;
- c) “horizontal” – information held by one unit of the Bank must be provided to another unit requiring it to perform its functions, in order to avoid additional expenditure of time, labour and financial resources.

The Supervisory Board ensures constant monitoring (at least once a year) of the adequacy and effectiveness of the internal control system and its compliance with the scale and nature of the Bank’s activities.

5.4.5. Control over information flows and communications of the Bank

5.4.5.1. The Bank ensures control over information flows and communications (information exchange) to support the components of the internal control system to ensure:

- 1) provision of high-quality information to/by internal and external users for making informed judgments, timely and adequate management decisions;
- 2) creation and operation of information systems that ensure the implementation of internal and external communications of the Bank.

5.4.5.2. The Bank ensures the quality of information used in its activities, based on the principles of:

- 1) availability and accessibility – information can be easily obtained by those who need it to perform their job/job function. Users are familiar with the list of information available to them and the procedure for accessing the Bank’s information systems;
- 2) correctness – information is reliable and complete. The Bank’s information systems ensure that data is checked for reliability and completeness;

ПУМБ	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

3) relevance – the collected information is relevant and updated with an adequate frequency, including the periodicity determined by the legislation of Ukraine, regulatory legal acts of the National Bank, internal bank documents;

4) integrity – the information is protected from any unauthorized distortion or destruction. The Bank ensures the classification of information (for example, publicly available, with limited access) and other information protection procedures;

5) storage – the information is available within the terms set by the legislation of Ukraine, regulatory legal acts of the National Bank, internal bank documents;

6) sufficiency – the level of information details meets the needs of internal and external users. Excess information is eliminated to avoid any incorrect use or misinterpretation;

7) validity – information is obtained in accordance with approved procedures and represents events that actually occurred, except for hypothetical assumptions;

8) confirmability – the information is supported by evidence from an appropriate/reliable source.

5.4.5.3. The Bank establishes information management procedures with clear responsibility for the quality of the information, including procedures for distribution of information on identified deficiencies and inconsistencies in the internal control system. Control.

5.4.5.4. The Bank determines the form and frequency of information provision, taking into account the needs and requirements of internal and external users. Responsible unit – Marketing Department.


5.4.5.5. The Bank ensures the use of high-quality information at all its organizational levels in order to achieve the Bank’s goals and timely respond to identified deficiencies in the Internal Control System.

5.4.5.6. The Bank ensures the exchange of information on internal control at all organizational levels of the Bank, including information on:

- 1) the objectives of the internal control system, the importance and benefits of an effective ICS;
- 2) Policies and BIRD determining job functions of the Bank’s managers and employees in implementing control measures;
- 3) the roles, authorities and responsibilities of the Bank’s managers and other employees in implementing control measures;
- 4) significant issues of organization and functioning of the internal control system, including information on deficiencies and inconsistencies of the ICS.

5.4.5.7. The Bank ensures high-quality internal communications:

- 1) vertically (splash back) – information on risks and other issues of the Bank’s activities is provided to the Supervisory Board and the Board of the Bank for their further appropriate management decisions through management reporting of the Second and Third levels of control (lines of defence);
- 2) vertically (downward communication) – information about the Bank’s strategy and policy is brought to the attention of managers of all levels and other employees of the Bank through mandatory familiarization with the Bank’s BIRD, annual ICS training of employees, through publications on the internal corporate website (for example, the Bulletin of the ORMS and the Bulletin of the ISMS, etc.);

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

3) horizontally – information held by one unit of the Bank is provided to another unit requiring it to perform its functions (in accordance with internal BIRD).

5.4.5.8. The most appropriate method of communication is chosen by the MD and the HRD.

5.4.5.9. The Bank provides employees with high-quality information in accordance with their job functions, including information on:

- 1) strategic, current goals and plans of the Bank, the status of their implementation;
 - 2) changes in internal bank documents, including documents on the implementation of internal control;
 - 3) control culture;
 - 4) approved work plans of the Bank's units;
 - 5) orders of the Bank's managers and units, including orders on the implementation of control measures;
 - 6) safety and labour protection rules;
 - 7) the procedure for using, transferring, and storing documents and other information media constituting banking and commercial secrets;
 - 8) procedures for complying with information security requirements;
 - 9) liability (disciplinary, administrative, criminal) for violations;
- using electronic document management.

5.4.5.10. The Bank has implemented control measures for communication with external users (under responsibility of the MD and the CCB). Such measures include requirements for receiving information from external users and transmitting it within the organizational structure of the Bank, allowing the Bank's managers to identify trends, events or circumstances that may affect the achievement of the Bank's goals.


5.4.5.11. While communicating with external users the Bank ensures:

- 1) provision of relevant and timely information on the Bank's activities to external users, including shareholders, partners, Bank clients, supervisory, controlling, and law enforcement agencies;
- 2) obtaining information on the functioning of the Bank's internal control system from external auditors, supervisory authorities, and other external users in order to make adequate management decisions.

5.4.5.12. From external users the Bank receives information on the functioning of the ICS, which may include:

- 1) assessment of the ICS by external auditors and supervisory (control) authorities (reports and conclusions of inspections);
- 2) customer feedback on the quality of banking services (appeals);
- 3) publications about the Bank in the media, on information sites, and in external information systems (MD control).

5.4.5.13. The Board evaluates information on ICS of external users and informs the Supervisory Board about the identified ICS deficiencies. Reports are provided quarterly.

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

5.4.5.14. The MD selects the method of external communication, taking into account the target audience, nature of communication, timeliness, cost and requirements of the legislation of Ukraine, regulatory legal acts of the National Bank, and internal bank documents.

5.4.6. Monitoring of the internal control system.

The Supervisory Board, the Board and the ORMC carry out constant monitoring of the adequacy and effectiveness of the internal control system in accordance with the methodology approved by the Bank. Assessment of the ICS effectiveness is carried out by the IAD for the Supervisory Board of the Bank.

The Bank summarizes the results of monitoring the adequacy and effectiveness of the internal control system. Reports on the results of monitoring the effectiveness of the ICS functioning should be prepared at the level of all structural units involved in the Internal Control System, brought to the attention of members of the Board and Supervisory Board of the Bank, heads of other structural units and must contain information on generalized deficiencies of the ICS, their causes, their possible consequences which endanger the Bank's activities, as well as proposals for improving the ICS effectiveness.

The ICS is monitored on the basis of the following reports:

- Annual report of the IAD 3rd level (line of defence) of the ICS: assessment of the effectiveness of the ICS in the Bank as a whole.
- Quarterly report of the GBRD and the compliance management vertical (including ML/TF risk) 2nd level (line of defence) of the ICS: monitoring of the effectiveness of control procedures (monitoring of key control indicators).

5.5 IMPLEMENTATION OF INTERNAL CONTROL SYSTEM OF JSC “FUIB”


The Internal Control System is implemented in 5 stages:

1. Planning.
2. Development, approval and implementation of procedures.
3. Organization of ICS.
4. Familiarization/training of employees.
5. Direct implementation and control.

Note! Development and approval of procedures is one of the main stages of operational and compliance risks prevention, also providing inspection of the completeness of the envisaged controls.

All involved units/executors must participate in the approval of the Bank's internal documents in order to adopt a unified and effective approach to the organization of banking activities.

When implementing/developing new processes and making changes to existing processes/internal documents, the Bank conducts mandatory approval of internal documents in

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

accordance with the requirements of the Policy on the process of development, agreement, approval, posting, updating, cancellation of internal regulatory and administrative documents and review of employees of JSC “FUIB”.

The following internal documents of the Bank are fundamental for the effective functioning of the ICS:

1. The Bank’s organizational structure, approved by the Supervisory Board.
2. Distribution of functions and powers between the Members of the Board.
3. Distribution of responsibilities between units and employees of the Bank for timely identification and control of possible cases and areas of conflicts of interest.
4. Procedures and terms for documents storage (archiving) on paper and electronic media.
5. Documents on information security management, including the procedure for restriction of any unauthorized access and distribution of confidential information, as well as its use for personal purposes, the Bank’s plan of activities in emergency situations (natural disasters, fires, etc.).
6. Emergency action plan (with a description of “key systems” and “key units” actions in emergency situations, as well as instructions for ensuring continuity of activity).

The process-oriented approach regulating the Operational Risk Management System (ORMS) and the requirements of the Regulations on Business Process Management of JSC “FUIB” provide for a description of the Bank’s activity processes by type of activity. This approach envisages a detailed description of the main operations and management procedures carried out by the Bank, presented in schematic and text form and, in particular, determines the sequence of steps for implementing the described activity processes, relations between individual processes, etc.


In order to achieve the goals of the ICS, the Bank attracts and promotes the development of competent individuals, ensures the availability of an appropriate level of qualification of employees at all Bank’s organizational levels.

As part of the insider threat management, the Bank ensures the verification of all candidates for positions in the Bank regarding their experience and professional qualities (verification and analysis of the candidate’s work experience to assess their compliance with the requirements of the vacant position).

The Bank approves internal remuneration documents to ensure effective corporate governance and promote compliance with corporate values specified in the Code of Corporate Ethics.

6. 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 has implemented a three-level control of the ICS introduction process:

	TRADE SECRET	Version 7.0
	4. Risk management and internal control	
	Policy on Organisation of the Internal Control System of JSC “FUIB”	

<i>ICS levels</i>	<i>Controller</i>	<i>Supreme Supervisory Authority</i>
Current control	1st level of control (line of defence) The heads of all Bank’s units and the controllers of business processes appointed by them, support units	Members of the Board (according to their areas of responsibility)
Risk management and compliance control	II level of control (line of defence) Risk management units Compliance management units (including ML/TF risk)	CRO and CCO, functionally subordinated and accountable to the Supervisory Board of the Bank
Internal audit	III level of control (line of defence) Internal Audit Department	Supervisory Board of the Bank/Audit Committee

7. DOCUMENT REVIEW PROCEDURE

This Policy shall come into force on the date of its approval by the Supervisory Board of the Bank.
This Policy shall be updated at least once a year.