APPROVED
by the decision of the Supervisory Board
of JSC “Ukrposhta”
dated 28 March 2025
Minutes of the Meeting No.4

RISK MANAGEMENT POLICY OF JSC "UKRPOSHTA"

CONTENTS

I. INTRODUCTION

1.1 The Risk Management Policy of JSC "Ukrposhta" (hereinafter "the Policy") defines the goals, objectives, and principles of the risk management system of JSC "Ukrposhta" (hereinafter "the Company"), the risk management structure, the main stages of the risk management process, risk management and assessment tools, and establishes a systematic approach to risk management of the Company.

1.2 The Policy is developed in line with the best international practices and standards: ISO 31000:2018 "Risk Management", DSTU IES/ISO 31010:2014, COSO ERM Framework (Committee of Sponsoring Organizations of the Treadway Commission), FERMA (Federation of European Risk Management Associations) standards, as well as regulatory requirements of the National Bank of Ukraine (hereinafter "the NBU") and the Ministry for Development of Communities and Territories of Ukraine (hereinafter "the Ministry").

1.3 The purpose of implementing a comprehensive risk management system in the Company is to organize a clear process for sound risk management and to facilitate the achievement of the Company's strategic goals by timely and complete identification of risks and opportunities, ensuring their comprehensive analysis, conducting risk assessments, developing risk mitigation measures, and monitoring and controlling the level of risk acceptable to the Company.

1.4 Risk management is an integral part of effective corporate governance, planning and decision-making processes, and accordingly, risk management is integrated into all the Company's processes and ensures that stakeholders are able to make well-balanced and effective decisions.

II. SCOPE OF APPLICATION

2.1 This Policy applies to all processes and activities of all employees and all structural units of the Company.

2.2 The Policy is part of the Company's internal labor regulations and is mandatory for all employees of the Company to read and use. In performing their functional duties and implementing their tasks, if it is related to risk management, each employee of the Company shall be guided by the following Policy clauses.

2.3 Each head of a structural unit of the Company shall be responsible for compliance with the requirements of this Policy by the employees of the respective structural units.

2.4 The Policy shall be approved by the Supervisory Board and is subject to review by the decision of the Supervisory Board, but at least once every two years.

2.5 The General Director of the Company (hereinafter "the Head of the Company ") is responsible for the implementation of this Policy.

III. TERMS, DEFINITIONS, AND ABBREVIATIONS

3.1 The following terms and definitions are used in the Policy:

- CCO (Chief Compliance Officer) – The primary officer of the Company responsible for ensuring compliance with regulations and internal policies.

- CRO (Chief Risk Officer) – The primary officer of the Company responsible for risk management.
- Cost-benefit analysis – A method of assessing the effectiveness of potential investments by comparing the expected total costs with the possible benefits of an investment project. The main purpose of this analysis is to make an informed decision on whether the expected benefits exceed the costs associated with the project.
- ESG principles (Environmental, Social, and Governance) – A set of standards used to assess the Company's activities in terms of their environmental impact, social responsibility, and corporate governance.
- ESG risks (Environmental, Social, and Governance Risks) – Risks associated with environmental factors, social development, and corporate governance levels.
- Risk Universe ("Long List" of Risks) – A comprehensive classified list of risks that may be relevant to the Company. This "long list" is used for further analysis of risks to determine their relevance to the Company's processes or functions.
- Risk owner – A person (employee, structural unit, or collective body) within the Company responsible for implementing risk management measures and possessing sufficient authority to execute such measures.
- Internal control – A set of measures set of measures used to ensure compliance with the legality and efficiency of the use of funds, achievement of results in accordance with the established goals, objectives, plans and requirements for activities.
- Risk impact – The amount of losses and/or potential losses that may be incurred by the Company because of the risk.
- Key Risk Indicator (KRI) thresholds – Possible values (or range of values) of KRIs that signal such a change in the level of risk that may lead to failure to achieve the goals. These thresholds are a tool for controlling and monitoring the risk factors, exceeding which is a signal to the Risk Owner to make appropriate risk management decisions
- Risk Appetite Statement (RAS) – An internal document that defines the aggregate amount of risk appetite, the types of risks that the Company will accept or avoid in order to achieve its business goals, and the level of risk appetite for each of them (individual level).
- Risk source – An element that, by itself or in combination with others, may give rise to a risk.
- Escalation – The procedure for reporting material (critical) events to the level of the Supervisory Board.
- Residual risk – The risk remaining after the actions taken to reduce the inherent risk.
- Probability – The possibility that a certain event will occur
- Risk Heat Map – A tool for summarising information on the Company's top risks. It provides a graphical representation of risk assessment based on two parameters: the probability of risk realisation and the level of risk impact on the Company's operations
- Key Risk Indicators (KRIs) – Metrics used to assess risk levels and their dynamics over time. KRIs serve as an early warning system for changes in risk levels and the effectiveness of risk management (including control) measures.

- Compliance risk – The risk of non-compliance of the Company's activities with the requirements of legislation, regulatory norms, internal policies, as well as ethical requirements, which may entail legal, reputational and other consequences.
- Risk culture – The principles, rules, and behavioral norms of employees related to risk awareness, risk acceptance, and risk management. It also includes management tools that influence risk-related decision-making. Risk culture is a component of the Company's overall corporate culture and contributes to the formation of a sufficient level of awareness of all employees about the importance and rules of the risk management system and the involvement of all employees in the risk management process.
- Risk limit – Restrictions set by the Company to control the level of risks it faces during operations.
- Risk mitigation – The process of risk modification aimed at reducing or eliminating negative impact.
- Three Lines Defense model – A model developed by the Institute of Internal Auditors that links all levels of management: operational management (first line), control functions (second line), and an independent control function – internal audit (third line).
- First line of defense – The level of the Company's structural units directly related to the provision of goods/services to customers, as well as units that support the Company's operations. These units take on risks in the course of their activities and are responsible for the ongoing management of these risks, and implement control measures
- Second line of defense – The level of the CRO/Risk Management Division, CCO/Compliance Unit, the Corruption Prevention and Detection Service, and the Financial Monitoring Division. These units ensure that the Company's bodies are confident that the risk control and management measures implemented by the first line of defense have been developed and are functioning properly.
- Third line of defense – The level of the Internal Audit Department, which independently assesses the effectiveness of the first and second lines of defense and the overall effectiveness of the risk management and internal control system.
- Opportunity – The impact of uncertainty on the goals, expressed through the ratio of the level of probability and the amount of positive impact from the consequences of events and actions that cause uncertainty in achieving the Company's goals.
- Risk monitoring –The process of periodically reviewing identified risks and monitoring the implementation of mitigation measures through special reporting.
- Consequences – The result of an event that affects goals.
- Risk treatment – The process of risk modification aimed at reducing or eliminating negative impact.
- Operational incident – An event that leads to the realization of operational risk.
- Risk assessment – A process that combines the identification, analysis and comparative assessment of risk in terms of probability of occurrence and the size of the impact. Risk can be assessed for the entire Company, its structural units, individual projects or a single event. Risk assessment is carried out in order to make decisions for effective risk management that affect the achievement of the set goals

- Event – The occurrence or change of a certain set of circumstances. An event may: 1) have one or multiple manifestations, multiple causes, and multiple effects, 2) be something expected that does not occur or something unexpected that does occur, 3) be a source of risk.
- Inherent risk – The risk assessed without taking into account any actions taken by the Company to change the likelihood of the risk occurring or its impact.
- Risk register – A database of identified risks and opportunities with a defined risk assessment, which contains all information about the Company's risks, including: description and classification of risks, assessment with the level of impact and probability, monetary value, risk response strategy, those responsible for mitigation measures and other risk-related information. The Register is a working tool that should be updated as risks are updated. The Register is a source of analytics on the Company's risks.
- Risk level – A value expressed as a combination of consequences and its probability.
- Risk – A potential event that may lead to negative consequences for the Company.
- Risk coordinator – An employee of a structural unit of the Company responsible for identifying, self-assessing risk, taking management measures and reporting on such events, as well as for internal control in the Company within his/her authority
- Risk management system – A set of properly documented and approved risk management policies, practices and procedures that define the procedures for carrying out a systematic process of identifying, measuring, monitoring, controlling, reporting and mitigating all types of risks at all organizational levels.
- Specialized units –units of the Company that perform risk management functions.
- Stress testing – A risk measurement method used to assess potential adverse outcomes of risk exposure by estimating potential financial losses due to shock changes in various risk factors under extreme but plausible conditions.
- Material risk – A risk the realization of which in the forecast period will lead to a deviation of the Company's key performance indicator (efficiency) by an amount exceeding the approved level of risk exposure. A material risk is determined on the basis of a risk map.
- Risk appetite – The aggregate value for all types of risks and separately for each risk identified in advance and within the risk tolerance level, in respect of which the Company has decided on the expediency/necessity of their retention in order to achieve its strategic goals and implement the business plan. The risk appetite is set out in the Risk Appetite Statement.
- Risk tolerance – The ability to accept risks in business operations. It is determined not only by a willingness to take risks but also by the ability to manage them effectively and ensure the Company's resilience against potential negative impacts.
- Risk management – A continuous process of identifying, analyzing, assessing, processing, developing loss mitigation measures, monitoring and controlling risks and financial resources to mitigate adverse risk effects. An effective risk management and internal control system helps the Company achieve its goals.

IV. GOALS AND OBJECTIVES OF THE RISK MANAGEMENT POLICY

4.1 The main goals of the Policy are:

4.1.1 Establishing an effective system and structure for risk management and control, including risk identification, analysis, assessment, treatment, development of mitigation measures, monitoring, reporting, and control, to support the Company’s management and structural unit leaders in achieving strategic goals and enhancing corporate governance efficiency.

4.1.2 Ensuring integrity, completeness, and reliability of risk management information used for decision-making; creating information flows both vertically and horizontally within the Company's organizational structure; and providing management and stakeholders with reliable reporting.

4.1.3 Implementing and formalizing unified risk management approaches within the Company to limit negative impacts, optimize processes, and efficiently use resources.

4.1.4 Defining a clear responsibility structure within the risk management system.

4.1.5 Ensuring operational continuity of the Company.

4.1.6 Effectively allocating resources based on risk impact ranking and risk appetite.

4.1.7 Embedding risk management practices into the Company’s business culture.

4.1.8 Supporting the Company’s sustainable development in accordance with ESG principles.

4.1.9 Increasing investor confidence by creating a transparent risk and opportunity management system and ensuring its effective implementation.

4.1.10 Ensuring compliance with the legislation of Ukraine, regulatory acts of the Ministry and the NBU, internal policies, and professional association standards applicable to the Company.

4.2 The Policy is aimed at achieving the following objectives:

4.2.1 Integrating the risk management structure into the management and planning processes, improving decision-making quality, formulating and approving long-term Company strategies and plans with risk considerations, and maintaining acceptable risk levels that impact strategic goals and key performance indicators.

4.2.2 Establishing a comprehensive and adequate risk management system that aligns with the Company's operational specifics and meets the requirements set by the NBU and the Ministry for Development of Communities and Territories of Ukraine.

4.2.3 Describing the methodological support for risk management processes within the Company.

4.2.4 Outlining approaches to risk appetite determination and ensuring effective management of significant risks to the Company.

4.2.5 Establishing a continuous risk management process based on timely identification, assessment, analysis, treatment, and monitoring of risks.

4.2.6 Identifying key risks inherent in the Company’s operations.

4.2.7 Preventing direct and indirect losses caused by risk realization and preserving the Company’s assets.

4.2.8 Monitoring and preventing violations of risk threshold indicators and internal risk limits, escalating identified violations.

4.2.9 Defining key requirements for organizing risk coordinator activities.

4.2.10 Developing a risk management culture across all levels of the Company’s management.

4.2.11 Protecting the interests of shareholders, customers, creditors, and other stakeholders concerned with the Company’s stability.

4.3 The main principles of the Company's risk management process are:

4.3.1 Integration. Risk management should be integrated into the Company's overall management, decision-making processes and operational activities. Risk management is not a separate or isolated function, but an integral part of the Company's activities.

4.3.2 Structured and integrated approach. A structured and integrated approach to risk management contributes to obtaining consistent and comparable results of risk identification, analysis, assessment, processing, monitoring and control.

4.3.3 Relationship to the Company's goals. Risk management is aimed at achieving the Company's strategic and operational goals, taking into account the external and internal environment, and contributes to continuous improvement of operations and identification of opportunities for development.

4.3.4 Prevention. Risk management is preventive in nature and is aimed at reducing the likelihood of risks and/or the consequences of their occurrence.

4.3.5 Adaptability to changes. Risks may arise, change or disappear as the external and internal environment of the Company, its strategic and operational goals change. Risk management anticipates, identifies, recognises and responds to these changes and events in an appropriate and timely manner.

4.3.6 Communication and engagement. Appropriate and timely involvement and communication with stakeholders allows taking into account their experience, views and perceptions. This will contribute to informed risk management.

4.3.7 Continuous improvement. Risk management is continuously improved through learning and experience and follows the Plan-Do-Check-Act cycle.

4.3.8 Best available information. The inputs to risk management are based on historical and current information as well as future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and accessible to relevant stakeholders.

4.3.9 Ensure the "three lines of defense". In the process of carrying out risk management activities, all structural divisions of the Company shall be involved in the assessment, acceptance and control of risks.

4.3.10 Limitation of the level of accepted risks. Determination of the risk appetite and its transfer to the system of restrictions allows to ensure an acceptable level of risks, transparent distribution of the total risk limit by the Company's business areas. The risk management system provides control over the implementation of the Company's risk appetite.

V. ROLES, POWERS, AND RESPONSIBILITIES OF PARTICIPANTS

5.1 The Company's risk management system is implemented through the Three Lines of Defense model and involves the participation of all Company’s units in the processes of risk identification, assessment, analysis, treatment, and monitoring (Figure 1).

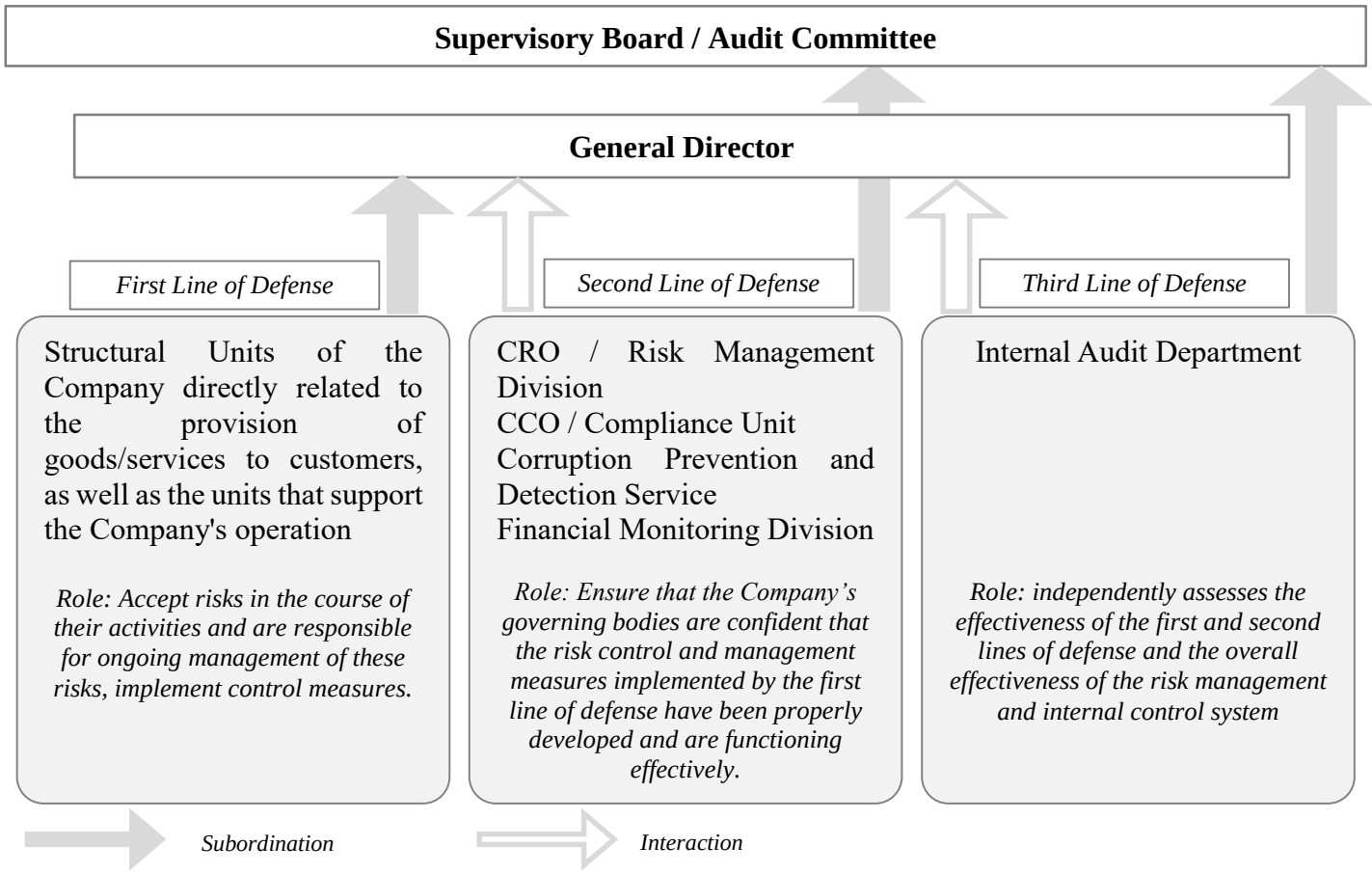

Fig 1. Three Lines of Defense model for JSC "Ukrposhta"

5.2 The subjects of the Company's risk management system are:

- Supervisory Board of the Company;
- Audit Committee of the Supervisory Board;
- General Director of the Company;
- CRO;
- Risk Management Division;
- CCO/ Compliance Unit;
- Corruption Prevention and Detection Service;
- Financial Monitoring Division;
- Internal Audit Department;
- Business and support units on the first line of defense are risk owners;
- Risk coordinators.

5.3 The Supervisory Board ensures the independence of the risk management and compliance units in the following ways:

- The Risk Management Division reports to the CRO, and the CRO reports to the Supervisory Board; the Compliance Unit reports to the CCO, and the CCO reports to the Supervisory Board
- The CRO and CCO report directly to the Supervisory Board and the Audit Committee under the Supervisory Board

- The CRO/Risk Management Department and the CCO/Compliance Unit have direct access to discuss risk-related issues with the Supervisory Board without the obligation to inform the Company's General Director
- Organizational and functional separation of the CRO/Risk Management Division and the CCO/Compliance Unit from the first and third lines of defense (including their managers)
- Ensuring sufficient staffing levels and qualifications within these units to achieve their objectives
- Guaranteeing access for the CRO/Risk Management Division and the CCO/Compliance Unit to the necessary information for effective operations, with the obligation of Company management and staff to provide such information
- Prohibiting the CRO/Risk Management Division and the CCO/Compliance Unit from controlling operations they were previously responsible for or had decision-making authority over, to prevent conflicts of interest

5.4 The Company's Senior Management Bodies Define the Strategic Direction, Mission, Values, and Risk Appetite of the Company. They establish the risk management system and delegate authority and responsibility for achieving its objectives. Their responsibilities and functions in the risk management system are distributed as follows:

5.4.1 Supervisory Board:

- Responsible for establishing a comprehensive, adequate, and effective risk management system to address the risks the Company faces
- Oversees the functioning of an appropriate, effective, and continuous risk management system and promotes a risk management culture
- Approves the Company's overall risk appetite as well as by risk types
- Approves and supervises the implementation, compliance, and timely updates of risk management documents;
- Reviews and approves risk management reports and issues with the highest level of importance to the Company
- Based on information provided by the CRO and CCO, assesses risks related to strategic initiatives, their likelihood, and potential impact, and makes decisions regarding their acceptance, mitigation, or avoidance
- Ensures the allocation of necessary resources (financial, human, and informational) for the implementation of risk management tasks within the Company's financial capabilities
- Promotes a leadership attitude ("tone from the top") regarding the importance of risk management principles and processes
- Reviews the results of risk management system assessments

5.4.2 Audit Committee under the Supervisory Board:

- Reviews and approves the results of the independent assessment of the risk management system and related controls conducted by the Internal Audit Department
- Conducts a preliminary review of internal risk management documents
- Reviews risk management reports, including periodic risk assessments and event-based risk reports
- Reviews the annual risk assessment plan

- Participates in the Company's strategy development to ensure proper risk consideration
- Provides risk management recommendations to the Supervisory Board when defining the Risk Appetite Statement
- Supports the Supervisory Board and, if necessary, engages external risk management experts

5.4.3 General Director of the Company:

- Ensures the implementation of risk management policies and internal documents approved by the Supervisory Board
- Approves internal risk management documents and provides recommendations for improvement
- Integrates risk management into the Company’s management system by incorporating risk assessments into strategic, investment, budgetary, and other management decisions
- Monitors key risks, risk appetite indicators, and limit settings
- Reviews and makes decisions on significant risks and operational incidents that have a material impact on the Company
- Facilitates and supports the implementation of action plans, recommendations, and other regulatory documents aimed at risk treatment and internal control implementation
- Reviews and approves risk management reports and risk assessment results
- Approves key risk management objectives
- Ensures compliance with legal, regulatory, and ethical requirements
- Reviews and approves the results of risk management system assessments
- Ensures the allocation of sufficient resources for the effective functioning of risk management activities and grants access to relevant risk management information for compliance and risk coordinators
- Encourages a strong risk management culture within the Company through managerial decisions and directives
- Ensures colleagues throughout the business are educated about risks associated with their job roles and pass regular training and certifications on the knowledge of risks, appetites, and policies.

5.5 First Line of Defense – Business and Support Units. The first line of defense includes business and support units directly involved in providing goods/services to customers and ensuring the Company’s operational efficiency. Their responsibilities in the risk management system are distributed as follows:

5.5.1 Company’s Structural Units – Risk Owners:

- Responsible for daily risk management within their areas of activity, including risk identification, assessment, analysis, and mitigation
- Ensure compliance with this Policy and other documents regulating the risk management system
- Provide risk-related information to the CRO/Risk Management Division, CCO/Compliance Unit, and Financial Monitoring Division
- Optimize Company processes to reduce risks and their consequences
- Participate in developing key risk indicators
- Participate in creating action plans for risk mitigation
- Report incidents and losses to risk coordinators or the Risk Management Division

5.5.2 Risk Coordinators:

Risk coordinators are designated within business units and their functional responsibilities include:

- Coordinating with the Risk Management Division on risk management activities
- Identifying, analyzing, assessing, and mitigating risks regularly
- Reporting realized risks (events) and conducting regular risk analysis
- Coordinating risk management within their unit and fostering a risk management culture
- Escalating risk-related issues to senior management using risk management knowledge
- Completing risk management and internal control training.

Risk coordinators are appointed by the General Director from among senior employees (at least deputy head level). Their responsibilities are documented in their job descriptions. Their rights and duties are outlined in Annex 1.

5.6 Second Line of Defense – Risk Management and Compliance Units. The second line provides additional expertise, support, monitoring, and problem-solving in risk management. Responsibilities are assigned as follows:

5.6.1 Chief Risk Officer (CRO):

- Implements the risk management system and oversees its operation
- Ensures coordination of risk management activities among the Company’s structural units and contributes to the development of an effective internal control system
- Conducts risk identification, analysis, assessment, monitoring, prevention, and mitigation
- Reviews and makes decisions on risk management issues
- Develops and approves Key Risk Indicators (KRI)
- Develops and approves risk mitigation action plans
- Develops and approves the internal control system
- Reports on risks to the General Director and the Supervisory Board on a quarterly and annual basis
- Develops and submits proposals for the approval, implementation, amendment, or repeal of the Company’s regulatory, procedural, methodological, and other internal documents related to risk management
- Develops the Risk Appetite Statement (RAS) and submits it for review and approval by the General Director and the Supervisory Board
- Provides proposals to the Supervisory Board and the General Director on risk mitigation measures, including initiating risk limits and/or adjusting existing risk limits
- Embeds risk management practices into the Company's business culture
- Monitors compliance with this Policy within the Company

5.6.2 Risk Management Division:

- Directly coordinates the Company’s risk management processes in collaboration with senior management, first, second, and third lines of defense
- Develops and implements the risk management system
- Conducts risk assessment, analysis, and monitoring of compliance with risk limits
- Develops, improves, implements, and supports the Company’s internal regulatory documents on risk management
- Monitors compliance with this Policy and the implementation of relevant risk management procedures

- Participates in risk assessment, treatment, and monitoring processes within the Company
- Contributes to the development of Key Risk Indicators (KRI)
- Assists in the formulation of risk mitigation action plans
- Participates in the development of the internal control system
- Facilitates collaborative problem-solving within working groups through interviews, surveys, and group sessions for risk identification and assessment within the Company's units
- Prepares the annual risk assessment plan and risk assessment reports
- Conducts self-assessment of the risk management system and submits results for approval to the CRO;
- Promotes risk management culture and awareness through information campaigns, training materials, and employee education
- Provides guidance and consultations to employees on the application of internal risk management policies
- Coordinates the activities of risk coordinators
- Works hand in hand with the HR to organize a set of courses and training for the first line of defense, ensuring that employees throughout the business are educated to the highest risk management standards and there is a traceable evidence of colleague trainings

5.6.3 CCO/ Compliance Unit (in cooperation with the Corruption Prevention and Detection Service):

- Participates in the management of compliance risks, particularly in ensuring compliance with anti-corruption laws and conflict of interest regulations
- Ensures the organization of control measures to comply with legislation, internal policies, and professional association standards applicable to the Company
- Manages compliance risks related to conflicts of interest, ensuring process transparency at all levels of the Company's structure, including:
  - Mandatory declaration of employees' external activities
  - Monitoring the giving and receiving of gifts and invitations
  - Reviewing reports on relatives working together within the Company
- Maintains the compliance risk events database within the Company's overall operational and compliance risk events database
- Informs the Risk Management Division about events and operational incidents identified in the course of its work that may impact risk assessment and mitigation
- Ensures the functioning of the risk management system through timely identification, measurement, monitoring, control, reporting, and recommendations for compliance risk mitigation
- Takes all necessary measures to prevent decision-making that exposes the Company to significant compliance risks and ensures proper reporting to the General Director and Supervisory Board
- Reviews risk management reports and risk assessment results

5.6.4 Financial Monitoring Division:

- Ensures the proper organization of the system for preventing and combating money laundering and terrorist financing (AML/CTF)
- Ensures compliance with Ukrainian laws on AML/CTF

- Monitors currency transactions of clients to ensure compliance with Ukrainian foreign exchange laws
- Manages AML/CTF risks within financial monitoring to reduce them to an acceptable level
- Identifies high-risk financial transactions and determines whether they contain indications of money laundering or terrorist financing, taking appropriate actions where necessary
- Conducts second-level controls to ensure compliance with AML/CTF requirements at the first line of defense
- Participates in the identification, assessment, and mitigation of AML/CTF risks based on the Company's risk-based approach
- Contributes to the development of internal documents regulating risk management in compliance with AML/CTF requirements

5.7 Third line of defense – Internal Audit Department. The Internal Audit Department regularly evaluates the risk management and internal control systems' effectiveness, identifies weaknesses, and provides recommendations for improvement. Findings are reported to the Supervisory Board, General Director, CRO, and CCO to enhance the risk management system.

VI. RISK MANAGEMENT PROCESS

6.1 Risk management in the Company is a constant, dynamic and continuous process and consists of the following stages

- risk identification;
- risk assessment;
- risk treatment;
- monitoring and control of risks.

6.2 **Risk Identification** is the process of identifying risk elements, compiling a list of them and describing each risk element. The purpose of the risk identification process is to build a Risk Universe, which includes risks that may affect the achievement of the Company's goals and key performance indicators.

6.2.1 The Company strives for comprehensive risk identification based on the principle of the widest possible coverage of risk areas for each Company goal and development indicator.

6.2.2 Various combinations of methods and tools are used to identify risks, such as identifying risks based on the goals and objectives set, industry and international comparisons, seminars and discussions, interviews, databases of events that have occurred in the Company and in the market.

6.2.3 In particular, risk identification methods may include:

- methods based on past facts (for example, analysis of the risk event base);
- empirical methods, including testing and modelling to determine what might happen under specific circumstances;
- methods in which the subject matter under consideration is divided into smaller elements, each of which is in turn examined using methods that ask "what if" questions;
- methods that encourage imaginative thinking about future possibilities, such as scenario analysis;
- brainstorming methods.

6.3 **Risk assessment** is a process that combines risk analysis and comparative assessment and involves a detailed consideration of uncertainties, sources of risk, consequences, probabilities, events, scenarios, controls and their effectiveness. An event may have multiple causes and consequences and affect multiple objectives. Risk can be assessed for the entire Company, its units, individual projects or a single event.

6.3.1 Risk analysis is the basis for risk assessment – determining the acceptability of the level of risk, deciding whether and how to manage the identified risks, and the most appropriate risk management strategy and methods.

6.3.2 Risk analysis involves analyzing the likelihood of risk occurrence and the impact of identified hazardous events, taking into account the availability and effectiveness of risk management techniques already in place. Data on the probability of events and their consequences are used to determine the level of risk.

6.3.3 Risk analysis is carried out to identify the most significant (material) risks that may adversely affect the Company's activities, achievement of its strategic goals and objectives. The identified material risks are submitted for consideration to the Head of the Company, who makes decisions on their management and minimization, followed by approval by the Supervisory Board.

6.3.4 Risk analysis in the Company may involve qualitative, quantitative, or combined assessments.

6.3.4.1 Qualitative assessment involves setting a benchmark in qualitative terms. The basis for assignment to a particular group is a predetermined system of parameters, and the main method of assessment is the expert method. Qualitative assessment is carried out when it is impossible to use a mathematical approach.

6.3.4.2 Quantitative assessment involves assigning a quantitative parameter to a qualitative parameter. The intermediate step in the calculation may be indicators and coefficients that have different units of measurement, but the final result of the quantitative assessment is the amount of damage in monetary terms. Quantitative assessment allows comparing all types of risks and assessing their impact on the Company's operations.

6.3.5 The risk assessment process involves periodic self-assessment of risks, risk assessment upon occurrence of an event, collection of data on operational incidents, consolidation of risk assessment data from structural units performing the risk management function.

6.3.6 Risk assessment shall be carried out by the Risk Management Division in cooperation with key first- and second-line stakeholders annually, quarterly or in case of changes in internal and external factors affecting the Company's business processes.

6.3.7 For the purpose of risk assessment, the Risk Management Division may request information related to risks and events that affect the probability and level of risk impact on the achievement of strategic goals from the Company's structural units.

6.3.8 Data collection on operational incidents is carried out in the event of operational incidents and consists of

- identifying the operational incident;
- informing the risk coordinator about the incident;
- notification of the incident to the employees of the Risk Management Division;

- entering a report on an operational incident into the database of operational risk events (incidents) by the Risk Management Division;
- informing the authorised bodies and units about the incident in accordance with the relevant regulations for the interaction of the Company's structural units in the process of risk management.

6.3.9 For each risk, two risk assessments are determined - the inherent risk (worst-case scenario) and the residual risk (assessment of the scenario after the implementation of risk management measures).

6.3.10 The material risks identified at the assessment stage are reflected in the Risk Appetite Statement.

6.4 **Risk Heat Map**. The results of risk assessments are visually displayed using a risk map – a graphical and textual description of the risks relevant to the Company, placed in a rectangular table, one axis of which indicates the probability of risk occurrence, and the other - the level of risk impact on the Company's activities. The risk map allows assessing the relative importance of each risk for the Company on a 5-point scale, as well as identifying the risks that are key and require the development of management mechanisms.

6.4.1 Consideration of the probability of risk occurrence is defined as the probability of a single event with a significant impact or several events related to one risk that will have a significant impact on the Company's activities in aggregate.

6.4.2 When assessing the probability of a risk, the Company shall adhere to the following principles:

6.4.2.1 If there is data on risk realization in the database of operational incidents, historical data on operational incidents shall be used to substantiate the probability.

6.4.2.2 If there is historical data on risk realization in other sources (external databases of operational incidents, data from other organizations, enterprises, countries, normative values, data from financial or management reporting, other internal data), data from other sources of historical data are used to substantiate the probability.

6.4.2.3 If there is historical data on changes in the factor that leads to the risk, historical data on changes in the risk factor are used.

6.4.2.4 In the absence of historical data on risk realization, expert estimates (expert judgements) are used.

6.4.3 Risk Probability Assessment Table

The probability of risk realization is classified in a table format, where risks are categorized based on their likelihood and potential impact.

Score	Risk Probability Assessment	Probability of risk realisation	Frequency based on historical data
5	Critical	80%< *** <=100%	More than once per year
4	High	60%< *** <=80%	Once every 1–2 years
3	Moderate	40%< *** <=60%	Once every 2–3 years
2	Low	20%< *** <=40%	Once every 3–5 years
1	Insignificant	0%<= *** <=20%	Once every 5 years or less frequently

6.4.4 Principles for Assessing Risk Impact

6.4.4.1 The significance level of risk impact should be determined based on its effect on achieving strategic objectives within a one-year timeframe.

6.4.4.2 Impact analysis should include both quantitative and qualitative assessments of risk significance, using planned financial indicators from the Company's financial plan for the current year as a common benchmark.

6.4.4.3 Risks should be assessed considering the highest potential impact.

6.4.4.4 When assessing risk impact, potential cumulative effects associated with risk realization should be taken into account. If risk-related losses may accumulate over multiple years, the total impact should be evaluated over the corresponding time horizon.

6.4.4.5 Impact assessment should be conducted in the context of the Company's strategic goals and operational plans.

6.4.5 Risk Impact Level Ranking

The ranking of risk impact levels follows the same scale as the risk probability assessment, from "Critical" to "Insignificant", ensuring consistency in risk evaluation. I will now format the corresponding table for this ranking.

Score	Assessment of Risk Impact
5	Critical
4	High
3	Moderate
2	Low
1	Insignificant

6.4.6 Risk Impact Assessment Considering the Following Aspects:

- Financial Aspect – Reflects the impact of risk realization on financial performance.
- Impact on Operations – Analyzes potential disruptions in production processes that could harm the Company's operations, core processes, and product delivery.
- Regulatory and Legal Aspect – Assesses potential liability under current legislation in the event of risk materialization.
- Strategic Aspect – Examines the consequences of risk realization for achieving strategic objectives.
- Health & Safety Impact – Determines the event's effect on employee health and safety.
- Reputation & Social Responsibility Aspect – Evaluates how the event is perceived by the media and the extent of negative information dissemination (national/international level).
- Environmental Aspect – Analyzes the impact on ecology, biodiversity, and greenhouse gas emissions.

6.4.7 Based on the **risk probability assessment** and the **risk impact level**, the **risk level** is determined as the **product of the two values**:

Risk level						
Impact	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Probability				

6.4.8 Description of risk levels

Score	Risk Level	Description
16-25	Critical	If the risks materialize, they could lead to critical consequences, including business interruption, significant financial losses or serious reputational damage.
12-15	High	Significant negative impact on the Company's operations; significant deviations from plans, significant financial losses or serious disruptions in processes. They require immediate measures to mitigate them.
8-10	Moderate	Moderate impact on certain aspects of the Company's operations; possible delays, cost increases or quality deterioration are possible. Requires attention and planning to minimize their impact.
4-6	Low	Minor impact on processes or outcomes; minor delays or additional costs may occur, but the impact is easily controlled and does not require significant resources to address.
1-3	Insignificant	Minimal or no impact on the Company's operations; insignificant deviations from targets, no significant financial losses or disruptions in processes.

6.4.9 Risk Level Calculation. The risk level is calculated in the national currency by assessing the potential impact of the risk or opportunity on EBITDA, operating profit, and free cash flow (FCF). If monetary evaluation is not feasible, an expert scoring scale is applied.

6.5 **Risk treatment** is the process of selecting, developing, and implementing measures to reduce the negative effects and likelihood of losses associated with the Company's risks. These measures aim to prevent exceeding the established risk appetite levels.

6.5.1 Risk Treatment Options. Risk management strategies are not mutually exclusive and may be applied in combination. The following approaches may be used:

6.5.1.1 Risk Acceptance – The Company accepts the risk without taking action if:

- The risk cannot be influenced, or
- The cost of mitigation exceeds the potential losses, or
- The risk is within the defined risk appetite and is not significant.

6.5.1.2 Risk Avoidance – The Company does not accept the risk, even with mitigation efforts. The Company avoids any actions or decisions that may lead to this risk. This method is preferable for critical risks.

6.5.1.3 Risk Transfer (Sharing) – The Company transfers part or all of the risk to external contractors or outsources functions/processes. This method is used for risks that the Company cannot manage effectively or influence their source.

6.5.1.4 Risk Mitigation – The Company reduces the potential impact and/or probability of risk through mitigation actions, such as:

- Implementing corrective and/or control measures
- Enhancing existing procedures
- Introducing additional risk control mechanisms

6.5.1.5 Contingency Planning – The Company develops action plans for potential risk events, emergencies, or crisis situations. The plan includes:

- Response procedures
- Roles of employees
- Resources required in case of risk occurrence

This method is mainly used for operational risks that may cause business disruptions.

6.5.1.6 Strengthening Internal Controls – The Company enhances preventive control procedures if they are effective and/or implements new post-factum control procedures.

6.5.1.7 Leveraging Opportunities – The Company actively utilizes opportunities that arise from risk events to generate additional benefits.

6.5.2 Selecting Risk Treatment Options

The selection of the most appropriate risk treatment strategy is based on balancing potential benefits with the associated costs, efforts, and drawbacks.

6.5.3 Approval of Risk Treatment Decisions

Decisions regarding risk treatment are reviewed and approved by the Chief Risk Officer (CRO) and the General Director, as needed. These decisions are mandatory for all Company departments.

6.5.4 Responsibility for Risk Treatment Implementation

The risk owners are responsible for the implementation of approved risk treatment measures.

6.6 **Risk monitoring and control** are key components of the risk management process.

6.6.1 Risk monitoring involves:

- Calculating the current risk level
- Tracking its dynamics over time
- Analyzing causes of change
- Developing preventive measures to normalize risk levels if negative trends are detected
- Establishing a controlled process for influencing the size and dynamics of the accepted risk

6.6.2 Risk Control Objective. The goal of risk control is to ensure that the accepted risk level aligns with the defined risk appetite.

6.6.3 Key Components of Risk Monitoring

6.6.3.1 Establishing a Risk Monitoring System – Developing a framework or procedures to monitor risks, including:

- Defining Key Risk Indicators (KRI)

- Selecting tools and processes for identifying and tracking risks

6.6.3.2 Setting Key Risk Indicators (KRI) and Thresholds – Establishing thresholds to track risk level changes.

6.6.3.3 Defining Monitoring Frequency – Regular reviews based on risk dynamics and significance.

6.6.3.4 Data Analysis – Risk data collected from risk owners is analyzed by the Risk Management Division to:

- Assess the current risk portfolio
- Track risk trends and dynamics

6.6.3.5 Regular Risk Reporting – Ensuring periodic reporting on the risk portfolio, including:

- Risks exceeding predefined thresholds
- Effectiveness of existing control measures

6.6.3.6 Communication with Stakeholders – Keeping stakeholders informed about the risk situation and actions taken.

6.6.3.7 Review of Control Measures – If existing risk treatment measures are ineffective or if KRI trends are negative, the control framework is reviewed and adjusted.

6.6.4 Risk Control Mechanisms

Risk control includes:

- Aggregated risk monitoring (Company-wide risks)
- Individual risk monitoring (specific risk categories)
- Compliance with established risk limits
- Risk management authority and control structure
- Internal control mechanisms
- Internal and external audits

VII. RISK CLASSIFICATION

7.1 The Company Identifies the Following Groups of Material Risks:

- Strategic Risks
- Operational Risks
- Compliance Risks
- Financial Risks

7.2 Strategic risk refers to the risk of losses due to changes or errors in the definition and implementation of the Company's strategy, as well as external systemic factors such as:

- Political environment changes
- Regional market trends
- Market downturns
- Other external systemic factors

7.3 Operational risk is the risk of losses, additional costs, or missed revenues resulting from:

- Deficiencies or errors in internal processes
- Intentional or unintentional actions by employees or third parties
- Failures of information systems
- External disruptive factors that impact the Company's daily operations

This category includes cybersecurity risks and information security risks.

7.4 Compliance Risk

Compliance risk refers to the risk of losses due to the Company's failure to comply with:

- Ukrainian legislation
- Regulatory requirements
- Market standards
- Internal corporate ethics policies
- Conflict of interest policies
- Anti-corruption regulations
- Sanction restrictions
- Financial monitoring obligations

7.5 Financial risk refers to events that may directly or indirectly cause financial losses for the Company. These risks include:

- Liquidity and solvency risk
- Investment risk
- Currency risk
- Counterparty risk

7.6 The above-listed risks are not mutually exclusive, meaning a single event or series of events may lead to multiple risks occurring simultaneously.

7.7 Risk Register and Internal Regulations

A detailed classification of these material risk groups is outlined in:

- The Risk Register
- Internal documents that regulate specific risk management processes

7.8 The Risk Management Division is responsible for:

- Developing and maintaining an up-to-date Risk Register
- Ensuring it contains a comprehensive, evolving list of risks the Company may face

7.9 The Risk Register serves as the foundation for risk identification. It is updated as needed, but at least once per year.

7.10 Risk identification is mandatory before implementing new services, products, or processes.

7.11 The Risk Management Division maintains an up-to-date Risk Events Database, which is updated quarterly based on reports from risk coordinators in business units.

7.12 Regulation of the Risk Events Database.

The Risk Events Database is governed by a separate internal regulatory document.

VIII. APPROACH TO DETERMINING RISK APPETITE

8.1 The Company's objectives and tasks must align with its approved risk appetite, which defines the acceptable level of uncertainty in achieving strategic goals.

8.2 Basis for Determining Risk Appetite

Risk appetite is determined using key performance indicators (KPIs) such as:

- EBITDA
- Operating profit
- Free cash flow (FCF)

8.3 Risk Appetite Review

The Company reviews its risk appetite in the event of:

- Changes in strategic objectives
- Changes in acceptable risk levels

IX. RISK REPORTING AND ESCALATION SYSTEM

9.1 Establishing an Effective Risk Reporting System

The risk management system ensures effective interaction between stakeholders through a regular, transparent reporting process.

9.2 Risk Reporting Requirements

Risk reports must:

- Provide clear and comprehensive information for timely decision-making
- Be accurate, verified, and reliably reflect the Company's risk exposure
- Cover all material risk types, including: risk concentrations, compliance with risk appetite limits

9.3 Quarterly Reporting to the Supervisory Board and Audit Committee

At least once per quarter, the Supervisory Board and Audit Committee receive reports from the Risk Management Division detailing:

- The current status of the risk management system
- The most significant risks and mitigation plans

9.4 Quarterly Reporting to the General Director

At least once per quarter, the General Director receives information from the Risk Management Division on:

- Risk identification results
- Risk treatment measures

9.5 Regular Risk Data Collection from Business Units

The Risk Management Division collects risk-related information from all business units at least quarterly, covering:

- Potential risks
- Realized risks

9.6 Components of Risk Management Reports

Risk reporting consists of:

- Annual Consolidated Risk Assessment Report
- Quarterly Risk Management Report

9.7 Annual Consolidated Risk Assessment Report

This report includes:

- Risk Heat Map highlighting key risks
- Tables with risk assessments by business activities
- Identified risk events and incidents over the year
- Implementation status of risk treatment plans
- Developments in the risk management system

9.8 Quarterly Risk Management Report

This report includes:

- Risk Heat Map with key risks

- Key Risk Indicators (KRI)
- Newly identified risks and incidents
- Execution status of risk treatment plans
- KRI trends over time
- Current Risk Management Division objectives

9.9 Compilation of Risk Reports.

The Risk Management Division prepares reports based on data from business units.

9.10 Approval Process for Risk Reports.

Risk reports are submitted to:

- The General Director
- The Audit Committee under the Supervisory Board
- The Supervisory Board for approval

9.11 Principles of the Risk Reporting System.

Risk reporting must adhere to the following principles:

- Rationality – Focus on efficiency while ensuring all necessary information is included
- Clarity – Reports must be understandable to the target audience
- Transparency – Data should be accurate, correct, and comparable
- Completeness – Must include all significant risks and financial resource comparisons
- Comparability – Allows for aggregation of risk data across business units
- Terminological Consistency – Ensures a unified risk terminology for crisis response
- Integrity – Reports must be structured and issued at set intervals

X. RISK CULTURE

10.1 Risk management culture is a component of the Company's overall corporate culture and contributes to the formation of a sufficient level of awareness among all employees regarding the importance and rules of the risk management system. The development of risk management culture is carried out through training, thematic focus group meetings in order to promote the risk management process and maximize employee involvement in this process.

10.2 The Company’s risk management culture fosters employee awareness of:

- The importance of risk management
- The functioning of the risk management system

10.3 Development of risk culture is achieved through:

- Training programs
- Focus group discussions
- Employee engagement initiatives

10.4 The goal is to ensure that management and employees:

- Avoid decisions that result in excessive risk
- Take actions to reduce risk exposure
- Understand the importance of risk management at all levels

XI. RISK MANAGEMENT SYSTEM EVALUATION

11.1 The risk management system assessment is conducted based on international standards (ISO 31000, COSO) and includes maturity level analysis, self-assessment of departments, monitoring of key risk indicators (KRI), risk event analysis, and scenario modeling.

11.2 The risk management system assessment is carried out on a regular basis to determine its maturity, effectiveness, and alignment with the Company's strategic objectives. This enables structural unit managers and the Risk Management Division to obtain an objective view of the current state and tools for improving risk management.

11.3 The objectives of the risk management system evaluation:

- Determining the maturity level of the risk management system in accordance with international standards ISO 31000, COSO
- Evaluating the effectiveness of risk management processes
- Identifying areas for improvement and eliminating weaknesses
- Developing and implementing measures to enhance the effectiveness of risk management

11.4 The assessment is based on key performance indicators grouped into the following areas:

- Integration of risk management into operational activities and management decisions
- Incorporation of risks into strategic planning and budgeting processes
- Activities of the responsible unit aimed at developing a risk management culture within the Company
- Optimization of risk management approaches and their adaptation to environmental changes
- Distribution of responsibility for risk management between managers and employees
- Competency level of personnel in risk management
- Management of key risks

11.5 The risk management system assessment utilizes the following methods:

- Risk management maturity analysis – evaluating the effectiveness of the risk management system, its integration into the organization's activities, compliance with international standards, and the control and improvement mechanisms applied
- Surveys of structural units
- Monitoring of key risk indicators (KRI)
- Use of risk matrices and scenario analysis, among others

11.6 The Internal Audit Department evaluates and provides conclusions and recommendations regarding the effectiveness of the risk management system.

XII. FINAL PROVISIONS

12.1 All employees are responsible for complying with this Policy. Violations such as:

- Hiding information
- Providing false information
- Non-disclosure of conflicts of interest

may lead to disciplinary action, including:

- Termination of employment
- Administrative or criminal liability under Ukrainian law

APPENDIX 1. FUNCTIONS, RIGHTS, AND REQUIREMENTS FOR THE RISK COORDINATORS

1. Functions of Risk Coordinators include:

1.1 Participate in the validation of risk probability and impact assessments, support business units in applying the methodology.

1.2 Participate in the development of risk mitigation plans.

1.3 Timely submission of risk assessment reports and proposals on how to handle risks and risk incidents to the Risk Management Division.

1.4 Foster a risk management culture within the Company.

1.5 Informing the Risk Management Division about the results of risk assessment of the Company's structural units.

2. **In order to perform their main functions in accordance with the established procedure, Risk Coordinators shall have the right to:**

2.1 Interact with the Company's employees on risk management issues.

2.2 Have access to all necessary documentation and other information on the sources of risk, in case of resolving issues within their competence and within their authority.

2.3 Make requests and receive information from employees of the relevant departments on identified risks and the results of their assessment, operational incidents and the results of internal investigations.

2.4 To make proposals to the Chief Risk Officer and the Head of the Company on risk assessment and processing measures and other issues within the competence of the Risk Coordinator.

2.5 Provide the structural units of the Company involved in risk management processes with methodological recommendations and expert advice on the identification, analysis, assessment, processing and monitoring of risks.

2.6 Participate in meetings, seminars and conferences related to risk management.

2.7 Plan and coordinate resources to perform their functions.

2.8 Initiate consideration of issues related to risk management by the head of the relevant department and the Head of the Company.

3. Qualification Requirements for Risk Coordinators:

3.1 Knowledge of the processes inherent in postal service companies.

3.2 Knowledge of the postal service market.

3.3 Knowledge of regulations governing the postal service sector.

3.4 Ability to analyze economic processes.

3.5 Skills in organizing and conducting structured meetings, working independently and in a team, and managing workflows efficiently.

3.6 Analytical thinking, ability to draw well-grounded conclusions.

4. The performance of Risk Coordinators shall be assessed by the Chief Risk Officer, based the following KPIs:

4.1 Timely reporting of risks and incidents identified within the unit's scope of activities to the Risk Management Division.

4.2 Timely execution of the annual risk assessment plan identified within the unit.

4.3 Timely updating of the Register of risks inherent in the unit's activities.

4.4 Timely updating of the database of operational risks (incidents) identified within the unit's activities.

4.5 Calculation of key risk indicators (KRIs) identified within the unit's activities within the timeframe established by internal procedures.