APPROVED
by the decision
of the Audit, Risk, Compliance and Sustainable Development Committee
of VK Company Limited
on August 2, 2023
(Changes:
BoD Minutes № 04-2023,
November 8, 2023)

CORPORATE RISK MANAGEMENT POLICY OF VK INTERNATIONAL PUBLIC JOINT-STOCK COMPANY ITS SUBSIDIARIES AND AFFILIATED COMPANIES

2023

Table of contents

ARTICLE 1. GENERAL PROVISIONS

1.1. The Corporate Risk Management Policy of VK International Public Joint-Stock Company (hereinafter referred to as the "Policy") describes the goals, objectives, principles and structure of the Corporate Risk Management System.

1.2. This Policy applies to VK International Public Joint-Stock Company, all of its subsidiaries and affiliates (collectively referred to as the "Company") and is binding on all employees of the Company.

1.3. The Policy takes into account best practices, proposed national and international standards for corporate risk management, as well as the requirements of applicable law.

1.4. The Policy is supplemented by the Corporate Risk Management Procedure and other documents that define the corporate risk management process.

ARTICLE 2. CORPORATE RISK MANAGEMENT SYSTEM

2.1. The purpose of the Corporate Risk Management System is to reduce the negative impact of external and internal risk factors on the Company's performance, as well as to contribute to the advancement of the Company's strategic and operational goals in a changing internal and external environment, to reduce the level of uncertainty in decision-making processes, to increase operational stability, and to improve risk analysis and assessment procedures, risk level control, and the quality of the reporting system.

2.2. Objectives of the Corporate Risk Management System:

- Timely identification of risk factors, prevention of risk materialization and/or mitigation of risk consequences, including potential damage, to an acceptable level;
- Provision of risk management information to the Audit Committee;[1]
- Regular monitoring of the impact of risks on the Company's operational and financial well-being, ability to achieve strategic and tactical/operational goals, ability to comply with the legislation of the Russian Federation, and the Company’s reputation;
- Keeping regulatory requirements and corporate risk management processes up to date;
- Developing a corporate risk management culture within the Company.

2.3. Management structure:

- The Audit Committee is a collegial body reporting to the Board of Directors. Its responsibilities include assisting the Board of Directors in monitoring the reliability and effectiveness of the risk management and internal control systems, as well as the efficiency of the internal control and risk management processes.
- The Corporate Risk Management and Compliance Commission is a collegial internal body composed of representatives of Senior Management and the Director of the Corporate Risk Management Department, which ensures the effective operation of the corporate risk management system. The Committee is responsible for managing and monitoring corporate risks, making recommendations to strengthen the corporate risk management culture, and reviewing information on serious incidents that have materialized in the Company. The Committee also provides appropriate assurance to the Audit Committee and the Board of Directors that the Company has a clearly defined, efficient and effective corporate risk management and compliance system.

[1] Audit, Risk, Compliance and Sustainable Development Committee of the Board of Directors

- The Corporate Risk Management Department provides methodological support, coordinates and monitors the Company's corporate risk management process and ensures compliance with the Corporate Risk Management Policy. It also works to improve the Corporate Risk Management System and serves as the Company's Corporate Risk Management Expert Center.
- The Company's management and employees are responsible for regularly identifying and, within the scope of their authority, managing the Company's risks with the support of the Corporate Risk Management Department.

ARTICLE 3. CORPORATE RISK MANAGEMENT PROCESS

3.1. The goal of the Corporate Risk Management Process is to identify threats, prevent potential losses, analyze the causes, and mitigate the effects of materialized risks.

3.2. Risks that may affect the company's ability to achieve its goals and results should be classified, evaluated, and prioritized. Countermeasures (response plans) should be developed and implemented as part of corrective action plans aimed at reducing the level of risk.

3.3. The corporate risk management process consists of five steps:
- *Identifying risks.* The Company's management and employees analyze risk assessment areas (changes in the external and internal environment), identify and explain events that could result in large losses or failure to achieve the Company's strategic or operational objectives.
- *Evaluating and prioritizing risks.* Analyzing the likelihood of risk materialization and its impact on the Company, determining the contribution of each risk to the overall risk portfolio, evaluating their impact on the Company’s key performance indicators, and then prioritizing them based on magnitude, speed of materialization, and severity of impact.
- *Developing and coordinating response plans.* Countermeasure plans are developed and approved to reduce the likelihood of risk materialization and/or its impact on the Company. Countermeasures are implemented by designated personnel.
- *Implementing response plans.* Implementing risk mitigation plans for identified risks to limit the negative impact of risks on the Company's operations to an acceptable level within the risk appetite (Appendix 2).
- *Risk monitoring.*

3.4. The following risk response measures are used in the Enterprise Risk Management process:
- *Mitigate risk.* Reducing the likelihood and magnitude of potential losses by applying methods to reduce the probability of risk materialization or the magnitude of the consequences of the risk.
- *Avoid risk.* Rejecting activities and operations associated with a high risk to the Company, its assets, strategic development, operations, and stakeholder activities.
- *Transfer risk.* Transferring risk responsibility to a third party for risk regulation or financing using the following tools: risk insurance, risk hedging, appropriate contractual forms, and protective clauses.
- *Accept risk.* A reasoned and formalized judgment that there is no need to respond to a risk and a willingness to accept damage from the possibility of a negative event materializing.

3.5. The Corporate Risk Management Process distinguishes between the following risk categories: strategic, financial, legal (including compliance), and operational.

ARTICLE 4. BASIC PRINCIPLES OF CORPORATE RISK MANAGEMENT

4.1. The corporate risk management process is an integral part of the management of the Company and its business processes. It implies a unified risk management strategy.

4.2. Corporate risk management is an essential component of every Company employee's activity within their field.

4.3. Managers at all levels are responsible for providing timely information to stakeholders about risks that threaten the achievement of the Company's objectives.

4.4. The Company's General Director is responsible for the establishment, operation, and effectiveness of the Enterprise Risk Management process.

4.5. The Company's corporate risk management is performed at three levels: 1) at the level of management and risk owners who directly execute business processes and manage the risks associated with them; 2) at the level of departments that perform methodological and control functions for risk management; and 3) at the level of departments that perform an independent assessment of the corporate risk management system (Appendix 1).

4.6. The Company provides risk owners with all the resources necessary to perform their duties, including information, financial, human, and intangible resources.

4.7. As part of the risk management process, the Company maintains an appropriate balance between the cost of risk management and the amount of potential loss from the risk event materialization. If the level of risk is acceptable and the cost of managing the risk exceeds the potential impact, the Company may not implement risk mitigation measures.

4.8. The Company ensures the accumulation of knowledge about risks, including the analysis of materialized risks, and the dissemination of such knowledge among employees in compliance with the Company's information security and information protection rules.

4.9. In order to reduce the likelihood of potentially undesirable events materializing, the Policy and related internal regulatory documents should be used in the Company's risk management process as guiding principles in the implementation of all project initiatives, as well as in the day-to-day operations of the Company.

ARTICLE 5. OTHER PROVISIONS

5.1. The Policy is intended to provide reasonable, but not absolute, assurance that Corporate Risk Management objectives will be achieved, taking into account the following:

- Risks may exist beyond of the Company's scope of responsibility or control;
- There may be an insurmountable level of uncertainty about future events and a lack of reliable data for risk assessment;
- Control of the Risk Level may be limited by insurmountable factors.

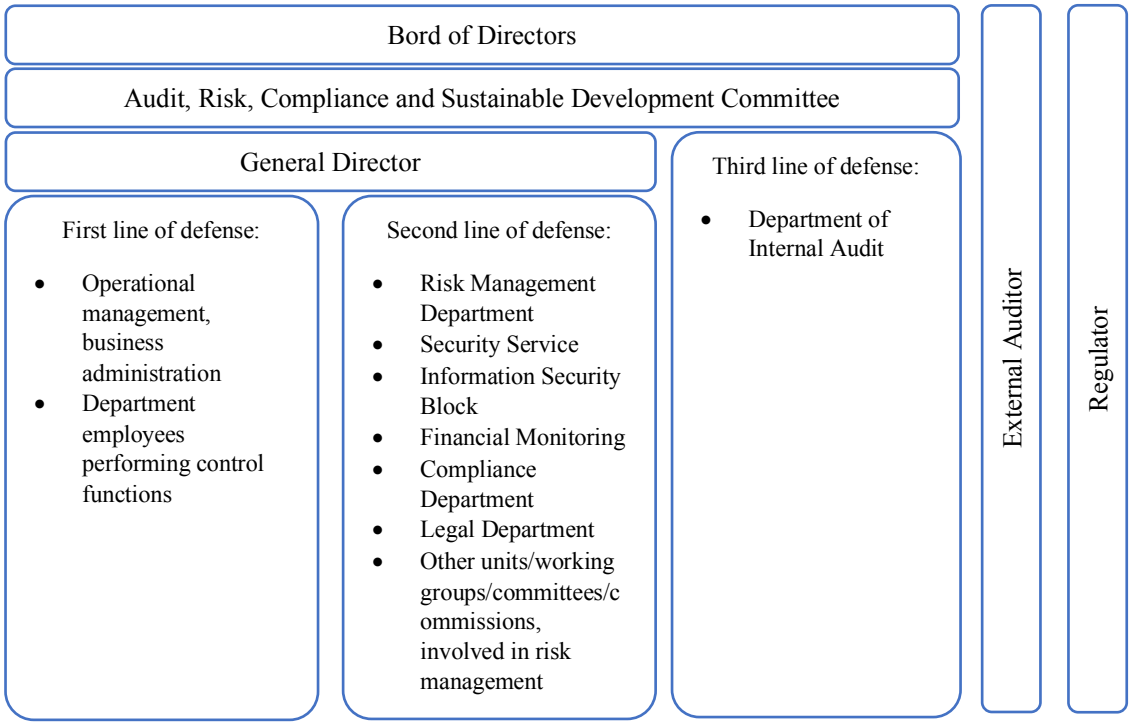
5.2. The Policy is reviewed and revised in the event of significant changes in the Company, in risk management methodology and practice, or in the applicable legislation of the Russian

Federation. The need to amend the Policy is discussed once a year by the Corporate Risk Management and Compliance Commission.

5.3. Other documents related to the Policy, such as the Corporate Risk Management Procedure, are revised in accordance with the policy review cycle. Appendix 2 provides is a list of common glossary and terms used in the Policy.

5.4. The Corporate Risk Management Department can provide comprehensive information on corporate risk management.

APPENDIX 1. THREE LINES OF DEFENSE[2]



Board of Directors
Oversees that the Company manages risk appropriately through structured and effective systems and processes. Establishes an acceptable risk appetite for achieving the Company's strategic objectives. Ensures an effective internal audit function based on the risk assessment.

Audit Committee of the Board of Directors
Assists the Board of Directors in monitoring the reliability and effectiveness of the risk management and internal control systems (see the Audit Committee Appendix for more information).

Corporate Risk Management and Compliance Commission
The Corporate Risk Management and Compliance Commission is a collegial internal body composed of representatives of the Company's senior management and the Director of Corporate Risk Management Department, ensuring the effective operation of the Corporate Risk Management System. The Commission is responsible for managing and monitoring corporate risks, making recommendations to strengthen the corporate risk management culture and reviewing information on serious incidents that have materialized in the Company. The Committee also provides appropriate assurance to the Audit Committee and the Board that the Company has a well-defined, efficient and productive enterprise risk management and compliance system.

General Director
Informs the Board of Directors of the Company's overall risk management issues.

[2] The Company's Three Lines of Defense model is based on the corresponding model of the Institute of Internal Auditors from 2020.

First line of defense
The first line of defense includes the operational management and the departments that manage corporate risks within their activities. Managers of business units and structural departments are responsible for achieving results and ensuring the effectiveness of their processes, as well as the effectiveness of the risk management and internal control system. Control procedures executors perform them in accordance with their job duties and regulatory documents.

Second line of defense
The second line of defense is provided by the Corporate Risk Management Department, which coordinates the Corporate Risk Management Process, as well as other departments, working groups, committees and commissions that are involved in Corporate Risk Management as part of their job.

Third line of defense
The Internal Audit Department conducts an independent evaluation of the effectiveness of the Company's enterprise risk management and internal control system, identifies deficiencies in the activities of the first and second lines of defense, provides recommendations for improving the enterprise risk management and internal control system, and monitors the implementation of corrective actions to improve the risk management and internal control system identified in the audit.

APPENDIX 2. TERMS AND DEFINITIONS

Risk owner is the head of a structural division or business unit of the Company who is responsible for identifying and managing corporate risks in the relevant business area, including the identification and availability of sufficient countermeasures and resources to control the risk, the implementation of risk mitigation measures, risk monitoring, and the identification and reporting of materialized risks (incidents).

Executing a response plan involves the implementation of countermeasure strategies for identified risks to reduce their negative impact on the Company's operations to an acceptable level within the risk appetite.

Risk identification is the process of identifying and describing events that could have a negative impact on the Company's goals.

Senior management – Company's leaders reporting directly to the General Director.

Internal Audit Department is an independent structural unit reporting to the Board of Directors. The Audit Committee determines the procedure for the work of the Internal Audit Department and its interaction with the Board of Directors. The Internal Audit Department performs internal reviews and analyzes business processes, the adequacy and effectiveness of control procedures, the results of the Company's operations, evaluates corporate governance and the Company's risk management system, and may perform other tasks related to the audit of subsidiaries and affiliates.

Information security and protection – the practice of preventing unauthorized access, use, disclosure, distortion, modification, inspection, recording, or destruction of the Company's information.

Incident is the result of the risk materialization or an event that has a negative impact on the Company/process/project and results in losses.

Countermeasure is an action designed to reduce the risk of an adverse event materialized and/or the damage caused by its materialization.

Corporate risks are the risks associated with the Company's activities.

Corporate risk management culture (risk culture) is the set of behaviors and beliefs that exist within the Company and contribute to forming an effective control environment, including corporate risk management.

Risk management measures are activities or countermeasures developed on one of the following risk management options: mitigating risks, avoiding risks, transferring risks, or accepting risks.

The Three Lines of Defense model is the Company's strategy for allocating authority and responsibility among the participants in corporate risk management.

Risk monitoring – the process of updating information on the level of risk, external and internal factors influencing the level of risk, and the status of the Company's risk management activities.

Risk assessment is the process of estimating the level of risk based on the likelihood of an adverse event materialized and the significance of its impact on the Company.

Response plan preparation and coordination - countermeasure plans are developed and agreed to reduce the likelihood of risk materialization and/or the level of impact of risks to the Company. Individuals responsible for implementing the countermeasure plans are assigned.

Risk consequences are the results of the risk materialization, expressed as a quantitative or qualitative impact on the Company, its activities, or its goals.

Acceptable level of risk is determined by the risk owner at the risk assessment and prioritization phase, considering the likelihood and magnitude of the risk's impact, as well as the risk appetite established by the Company.

Risk prioritization is the ranking of risks based on established priority factors, such as assessing their impact on the Company's key performance indicators, the speed with which they materialize and their impact, and so on.

Corporate Risk Management Procedure is a methodological document that complements the Corporate Risk Management Policy with additional, more detailed information on methods and tools for a more understandable, clear, systematic and consistent approach to corporate risk management in the Company.

Corporate Risk Management Process is the consistent and systematic application of policies, procedures, international best practices, as well as Company practices for information sharing and consulting, external and internal environmental analysis, risk identification and assessment, risk impact, risk monitoring, and risk re-assessment.

Risk materialization is the occurrence of a negative event.

Risk is a potential internal or external event that, if it happens, will have a negative impact on the Company's strategic or operational objectives and result in unfavorable outcomes. On the other hand, opportunities are certain events have a positive impact.

Risk appetite – the highest level of risk that the Company is ready to accept in order to achieve its business objectives.

Internal control system is a set of procedures implemented by the Company to monitor and manage operational and financial processes.

Corporate Risk Management System is a collection of the Company's practices and procedures, functions and roles, as well as risk-management activities.

Level of risk – the relevance of a risk determined by its likelihood and the magnitude of its potential impact of its materialization.

Risk factor is a set of circumstances or events that, alone or in combination with others, can contribute to the risk materialization.