"APPROVED"
decision of the Board of Directors
joint-stock company
"National company
"Kazakhstan Temir Zholy"
dated December 18, 2019 protocol No.20

Changes and additions were made by the
decision of the Board of Directors
joint-stock company
"National company
"Kazakhstan Temir Zholy"
dated October 28, 2022 protocol No.14

POLICY OF JSC “NC “KTZ”
RISK MANAGEMENT AND
INTERNAL CONTROL

Section 1. General Provisions.

1. This Policy of the National Company "Kazakhstan Temir Zholy" on risk management and internal control (hereinafter referred to as the Policy) is developed in accordance with recommendations of the Committee of Sponsorship Organizations of the Tradeway Commission (COSO) and other best practices in risk management and internal control.

2. The purpose of the Policy is to build an effective risk management and internal control system to support the achievement of strategic goals, protect assets and ensure the financial stability of the National Company Kazakhstan Temir Zholy Joint Stock Company (hereinafter referred to as the Company).In addition to the Policy, the Company has documents regarding certain types of risks and other internal regulatory documents.

2.1 The internal control process is an integral part of the Company's risk management system. Company risk management is a broader system than internal control, which includes and develops the internal control process, transforming it into a more effective, more risk-oriented form.

3. In addition to the Policy, the Company has documents regarding certain types of risks and other internal regulatory documents.

4. The Policy, being a part of the Company's corporate governance, is mandatory for the Company's structural subdivisions and branches. The Policy serves as the basic document for the approval of its Risk Management and Internal Control Policies in the Company's subsidiaries.

5. The policy applies to subsidiaries that are part of a group of companies, all voting shares (participatory interests) of which are directly or indirectly owned by the Company.

6. The Policy is posted on the Company's website and its main provisions are disclosed in the Company's annual report.

Section 2. Terms and abbreviations.

7. The following terms and abbreviations are used in the Policy:

process risk owner	-	business process owner;
risk owner	-	a person (employee/structural unit/collegial body) responsible for all aspects of managing a certain risk, in particular risk identification and assessment, reducing the likelihood of risk realization and/or reducing the possible impact of the consequences of risk realization on the Company;
owner/ executor of the control procedure	-	a responsible employee of the structural unit of the Company, carrying out procedures and actions aimed at preventing or reducing risk events within

		the business process;
internal control (VC)	-	the process designed to provide “reasonable assurance” regarding the achievement of operational goals, reporting objectives and compliance with the law, the requirements of the Company’s internal regulatory documents, carried out by the Board of Directors of the Company, the Management Board and employees of the Company, is part of the CRMS;
subsidiaries (DO)	-	legal entities, more than fifty percent of voting shares (participatory interests) of which are directly owned by the Company on the right of ownership or trust management of the Company;
guarantee card	-	determines the areas of responsibility and allocates responsibilities for confirming the effectiveness of the Company's business processes, risk management systems and internal controls and promotes effective coordination of activities between the participants in the internal control system of the first, second and third lines of defense.
risk map	-	a graphic representation of the Company's risks on a consolidated basis, located in a rectangular table, the vertical axis of which indicates the amount of damage to the risk, and the horizontal axis indicates the probability of its occurrence;
key risk indicator (KRI)	-	an indicator signaling trends in risk factors and the possible realization of risks that could have a negative impact on the Company's activities;
control (control procedure)	-	an element of internal control, a documented set of actions, system configuration or organization of processes that reduce the likelihood of a risk realizing or mitigate its consequences, the control procedure is an integral part of business processes;
«Three lines of defense» model	-	approach to the organization of the CRMS, based on the fact that for effective risk management and internal control under the leadership of the Board of Directors of the Company, it is necessary to divide the roles and responsibilities between three separate groups (lines of defense): business functions (each structural unit of the Company), the risk monitoring function and control, the function of independent assessment of the

		effectiveness of risk management and internal control (Internal Audit Service);
business continuity	-	the strategic and tactful ability of the Company to plan its actions and respond to emergency events in order to continue to provide services at an acceptable level;
risk assessment (risk damage)	-	risk assessment expected after the adoption of countermeasures accounted for in the Development Plan as an expense item. This risk assessment is done by calculating the five-year cumulative deviation of EBIT (if possible) if the risk materializes;
risk profile	-	a comprehensive review of the Company's risks, which allows considering the types, degree of influence and interdependence of risks, their consequences on the results of the Company's activities;
risk register	-	a document containing information about the identified risks of the Company on a consolidated basis (risk description, risk factors, risk owner, risk assessment indicators, etc.), in addition to the risks of the Company, the Register includes the risks of companies included in the red zones of the company risk maps;
risk	-	the likelihood of occurrence of events that may affect the achievement of the strategic and business goals of the Company;
risk appetite	-	the acceptable amount of risk and / or loss that the Company is ready to accept in order to achieve its goals;
risk coordinator	-	this is an employee who is responsible for organizing the management of operational risks of a particular structural unit of the Company;
risk division	-	structural subdivision of the Company responsible for organizing the risk management system, internal control and business continuity;
Structural unit (JV)	-	structural subdivision of the Company;
Tolerance (level of tolerance to key risks)	-	an acceptable level of deviation in relation to the achievement of a specific business goal due to the realization of the risk;
risk management (risk management)	-	culture, competencies methods and approaches integrated into all processes of the Company (from strategic planning to performance management),

		which the Company relies on (to manage risks) in creating, maintaining and realizing value. Risk management is one of the key elements of corporate governance, an integral part of the management decision-making process at all levels of the organization. In the Policy, the terms "risk management", "risk management", "corporate risk management system (CRMS)" are used interchangeably;
participant of the Corporate Risk Management and Internal Control System	-	the Board of Directors, its committees, the Internal Audit Service, the Management Board, the Company's employees, the Risk Division, structural divisions of the Company, risk coordinators;
risk factor (risk factor)	-	conditions, condition, circumstances under which the causes of the risk appear, leading to the realization of the risk;
external risk factors	-	risk factors arising outside the Company's operating activities and not dependent on the Company's activities;
internal risk factors	-	risk factors related to internal processes, organizational structure, human resources, assets of the Company and arising in the course of the Company's operations;
CRO	-	Member of the Management Board of the Company in charge of the Corporate Risk Management and Internal Control System.

Terms and definitions not disclosed in the Policy are used in the meaning defined in the legislation of the Republic of Kazakhstan, the Charter and other internal documents of the Company.

Section 3. Goals and objectives of the corporate risk management and internal control system

8. The CRMS is intended to provide reasonable assurance of the achievement of the following objectives:

1) strategic goals;
2) operational goals - the efficient and effective use of resources, preservation of assets;
3) goals in the field of reliable reporting;
4) goals in compliance with applicable laws and internal requirements.

Whereas the CRMS focuses on achieving the goals in the four categories outlined above, internal control focuses on achieving the operational goals, the goals of preparing reliable reporting and compliance with applicable laws and

internal requirements.

9. Risk management and internal control begins with each individual employee, and therefore the effectiveness of CRMS and internal control has certain limitations. Errors, collusion of two or more persons, other restrictions related to the human factor, do not allow an absolute guarantee to achieve the goals of the Company, but lead to the possibility of providing only reasonable assurance.

10.The objectives of CRMS and internal control are:

1) increasing the risk culture and integrating risk management and internal control in all aspects of the Company;

2) reducing the volatility of performance results by increasing the Company's ability to prevent situations that threaten goals, effectively respond to negative "surprises" and reduce the consequences of such situations, if they occur, to an acceptable level;

3) ensuring the use of opportunities to increase the value of assets and profitability of the Company in the long term.

10.1 A significant deficiency in relation to the functioning of the CRMS and VC component or the corresponding principle of its support, or in relation to the CRMS and VC components working together in an integrated mode, affects the degree of effectiveness of the Company's CRMS and VC.

10.2 The Company's risk management system is not a linear system in which one component influences the next. The Company's risk management system is a multidirectional system in which almost all components can interact and influence each other.

Section 4. CRMS components.

11. Risk management consists of the following interconnected components corresponding to the business life cycle: management and culture; strategy and goal setting; performance efficiency; monitoring and implementation of changes; information, communication and reporting.

Internal control consists of components that closely intersect with the components of CRMS: control environment (includes organizational structure, honesty and ethical standards, philosophy and leadership style, personnel policy, employee competency, intersects with the component “management and culture”), risk assessment (closely intersects with the component “activity efficiency”), control procedures (which is part of risk management), information and communications, monitoring (closely intersect with the components “monitoring and implementation of changes ”,“ information, communication and reporting ”.

Considering that internal control is an integral part of the CRMS and the components of CRMS and internal control are closely overlapping, in order to avoid duplication of principles that are similar in meaning, the Policy presents principles only on the structure of CRMS with an extension in the description of the requirements for control procedures. In doing so, the following should be

considered, inter alia:

- while CRMS focuses on creating and maintaining value, internal control focuses on taking measures to respond to risks of not achieving specific goals;
- the concept of CRMS, in contrast to the concept of internal control, includes the definition of Risk appetite, Tolerance, a comprehensive review of risks, focuses on risk culture, while the presence of Risk appetite, Tolerance, a comprehensive review of risks, the level of risk culture in the Company significantly affect functioning of internal control in the Company.

12. The “Management and Culture” component corresponds to the stage of determining the mission, vision, and values of the Company and is based on the principles of:

- Implementation of the supervisory function of risk management by the Board of Directors of the Company;
- Creation of operational structures;
- Definition of the desired culture;
- Demonstration of commitment to core values;
- Attracting, developing and retaining qualified professionals.

13. The component “Strategy and goal setting” corresponds to the stage of strategy development and is based on the principles:

- Analysis of business conditions;
- Definition of risk appetite;
- Evaluation of alternative strategies;
- Formulation of business goals.

14. The component "Performance" corresponds to the stage of formulating business goals and is based on the principles:

- Risk identification;
- Assessment of the materiality of risks;
- Prioritization of risks;
- Responding to risks;
- A comprehensive view of risks.

15. The component “Monitoring and implementation of changes” corresponds to the stage of implementation of the strategy and performance evaluation and is based on the principles:

- Assessment of significant changes;
- Analysis of risks and performance (factor analysis);
- Improving risk management effectiveness.

16. The “Information, Communication and Reporting” component promotes value and is based on principles:

- Use of information and technology;
- Dissemination of risk information;
- Reporting on risks, corporate culture and performance.

Section 5. Principles of CRMS.

5.1 Board Supervision of Risk Management.

17. The Board of Directors of the Company oversees the effectiveness of risk management and internal control by performing the following functions in the field of risk management:

- defines the goals (short-term and long-term) of the Company;
- in the framework of the Policy: approves the principles and approaches to organizing the CRMS, the requirements for organizing internal control and conducting control procedures, the distribution of roles of CRMS participants in the field of risk management and internal control of the Company;
- approves Risk appetite, Tolerance, Key risk indicators, Register, Risk card, Risk response plan, consolidated risk reports of the Company;
- approves an organizational structure that meets the needs of the Company and ensures effective risk management;
- ensures proper consideration of issues falling within the competence of the Board of Directors of the Company, taking into account the associated risks when making decisions;
- takes appropriate measures to ensure that the current risk management and internal control system complies with the principles and approaches to its organization as determined by the Board of Directors of the Company and functions efficiently, including (but not limited to) considering reports of the Internal Audit Service on assessing the effectiveness of CRMS and internal control, analyzes the findings of external auditors to improve internal control and risk management.

18. The Board of Directors of the Company should regularly determine for itself whether it has the necessary independence, skills, experience and knowledge of the business and whether it has access to complete information on current issues of the Company's activities for the supervision of risk management and internal control.

19. The Audit Committee of the Company assists the Board of Directors of the Company in matters of monitoring the reliability and effectiveness of CRMS and internal control.

5.2 Creation of operational structures.

20. The Management Board of the Company ensures the creation and maintenance of the effectiveness of the risk management and internal control system by performing the following functions:

- ensures the implementation of the Policy, the development and implementation of internal documents, their updating taking into account changes in the external and internal environment of the business and informs the Board of

Directors of the Company of all approved internal documents in the field of risk management and internal control;

- implements decisions of the Board of Directors of the Company, recommendations of the Audit Committee of the Company in the field of organization of the risk management system and internal control;
- distributes powers, duties and responsibilities for specific risk management and internal control procedures between the managers of the following level and / or the heads of structural divisions / owners of business processes;
- ensures the implementation of risk management and internal control procedures for employees with relevant qualifications and experience;
- ensures the integration of risk management and internal control with all business processes of the Company, including, but not limited to, considering and discussing information about risks in the framework of reports on the results of activities in various areas and in the consideration of issues falling within the competence of the Management Board of the Company;
- approves Risk appetite, Tolerance, Risk Register and Risk Map, PKK, Risk Response Plan, consolidated risk reports of the Company for subsequent submission to the Board of Directors of the Company;
- considers issues on the limits of the Company and other issues in accordance with the internal documents of the Company;
- considers consolidated reports on the risks of the Company, the results of monitoring control procedures and takes appropriate measures within its competence;
- provides the Board of Directors with a statement on the functioning of internal controls as part of the consolidated risk report.

20.1 CRO organizes and coordinates the Company's risk management and internal control system by performing the following functions:

- ensures the implementation of the Policy, the development and implementation of internal documents, their updating taking into account changes in the external and internal business environment and informs the Management Board, the Audit Committee and the Board of Directors of the Company about all approved internal documents in the field of risk management and internal control;
- ensures the development of a unified corporate culture for the reliable and efficient functioning of the Company's CRMS and VC, including the organization of the process of informing, training on an ongoing basis (but not less than once a year) for the Company's risk coordinators, and, if necessary, organizes classes / seminars for members of the Board of Directors and the Management Board of the Company, followed by a survey to assess the effectiveness of training and periodically confirm the knowledge of the Company's risk coordinators and understanding of the corporate culture and ethical principles, requirements and provisions of internal local acts that affect the operation of the Company's CRMS and VC;

- ensures the integration of risk management and internal control with all business processes of the Company, including, but not limited to, reviews information on risks as part of performance reports in various areas and as part of the consideration of issues within the competence of the Company's Management Board;
- ensures the timely formation and approval of the Risk Appetite, Tolerance, Risk Register and Map, KRP, Risk Response Action Plan, Action Plan to improve the CRMS and VC, consolidated risk reports and reports on the implementation of the Action Plan to improve the Company's CRMS and VC for subsequent submission for consideration and approval by the Management Board and the Committee and approval by the Board of Directors of the Company;
- monitors the implementation of measures to eliminate significant deficiencies identified in the development of flowcharts, risk matrices and controls of the Company (documentation of process risks and control procedures, including an assessment of the effectiveness of the design of control procedures);
- ensures the timely development of the Company's business continuity plans, which regulate the ways of managing incidents, restoring and supporting the Company's activities to the established level in case of violations (including the information technology continuity plan);
- ensures the implementation of the Action Plan to improve the CRMS and VC, approved by the decision of the Board of Directors of the Company;
- provides timely information to the Board of Directors, the Committee and the Management Board on the current state of risks and the response measures taken, changes in the control environment, significant deviations in the risk management and internal control process, ongoing measures to improve risk management and internal control, and other issues in the field of risk management;
- implements decisions of the Management Board and the Board of Directors of the Company, recommendations of the Company's Committee in the field of organization of the risk management and internal control system.

The CRO functions are assigned to one of the current members of the Company's Management Board. To avoid a conflict of interest, the CRO should not combine the functions of economic planning, corporate finance, treasury, investment activities, and internal audit.

21. The Board of Directors and the Management Board of the Company, in carrying out their functions, rely on the Three Lines of Defense model.

22. The first line of defense (business functions) is represented by structural units in the face of each employee within their competence. When fulfilling their duties, Company employees (risk owners) directly manage risks and carry out control procedures within their competence, including the following main functions:

- identify and evaluate risks, propose and implement strategies for responding to risks (accepting, avoiding risk, increasing risk, reducing risk or transfer) and specific measures for responding to risks, if necessary, suggest ways

to improve CRMS within the framework of supervised activities on an ongoing basis;

- develop and update policies and procedures governing the business processes entrusted to them;
- determine / document / improve the design of control and carry out control procedures, develop risk and control matrices within the framework of entrusted business processes on an ongoing basis;
- comply with risk appetite for all its components within the competence;
- fill in the database of realized and potential risks in accordance with an internal document for accounting and analysis of realized and potential risks;
- monitor external and internal factors that can have a significant impact on the risks associated with the performance of their functions;
- provide timely and complete information on risks to interested parties, including (but not limited to) provide information to the Risk Department on a quarterly basis for the purpose of regular monitoring of Tolerance, PKK; definitions of Tolerance, the formation of the Risk Register and Risk Map, the Risk Response Plan, the consolidated risk reports, and also send information about changes in the risk profile (including, but not limited to, data on exceeding or approaching the PKP threshold value), new risks and proposals on response within one business day from the date of discovery of a new risk or change in risk.

In each structural subdivision of the Company, a risk coordinator is appointed, whose responsibilities include organizing risk management work in his structural subdivision and cooperation with the Risk division of the Company at all stages of the implementation of the CRMS procedures of the Company.

Risk owners must ensure that risk information and risk coordinators are submitted to the Risk Department.

23. The second line of defense - structural units, including the Risk division, which carry out the functions of monitoring the activities of the first line of defense and key risks, ensure and monitor the implementation of effective risk management practices, internal control, compliance with laws, administrative rules / internal regulations and investigation of fraud within the established competencies. The second line of defense monitors, reviews, evaluates, examines the activities of the first line of defense.

The risk division reports directly to the CRO.

24. The third line of defense (independent guarantee) is provided by the Internal Audit Service of the Company, conducts an independent assessment of effectiveness and helps to improve risk management and internal control, provides support to the Audit Committee and the Board of Directors of the Company, provides them with an independent assessment of the effectiveness of the risk management and internal control system.

25. On a periodic basis, structural units of the second line of defense and the Internal Audit Service hold joint meetings based on the results of inspections and audits in order to exchange information, discuss plans, and recommendations.

26. A risk coordinator is appointed in each structural unit of the Company, whose responsibilities include the organization of risk management work in its structural unit and cooperation with the Risk division of the Company at all stages of the implementation of the Company's CRMS procedures.

Risk owners must ensure that risk information and risk coordinators are submitted to the Risk Department.

27.The mechanism for implementing this Policy (the organizational structure of the internal control system, the distribution of powers and responsibilities between the subjects of the internal control system, as well as the internal control procedure) is determined by the internal documents of the Company in the field of the internal control system.

5.3 Determination of the desired culture.

28. Risk management culture (risk culture), being the basis of risk management, includes beliefs, understanding and knowledge in the field of risk management, shared and applied by all officials and employees in the performance of their duties.

Risk culture is part of the corporate culture of the Company. The level of risk culture determines how risks are identified, assessed and managed from the moment a strategy is developed to its implementation and performance monitoring.

29.Risk culture is based on four principles:

29.1 Tone at the highest level: the Board of Directors, the Management Board and the Company Management set the tone from the top and, when making decisions, proceed from the optimal balance between long-term value, profitability and risks associated with both decision-making and non-decision-making; management encourages subordinates to risk-oriented behavior. Each item on the agenda of meetings of the Company's bodies must be accompanied by an analysis of risks and compliance with the established Risk appetite.

29.2 Corporate governance: The activities of the Company are aimed at creating such a control environment that ensures that employees understand that the Policy and all internal documents are binding. All officers and employees of the Company are clearly aware of their area of responsibility and authority for risk management and internal control. Risk owners within their competence understand the risks, manage them and duly inform about the risks in accordance with the internal regulatory documents of the Company.

29.3 Decision-making: The internal environment is characterized by open communication and transparency of risk information, this contributes to an open and constructive discussion of the associated risks and potential opportunities between the employees and officers of the Company and allows you to jointly make effective decisions in response to external challenges.

The remuneration system at all levels uses financial and non-financial incentives for Management and employees to formulate their right attitude to risk

in the process of making managerial decisions. With a developed risk culture, the decisions made are clearly defined by risk appetite.

29.4 Competence: The organizational structure of the Company is based on the “three lines of defense” model. The risk division effectively performs the role of the second line of defense, thereby increasing the confidence of Management in achieving the goals of the Company. The risk division maintains a commitment to the continuous development of a risk culture in the Company, including through the use of adaptation mechanisms for newly hired employees of the Company, the provision of risk documents as part of the introduction of members of the Board of Directors of the Company, mandatory and functional certification, SCRUM meetings etc. The risk division, if necessary, can initiate anonymous risk surveys among Company employees.

30. Sources of information about the level of risk culture for the Management Board and the Board of Directors of the Company may be documents on evaluating the effectiveness of the risk management and internal control systems in the Company, reports on diagnostics of corporate governance, etc.

31. The Company has a Confidential Information Policy, which establishes the procedure for reporting violations of the Code of Conduct, anti-corruption requirements, fraud, bribery and other violations.

5.4 Commitment to core values.

32. The Company's commitment to values is the basis for the effective functioning of CRMS.

The Company defines values, basic principles and standards of behavior, guided by which employees and officials together will be able to protect the interests and trust of interested parties, which ultimately will help achieve the strategic goals of the Company.

5.5 Attracting, developing and retaining qualified personnel.

33. Based on the analysis and results of monitoring the activities of the Company, responsible structural units determine the need for human resources necessary to achieve the goals of the Company. The Company should develop internal documents on the distribution of responsibilities and succession for key personnel.

Internal documents in the field of human resources management determine the basis for attracting, developing and retaining qualified personnel.

5.6 Risk management infrastructure analysis.

34. In order to comply with the mission, vision, obligations, values and principles of the Company, the external and internal environment are taken into

account.

The external environment includes political, economic, social, technological, legal, environmental factors. The relationship of the Company with the external environment (business structures, social, regulatory, and other government bodies) is reflected in the internal environment and affects its formation.

The internal environment determines the general attitude of the Company to risks, and how its employees consider and react to risks. The internal environment is the basis for all other components of the risk management system, includes a risk management philosophy, risk appetite, control by management bodies, ethical values, competence and responsibility of employees, the structure of the Company, its capabilities, determined by human, financial and other resources.

The Company's activities are aimed at creating an internal environment that increases the understanding of risks by employees and increases their responsibility for risk management.

5.7 Definition of Risk Appetite.

35. Risk appetite is formed in parallel with the strategic planning process. Within three months after the approval / revision of the Company's Development Strategy, the Risk department takes measures to present a Risk appetite for approval by the Board of Directors of the Company. Risk appetite takes into account the mission, vision and strategic goals, is determined in relation to investment, financial and operational activities in the context of the creation, preservation and realization of the value of the assets of the Company.

36. Every year until November 30, the Risk department analyzes the relevance of Risk appetite, and if significant changes are found in the internal (for example, when changing strategies) or external environment (for example, new regulatory requirements), the Risk department initiates a review Appetite risk.

37. The risk appetite is established no more than for the period of validity / approval of the Company's Development Strategy, in the form of qualitative and quantitative indicators. Risk appetite indicators can take annual values (for example, losses from operating activities accumulated during the financial year should not exceed 10% of EBITDA) and / or longer-term indicators (for example, the discounted amount of losses from capital investment expected during the entire life of the investment project or organization should not exceed 3% of the equity capital of the Company). When forming the risk appetite, the risk profile is mandatory taken into account and the impact of losses (equal to the size of the risk appetite) on the financial results of the Company is analyzed.P

38. Risk appetite is integrated into the decision-making process at all levels of the Company. Risk appetite, Tolerance, Key risk indicators and risk limits are interconnected and constantly monitored for compliance.

Compliance with the risk appetite is mandatory for employees of the Company when conducting transactions, initiating transactions, analyzing projects and for officials of the Company when making management decisions.

5.8 Evaluation of Alternative Strategies.

39. When choosing a strategy, the Company takes into account the risk profile and risk appetite, and also analyzes alternative strategies for risks and opportunities of each of the alternatives.

Understanding the risk profile allows you to determine the need for resources to implement the strategy, while remaining within the risk appetite.

Risk management includes evaluating strategies from two sides: 1) the likelihood that the strategy will not correspond to the mission, vision and values of the Company; 2) the consequences of the implementation of the selected strategy.

If the risk associated with a particular strategy exceeds the established risk appetite, you must choose an alternative strategy or review the risk appetite.

5.9 Formulation of business goals.

40. The company formulates business goals in accordance with internal documents on strategic and business planning.

When setting goals, the Company takes into account that an aggressive target may lead to a greater amount of risk. In this regard, when setting goals, the Company takes into account the risk appetite.

41. In order to effectively monitor and prevent exceeding the level of Risk appetite, Tolerance is established, which reflects an acceptable deviation from certain business goals due to the implementation of risks.

Tolerance is subject to quarterly monitoring and may be revised in case of changes in the external and internal environment.

5.10 Identification of risks.

42. Risk identification is important as a method of optimizing the Company's expenses, since the early identification of risks, the identification of adequate measures to minimize them and eliminate the consequences, allows you to plan the sources and amounts of financing for such events, which ultimately affects the efficiency of the Company.

43. Risks are identified both during the risk inventory (annually as part of the preparation of the Register, quarterly as part of the preparation of risk reports), and in the course of ongoing activities. If a significant risk is detected that has not previously been included in the Register, the risk owner must inform the Risk department about this. The risk division analyzes the information received, and, if necessary, includes a new risk in the Risk Register.

44. To identify risks, employees of the Company may use the following methods and tools:

44.1 Identify risks that may affect the achievement of goals, objectives, key performance indicators.

44.2 . They conduct industry and international comparisons to identify potential events specific to organizations similar to the Company and subsidiaries based on industry specifics or functional activities.

44.3 They discuss risks within each structural unit to determine the risks that affect the activities of each such unit and, in general, the Company and its subsidiaries. In order to integrate the substantial risks of each structural unit into the Register, the risk unit initiates meetings during which the draft Risk Register or changes to the Risk Register are discussed.

44.4 The risk division conducts targeted interviews with key employees (experts) of the Company to openly discuss existing and potential risks and ways to manage them.

44.5 analyze reports on the results of audits, etc.

44.6 Analyze Near Miss. Near Miss are incidents related to the violation of business processes, operational, production regulations, which, under certain circumstances, could lead to risks (injuries, fire, spills, accidents, etc.), but did not lead to. The larger the Near Miss, the greater the likelihood of risk. Near Miss should be registered by risk owners and companies in an electronic database of realized and potential risks.

44.7 It monitors the base of realized and potential risks. The risk unit manages the database, structural units. The database is based on realized and potential risks.

44.8. Conduct a SWOT analysis, including analysis of internal (strengths and weaknesses) and external (threats and opportunities) factors, and also use other risk identification tools.

45. The identified risks are systematized in the form of a risk register, using the following classification of risks by type:

- strategic risk - the risk of losses due to changes or errors (deficiencies) in the determination and implementation of the strategy of activity and development, changes in the political environment, regional conditions, industry downturn, and other external factors of a systemic nature;
- financial risks - include risks associated with capital structure and a decrease in financial profitability. Financial risks include market risks (fluctuations in interest and currency rates, fluctuations in prices for natural resources), liquidity risks, credit risks (for corporate counterparties, individuals, second-tier banks and requirements in other countries);
- legal risks - risks of losses resulting from non-compliance with the requirements of the legislation of the Republic of Kazakhstan, in relations with non-residents of the Republic of Kazakhstan - the laws of other states, as well as internal rules and procedures;
- operational risk - the risk of losses, industrial accidents as a result of

shortcomings or errors in the implementation of internal processes committed by employees (including personnel risks), the functioning of information systems and technologies (technological risks), industrial safety, as well as external events.

The following operational risk factors are identified: external and internal fraud; labor disputes; failures in business processes and information and technical systems; damage to tangible assets; industrial accidents; failures in contractual relations with customers.

46. The risk register contains at least the following information: type and name of risk; risk factors (internal and external); consequences of the implementation of risks; risk owner; inherent and residual risk assessment; if available, a key risk indicator. The Risk Register must reflect which business objective is affected by each risk, as well as Tolerance regarding the business goal.

The principles: "Assessment of the materiality of risks", "Prioritization of risks" are regulated in the Rules for identification and assessment of risks of the Company.

5.11 Risk Response.

47. The company determines strategies for responding to risk, taking into account the conditions of business, the ratio of benefits and costs, obligations and expectations, risk prioritization, risk appetite.

48.The following response strategies are distinguished:

- *risk taking*, implying that its level is acceptable and it is not planned to take measures to reduce it;
- *risk aversion* by abandoning activities that could lead to risk;
- *a deliberate increase* in risk in order to obtain more financial and other benefits;
- *risk reduction* - impact on the probability of occurrence and / or impact of risk (amount of losses) through the use of preventive measures and action planning in case of risk occurrence;
- *risk transfer (financing)* - transfer to another party or partial distribution of risk.

49. The reduction of the strategic risk of the Company is carried out by monitoring the implementation of the approved strategy, development plan, according to the results of which corrective measures are taken.

50.Methods to reduce financial risk include (non-exhaustive list):

- for credit risks - setting limits on the level of accepted credit risk. Credit risk limits are governed by an internal credit risk management document;
- for market risks - control and calculation of the level of possible losses, the use of hedging and diversification tools. Response methods are regulated by an internal document on market risk management.
- for liquidity risks - setting limits on the degree of debt burden of the Company and its subsidiaries. The threshold values of financial stability ratios are

regulated by an internal document on debt management and financial stability.

51. Methods of reducing and controlling the legal risks of the Company are monitoring changes in legislation by the authorized legal service of the Company, which, together with interested structural units, assesses the impact of changes on the activities of the Company and develops measures necessary for their adoption. Any document that governs the internal procedures of the Company or in accordance with which the Company has obligations must undergo a mandatory examination in the authorized legal service of the Company.

52. The reduction and control of operational risks in the Company is carried out by analyzing established business processes and developing appropriate action plans for their improvement, implementing internal controls.

53.Transfer (financing) of risks includes the following tools:

- insurance (used in relation to risks, the occurrence of which entails only losses and cannot lead to income), is regulated by the corporate standard for the organization of insurance coverage;
- hedging (used in relation to risks, the implementation of which can lead to both losses and income) is regulated by an internal hedging document;
- transfer of risk under the contract (transfer of liability for risk to the counterparty for additional remuneration or a corresponding increase in the value of the contract);
- conditional credit line - access to bank financing on agreed terms upon the occurrence of certain events;
- other alternative methods of financing risks.

54. If the applied methods for responding to risks are associated with costs and these costs are significant, it is analyzed:

- how necessary are these measures, and whether they can be reduced due to a different risk response strategy;
- what is the opportunity cost of event costs.

55. In the course of identification and ongoing activities, risk owners submit proposals regarding strategies and response measures for the risk department, for further inclusion in the Risk Response Action Plan.

56. The plan is mandatory for execution by all structural divisions of the Company and includes activities, deadlines, responsible persons.

57. Internal controls are used to prevent and limit certain risks and possible illegal actions.

58. Control procedures should be carried out at all levels of the Company and are aimed at:

- reducing the likelihood of potential risks;
- preventing errors and / or identifying errors after they have been committed;
- identification and elimination of duplicate and redundant operations;
- identification of gaps and areas for improvement;
- further improvement of internal control.

59. The introduction of effective control procedures includes the

development / updating by owners of business processes and risk matrices and controls on business processes, testing by the Risk department of the design of control procedures and assessment by the Risk department and IAS of operational efficiency, all measures taken by the CRMS to improve internal control in company.

60.Control procedures include:

1) setting goals, distribution of powers and responsibilities at all levels of the Company;

2) establishment of authority to authorize operations: approval and implementation of operations only by those persons who are endowed with the relevant authority;

3) separation of duties and the absence of conflicts of interest in the performance of their duties by officers and employees of the Company;

4) the creation and operation of a reliable information support system and effective channels for the exchange of information between bodies, structural divisions and employees of the Company;

5) bringing to the notice of all employees and officers of the Company their obligations to comply with internal control and their awareness of their role in risk management and internal control;

6) establishment of key performance indicators of the Company;

7) establishing criteria and assessing the effectiveness of the bodies, structural divisions and employees of the Company;

8) Company risk management;

9) monitoring the acquisition / disposal, restructuring of the Company's assets and compliance with property rights to them (preservation of assets);

10) monitoring the efficient use of Company resources;

11) monitoring the implementation of the development plan and budget of the Company;

12) diagnostics of corporate governance in the Company;

13) control over the implementation of investment projects;

14) monitoring compliance with the established procedure for conducting accounting and tax accounting, preparation and timely submission of reports (accounting, tax, management, etc.);

15) monitoring compliance with applicable laws, internal documents of the Company;

16) control over the implementation of decisions made by the bodies of the Company;

17) control over the implementation of the recommendations of the audit organization that audits the annual financial statements of the Company, as well as the recommendations of IAS;

18) monitoring compliance with established procedures for the disclosure of information by the Company;

19) monitoring compliance with the established procedure for document circulation in the Company;

20) assessment of the effectiveness of risk management and internal control;

21) other procedures.

The additional distribution of responsibility, the requirements for the formation of control procedures and the construction of risk and control matrices, the procedure for monitoring control procedures and other functions in the field of internal control are regulated by internal documents on the organization and implementation of internal control.

5.12 A comprehensive view of risks.

61. A comprehensive view of risks allows you to determine how much the residual risk profile corresponds to the established risk appetite.

61.1 The Company's management adheres to the approach in which the risk is considered first for each JV. At the same time, JV managers (risk owners) conduct a comprehensive risk assessment for their JV, reflecting the residual risk profile in relation to the goals and the level of acceptable risk.

Having a picture of the risks in each JV, the Management Board of the Company is able to review the entire risk portfolio of the Company within the framework of the information and / or reports provided by the Risk Department and determine whether the Company's residual risk profile is consistent with its overall level of risk appetite in achieving its goals.

61.2 By taking a holistic view of the risk portfolio at the Company level, the Management Board of the Company is able to assess how it corresponds to its Risk Appetite.

61.3 The Management Board of the Company may re-evaluate the nature and types of risks that the Company is ready to take on.

In the event that a holistic approach indicates that the level of risks is significantly lower than the overall level of risk appetite, the Management Board of the Company may decide to influence the leaders of individual JVs so that they accept higher risk in their areas in order to expand growth opportunities and increase profit of the Company as a whole.

62. A review of the risk portfolio provides an opportunity to identify offsetting risks (acting as a natural hedge), risks that have a positive and negative correlation, the materiality of which increases / decreases along with their gradual consolidation at the corporate level.

5.13 Assessment of significant changes.

63. The company monitors external and internal changes that can significantly affect the development strategy and plan and, if necessary, updates the Risk appetite, Tolerance, Risk Register and Risk Map, and Risk Response Action Plan. The risk division takes measures to submit to the Board of Directors of the

Company updated risk documents within three months from the date of detection of a material change.

5.13 Analysis of risks and performance (factor analysis).

64. The analysis of risks and performance is integrated into the activities of the Company. The company conducts a review of performance, including in the context of individual areas, taking into account risks: it considers risks that affected the performance; how effectively the risks were previously assessed and response measures identified; how effectively the measures themselves were implemented.

65. If the results of the Company's activities exceed the permissible deviations, an analysis of the relevant indicators is necessary. After the analysis, the Company's management, which oversees the structural unit responsible for the relevant indicators, makes a decision on the need to review business goals, the desired culture, Risk appetite, risk prioritization, response measures, etc.

5.14 Improving Risk Management.

66. The Company strives to improve risk management and internal control of the Company on an ongoing basis.

67. Risk owners, if necessary, update policies and procedures for risk management, improve the design of control procedures as part of the business processes entrusted to them, etc.

68. Risk unit:

- at least once a year, analyze the Policy and other internal documents on risk management and internal control for their accuracy and relevance and determine the appropriateness of revising and / or making changes and additions. If appropriate, the revised documents in the prescribed manner are submitted for approval by the authorized bodies of the Company;
- в as part of the implementation of the annual monitoring procedures monitoring schedule, prepares recommendations for improving the design of controls for processes - objects of monitoring;
- within the framework of consideration of materials initiated by risk owners, makes proposals on improving risk management and control procedures;
- performs other measures to increase the effectiveness of CRMS and internal control in the Company.

69. IAS of the Company independently evaluates the effectiveness of CRMS and internal control, and provides recommendations for their improvement.

5.15 Use of information and technology.

70. The company uses information from external and internal sources and

technology to support risk management and internal control.

71. To maintain the quality of information, the Company has a data management system.

72. Information technology is used to automate the CRMS processes taking into account the results of the “benefit - cost” analysis.

5.16 Dissemination of risk information.

73. The risk management structure provides an adequate flow of information - vertically and horizontally.

At the same time, information coming from bottom to top provides the Board of Directors and the Management Board with information on: current activities; on risks accepted in the course of activities, their assessment, control, response methods and the level of their management.

Information sent from top to bottom provides the communication of goals, strategies, desired culture, Risk appetite and Tolerance, by approving internal documents and instructions.

Horizontal information transfer implies the interaction of structural divisions within the Company and the interaction of the Risk divisions with structural divisions responsible for risk management and internal control in subsidiaries.

74. Communication channels allow providing CRMS participants with reliable and timely information on risks, and increase awareness of risks, methods and tools for responding to risks. Relevant information is prepared and provided in the form and on time that allows employees to effectively fulfill their functions.

75. Access to information is subject to the prevailing information dissemination regime in the Company.

5.17 Reporting on risks, corporate culture and performance.

76. The Company prepares a quarterly consolidated risk report, the main users of which are: Board of Directors, Audit Committee, Management Board, risk owners. Subsidiaries are obliged to provide the Company with consolidated reporting on the risks of subsidiaries within the time periods specified in Appendix 1 to the Policy and taking into account the minimum requirements for the content of risk reports established in Appendix 2 to the Policy.

77. The Company regularly and timely submits information in the Management Reporting System based on SAP BPC of the Shareholder. The information of the Company sent to the Shareholder is provided within the terms specified in the Shareholder's Management Reporting System, and will be based on the relevant risk management report. Should the information submitted into the Management Reporting System contain newly identified risks and/or significant changes in inherent risks, the risk management department of the company will inform the Chairman of the Audit Committee of such changes, who, in turn, will decide if and

when to inform the Board of Directors.

78. The company, within the framework of the consolidated risk report, at least once every three years, taking into account the monitoring monitoring coverage, submits a Statement of the functioning of internal controls and a Statement of effectiveness / inefficiency of risk management and internal control.

79. The company communicates to partners, creditors, external auditors, rating agencies and other external stakeholders (including as part of the annual report) risk management and internal control information, while ensuring that the degree of detail of the disclosed information is consistent with the nature and scope of the Company's activities.

Section 6. ESG risk management

80. As part of sustainable development, at all stages of the implementation of the Policy, the Company pays special attention to environmental, social and management risks (hereinafter referred to as ESG risks).

81.Management of the Company's ESG risks consists of the following elements:

1) adoption of corporate governance required for effective CRMS and VC;
2) understanding the business context and strategy of the Company;
3) identification of ESG risks;
4) assessment and ranking of ESG risks;
5) response to ESG risks;
6) review and revision of ESG risks;
7) communication and reporting on ESG risks.

81.1 The element "Adoption of corporate governance necessary for effective CRMS and VC" is based on the principles of the Board of Directors exercising an oversight function for risk management, creating operational structures, defining the desired culture, demonstrating commitment to core values, attracting, developing and retaining qualified personnel, defined in sections 5.1 , 5.2, 5.3, 5.4 and 5.5 of this Policy.

81.2 The element "Understanding the business context and strategy of the Company" is based on the principles of analyzing the risk management infrastructure, determining the risk appetite and forming business goals, defined in sections 5.6, 5.7 and 5.9 of this Policy.

81.3 The "ESG Risk Identification" element is based on the principle of risk identification (identification) defined in Section 5.10 of this Policy.

81.4 The ESG Risk Assessment and Rating element is based on the principles of risk materiality assessment, risk prioritization provided in the Risk Identification and Assessment Rules, and a comprehensive view of risks defined in Section 5.12 of this Policy.

81.5 The ESG Risk Response element is based on the principles for evaluating alternative strategies and significant changes, as defined in Sections 5.8 and 5.11 of this Policy.

81.6 The "Review and revision of ESG risks" element is based on the principles of assessing significant changes, analyzing risks and performance (factor analysis),

improving the efficiency of risk management, defined in sections 5.13, 5.14 and 5.15 of this Policy.

81.7 The ESG Risk Communication and Reporting element is based on the principles of using information and technology, disseminating information about risks, reporting on risks, corporate culture and performance, as defined in sections 5.16, 5.17 and 5.18 of this Policy.

82. ESG risk management is integrated into the overall process of the Company's CRMS and VC.

83. The Company pays special attention to ESG risks in the framework of project and program evaluation (planning, review, implementation, financing, etc.) as one of the main criteria.

84. Information on the management of the Company's ESG risks is disclosed in the Company's corporate reporting.

Section 7. Limitations of CRMS and VC.

85. The effectiveness of the CRMS and VC may be limited by the following factors:

1) a change in economic conditions or applicable law, the emergence of new circumstances outside the sphere of influence of management;

2) abuse of authority by the managers and (or) employees of the Company;

3) the occurrence of errors in the process of making managerial decisions and carrying out operational activities;

4) conspiracy of two or more employees of the Company, involving deliberate actions to violate controls.

Section 8. Final Provisions.

86. Issues not regulated by the Policy are governed by the legislation of the Republic of Kazakhstan, the Corporate Governance Code of the Company and other regulatory documents of the Company. In the event of a change in the legislation or regulations of the Republic of Kazakhstan and entry into conflict with certain articles of this Policy, these articles become invalid. Until the relevant changes are made to the Policy, it is necessary to be guided by the legal acts of the Republic of Kazakhstan.

Appendix 1. Risk reporting deadlines for subsidiaries of the Company

Name of reporting	Terms of submission
Risk report submitted for approval by the authorized body of the subsidiary	Not later than the 10th day of the second month following the reporting quarter.

Appendix 2. Minimum requirements for the content of the risk report

1. Card and Risk Register:
- Map and Risk Register for the forecast year, taking into account changes in risks for the reporting quarter (if any), including information on new risks.
- Tolerance and PKK status.
- Separate identification of critical risks with an indication of the reasons for the occurrence and an Action Plan to respond to them.
- Status of the implementation of the Response Plan for critical risks for the reporting quarter.
- Information on non-fulfillment of the Response Action Plan regarding non-critical risks (if any).
- Changes for the reporting quarter in the Risk Response Action Plan (if any).
2. Report on the observance of Risk appetite and, if necessary, proposals for the review of Risk appetite.
3. Reporting on financial risks in accordance with internal regulatory documents on the management of certain types of risks.
4. Information on the risks of investment projects.
5. Information on the risks realized with the obligatory indication of damage (in quantitative, if possible calculation, and in a qualitative assessment) and the actions taken to respond to these risks with an assessment of the effectiveness of measures. This section should also include information on accidents and catastrophes, industrial accidents.
6. Information on significant deviations from established risk management and internal control processes (if any).
7. Activities aimed at improving the CRMS and internal control in accordance with the recommendations of the IAS (if any).
8. Information on the corporate risk reinsurance program implemented in accordance with the internal regulatory document on the organization of insurance coverage.