Approved
by the decision of the
Board of Directors of
JSC NMC Tau-Ken Samruk
March 12, 2020
(Minutes No.02/20)

POLICY OF JSC NMC TAU-KEN SAMRUK ON RISK MANAGEMENT AND INTERNAL CONTROL

Nur-Sultan, 2020

TABLE OF CONTENTS

Section 1. General Provisions

1. This Policy of JSC NMC Tau-Ken Samruk on Risk Management and Internal Control (hereinafter - the Policy) is developed in accordance with the internal documents of JSC NMC Tau–Ken Samruk (hereinafter - the Company), recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and other best practices in the field of risk management and internal control.
2. The Policy defines the basic principles and approaches to the organization of the corporate risk management and internal control system in the Company.
3. In development to the Policy, the Company has risk management rules, regulations on the internal control system, rules for managing certain types of risks and other internal regulatory documents.
4. Officials and employees of the Fund are obliged to follow the Policy in the performance of their duties and the implementation of their tasks.
5. The Policy applies to the member companies and organizations of the Company's Group, more than fifty percent of whose voting shares (interest) of which is owned by the Company on the right of property or trust management.
6. The Policy is posted on the Company's website and its main provisions are disclosed in the Company's annual report within the framework of the information disclosure regulations.

Section 2. Terms and Definitions

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

RMICS (Risk management and Internal Control Service)	-	the structural subdivision of the Company responsible for the organization of the risk management and internal control system;
Owner of process risk	-	business process owner;
Risk owner	-	an employee or a structural subdivision, or a collegial body of the Company responsible for aspects of managing a certain risk;
Internal control	-	a process designed to provide reasonable assurance regarding the achievement of operational goals,

		objectives in the field of reporting and compliance with legislation, requirements of internal regulatory documents of the Company, carried out by the Board of Directors of the Company, the Management Board and employees of the Company, is part of the corporate risk management system (CRMS);
Control design	-	the planned procedure for the implementation of the control procedure (as opposed to the actual implementation of the control procedure) is a set of elements that make up the control procedure;
Risk map	-	graphical representation of the Company's risks on the consolidated basis; located in a rectangular table, the vertical axis of which indicates the extent of the risk damage, and the horizontal axis indicates the probability of its occurrence;
Key Risk Indicator (KRI)	-	An indicator that indicates the changing trends of risk factors and possible realization of risks that could have a negative impact on the activities of the Company;
Subsidiary organization (SO)	-	a legal entity, more than fifty percent of the voting shares (interest) of which is owned by the Company on the right of property or trust management;
Control (control procedure)	-	an element of internal control, a documented set of actions, the configuration of systems or the organization of processes that reduce the likelihood of risk realization or mitigate its consequences, the control procedure is an integral part of business processes;
The "Three lines of defense" model	-	an approach to the organization of 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 roles and responsibilities between three separate groups (lines of defense): business functions (each structural subdivision of the Company), risk monitoring and control function (Internal Control and Risk Management Service and Compliance Service), the function of independent assessment of the effectiveness of risk management and internal control (Internal Audit Service);

Sectorial Directorates	-	structural units of the Company supervising SOs;
Risk profile	-	comprehensive review of the Company's risks which allows considering the types, degree of influence and interdependence of risks, their consequences on the Company's performance;
Reasonable confidence	-	high, but not absolute level of confidence;
Risk Register	-	a document containing information on the identified risks of the Company on the consolidated basis (risk description, risk factors, risk owner, risk assessment indicators, etc.), in addition to the Company's risks, the Register includes the risks of companies included in the red zone of the SO's risks;
Risk	-	probability of occurrence of events that may affect the achievement of the strategic and business goals of the Company;
Risk appetite	-	an acceptable amount of risk and / or loss that does not prevent the Company from achieving its goals;
Tolerance	-	an acceptable level of deviation in relation to the achievement of a specific business goal due to the risk realization;
Risk management (risk-management)	-	culture, competence, methods and approaches integrated into all Company processes *(starting with strategic planning and ending with performance management)* that 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 decision-making process at all levels of the organization. The terms "risk management", "corporate risk management system (CRMS)" are interchangeable in the Policy;
CRMS participant	-	Board of Directors, its committees, Internal Audit Service, Management Board, employees of the Company, Risk subdivision, structural units of the Company, risk coordinators.

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. Tasks and Objectives of the Corporate Risk Management System

8. The CRMS is designed to provide a reasonable guarantee for achieving the following objectives:

1) strategic goals;

2) operational objectives - effective and efficient use of resources, safety of assets;

3) objectives for preparation of reliable reporting;

4) objectives in compliance with applicable law and internal requirements.

While CRMS focuses on achieving the goals in the four categories mentioned above, internal control focuses on achieving operational goals, goals in the field of preparing reliable reporting and compliance with applicable legislation 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. Mistakes, collusion of two or more persons, and other limitations related to the human factor do not allow us to have an absolute guarantee in achieving the goals of the organization, but lead to the possibility of providing only reasonable confidence.

10. The objectives of the CRMS are as follows:

1) increase risk culture and integrate risk management in all aspects of the organization;

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

3) ensure that opportunities are used to increase the value of assets and the profitability of the Company in the long term.

Section 4. CRMS Components

11. Risk management consists of the following interrelated components[1] that correspond to the business life cycle: management and culture; strategy and goal setting; performance; monitoring and implementation of changes; information, communication and reporting. Internal control consists of components that closely overlap with CRMS components: the control environment (includes organizational structure, integrity and ethical standards, philosophy and leadership style, personnel policy, employee competence, intersects with the component "management and culture"), risk assessment (closely intersects with the component "operational

[1] Source: Organizational Risk Management Framework (COSO): Integration with Strategy and Performance Indicators

efficiency”), control procedures (part of risk management), information and communication, 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 the CRMS and internal control closely overlap, in order to avoid duplication of principles similar in meaning, the Policy presents principles only on the structure of the CRMS with an extension in terms of describing the requirements for control procedures. This should take into account, among other things, the following:

• whereas CRMS focuses on creating and preserving value, internal control focuses on taking measures to respond to the risks of not achieving specific goals;

• the concept of CRMS, unlike the concept of internal control, includes the definition of Risk appetite, Tolerance, comprehensive risk review, focuses on risk culture, while the presence of Risk appetite, Tolerance, comprehensive risk review, the level of risk culture in the Company significantly affect the functioning of internal control in the Company.

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

- Implementation of the oversight functions for risk management by the Board of Directors.
- Creation of operational structures.
- Determination 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 of:

- 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 formulation of business goals and is based on the principles of:

- Identification of risks.
- Risk assessment.
- Risk prioritization.
- Risk response.
- Comprehensive Risk Perspective

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 of:

- Evaluation of material changes.

- Risk analysis and business performance (factor analysis).
- Improved risk management.

16. The Information, Communication and Reporting component contributes to value increase and is based on the principles of:

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

Section 5. CRMS Principles

5.1 Risk Management Control by the Board of Directors

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 objectives (short-term and long-term) of the Company;
- within the framework of the Policy: approves the principles and approaches to the CRMS organization; requirements for the organization of internal control and control procedures; distribution of the roles of the CRMS participants in the field of risk management and internal control of the Company;
- approves the risk appetite, tolerance, key risk indicators, register, risk map, Action Plan for risk responding, consolidated reports on the risks of the Company;
- ensures proper consideration of risks when making decisions on matters within the competence of the Board of Directors of the Company taking into account the associated risks;
- takes appropriate measures to ensure that the current risk management and internal control system complies with the principles and approaches to its organization defined by the Company's Board of Directors and functions effectively, including (but not limited to) reviews reports of the Internal Audit Service on the assessment of the effectiveness of CRMS and internal control, analyzes the conclusions of external auditors on improving internal control and risk management.

18. The Board of Directors should check on a regular basis whether it has necessary independence, skills, experience and knowledge of the business and whether it is adequately informed about current business issues in order to be able to oversee risk management and internal control.

19. The Company's Audit Committee assists to the Company's Board of Directors in controlling the reliability and effectiveness of the CRMS and internal control.

5.2 Establishment of Operational Structures

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

- ensures the implementation of the Policy, development and implementation of internal regulatory documents, their updating taking into account changes in the external and internal business environment and informs the Board of Directors of the Company on all approved internal regulatory documents in risk management and internal control;
- executes decisions of the Board of Directors of the Company, recommendations of the Company's Audit Committee in organization of risk management and internal control system;
- approves the organizational structure that meets the needs of the Company and ensures efficient risk management,
- distributes authority, duties and responsibility for specific risk management and internal control procedures between the managers of the lower levels and / or heads of structural units / business processes owners;
- ensures the implementation of risk management and internal control procedures by 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, examines and discusses information about risks within the framework of reports on performance results in various areas and within the framework of issues falling within the competence of the Management Board of the Company;
- approves the risk appetite statement, register and risk map, KRI, risk response action plan, consolidated Company risk reports for subsequent submission to the Company Board of Directors for consideration;
- ensures the development of business continuity plans governing the ways of managing incidents, restoring and supporting activities to the established level in case of violations (including an information technology continuity plan);
- monitors the CRMS and internal control, including monitoring compliance with internal regulatory documents in risk management and internal control, compliance with risk appetite and tolerance, reviews reports on the Company's risks, monitoring results of control procedures and takes appropriate measures within its competence;
- submits to the Board of Directors a statement on the effectiveness and completeness of internal controls.

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

22. The first protection line (business functions) is represented by structural units by each employee within its competence. Employees of the Company (risk owners) in the performance of official duties directly manage risks and perform control procedures within their competence, including the following basic

functions:

- identify and evaluate risks, propose and implement risk response strategies (acceptance, risk aversion, risk increase, risk reduction or transfer) and specific risk response measures, improve the CRMS in the framework of the supervised activity on the regular basis;
- develop and update the policies and procedures governing business processes;
- determine / document / improve the control design and carry out control procedures, develop risk and control matrices within the framework of the entrusted
- business processes on the regular basis;
- comply with the risk appetite for all its components within the competence;
- fill in the base of realized and potential risks in accordance with the Rules for Accounting and Analysis of Implemented and Potential Risks;
- monitor external and internal factors that may have a significant impact on the risks associated with the performance of their functions;
- provide timely and complete information about the risks to the stakeholders, including (but not limited to) provide the RMICS on a quarterly basis with information for the regular monitoring of KRI; creating the Register and Risk Map, a risk response plan, risk reports; and also submit information on changes in the risk profile (including but not limited to data on exceeding the threshold value of the KRI), new risks and proposals for response measures within one working day from the date of detection of a new risk or changes in risk.

23. A risk coordinator is appointed in each structural unit of the Company whose activities are regulated by an internal regulatory document on accounting and analysis of realized and potential risks.

23. The second protection line (monitoring function) is represented by the RMICS and Compliance Service of the Company.

The second protection line is responsible for monitoring the implementation by structural units (business functions) of effective risk management and internal control practices, compliance with legislation and internal regulatory documents of the Company, alleged violations of the Code of Business Ethics, internal documents of the Company and/or legislation on anti-corruption and other regulatory requirements applicable to the Company.

The RMICS performs the following functions:

- coordinates risk management and internal control processes in the Company;
- ensures the functioning of the internal control environment, monitors the control procedures in the Company;
- develops and updates internal regulatory documents in risk management and internal control for the Company and companies, informs about the approved

documents of risk owners, makes proposals on the integration of risk management and internal control in business processes;

- annually generates a Register and a Risk Map, an Action plan for responding to risks, quarterly consolidated risk reports;
- forms a statement of risk appetite;
- when preparing consolidated risk reports, as well as reviewing materials submitted for consideration of the Management Board and Board of Directors of the Company, critically evaluates the completeness of the risks identified by risk owners and adequacy of response measures to these risks, analyzes the risk portfolio and develops response strategy proposals and, if necessary, redistribution of resources in relation to the management of relevant risks, focuses management attention on new risks and significant changes in risks;
- as required, organizes training as required, provides methodological and practical support to risk owners and companies in risk management and internal control;
- administers a database of realized risks on a regular basis;
- cooperates with the Internal Audit Service of the Company regarding the formation of an annual audit plan, a guarantee card, discusses the results of audits and monitoring of control procedures, exchanges knowledge and methodologies.

The RMICS and supervising Managing Director are responsible for informing the Board of Directors, Audit Committee and Management Board of the Company on the current risk situation and response measures taken, changes in the control environment, significant deviations in the risk management and internal control process, measures implemented to improve management risks and internal controls, other issues in risk management.

The RMICS should have access to all information, documents of the Company, necessary for the performance of their functional duties.

The Compliance Service is responsible for developing and implementing a compliance program aimed at managing the risks of violating the Code of Conduct, legislation and regulatory requirements on anti-corruption issues.

25. The third protection line (independent guarantee) is represented by the Company's Internal Audit Service (hereinafter - IAS), conducts an independent audit of risk management procedures, provides support to the Audit Committee and Board of Directors of the Company, provides them with an independent guarantee of the effectiveness of the risk management and internal control system.

5.3 Desired Culture Determination

26. Risk management culture (risk culture) is the foundation of risk management; it is the beliefs, understanding and knowledge of risk management shared and applied by all officials and employees in the performance of their duties.

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

27. Risk culture is based on “four pillars”:

27.1 The tone at the highest level: Board of Directors, Management Board and management of the Company set the tone from above and, when making decisions, they proceed from the optimal balance between long-term value, profitability and risks associated with both taking and not taking decisions, the management encourages risk-oriented behavior of subordinates. Each agenda item of meetings of the Company’s bodies must be accompanied by the analysis of risks and compliance with the established risk appetite.

27.2 Corporate Governance: The activities of the Company are aimed at creating such a control environment that provides employees with understanding that the Policy and all internal regulatory documents are mandatory for compliance. All officials and employees of the Company are clearly aware of their area of responsibility and authority for risk management and internal control. Risk owners understand risks, manage them and properly inform about risks in accordance with the Company’s internal regulatory documents.

27.3 Decision-making: The internal environment is characterized by open communications and transparency of information about risks. It promotes an open and constructive discussion of associated risks and opportunities between employees and officials of the Company and allows making joint effective decisions in response to external challenges.

The remuneration system at all levels uses financial and non-financial incentives for management and employees to form the right attitude to risk in their management decisions. With a developed risk culture, the decisions made are clearly outlined by risk appetite.

27.4 Competence: The Company’s organizational structure is based on the model of three protection lines. The RMICS effectively serves as a second protection line, thereby increasing the confidence of the Board of Directors and management in achieving the objectives of the Company. The RMICS is aimed at the continuous development of risk skills in the Company, also using the adaptation course mechanisms for the newly hired employees of the Company, submitting documents as part of induction of members of the Company Board of Directors, mandatory and functional certification, SCRUM meetings, etc. If necessary, RMICS can initiate anonymous surveys on risks among the Company’s employees.

28. The sources of information about the level of risk culture for the Management Board and Board of Directors of the Company may be reports on the assessment of the risk management and internal control systems, reports on diagnostics of corporate governance in companies.

29. The Company has the Whistleblowing Policy, which establishes the

procedure for information about violations of the Code of Conduct, requirements for anti-corruption, fraud, bribery and other violations.

5.4 Demonstration of Commitment to the Key Values

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

The Company should define the values, basic principles and standards of conduct, guided by which employees and officials together can ensure protection of interests and trust of interested parties, which ultimately will contribute to the achievement of strategic goals of the Company.

5.5 Attraction, Development and Retaining of Qualified Staff

31. The management under the supervision of the Board of Directors determines the need for human resources necessary to achieve the objectives of the Company. The Company should develop plans for allocation of responsibilities in the event of a crisis, succession plans for key personnel.

The HR internal regulations should define the basis for attracting, development and retaining qualified staff.

5.6 Analysis of Business Conditions

32. To support mission, vision and values, the Company takes into account the external and internal environment in the development of a strategy.

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

5.7 Risk Appetite Determination

33. Risk appetite is formed in parallel with the strategic planning process. Within one month after the approval/revision of the Company's Development Strategy, RMICS takes measures to submit the Risk Appetite for approval by the Company's Board of Directors. 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 creating, preserving and realizing the value of the Company's assets.

34. Every year, when forming the risk register, the RMICS analyzes the relevance of Risk Appetite, and within one month from the date of detection of significant changes in the internal (for example, when changing the strategy) or external environment (for example, new regulatory requirements), the RMICS initiates a review of Risk Appetite.

35. The risk appetite is established within the period of validity / approval

of the Company's 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 fiscal year should not exceed 10% of EBITDA) and / or more long-term indicators (for example, the discounted amount of losses from investments in capital expected during the entire lifetime of the investment project or company must not exceed 3% of the Company's equity capital). When forming the Risk Appetite, the Risk Profile is taken into account and the effect of losses (equal to the Risk Appetite size) on the Company's financial results is analyzed in the mandatory manner.

36. 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 interrelated and are constantly monitored for compliance.

Employees of the Company, when carrying out transactions, initiating transactions, analyzing projects as well as officials of the Company, when making management decisions, must act so that to observe the Risk appetite.

5.8 Evaluation of alternative strategies

37. When choosing a strategy, the Company takes into account the risk profile and Risk Appetite and analyzes alternative strategies for risks and opportunities of each of the alternatives.

Understanding the risk profile enables to determine the need for resources for the strategy implementation, while remaining within the Risk Appetite.

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

If the risk associated with a particular strategy exceeds the established Risk Appetite, it is necessary to choose an alternative strategy or revise the Risk Appetite.

5.9 Formulation of business goals

38. The Company formulates business goals in accordance with internal regulatory documents on strategic and business planning.

When setting goals, the Company takes into account that an aggressive goal can result in a greater amount of risk. In this regard, when setting goals, the Company takes into account Risk Appetite.

39. In order to carry out effective monitoring and prevent exceeding the level of Risk Appetite, Tolerance is established, which reflects an acceptable deviation from some business goals due to the implementation of risks.

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

5.10 Identification of risks

40. Identification of risks is important as a method of optimizing the Company's expenses, since early identification of risks, determination of adequate measures to minimize them and eliminate consequences, permits to plan sources and amounts of financing of such measures, which ultimately affects the Company performance.

41. 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 current activities. If a significant risk is identified that was not previously included in the Register, the risk owner must inform the RMICS about it. The RMICS analyzes the information received and, if necessary, includes a new risk in the Risk Register.

42. The Company's employees can use the following methods and tools for the risk identification:

42.1. Identifying risks that may affect the achievement of goals, objectives, and key performance indicators.

42.2. Carrying out sectorial and international comparisons for identification of potential events specific to peer organizations of the Company and companies in terms of sectorial specifics or functional activities.

42.3. Discussing risks within each structural subdivision to determine risks affecting the activities of each such subdivision and the Company and the company as a whole. In order to integrate significant risks of each structural subdivision in the Register, the RMICS initiates meetings during which the draft Risk Register or changes to the Risk Register are discussed.

42.4. The RMICS conducts target interviews of key employees (experts) of the Company for open discussion of existing and potential risks and ways to manage them.

42.5. Analyzing reports on the results of audits, etc.

42.6. Performing the Near Miss analysis. Near Miss are incidents related to the violation of business processes, operational, production regulations, which, under certain circumstances, could result in risks (injuries, fire, spill, accident, etc.), but did not. The greater the Near Miss, the higher the probability of risk. Near Miss should be registered by risk owners and companies in the electronic database of realized and potential risks.

42.7. Using an electronic database of realized and potential risks. The RMICS administers the database, and structural subdivisions of the Company and companies provide information on realized risks. The electronic database of realized and potential risks is regulated by the relevant internal regulatory document.

42.8. Conducting SWOT analysis, including analysis of internal (strengths and weaknesses) and external (threats and opportunities) factors, as well as using other risk identification tools.

43. The identified risks are systematized in the form of a Risk Register, using the following classification of risks by type:

- strategic risk is the risk of losses due to changes or errors (deficiencies) in the definition and implementation of the strategy activity and development, changes in the political environment, regional conjuncture, sectorial recession, and other external factors of a systemic nature;
- financial risks include risks related to the capital structure and 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 are risks of losses due to non-compliance with 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 is the risk of losses, accidents at work as a result of deficiencies or errors in the implementation of internal processes committed by employees (including personnel risks), the functioning of information systems and technologies (technological risks), occupational safety, as well as due to external events. The following operational risk factors are distinguished: external and internal fraud; labor disputes; failures in business processes and information and technical systems; damage to tangible assets; accidents at work; failures in contractual relations with customers.

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

5.11 Assessment of the risk materiality

45. The risk assessment process is carried out for the identification of the most significant risks that may negatively affect the Company’s activities on a consolidated basis and the achievement of strategic goals and objectives. Results of the risk assessment determine the choice of risk response measures. Information on the most significant risks should be submitted for consideration of the Board of Directors, which takes decisions on the management and control of these risks.

46. Risks are assessed by risk owners in terms of the probability or frequency of their occurrence and impact on strategy and business plans, using qualitative and quantitative methods. Quantitative assessment permits obtaining more accurate analytical data, and is especially useful when developing risk financing methods. Risks that cannot be quantified, there is no reliable statistical information for their modeling, or the construction of such models is not cost-effective, are evaluated only on a qualitative basis.

47. Qualitative risk assessment is carried out either by target interviewing of

key employees, or by means of a questionnaire, in which experts are asked to select risks that they consider the most significant for the Company, evaluate them on the proposed point scale, and give proposals (recommendations) for their management. A combination of both methods can be used: extensive questioning of the Company's employees based on an electronic questionnaire system and interviewing the Heads of structural subdivisions and Managing Directors of the Company.

48. When conducting the quantitative assessment, the risk is assessed first on a gross basis, then on a net basis, considering the risk management measures taken.

Following methods and tools can be used for quantitative assessment:

48.1 Quantitative risk assessment based on the value of property that may be damaged as a result of the occurrence of risk. With such a model, scenarios of material damage are constructed when a risk occurs, and the replacement value of property that may be damaged and subsequently subject to repair or replacement is calculated. It is usually used to quantify operational risks (material damage to property as a result of man-made disasters, fire, etc.).

48.2 Quantitative assessment based on the calculation of non-received income. Such an assessment is usually used to assess the risks of production interruption or supply disruption.

48.3 Quantitative risk assessment based on benchmarking. The assessment of the maximum damage from certain types of risks, for example, risks of liability for causing harm or for environmental pollution, cannot be calculated using any formulas, and therefore precedent statistics (sectoral and territorial) are used to quantify such risks. To assess such risks, the scenarios of their occurrence and parties that may be involved (suffer damage), as well as the overall impact of such risk are usually evaluated, and the maximum possible damage is determined based on existing information (statistics) on the cost of damage during the implementation of such scenarios. Precedent statistics are also used to assess the impact of any risks on the market value of shares and other securities of the company.

48.4 Quantitative risk assessment based on statistics models. Such assessment is used for risks that have a specific monetary expression and depend on certain external factors (for example, fluctuations in oil prices, fluctuations in exchange rates, interest rates, etc.) and are based on the construction of statistical dependencies (for example, using regression analysis methods). In this case, it is possible to clearly determine under what conditions the risk may be significant.

Main methods of risk assessment under this approach are used by the Company separately or in combination according to the internal regulatory document on market risk management and may include:

48.4.1 The Value-at risk - VaR - is a value that will not exceed the losses expected during a given period of time from the revaluation of market risk factors with a given probability. The VaR value has a monetary value.

48.4.2 The Cash-flow at risk - CFaR - is a value that expresses an estimate of the maximum deviations of cash flows from the planned values that will not be exceeded within a given period of time with a given probability.

48.5 Stress testing. This is a method of changing market risk factors to exceptional, but possible values.

Depending on the number of risk factors being changed, one-factor and multi-factor stress testing are distinguished.

Depending on scenarios of changes in risk factors, there are historical and expert scenarios of stress testing. The historical scenario implies a change in the risk factor that took place in the past. The expert scenario is determined by the expectations of various experts (risk owners or external sources such as Bloomberg, Reuters, etc.) regarding the values of market risk factors.

48.6 A quantitative assessment based on a statistical analysis of the sources of operational risks makes it possible to forecast the potential operational losses based on the size of operational losses that occurred in the Company in the past. When applying this method, information accumulated in the electronic database of realized and potential risks can be used as initial data.

49. As part of the risk assessment, risk owners and the RMICS distinguish between inherent (risk, in the absence of response measures), residual (risk, taking into account response measures) risk. Comparison of these values makes it possible to identify measures that were not effectively planned or implemented.

50. The following point scale is introduced to ensure comparability of risks:

Frequency or probability of risk

Grade	**Value**	**Frequency or probability**
1	Very rarely	Every 7 years or more (or the probability of occurrence is up to 5%)
2	Rarely	Every 5 years (or the probability of occurrence is up to 25%)
3	From time to time	Every 3 years (or the probability of occurrence is up to 40%)
4	Often	Once a year (or the probability of occurrence is up to 80%)
5	Very often	Twice a year and more often (or the probability of occurrence is over 80%)

The amount of risk, impact of which can be quantified

Grade	**Impact degree**	**Potential loss from the occurrence of risk**
1	Insignificant	Below 25% of the risk appetite level
2	Significant	25-50% of the risk appetite level
3	Major	50-75% of the risk appetite level

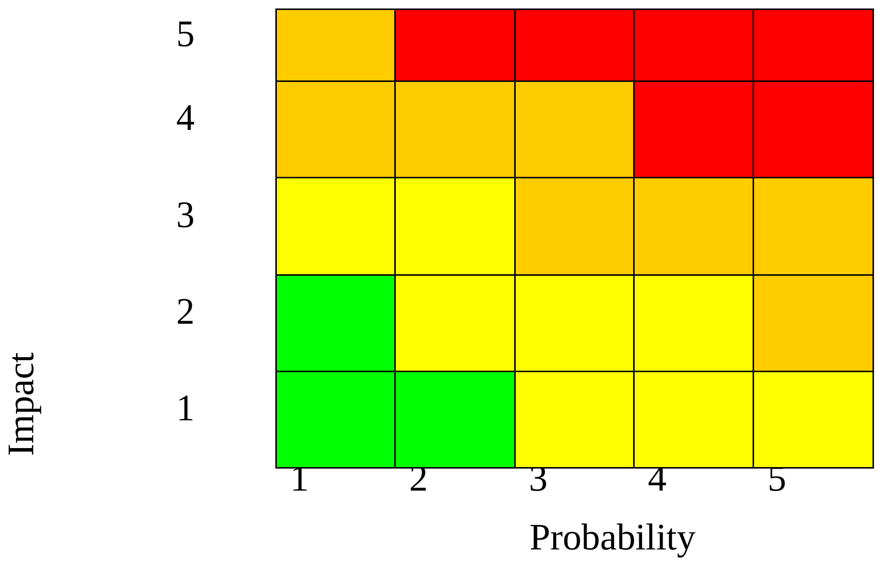
4	Critical	75-100% of the risk appetite level
5	Catastrophic	Above the risk appetite level

The amount of risk, impact of which is difficult to quantify (for example, risks of personnel, reputation, etc.)

Grade	**Impact degree**	**Potential loss from the occurrence of risk**
1	Insignificant	Absence of any consequences, if the risk is realized
2	Low	Consequences from the corruption risk realization are not significant
3	Average	Consequences of the risk implementation are not significant and can be completely corrected
4	Significant	Consequences of the risk implementation are very significant, but can be corrected to a certain extent
5	Catastrophic	If the risk is realized, the Company will practically be not able to recover from consequences related to this risk

51. Identified risks are reflected on the Risk Map given the result of their assessment. The risk map permits to assess the relative importance of each risk (as compared to other risks), as well as to identify risks that are critical.

52. The risk map includes several areas highlighted in different colors: red, orange, yellow and green zones.



53. The risk identification numbers are plotted on the Risk Map (according to the Risk Register) depending on indicators of the frequency (probability) of

occurrence and the size (impact) of the risk.

54. During the risk assessment, risk owners develop a risk assessment for risks with an inherent impact assessment of “four” or more. Exceeding the threshold values of the KRI will be an early signal of the need to revise the risk (risk assessment, response measures, etc.).

55. The developed KRIs are displayed in the Risk Register and approved simultaneously with the issuance of the Risk Register and the Risk Map for the next year. Information on the KRIs may include calculation formula; sources of information; unit of measure; monitoring frequency; threshold level; direction of the KRIs, signaling the possible realization of the risk.

56. Depending on the purpose, the following KRIs are distinguished:

- advanced KRIs are used to identify risks that may be realized in the near future;
- final KRIs are used to identify risks that have already been realized and may be realized again.

KRIs should be measurable, comparable in time, understandable for perception, data sources for their calculations should be available.

57. KRIs can be determined on the basis of:

- external and/or internal risk factors, can be expressed in the form of coefficients, numerical values;
- preventive measures to respond to risk, can be expressed in percentage or actual execution of preventive measures;
- key performance indicators of the Company, can be expressed in the percentage achievement of KPIs.

58. Macro/micro indicators and indices are used as external information (such as: gross domestic product, unemployment rate, changes in remuneration rates, country rating, etc.), information on the introduction of new legislative requirements, etc.

59. The threshold level of KRIs is determined using the following approaches: statistical; objective with the use of external and internal requirements for the Company’s activities; subjective with the use of expert opinion survey tools, etc.

60. Risk owners monitor KRIs and provide information to the RMICS on the actual level of KRIs, taking into account the established frequency of its monitoring. And if the threshold level is exceeded, the risk owner analyzes the reasons for the deviation within one working day from the date of detection, notifies the RMICS and initiates measures to prevent the implementation of a risk event or prevent its re-implementation.

5.12 Risk prioritization

61. To ensure the efficiency of the process and reduce the costs of its implementation, the Company should focus on risks that may have the most significant impact on its financial condition and the achievement of goals and objectives.

62. The risk priority is set according to the position of each of risks on the Risk Map:

- critical risks – the red zone of the risk map – the risks that have the highest priority. Such risks, which amount to 75% and more of the Risk Appetite level;
- major risks – orange area of the risk map – the second highest priority risks, the damage from the implementation of which remains within 50 - 75% of the Risk Appetite level;
- medium risks - yellow area of the risk map – the third priority risks, the damage from the implementation of which remains within 25 - 50% of the Risk Appetite level;
- low risks – green area of the risk map – risks ranging up to 25% of the Risk Appetite level.

63. In addition to results of the assessment, the following criteria may be taken into account when prioritizing risks: the ability of the Company to adapt to risk and respond to it, the interdependence of risks, as a result of which the complexity of managing them increases, the speed of the impact of risk on the Company's activities, the duration of the negative impact of consequences of the risk on the Company, etc.

5.13 Responding to risks

64. The Company determines risk response strategies taking into account business conditions, the ratio of benefits and costs, obligations and expectations, risk prioritization and the Risk Appetite.

65. There are the following response strategies:

▪ risk acceptance, implying that its level is acceptable and there are no plans to take measures to reduce it;

▪ risk avoidance by abandoning activities that may result in the occurrence of risk;

▪ risk deliberate increase 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) by using preventive measures and planning actions in case of risk realization;

▪ risk transfer (financing) - transfer to another party or partial distribution of risk.

66. The Company's strategic risk is reduced through monitoring the implementation of the approved strategy, development plan, based on results of which corrective measures are taken.

67. Methods of reducing financial risks include (non-exhaustive list):

▪ for credit risks - setting limits on the level of accepted credit risk. Credit risk limits are regulated by an internal regulatory document on credit risk management;

▪ for market risks – control over and calculation of the level of possible losses, the use of hedging and diversification tools. Response methods are regulated by an internal regulatory document on market risk management.

- for liquidity risks – setting limits on the degree of debt burden of the Company and companies. Threshold values of financial stability ratios are regulated by an internal regulatory document on debt management and financial stability.

68. The methods of reducing legal risks of the Company include monitoring changes in legislation and legal examination of documents that regulate the internal procedures of the Company or according to which obligations of the Company arise.

69. Reducing operational risks in the Company is carried out through analyzing established business processes and developing appropriate action plans for their improvement, the introduction of internal controls. For operational risks at work, risk reduction and control is carried out by observing the rules of occupational safety and health, rules for environmental safety, rules of operations at work.

70. Risk transfer (financing) includes the following tools:

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

71. If methods used to respond to risks are associated with costs and these costs are significant, the following shall be analyzed:

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

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

73. The Plan is compulsory for execution by all structural subdivisions of the Company and includes measures, deadlines and responsible persons.

74. The internal controls are used to prevent and limit certain risks and possible illegal actions.

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

- reducing the likelihood of risks occurring;
- preventing mistakes and/or, when they occur, determine them;
- identifying and eliminating duplicated and excessive operations;
- identifying weaknesses and areas for improvement;
- further improvement of internal control.

76. The introduction of effective control procedures provides for the

development/updating by business process owners of flowcharts and risk matrices and controls for business processes, testing by the RMICS of the control procedures design and evaluation by the RMICS and the IAS of the operational efficiency, taking by all CRMS participants measures to improve internal control in the Company.

77. Control procedures include:

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

2) establishing the authority to authorize operations: approving and executing operations only by those persons who have the appropriate authority;

3) segregating duties and absence of conflicts of interest when officials and employees of the Company perform their duties;

4) creating and maintenance of a reliable information support system and effective channels for information exchange between the Company's bodies, structural subdivisions and employees;

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

6) establishing key performance indicators of the Company;

7) establishing criteria and evaluating the effectiveness of the Company's bodies, structural subdivisions and employees;

8) Company's risk management;

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

10) monitoring the effective use of the Company's resources;

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

12) diagnostics of corporate governance in companies;

13) control over the implementation of investment projects;

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

15) control over compliance with requirements of applicable legislation, internal regulatory documents of the Company;

16) control over the execution of decisions taken by the Company's bodies;

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

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

19) control over compliance with the established procedure of document management in the Company;

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

21) proper documentation of internal control procedures;

22) other procedures.

Additional allocation of responsibilities, requirements for the formation of control procedures and the construction of risk matrices and controls, the procedure for monitoring control procedures, and other functions in the field of internal control are given in the internal regulatory document on the organization and implementation of internal control.

5.14 Comprehensive view on risks

78. A comprehensive view on risks permits to determine how much the residual risk profile corresponds to the established Risk Appetite.

79. The risk portfolio review makes it possible to identify compensating risks (acting as a natural hedge), risks with positive and negative correlation, the materiality of which increases / decreases along with their gradual consolidation at the corporate level.

5.15 Assessment of significant changes

80. The Company monitors external and internal changes that may significantly affect the strategy and development plan and, if necessary, updates the Risk Appetite, Tolerance, Risk Register and Risk Map, Risk Response Action Plan. The RMICS takes measures on submitting updated risk documents for consideration of the Board of Directors of the Company within three months from the date of the significant change detection.

5.16 Risk and performance analysis (factor analysis)

81. Risk and performance analysis is integrated into the Company's activities. The Company reviews the performance, including in the context of individual areas, considering risks: risks that affected the performance are considered; how effectively risks were pre-assessed and response measures were determined; how effectively the measures themselves were implemented.

82. If the Company's performance exceeds acceptable deviations, it may be necessary to revise business goals, desired culture, Risk Appetite, risk prioritization, response measures, etc.

5.17 Improving the effectiveness of risk management

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

84. Risk owners, if necessary, update risk management policies and procedures, improve the design of control procedures within the business processes entrusted to them, etc.

85. RMICS:

• at least once a year analyzes the Policy and other internal regulatory documents on risk management and internal control for their accuracy and relevance and determines the feasibility of revision and/or amendments and additions. If appropriate, the revised documents are submitted for approval of authorized bodies of the Company according to the established procedure;

• as part of the execution of the annual monitoring schedule of control procedures, it prepares recommendations for improving the design of controls on monitoring processes – objects;

• as part of the materials consideration initiated by risk owners, it makes proposals on improving risk management and control procedures.

• it performs other measures on improving the effectiveness of CRMS and internal control in the Company.

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

5.18 Use of information and technology

87. The Company uses information from external and internal sources and technologies to support risk management and internal control.

88. To maintain the quality of information, the Company operates a data management system.

89. Information technologies are used to automate CRMS processes, considering results of the "benefits – costs" analysis.

5.19 Dissemination of information about risks

90. The risk management structure ensures an adequate flow of information – vertically and horizontally.

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

Top-down information ensures the achievement of goals, strategies, desired culture, Risk Appetite and Tolerance, through the approval of internal regulatory documents and instructions.

The horizontal transfer of information implies the interaction of structural subdivisions within the Company and the interaction of the RMICS with structural subdivisions responsible for risk management and internal control in companies.

91. Communication channels enables to provide CRMS participants with reliable and timely information about risks, increase the level of awareness about risks, methods and tools for responding to risks. Relevant information is prepared and provided in a form and within a time frame that permits employees to effectively perform their functions.

92. Access to information is carried out given the current regime of information dissemination in the Company.

5.20 Reporting on risks, corporate culture and performance

93. The Company prepares a consolidated risk report on a quarterly basis, the main users of which are the Board of Directors, the Audit Committee, the Management Board of the Company and risk owners. Subsidiaries should submit consolidated statements on the risks of companies to the Company within the time limits set out in Annex 1 to the Policy and considering minimum requirements for the content of risk reports set out in Annex 2 to the Policy.

94. Reporting on corporate culture, performance (including in the context of activities) is prepared and distributed in accordance with individual internal regulatory documents of the Company.

95. The Company communicates to partners, lenders, external auditors, rating agencies and other external stakeholders (including as part of the annual report) information on risk management and internal control, while ensuring that the degree of detail of the disclosed information corresponds to the nature and scope of the Company's activities.

Section 6. Final Provisions

96. Issues not regulated by the Policy are regulated by the legislation of the Republic of Kazakhstan, as well as internal regulatory documents of the Company. In case of amendments to the legislation or regulations of the Republic of Kazakhstan and running into conflict with them of certain articles of this Policy, these articles shall be declared null and void. Until relevant amendments are introduced to the Policy, it is necessary to be guided by the legal acts of the Republic of Kazakhstan.

Annex 1. Deadlines for submitting risk reports

Reporting name	**Deadline**
Managerial reporting on risks of the company	According to the Management Reporting Package of the Company.
Report on the financial stability of the company	According to the internal regulatory document on debt and financial stability management.
Risk report submitted for consideration of the authorized body of the company	Before the 20th day of the second month next to the reporting quarter.

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

1. Risk Map and Risk Register:
- Risk Map and Risk Register for the forecast year, considering changes in risks for the reporting quarter (if any), including information about new risks.
- Tolerance and KRI Status.
- Separate allocation ofcritical risks the specifying reasons for the occurrence and the Response Action Plan.
- Status of implementation of the Response Action Plan to Critical Risks for the reporting quarter.
- Information about non-fulfillment of the Response Action Plan to Non-critical Risks (if any).
- Changes for the reporting quarter in the Response Action Plan to Risks (if any).
2. Report on compliance with Risk Appetite and, if necessary, proposals for revising the Risk Appetite.
3. Financial risk reporting according to internal regulatory documents on the management of certain types of risks.
4. Information on the risks of investment projects implemented within the framework of state programs, as well as Instructions of the President of the Republic of Kazakhstan and the Government of the Republic of Kazakhstan.
5. Information on realized risks with compulsory indication of damage (in quantitative, if possible, its calculation, and in qualitative assessment) and actions taken to respond to these risks with an assessment of the measures effectiveness. This section should also include information on accidents and catastrophes, accidents at work.
6. Information on significant deviations from the established risk management and internal control processes (if any).
7. Measures carried out to improve CRMS and internal control in accordance with the recommendations of the IAS (if any).
8. Information about the corporate risk reinsurance program implemented in accordance with the internal regulatory document on the organization of insurance protection.
9. Statement on the effectiveness/inefficiency of risk management and internal control (at least once every three years, given the scope of monitoring of control procedures).