Approved
by the Board of Directors
of Air Astana JSC
Minutes No. 217 as of 30.11.2021

Risk Management Policy of Air Astana JSC

Almaty 2021

Contents

1. General Provisions

The Risk Management Policy of “Air Astana” JSC (hereinafter referred to as the "Policy") has been developed in accordance with the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the legal and regulatory acts governing the activities of “Air Astana” JSC (hereinafter referred to as the "Company"), as well as with the Company's internal documents approved by the Company's Board of Directors.

The Company acknowledges the importance of risk management as a key component of Company's corporate management. It is a process in which the Company regularly identifies, assesses and monitors threats and opportunities; adapts its activities to reduce the probability and potential impact of threats and to realize opportunities; and also informs interested parties about it.

The corporate risk management system (hereinafter referred to as the "CRMS") is a set of interrelated elements united within a single process involving the Board of Directors, the management and the employees, at their own particular levels, in the detection of any events potentially affecting the Company's activities, as well as in the control of such events within the acceptable level of risk for the shareholders.

The main goal of CRMS is to increase the efficiency of the management of opportunities and threats, thus contributing to the capitalization growth. The main tasks of the Company's CRMS shall be as follows:

- to integrate risk management with all other aspects of the business, including governance, performance management, and internal control practices;
- to prevent the realization of any events that threaten the achievement of the strategic and operational goals;
- in case of such realization, to reduce its impact to an acceptable level;
- to efficiently respond to and manage unexpected situations;
- to improve Company’s sustainability, resilience, and agility to adapt to changing circumstances;
- to maintain systematic risk management as a part of the general process of the support of efficient internal control environment;
- to provide stakeholders with reasonable guarantees of the Company's efficient risk management;
- to help board and the management optimize outcomes with the goal of enhancing capabilities to create, preserve, and ultimately realize value.

The main principles of the Company's risk management process shall be as follows:

- awareness and involvement – the process of risk management is conducted by every employee of the Company, which is accompanied by the provision of objective, accurate and relevant information.
- continuity – the process of risk management should not be an additional burden for the management and employees of the Company, although it assumes constant strengthening of management actions. CRMS is most effective when it is organically integrated into the Company's infrastructure and its daily operations.
- centralization – Company defines common terminology, methods, and approaches to the CRMS and determines the risk appetite.
- strategic approach – the risk management system is built throughout the organization and requires each of its

units - the owner of the process, to obtain a portfolio of risks (qualitative and/or quantitative) generated by the processes, and then to assess the adequacy of the overall risk portfolio to Risk appetite.

At the same time, the risk management process should consider not only existing, but also potential events. CRMS is integrated into all business processes of the Company. The process of risk management should be integrated with the planning processes (strategy, business plans and annual budget) and evaluation of the performance of the organization. Reports on the results of activities should contain the necessary information on risks. Benefits of integrating risk management include the ability to:

- Increase the range of opportunities.
- Increase positive outcomes and advantages while reducing negative surprises.
- Identify and manage Company-wide risks.
- Reduce performance variability.
- Improve resource deployment.

Company's CRMS is based on the advanced standard "COSO Enterprise Risk Management – Integrating with Strategy and Performance", which consists of five interrelated components that are based on 20 principles, which represent fundamental concepts associated with each component.

The five components and their principles are as follows:

1. Governance and Culture:

   Principle 1: Exercises Board Risk Oversight.

   Principle 2: Establishes Operating Structures.

   Principle 3: Defines Desired Culture.

   Principle 4: Demonstrates Commitment to Core Values.

   Principle 5: Attracts, Develops, and Retains Capable Individuals.

2. Strategy and Objective-Setting:

   Principle 6: Analyzes Business Context.

   Principle 7: Defines Risk Appetite.

   Principle 8: Evaluates Alternative Strategies

   Principle 9: Formulates Business Objectives.

3. Performance:

   Principle 10: Identifies Risk.

   Principle 11: Assesses Severity of Risk.

   Principle 12: Prioritizes Risks.

   Principle 13: Implements Risk Responses.

   Principle 14: Develops Portfolio View

4. Review and Revision:

   Principle 15: Assesses Substantial Change.

   Principle 16: Reviews Risk and Performance.

Principle 17: Pursues Improvement in Enterprise Risk Management.

5. Information, Communication, and Reporting:

   Principle 18: Leverages Information Systems.

   Principle 19: Communicates Risk Information.

   Principle 20: Reports on Risk, Culture, and Performance.

Mission of the Policy is the maintenance of CRMS, which allows the Company to operate effectively and distribute resources in the priority directions for ensuring the acceptable level of risks for the Company and receiving the greatest return from such investments owing to identification, assessment, management and monitoring of risks.

The goals of the Policy is to establish the elements and the overall policy framework for integrated risk management towards any kind of risk that the Company faces; it takes part of determination of the risk appetite and ensuring efficient management of the risks taken.

The tasks of the Policy are as follows:

- development of a full-fledged base for the decision-making and planning process;
- arrangement of a continuous and coordinated risk management process based on timely identification, assessment, analysis, monitoring, and control in order to ensure the achievement of the goals set;
- introduction and enhancement of the management system enabling the prevention and minimization of negative events;
- enhancement of the efficiency of resource utilization and allocation;
- avoidance of damage and losses by increasing efficiency of the Company's activities, which will protect the Company's assets and equity;
- ensuring the efficiency of business processes, as well as the reliability of internal and external reporting, and facilitation of the compliance with legal regulations.

The Policy shall also contain the following Appendices, which form the integral part hereof:

- requirements on the structure and contents of the reports on risks (Appendix 1).

2. CRMS Main Terms

In the framework hereof, the following main terms and definitions shall mean as follows:

- **Business Context** – the trends, events, relationships and other factors that may influence, clarify, or change Company's current and future strategy and business objectives.
- **Business Objectives** – measurable steps the organization takes to achieve its strategy.
- **Culture** – the attitudes, behaviors, and understanding about risk, both positive, negative that influence the decisions of management and personnel, and reflect the mission, vision, and core values of the organization.
- **Enterprise Risk Management** – the culture, capabilities, and practices, integrated with strategy-setting and its performance that organizations rely on to manage risk on creating, preserving, and realizing value.
- **Event –** an accident or occurrence having internal or external source in relation to the Company, influencing the achievement of objectives.
- **External Environment –** anything outside of the Company that influences the ability to achieve strategy and business objectives.
- **External Stakeholders –** any parties not directly engaged in the Company's operations but whom the Company affects, directly influence the Company's business environment, or influence the Company's reputation, brand, and trust.
- **Impact –** the result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the Company's strategy or business objectives.
- **Internal Environment** – anything inside of the Company that influences its ability to achieve strategy and business objectives.
- **Internal Stakeholders** – parties working within the Company such as employees, management, and the board.
- **Key Risk Indicator (KRI)** – indicator providing early warning of risk factor changes in various areas of activity.
- **Probability** – the possibility that a given event will occur.
- **Opportunity** – an action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value.
- **Organizational Sustainability** – the ability of Company to withstand the impact of large-scale events.
- **Portfolio View** – a composite view of risk the Company faces, which positions management and the board to consider the types, severity, and interdependencies of risks and how they may affect the Company's performance relative to its strategy and business objectives.
- **Risk** – the possibility that events will occur and affect the achievement of strategy and business objectives.

- **Risk Appetite** – the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
- **Risk Capacity –** the maximum amount of risk that Company is able to absorb in the pursuit of strategy and business objectives.
- **Risk Coordinator** – an employee of a Company's structural unit whose responsibility is to coordinate the identification and assessment of risks of the structural unit, and to ensure compliance of the structural unit's risk management with the Policy as well as with other Company's internal risk management documents approved by the Board of Directors of the Company, or other bodies of the Company.
- **Risk Factor –** a condition, a state, circumstances under which reasons of risk appear to precede realization of risk.
- **Risk identification** means estimation of the Company's exposure to events capable of negatively affecting the ability to attain target goals and implement set objectives. The aim of the risk identification procedure is to identify, new, emerging and changing risks to the achievement of the strategy and business objectives.
- **Risk Inventory** – all risks that could affect Company.
- **Risk Management unit of Management Accounts and Risk Management Department** – the Company's structural unit responsible for risk management issues.
- **Risk Map** – a graphic and textual representation of a limited number of Company's risks arranged as a rectangular table, with the risk's impact or significance indicated along one "axis", and the probability or frequency of its realization along the other one.
- **Risk Owner** – a person (employee/structural unit/collegiate body) in charge of any and all aspects of the management of a certain risk; particularly, in charge of decreasing the risk realization probability and/or the probable impact of the risk realization consequences on the Company's activities.
- **Risk Profile –** a composite view of the risk assumed at a particular level of the Company or aspect of the business that positions management to consider the types, severity, and interdependencies of risks, and how they may affect performance relative to the strategy and business objectives.
- **Risk Register –** a register of all Company’s risk with relevant objectives, risk factors, risk assessment, risk management actions, risk management action owners, risk owners and tolerances.
- **Severity –** a measurement of considerations such as the probability and impact of events or the time it takes to recover from events.
- **Stakeholders –** parties that have a genuine or vested interest in the Company.
- **Tolerance –** the boundaries of acceptable variation in performance related to achieving business objectives.
- **Uncertainty** – the state of not knowing how or if potential events may manifest.

3. Governance and Culture

Principle 1: Exercises Board Risk Oversight.

1. The Board of Directors has the primary responsibility for risk oversight in the Company and delegates some of the responsibility to a specific committee (i.e. Audit committee). Board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. The Company's **Board of Directors** shall perform the risk management functions which are as follows:
    - setting (short-term and long-term) goals/objectives of the Company;
    - approval of the Company's Risk Management Policy;
    - approval of other Company's policies for managing specific risks;
    - approval of methodology for evaluation of the risk management system effectiveness;
    - analysis of the reports of external auditors on the improvement of internal control and risk management, as well as the results of any inspections by the Internal Audit Department;
    - review and approval of the Company's risk register on a quarterly basis;
    - review and approval of risk map on a quarterly basis;
    - final approval of Risk Appetite of the Company and tolerances after the Risk Committee’s preliminary approval;
    - review of the reports provided by the head of the structural unit responsible for risk management with description and analysis of the Company's risks;
    - review of the reports on the efficiency of risk management system;
3. **Audit Committee** of the Board of Directors has the following responsibilities in the framework of risk management:
    - review reports on changes of risk map on a quarterly basis;
    - review changes to the risk register, and the information it contains;
    - review reports on risks;
    - review risk appetite on annual basis;
    - review reports with information on realized risks on quarterly basis;
    - review reports with information on non-compliance with regulatory requirements regarding risk management if necessary.

Principle 2: Establishes Operating Structures.

1. Company establishes its operating structure in pursuit of strategy and business objectives, which describes how Company organizes and carries out day-to-day operations.
2. Through the operating structure, employees are responsible for developing and implementing practices to manage risks and stay aligned with the core values of the Company.

3. The Board of Directors ultimately holds the President/CEO/CEO accountable for managing the risk faced by the Company by establishing risk management practices and capabilities to support the achievement of the strategy and business objectives
4. The Risk Committee is an advisory-consultative body, chaired the President/CEO of the Company, which provides preliminary reviews and makes recommendations to the President/CEO for decision-making in risk management issues of the Company.
5. Size and composition of the Committee members are approved by the order of the President/CEO of the Company, with the obligatory inclusion of the chief officers, heads of the financial, legal structural unit, safety department, the head of internal audit, as well as the heads of other departments at the discretion of the President/CEO of the Company. The Chairman of the Committee can delegate its rights to the Chief Financial Officer.
6. A detailed description of the Risk Committee's objectives and functions is provided in the Risk Committee Charter of “Air Astana” JSC.
7. The **Risk Committee** shall be in charge of the arrangement of an efficient corporate risk management system, and of the creation of the risk control structure to ensure performance and compliance with the corporate policies.
8. The **Risk Committee** shall ensure the integrity and the functionality of the risk management system by performing the functions which are as follows:
   - annual approval of Strategic plan of CRMS;
   - ensuring that the Company's structural units comply with the provisions of the Policy;
   - quarterly review and preliminary approval of the Company's risk register;
   - quarterly review and approval of risk map;
   - annual review and preliminary approval of Risk Appetite of the Company;
   - quarterly review reports with information on realized risks;
   - review and approval of KRI panel on annual basis and consideration of KRIs status stated in the KRI panel;
   - review and approval of the risk management action plans on risks in red and dark red zone of the risk map at least on annual basis;
   - review of the Company's risk management reports if any, and adoption of adequate measures within the framework of its competence;
   - improvement of internal procedures in the field of risk management;
   - holding regular (at least) quarterly based meetings with the established agenda, including new and existing risks, financial losses, internal/external audit reports, management issues. At that, all meetings of the Committee are recorded.
9. The operating structure of the Company incorporates the Three Lines model that offers a balanced approach to managing risk:

   First Line: Structural units and each employee of the Company. The main functions of the Company's structural units in the process of risk management are:

- identification and assessment of risks, determination of a risk response strategy, development and implementation of risk management actions for risks, improvement of risk management system within the scope of supervised/performed operations;
- implementation, monitoring and improvement of control procedures in the framework of entrusted business processes;
- compliance with the Risk Appetite within the competence;
- provision of reports on the implementation of risk management action plans on risks to Risk management unit.
- maintenance of a database on the realized risks and business incidents in accordance with the Regulation of record keeping and analysis of realized risks of “Air Astana” JSC;
- provision of timely and complete information on risks to interested parties, including, but not limited to, provision of information on risks to the Risk management unit in accordance with their requests.

Second Line: Structural unit responsible for risk management (Risk management unit of Management Accounts and Risk Management department).

Risk management unit is responsible for ensuring and monitoring the implementation of effective risk management practices. The main functions of the Risk management unit include, but are not limited to:

- coordination of activity of corporate risk management system in the Company;
- arrangement and coordination of the process of risk identification and assessment; as well as agreement with the risk owners the risk register, tolerances, key risk indicators, risk management actions, risk management action plans on risks; and monitoring the implementation of risk management actions in accordance with approved documents;
- notification of the Risk Committee and the Company's Board of Directors of any substantial deflections in risk management processes;
- provision of regular reports on risks to the shareholders of the Company;
- maintenance of a database of realized risks, trace external factors capable of substantial influence on the risks;
- preparation of Strategic plan of CRMS;
- control over the quarterly update of the risk register, the risk map, and risk management action plans on risks;
- control of the assessment of the identified risks/implementation of the risk assessment with the participation of the Company's experts;
- proposition for the attention of and preliminary approval by Risk Committee the Risk Appetite of Company;
- participation in the Risk Committee's meetings, preparation of the minutes on the Committee's resolutions, and distribution of them among the risk coordinators and risk owners;
- preparation of consolidated reports on risks, and submission of them to the Risk Committee, Audit Committee, and the Board of Directors of the Company (see Appendix 1);

- participation in the arrangement of regular assessment of the Company's risk management systems by means of making suggestions as to the assessment of "Risk Management" subcomponent within the framework of the corporate management level examination, and suggestions on methods of evaluation of efficiency of the corporate risk management system;
- development, implementation, and update (as appropriate) of the risk management methodological basis, policies, rules, and risk monitoring procedures;
- provision of the integration of risk management with other business processes, and develop risk management culture within the Company;
- coordination of strategic, investment projects in terms of sufficiency of disclosure and analysis of information on risks;
- provision Company's employees with methodological and consulting assistance as regards to risk management;
- suggestion of workshops and training on risk management for the Company's employees;
- cooperation with the Company's Internal Audit Department as regards to internal audit's plan formation, information exchange, discussion of audit inspections' results, exchange of knowledge and methods;
- identification of any possible risks, actual or potential, negative tendencies indicating the risk's strengthening, analysis of the factors causing the risk, and assessment of the scope of the expected loss.

It is required to comply with the following rules:

- Combining risk management functions with corporate management and strategic planning functions is allowed;
- To avoid any conflict of interest, head of the structural unit (the person) in charge of the company's risk management shall not be a member of the Company's Audit Committee.

Third Line: Internal Audit Department.

In course of risk management, the Company's Internal Audit Department shall perform the main functions, which are as follows:

- audit of risk management procedures and risk assessment methods, and development of suggestions as to the enhancement of efficiency of risk management procedures;
- submission of reports on the evaluation of efficiency of corporate risk management system to the Company's Board of Directors;
- other functions in accordance with any approved regulations.

Internal Audit Department of the Company shall perform regular inspection to analyse any gaps and drawbacks in the risk management system (including involvement of external independent consultant).

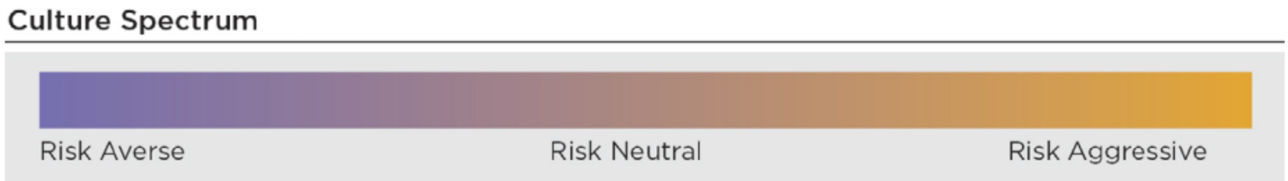
10. Policy shall apply to all Company's activities and shall be binding upon all Company's structural units and employees for familiarization and implementation. Management defines roles, responsibilities, and accountabilities of individuals, divisions, and functions aligned to strategy and business objectives.
11. Management delegates responsibilities and tasks to employees, committees to make decision to the extent required to achieve the Company’s strategy and business objectives by means of internal documents, job

descriptions, SL01 forms, and etc. When implementing its functions, responsibilities, and objectives, each employee of the Company shall abide by the provisions set forth herein.

12. To ensure efficient functioning of the risk management system, each structural unit of the Company shall appoint a risk coordinator responsible for the arrangement of risk management in their respective structural unit and for the cooperation with the Company's structural unit responsible for risk management at every stage of the Company's CRMS procedures implementation. It is recommended for Risk coordinator to have a grade MS1 or higher.
13. The responsibility and the authority of the employees of the Company's structural unit responsible for risk management, as well as the requirements to the reporting submitted, shall be stipulated by the Policy having provision on the structural unit responsible for risk management, and by the job descriptions for the employees of the Company's structural unit responsible for risk management.
14. The employees of the Company's structural unit responsible for risk management shall interact with other subdivisions, as well as external and internal auditors of the Company to efficiently fulfil the goals and the tasks of the CRMS.
15. The employees of the Company's structural unit responsible for risk management shall have access to the Company's information and documents necessary for the performance of their functions and responsibilities as specified herein and in the job description for such employees.

Principle 3: Defines Desired Culture.

1. Company defines the desired behaviour that characterizes Company’s desired culture through corporate documents and internal rules (e.g. Business Ethics Code, Code of Corporate Governance, etc.) that must be complied with by all officials and employees.
2. The desired behaviour and culture should be communicated to employees via forums, training, annual evaluation of knowledge of relevant corporate documents and regulations.
3. The culture, capabilities and practices are integrated into strategy and execution that Company relies on to manage risk and in creating, preserving and realizing value. Internal and external factors influence where the Company positions itself on the culture spectrum, which ranges from risk averse to risk aggressive:



4. The position of the Company in culture spectrum shall be reported to Risk Committee and Board of Directors.
5. Upon identified cases of non-adherence to the desired culture Company's employees and officials shall be entitled to address the Company's Audit Committee or the Board of Directors to report a violation of or improper compliance with any risk management or internal control procedures or other policies, as well as a case of fraud or legal infringement via hotline.

Principle 4: Demonstrates Commitment to Core Values.

1. Company demonstrates commitment to its core values (i.e. mission, goals, values), understanding values is fundamental to efficient functioning of CRMS.
2. Company shall embrace risk-aware culture by:
   - *Maintaining strong leadership:* The board and management places importance on creating the right risk awareness and tone throughout the Company. Culture and, therefore, risk awareness cannot be changed from second-line team or department functions alone;
   - *Employing a participative management style:* Management encourages personnel to participate in decision-making and to discuss risks to the strategy and business objectives;
   - *Enforcing accountability for all actions:* Management documents policies of accountability and adheres to them, demonstrating to personnel that lack of accountability is not tolerated and that practicing accountability is appropriately rewarded;
   - *Aligning risk-aware behaviours and decision-making with performance:* Remuneration and incentive programs are aligned to the core values of the organization including expected behaviours, adherence to codes of conduct, and promoting accountability for risk-aware decision-making and judgment;
   - *Embedding risk in decision-making:* Management addresses risk consistently when making key business decisions, which includes discussing and reviewing risk scenarios that can help everyone understand the interrelationship and impacts of risks before finalizing decisions;
   - *Having open and honest discussions about risks Company faces:* Management does not view risk as being negative, and understands that managing risk is critical to achieving the strategy and business objectives;
   - *Encouraging risk awareness across the Company:* The Company organizes training in the area of risk management and also that demonstrates the value of risk management and its critical need for the Company's success as well as the structure of the whole system and approach for managing separate risks.
3. The President/CEO/CEO and other members of management are responsible for all aspects of accountability – from initial design to assessment of the culture and risk management capabilities.
4. In order to raise the level of risk awareness, and develop risk culture and efficient risk management, information exchange shall be constantly performed within the Company. All employees shall obtain risk management tasks from their management in time, and shall clearly understand their function, the work they are supposed to do, and the way they should interact with their co-workers. Management should ensure that employees are aware of risks associated with their responsibilities and functions. The Company's management bodies shall be kept constantly updated on any existing risks and their management. There shall also be efficient communication with third parties, such as customers, partners, regulatory bodies, and shareholders.

Principle 5: Attracts, Develops, and Retains Capable Individuals.

1. Company is committed to building human capital in alignment with the strategy and business objectives.
2. Management, with board oversight, defines the human capital needed to carry out strategy and business objectives. Board of directors evaluates which competence CEO should have and management evaluates

which competence is required across the Company and addresses any shortcomings or excesses as necessary.

3. The human resources function helps to promote competence by assisting management in developing job descriptions and roles and responsibilities, facilitating training, and evaluating individual performance.
4. The relationship between the risk management process and the process of **personnel motivation** shall be as follows (including but not limited to):
    - The duties and responsibilities of CRMS participants as regards to implementation of all procedures imposed on them by the system shall be officially fixed, and the (non-) compliance with the respective duties and responsibilities during the reporting period shall be monitored;
5. The Board of Directors and management should develop contingency plans for assigning responsibilities, succession plans for key employees need to be defined, and succession candidates should be trained, coached, and mentored for assuming the role.

4. Strategy and Objective-Setting

Principle 6: Analyses Business Context.

1. Company considers business context and its potential effects on risks when developing strategy to support mission, vision and values. “Business context” refers to the trends, relationships, and other factors that influence a Company’s current and future strategy and business objectives.
2. Company considers the external and internal environment when developing strategy. Company's relations with **the external environment** (social, economic, legal, technological, political, and environmental) influence Company’s internal environment and its formation. The external environment is dynamic, unpredictable and complex in structure, includes various interrelated sectors, and favors the occurrence of systematic risks.
3. **The internal environment** defines the general Company's attitude towards risks, and the way the Company's employees respond and react to risks. The internal environment serves as a basis for all other components of the risk management system; includes risk management philosophy, risk appetite, control by management bodies, ethical values, competence and responsibility of employees, Company's structure, and its capabilities defined by human, financial, and other resources.

Principle 7: Defines Risk Appetite.

1. The Company defines risk appetite in the context of creating, preserving, and realizing value.
2. Risk appetite is the acceptable type and amount of risk for the Company in course of the achievement of the set goals.
3. The risk appetite is defined by the Risk Committee for each strategic goal (strategic directions of activity) or for all strategic goals together, which is more applicable for the Company, and approved by Board of Directors.
4. Risk appetite can be either quantitative or qualitative or combination of the both, the best approach is to align the analysis with risk assessment method.
5. Risk appetite (risk appetite statement) of the Company is characterized as one or several of following:
   - it reflects the Company's strategy, including goals, business plans, financial restrictions, and expectations of the stakeholders;
   - it embraces every key aspect (direction) of activity;
   - it considers the desire and the ability to take risks;
   - it defines the Company's attitude to risk;
   - it is regularly revised with the consideration of the industry and the market conditions;
   - it requires efficient monitoring of the risk.
6. The Company shall, revise the risk appetite, i.e. ability to take risks in order to pursue its goals, on an annual basis with the consideration of the industry and the market conditions.
7. One or several of the following parameters may be considered by the Company to determine risk appetite:
   - Strategic parameters, such as new products to pursue or avoid the investment for capital expenditures, and merger and acquisition activity.

- Financial parameters, such as the maximum acceptable variation in financial performance, return on assets or risk-adjusted return on capital, target debt rating, and target debt/equity ratio.
- Operating parameters, such as environmental requirements, safety targets, quality targets, and customer concentration.

8. Risk capacity statement is developed by the Risk Committee and approved by the Board of Directors.
9. All Company's risk appetite-related results and suggestions shall be agreed with the structural units concerned, including those in charge of the strategy, planning, and corporate financing.
10. The obtained risk appetite shall be regarded as a basis of further risk management-related decision-making. To fully embed risk appetite into decision-making at various levels, it needs to be cascaded through and align with other practices.
11. Risk appetite is communicated to appropriate levels of the Company, either broadly or to senior roles only.
12. The Company's risk appetite shall be funded at the expense of the Company's current income and retained income from recent years, and shall have no direct allocation to unplanned losses (i.e. losses due to risk realization directly reduce Company's income).
13. Management, with board oversight continually monitors risk appetite at all levels and accommodates change when needed.

Principle 8: Evaluates Alternative Strategies.

1. The company shall evaluate alternative strategies as part of strategy-setting and assess the risk and opportunities of each option. Alternative strategies shall be assessed in the context of the company resources and capabilities to create, preserve, and realize value.
2. The identified risks collectively form a risk profile for each option of alternative strategies. Determined risk profile allows management to consider the types and amount of risk Company will face in carrying out the strategy. It will allow management to determine what resources will be required and allocated to support carrying out the strategy.
3. Management and the board use these risk profiles when deciding on the best strategy to adopt, given the entity’s risk appetite. If the risk associated with a specific strategy is inconsistent with the entity’s risk appetite or risk capacity, it needs to be revised, an alternative strategy selected, or the risk appetite revisited;
4. Alternative strategies should be evaluated using the following approaches: SWOT analysis, modeling, valuation, revenue forecast, competitor analysis, and scenario analysis.
5. Company shall hold strategy-setting sessions to outline long-term strategies.

Principle 9: Formulates Business Objectives.

1. A company develops business objectives that are specific, measurable or observable, attainable, and relevant. Business objectives provide the link to practices within the company to support the achievement of the strategy.

2. The Company considers risk while establishing the business objectives at various levels that align and support strategy.
3. The goals of the Company's activities are determined at the strategic level, and set the basis for the development of the business objectives.
4. Business objectives are aligned with strategy, and cascaded throughout the Company and its divisions, operating units.
5. Business objectives are to be defined before identification of potential risks capable of negatively affecting the achievement of such objectives.
6. Company needs to have a reasonable expectation that a business objective can be achieved given the risk appetite and resources available to the Company. Otherwise, Company may choose to exceed its risk appetite, procure more resources, or change the business objective.
7. Company sets targets to monitor the performance and support the achievement of the business objectives.
8. The Company has defined tolerance (the range of acceptable outcomes variations related to achieving a business objective within the risk appetite) for each business objectives. It is important to consider that tolerance focuses on objectives and performance, not specific risks.
9. In setting tolerance, the Company considers the relative importance of each business objective.
10. Operating within the defined tolerance provides management with greater confidence that the Company remains within its risk appetite and provides a higher degree of comfort that the Company will achieve its business objective.
11. Performance measure related to business objective enables the confirmation that actual performance is within the established tolerance.
12. Tolerance also considers both exceeding and trailing variation (positive or negative).
13. Tolerance level should align with the Company's risk appetite to ensure that Company is not taking too much risk and exceeding its risk appetite.

5. Performance

Principle 10: Identifies Risk.

1. In order to demonstrate comprehensive risk identification risks need to be identified across all functions and levels.
2. Company identifies risks that affect the achievement of strategy and business objectives.
3. Risk identification allows raising the level of confidence in the achievement of the set goals by reviewing the risks and its main properties, determination risks' interrelation, increasing awareness of risks and methods of their management, and focusing the attention on the main risks.
4. The risks shall be grouped and classified as follows:
   - **strategic risk** (S):risks that affect or are created by Company’s strategy and strategic objectives;
   - **financial risk** (F): risks related to the Company's capital structure and financial profitability. Financial risks of the Company include market risks (interest and currency rates fluctuations, natural resources price fluctuation), liquidity risks, credit risks (related to corporate counterparties, second-tier banks, and claims of other countries);
   - **compliance risk** (C): risks of losses caused by the Company's non-compliance with the law of the Republic of Kazakhstan; with the laws of other countries; and with any internal rules and procedures;
   - **operational risk** (O): risks resulting from inadequate or failed procedures, systems or policies, employee errors, systems failures.
5. Risk identification provides a tool to register and state any potential negative events capable of negatively affecting the achievement of the goals and objectives of the Company and each of its employees, as well as to define the direction and the need of the risk management process improvement.
6. Every employee of a Company's structural units shall continuously identify and assess the risks with an impact on the achievement of the goals and objectives to be attained by the Company and each of its employees.
7. Company uses various approaches to identify the risks, such as data tracking, interviews, changes in key indicators, process analysis, workshops, risk identification based on the goals and objectives, industry-wide and international comparison, discussions, etc. (see more in the Rules of Identification and Assessment of Risk of “Air Astana” JSC).
8. Identified events and risks shall be arranged in the form of risk register. The Company's risk register represents a list of the risks the Company encounters in a course of its activities. Risk owners shall be assigned for each risk, i.e. departments dealing with the respective risks within the framework of their functions and responsibilities. As the new risks are identified, risk register shall be complemented by the Company's structural units on a permanent basis.
9. It is recommended to identify the risks and have the Company's risk register approved before approving the implementation of risk management actions, as well as risk management action plans on risks.

Principle 11: Assesses Severity of Risk.

1. Risk identification and assessment shall be aimed to provide the common vision on the existing risks and the scope thereof by means of basic ranking for determining the weak spots. The process allows evaluating the methods and procedures used to manage the main risks.
2. Risks that identified and included in a Company's risk register are assessed in order to understand the severity of each to the achievement of a Company's strategy and business objectives. Risk assessments inform the selection of risk responses and shows the significance of risks, which may negatively affect on Company's activities. Given the severity of risks identified, management decides on the resources and capabilities to deploy in order for the risk to remain within the Company's risk appetite.
3. Severity is determined in terms of Impact and Probability and its time of risk impact..
4. The time horizon used for assessment of risk should be the same as that used for the related strategy and business objectives.
5. In the framework of risk assessment and analysis, the Company shall use qualitative and quantitative analysis, or their combination that create the methodical base for the risk management process.
6. The Company shall assess certain risks with the use of various quantitative methods, such as VAR, gap-analysis, historic simulation method, stress-testing, etc. The order of the assessment shall be governed by the rules for the management of interest, currency risks, and liquidity risk, and by other internal regulatory documents of the Company.
7. All identified and assessed risks shall be reflected in the risk map. The probability or the frequency is indicated in the Map along the horizontal axis, and the impact or significance is along the vertical one. In this case, the probability of risk realization shall increase from left to right along the horizontal axis, and the impact of the risk shall increase upward along the vertical axis. The Risk Map allows assessing the relative importance of each risk (compared to other risks), and outlining the risks, which require the development of actions for the management thereof.
8. Key Risk Indicators (further referred to as KRIs), as defined in the Methodology of Development and Implementation of Key Risk Indicators of "Air Astana" JSC, are among the principal tools of risk and risk factors' monitoring. KRIs are indicators providing the organization with early warnings of risk factor changes in various areas of activity. KRIs allow identifying prospective risks and taking early measures to avoid the realization of risk and to minimize its impact on the organization's activities, and shall be developed for the corporate level risks.

Principle 12: Prioritizes Risks.

1. The prioritization of risks, given their severity, the importance of the corresponding business objective, and the Company's risk appetite helps management in its decision-making. The Company prioritizes risks in order to inform decision-making on risk responses and optimize the allocation of resources.
2. The Company prioritizes risks based on agreed upon criteria. Such criteria may include severity of risks, the importance of the corresponding business objective, and the entity's risk

3. In case of equal severity of risks considering the availability of resources Company must evaluate the trade-offs between allocating resources to mitigate one risk compared to another.
4. Priorities are determined based on agreed upon criteria:
   - Adaptability: The capacity of a Company to adapt and respond to risks.
   - Complexity: The scope and nature of a risk to the Company’s success. The interdependency of risks will typically increase their complexity.
   - Velocity: The speed at which a risk impacts the Company. The velocity may move the Company away from the acceptable variation in performance.
   - Persistence: How long a risk impacts the Company.
   - Recovery: The capacity of the Company to return to tolerance. Recovery excludes the time taken to return to tolerance, which is considered part of persistence, not recovery.

Principle 13: Implements Risk Responses.

1. Risk management represents the process of the development and the implementation of the measures allowing to reduce negative effect and the probability of loss or to obtain financial reimbursement in case of losses associated to the risks related to the Company’s activities. To ensure efficient process and to reduce the cost of its realization, the Company shall focus attention on the risks capable of exerting the most significant influence on its financial condition and achievement of goals and objectives. Risk management actions specified in the risk register shall be reviewed and approved by the Risk Committee, and further approved by the Audit Committee and the Company's Board of Directors, twice a year, and shall be binding upon all structural units of the Company.
2. For all risks identified, management selects and deploys a risk response.
3. The choice of the methods of responding to risks, and the development of risk management actions as well as risk management action plans for risks in order to secure the acceptable level of risk, shall include the following response categories:
   - Accept: No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite. Risk that is outside the Company’s risk appetite and that management seeks to accept will generally require approval from the board or other oversight bodies.
   - Avoid: Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, or selling a division. Choosing avoidance suggests that the organization was not able to identify a response that would reduce the risk to an acceptable level of severity.
   - Pursue: Action is taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance.

- Reduce: Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduce risk to an amount of severity aligned with the target residual risk profile and risk appetite.
- Share: Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialist service providers, purchasing insurance products, and engaging in hedging transactions. As with the reduce response, sharing risk lowers residual risk in alignment with risk appetite.

4. Suggestions as regards to risk management strategies, methods and actions shall be made by the risk owners.
5. The following must be considered while selecting and deploying risk responses:
   - Business context: Risk responses are selected or tailored to the industry, geographic footprint, regulatory environment, operating structure, or other factors.
   - Costs and benefits: Anticipated costs and benefits are generally commensurate with the severity and prioritization of the risk.
   - Obligations and expectations: Risk response addresses generally accepted industry standards, stakeholder expectations, and alignment with the mission and vision of the Company.
6. Company's structural units, which are the risk owners shall develop and quarterly update risk management actions.
7. The most suitable options shall be selected with the consideration of balancing the expenses related to a certain method with the benefits from the use thereof, and other expenses, whether direct or indirect.
8. The application of adequate measures and methods of responding to risks shall be described as part of risk management actions, as well as risk management action plans on risks. Risk Management Action Plans are developed for all risks in red and dark red zones of the risk map and contain information about the responsible employees, the implementation periods and cost of measures.

Principle 14: Develops Portfolio View.

1. Company develops and evaluates a portfolio view of risks in the form of risk register to view risk profile from a Company-wide, or portfolio perspective.
2. A portfolio view allows management and the board to consider the type, severity, and interdependencies of risks and how they may affect performance. Using the portfolio view, the Company identifies risks that are severe at the Company's level.
3. Portfolio view (full integration) – focus is on overall Company's strategy and business objectives. Greater integration supports identifying, assessing, responding to, and reviewing risk at the appropriate levels for decision-making. Boards and management focus greater attention on the achievement of strategy while responsibility and management of business objectives and individual risks within the risk inventory cascade throughout the Company.
4. Using portfolio view helps Company to observe risk that:
   - Increase in severity as they are progressively consolidated to higher levels within the Company.

- Decrease in severity as they are progressively consolidated.
- Offset other risks by acting as natural hedges.
- Demonstrate a positive or negative correlation to changes occurring in the severity of other risks.

5. Portfolio view allows management to determine whether the Company's risk profile is within the overall risk appetite.

6. Review and Revision

Principle 15: Assesses Substantial Change.

1. Company's strategy or business objectives and risk management practices and capabilities may change over time as the Company adapts to shifting business context. In addition, the business context in which the Company operates can also change, resulting in current practices no longer applying or sufficient to support the achievement of current or updated business objectives.
2. Company needs to be aware of the potential for large, substantial changes that may occur, since such change may lead to new or changed risks, and affect key assumptions underpinning strategy.
3. Company identifies internal environmental changes related to the business context and changes in culture, such as (but not limited to): Rapid Growth, Innovation, Substantial changes in leadership and personnel, and external environmental changes related to the business context and changes in culture, such as (but not limited to) changing regulatory or economic environment.
4. The identified changes shall be reflected in the risk register of the Company during the regular revisions and update sessions.

Principle 16: Reviews Risk and Performance.

1. Company reviews its performance and considers risks, and reviews its CRMS in order to identify incorrect assumptions, improper implemented practices, insufficient Company capabilities, or improper cultural factors.
2. If the Company determines that performance does not fall within its acceptable variation, or that the target performance results in a different risk profile than what was expected, it may need to:
   - *Review business objectives:* Company may choose to change or abandon a business objective if the performance is not achieved within acceptable variation.
   - *Review strategy:* Should the performance result in a substantial deviation from the expected risk profile, the organization may choose to revise its strategy. In this case, it may choose to reconsider alternative strategies that were previously evaluated, or identify new strategies.
   - *Review culture:* Company may wish to review its culture and determine whether it is embracing the actions in a risk-aware manner.
   - *Revise target performance:* Company may choose to revise the target performance level to reflect a better understanding of the reasonableness of potential performance outcomes and the corresponding severity of risks to the business objective.

- *Reassess severity of risks:* Company may reassess relevant risks, and results may alter based on changes in the business context, the availability of new data or information that enables a more accurate assessment, or challenges to the assumptions underpinning the initial assessment.
- *Review how risks are prioritized:* Company may decide to either raise or lower the priority of identified risks to support reallocating resources. The change reflects a revised assessment of the prioritization criteria previously applied.
- *Revise risk responses:* Company may consider altering or adding responses to bring risk in line with the target performance and risk profile. For risks that are reduced in severity, Company may redeploy resources to other risks or business objectives. For risks that increase in severity, the Company may reinforce responses with additional processes, people, infrastructure, or other resources. As part of reviewing risk responses, the organization may also consider monitoring activities developed and implemented as part of internal control.
- *Revise risk appetite:* Corrective actions are typically undertaken to maintain or restore the alignment of the risk profile with the Company's risk appetite, but can extend to revising it. However, this action requires review and approval by the board or other risk oversight body.

4. Corrective actions must align with the magnitude of the deviation in performance, the importance of business objective, and the cost and benefits associated with the changes in risk response.

Principle 17: Pursues Improvement in Enterprise Risk Management.

1. Company shall continuously pursue improvement of CRMS.
2. Continuous evaluations shall be embedded into business practices for identification of potential improvements to Company's risk management practices. Identified improvements to the CRMS shall be included to the Strategic plan of CRMS, which is annually reviewed and prepared by Risk management unit.
3. Internal Audit department conducts assessment of the effectiveness of the Company's risk management system, and develops suggestions as to the enhancement of efficiency of risk management procedures.
4. Regulatory documents regarding CRMS (as appropriate, including this Policy) shall be revised no less than once a year in order to ensure their conformity with the goals, scope and complexity of the Company's activities, to consider cutting-edge risk management practices and accumulated experience, as well as to comply with new regulatory requirements, experience and standards of risk management.

7. Information, Communication and Reporting

Principle 18: Leverages Information Systems.

1. CRMS requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the Company.
2. Company leverages its information and technology systems to support CRMS. Company uses information to anticipate situations that may obstruct the achieving of strategy and business objectives.
3. Company considers what information is available to management, what information systems and technology are in use for capturing that information (which may be more than is needed), and what the costs are of obtaining that information. Management and other personnel can then identify how information supports the risk management practices, which may include any of the following:
   - For governance and culture-related practices: Company may need information on the Code of conduct and individual performance in relation to those standards (e.g. through annual staff training, forums, etc.)
   - For strategy and objective-setting related practices: Company may need information on stakeholder expectations of risk appetite (e.g. through analyst calls, contract terms, etc.)
   - For performance-related practices, Company may need information on their competitors to assess changes in the amount of risk (e.g. through information published by competitors, market analysis, subscriptions, etc.)
   - For review and revision-related practices: Company may need information on emerging trends in enterprise risk management (e.g. through attending risk management conferences, seminars, following industry-specific blogs, etc.)

5. It is essential for information to be accessible to decision-makers and of high quality. To maintain high-quality information, Company implements data management systems and establish information management policies with clear lines of responsibility and accountability.

Principle 19: Communicates Risk Information.

1. Internally, management communicates Company's strategy and business objectives clearly throughout the organization so that responsible management (risk coordinators and risk owners) understand their individual roles. Specifically, communication channels enable management to convey:
   - The importance, relevance, and value of CRMS.
   - The characteristics, desired behaviours, and values that define the culture of the Company.
   - The strategy and business objectives of the Company.
   - The risk appetite and tolerance.
   - The principal expectations of management and personnel in relation to risk and performance management.

- The expectations of the Company on any important matters relating to risk management, including instances of weakness, deterioration, or non-adherence.

2. The Policy and other risk management-related documents must be available to all workers and officials of the Company via intranet.
3. Any changes in the principles of CRMS are communicated to all risk coordinators and risk owners.
4. Risk coordinators and risk owners of the Company regularly participate in joint internal meetings with RM unit where the existing and emerging risks, as well as methods of risks management are discussed.
5. Risk coordinators communicate changes in the CRMS to employees of their department and shares relevant information concerning the risks of their department and CRMS of the Company as a whole.
6. The following information is communicated by risk coordinators to Risk management unit:
   - Risks identified during the operational process;
   - Inefficient, unnecessary or unworkable controls identified during the operational process;
   - Information on risks realized in the department (immediate reporting);
7. Information on significant risks of the Company is published in the annual report.
8. Based on regular risk reporting, the Company shall control current risks and the implementation of risk management action plans on risks.
9. The Company's risk management structure shall enable appropriate information flow, both vertically and horizontally. The information going upwards (from bottom to top) shall timely provide the Board of Directors and the Risk Committee with the data on: current activities; risks taken in course of the activities; assessment, control, methods of responding to, and level of management thereof. The information going upwards shall enable the achievement of goals, strategies, and target objectives by means of approving internal documents, rules of procedure, and orders. Horizontal transfer of information suggests the interaction between the Company's structural units, and the interaction between the Company's structural unit responsible for risk management and other Company's subdivisions.
10. The decision on granting the access to Company's employees to the detailed information on the description, the assessment or the risk management action shall be made by the risk owner.
11. Members of the Company's Board of Directors and employees of the risk management unit shall have unrestricted access to any information on Company's risks.
12. Any outsider obtaining the access to the information on risks and their management actions may only be provided with such access upon signing a non-disclosure agreement of confidential information.
13. Information and communication in the Company shall allow providing the risk management process participants with reliable and well-timed risk information, raising the level of awareness of risks, as well as methods and tools of responding thereto. The relevant information is defined, fixed, and produced in the form and within the term allowing workers to efficiently perform their functions.
14. Board and management shall continually discuss risk appetite. As part of its oversight role, the board ensures that communications regarding risk appetite remain open.

Principle 20: Reports on Risk, Culture, and Performance.

1. Reporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy- and objective-setting, governance, and day-to-day operations.
2. Main results and conclusions on the Company's risk management process shall be regularly fixed in the reporting on risks and management actions thereof.
3. Company shall report on risk, culture, and performance at multiple levels and across the Company.
4. Risk Report Structure and Minimal Content Requirements are provided in the Appendix 1.
5. Company has developed "Regulation on reporting in corporate risk management system" in accordance with the Policy that ensures complete, consistent, transparent and accurate reporting on risk management for the effective operation of CRMS.
6. Procedures, responsibilities and timing on risk management reporting in the context of external and internal environment of the Company are summarized in the "Regulation on reporting in corporate risk management system". Reporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy- and objective-setting, governance, and day-to-day operations. Report users include:
   - Management and the board of directors with responsibility for governance and oversight of the Company.
   - Risk owners accountable for the effective management of identified risks.
   - Assurance providers who seek insight into performance of the Company and effectiveness of risk responses.
   - External stakeholders (regulators, rating agencies, community groups, and others).
   - Other parties that require reporting of risk in order to fulfill their roles and responsibilities.

8. Appendix 1. Risk Report Structure and Minimal Content Requirements

To the Risk Committee

1. Risk map and risk register:

a) The risk map once a year, modifications of the risk map on a quarterly basis, with detailed information on any changes in the risks' dynamics;

b) Separate risks, with the reasons of their appearance, risk management actions for the reduction of their probability/impact, the qualitative/quantitative assessment of impact;

c) The risk register once a year, the risk register with amendments on a quarterly basis, as appropriate;

d) Risk management actions once a year, with modifications to the risk management actions for the risks on a quarterly basis, as appropriate.

e) Newly identified risks (threats), with the reasons of their appearance, risk management actions for the reduction of their probability/impact, the qualitative/quantitative assessment of impact.

f) Risk owners.

2. Risk Management action plans on risks in the red and dark red zone of the risk map once a year.
3. Risk appetite once a year.
4. Tolerances once a year with amendments on a quarterly basis, as appropriate.
5. KRI panel once a year.
6. Strategic plan of CRMS and the annual reports on progress.
7. Information on any realized risks (quarterly), with obligatory indication of the damage (qualitative and quantitative) and the actions taken to respond to the risks with the assessment of the efficiency thereof.

To the Audit Committee and the Board of Directors:

1. Risk map and risk register:

a) The risk map once a year, modifications of the risk map on a quarterly basis, with detailed information on any changes in the risks' dynamics;

b) Separate risks, with the reasons of their appearance, risk management actions for the reduction of their probability/impact, the qualitative/quantitative assessment of impact;

c) The risk register once a year, the risk register with amendments on a quarterly basis, as appropriate;

d) Risk management actions once a year, with modifications to the risk management actions for the risks on a quarterly basis, as appropriate.

e) Newly identified risks (threats), with the reasons of their appearance, risk management actions for the reduction of their probability/impact, the qualitative/quantitative assessment of impact.

2. Risk appetite once a year.
3. Tolerances once a year with amendments on a quarterly basis, as appropriate.
4. Information on any significant deviations from the standard risk management process, as appropriate.
5. Information on compliance with regulatory requirements regarding risk management if necessary;
6. Information on any realized risks (quarterly), with obligatory indication of the damage (qualitative and quantitative) and the actions taken to respond to the risks with the assessment of the efficiency thereof.