

Joint-Stock Company "HansaMatrix" RISK MANAGEMENT POLICY

1. The purpose of the policy

1.1. The purpose of JSC "HansaMatrix" (hereinafter – the "Company") Risk Management Policy (hereinafter - the "Policy") is to determine common basic principles of risk management and the division of responsibilities to identify and manage the most significant negative factors affecting the Company's operations in a timely fashion to ensure the achievement of strategic goals, successful development and a reduction of potential loss and/or damage to reputation in accordance with international standards, good corporate governance practice and binding legislation in the Republic of Latvia.

1.2. The main task of the policy and other related documents is to facilitate the Company's employees to perform activities related to Risk management and at the same time to promote appropriate monitoring and the evaluation of employees in compliance with Risk management requirements to:

- 1.2.1. promote maximum sustainability for the Company's core business, strategy implementation and development plans;
- 1.2.2. promote and protect the permanence of the availability of the Company's services to customers;
- 1.2.3. promote the efficiency of the Company's operations;
- 1.2.4. promote the activities of the Company in case of various disturbances and other unplanned situations;
- 1.2.5. promote the good reputation of the Company;
- 1.2.6. promote effective management of stakeholders (including the Company's customers, cooperation partners, suppliers, etc.);
- 1.2.7. protect assets and property of the Company;
- 1.2.8. protect employees, members of the management board.

2. Access to the policy

2.1. The Policy will be available for viewing to any director or employee of the Company. In addition, this policy may be made available to any third party at the discretion of the Company's Chief Executive Officer.

3. Scope of the policy

- 3.1. The Policy applies to the Company and is applied - to the extent insofar as it does not contradict the provisions of applicable regulatory enactments.
- 3.2. The Policy sets out the general basic elements and principles of risk management, their mutual interaction and integration in the processes of the Company.
- 3.3. The Management Board of the Company is the owner of this Policy. The duties of organizing the risk identification, ensuring classification according to this policy, and risk mitigation plan preparation and other duties of the Company Risk Manager are carried out and coordinated by the Chief Financial Officer of the Company.
- 3.4. The Company wide risk identification and assessment is carried out once per year and all the identified risks, risk occurrence probability levels, risk severity (occurrence impact level) assessments, risk mitigation action plans and responsible persons for managing each identified risk of the Company are registered in the Risk register.
- 3.5. When implementing risk management, the Company divides risks into the following groups:
 - 3.5.1. Strategic risks.
 - 3.5.2. Operational risks.
 - 3.5.3. Legal and compliance risks.
 - 3.5.4. Financial risks.

4. Definitions

- 4.1. **Risk** - a possible event that may adversely affect the Company's ability to provide the services or to achieve the set business objectives and to effectively implement the strategy.
- 4.2. **Significant risks** - events that classify as "Intolerable" and "Substantial" based on the Risk level matrix in Figure 5 of this Policy and that may significantly adversely affect the Company's ability to provide the services or to achieve the strategic goals set by the Company, events, which may cause significant financial loss or damage to the Company's reputation, or events which may have an adverse effect on the health and / or life of natural persons, but whose probability of occurrence and / or possible adverse effects cannot be precisely determined.
- 4.3. **Strategic risks** - risks related to the definition and implementation of strategic goals.
- 4.4. **Operational risks** - risks related to employee errors, non - compliant or incomplete internal processes, information systems, projects, environmental impact, labour environment and external threats.
- 4.5. **Financial risks** - market risk (price, interest rate and currency risk), credit risk and liquidity risk.

- 4.6. **Legal and compliance risks** - risks due to the effects of external circumstances, which include legal risks and the risks associated with the documentation, as well as non-compliance or breach of the law, rules and standards.
- 4.7. **Risk Management** - identification of existing and potential risks, their development scenarios, analysis of causes, effects and probabilities of occurrence, identification of risk controls and critical identification of controls, risk assessment before and after existing risk controls, in addition identification, evaluation and implementation of risk mitigation measures to reduce the residual risk, if necessary, as well as risk control.
- 4.8. **Risk appetite** - the amount of risk and the type of risk that the Company is prepared to take to achieve the objectives set out in the strategy.
- 4.9. **Risk management system** - practices, tools and methods used in the Company to identify, analyse, assess, mitigate and manage risks.
- 4.10. **Probability** - the possibility of a particular risk event occurring.
- 4.11. **Impact** - the consequences, or effects of a Risk event on the Company operations.
- 4.12. **Risk level** is obtained by combining Probability and Severity and is expressed based on the Risk level matrix described in Article 8.X of this policy.
- 4.13. **Responsible person** is a Company employee responsible for existing Risk control measures and Risk mitigation plan implementation;
- 4.14. **Risk register** – the list of all Company risks as identified in the Risk management process of the Company, which also includes a description of each risk, existing control measures, mitigation plans, the impact, the probability, the responsible person and the risk level.

5. Basic principles of risk management

5.1. Risk management in the Company is an integral part of daily management processes and a component of activities, functions and other processes that is binding on all of the Company's management levels. Risk management decisions are based on risk awareness.

5.2. The Company's Risk Management Principles:

- 5.2.1. Risk management is integrated into both strategy development and implementation processes and in day-to-day operations.
- 5.2.2. Risk assessments will be conducted on all new ventures and projects prior to commencement to ensure alignment with the Company's risk appetite and organisational objectives.
- 5.2.3. the Risk management system and process are aligned with the Company's needs and risk specificity.
- 5.2.4. Risk management responds appropriately and in a timely manner to external and internal changes and events.
- 5.2.5. Historical, current and expected future information are used in risk management.
- 5.2.6. Regular and systematic staff training and information is provided, and clarification, promoting risk understanding and Risk management.

- 5.2.7. The Risk management system is constantly improved in accordance with the best practices, principles and experience.
- 5.2.8. Responsibility for Risk management is determined at various levels of the Company's management, precisely defining responsibilities for the purpose of achieving effective Company Risk management.
- 5.2.9. Important, objective and sufficient information for risk management is provided in a timely manner to the employees who need it.
- 5.2.10. Intolerance to fraud and corruption.

6. Policy implementation and monitoring

6.1. The Council of the Company:

- 6.1.1. Approves the Company's Risk Management Policy.
- 6.1.2. Monitors the operation of the Company's Risk Management System.
- 6.1.3. Annually reviews the report of the Company's Audit Committee on the Company's Risks and the efficiency of the Risk management system.
- 6.1.4. Annually reviews the Significant Risk Management Report prepared by the Management Board of the Company.

6.2. Company Audit Committee:

- 6.2.1. monitors the efficiency of the Company's risk management system.
- 6.2.2. makes proposals to the Council of the Company on how to prevent a risk of the Risk management system shortcomings.
- 6.2.3. at least once a year submits a report to the Council of the Company on the effectiveness of the Company's risk management system.

6.3. The Management Board of the Company:

- 6.3.1. Establishes a comprehensive Company Risk Management System, based on this Policy.
- 6.3.2. Develops a Risk Management Policy.
- 6.3.3. Approves the Company's annual Significant Risk Management Report, incl. current Significant risks.
- 6.3.4. At least once a year submits a report to the Council of the Company on the Company's Significant risk management.
- 6.3.5. Ensures risk management for the respective Risk Management System of the Company.
- 6.3.6. Approves the Company's internal regulatory documents for Risk Management.
- 6.3.7. Approves the Company's risks, incl. Significant risks and considers Significant risk critical controls and the implementation of the Significant risk mitigation action plan.

6.4. Company Risk Manager:

- 6.4.1. On behalf of the Board of the Company, develops internal regulatory documents, which regulates the Company's Risk Management.
- 6.4.2. Provides support to the implementation of the Company's Risk Management and related documentation provision.

- 6.4.3. Promotes cooperation between Risk management issues and promotes a common understanding of Company Risk Management.
- 6.4.4. Maintains and updates a unified Register of the Company's Significant Risks, ensures that the responsible person is assigned for each identified risk control and mitigation action plan fulfilment.
- 6.4.5. Ensures an annual assessment of the Company's Significant Risks.
- 6.4.6. Provides the Company's management with comprehensive information on the Company's Significant risks, their assessment, control and mitigation measures.

6.5. Heads of company functions / structural units:

- 6.5.1. constantly monitor the processes of its functions / departments and external business environment in a timely manner in accordance with the scope of its function / unit identity and manage existing and potential risks - ensure risk control and the identification, evaluation and enforcement of additional risk mitigation measures, where necessary.

6.6. Company employees:

- 6.6.1. Perform within their competence and this Policy.
- 6.6.2. report in a timely manner to his / her line manager on the identification of a new risk in his / her work.

6.7. Employees responsible for Risks of the Company:

- 6.7.1. Collect information about the Company's Risks, incl. Significant risks, estimate their occurrence probability and potential severity or impact.
- 6.7.2. Inform the Board of the Company and the Company Risk Manager about a new risk identification in a timely manner.
- 6.7.3. In cooperation with the Company Risk Manager perform a detailed analysis and assessment of the Significant Risks, which relates to the relevant function / structural unit of the Company.
- 6.7.4. Inform the Board of the Company about the Significant Risks, which relate to the relevant analysis and evaluation of the Company's operations, and submits for approval proposals for the implementation of Significant Risk Control Measures, if necessary.
- 6.7.5. In cooperation with the Company Risk Manager maintain and update a unified Register of the Company's Significant Risks.
- 6.7.6. Prepare and implement the Risk mitigation plans for Risks that are not considered as Significant and reports the implementation progress to the heads of company functions/structural units

7. The process of risk management

- 7.1. The process of Risk Management includes the following elements:
 - 7.1.1. Risk identification;
 - 7.1.2. Risk assessment;
 - 7.1.3. Deciding on the type of response;
 - 7.1.4. Registration of risks;
 - 7.1.5. Identification of risk mitigation measures;

- 7.1.6. Implementation of risk mitigation measures;
- 7.1.7. Risk monitoring;
- 7.1.8. Reassessment of risks;
- 7.1.9. Communication and consultations.

Figure 1. Risk management process



7.2. The activities of the Company's Processes are divided between two Risk Management protection levels:

- 7.2.1. the first level of protection - continuously in the company's operations and day-to-day decision-making. The Company's management is responsible for holding the risks (ownership) and in their areas of responsibility by establishing effective management system. The Company's management is responsible for all risks that are under its responsibility identification, monitoring and regular inspections, as well as a business plan fulfilment in accordance with the approved risk appetite;
- 7.2.2. the second level of protection - includes oversight by the Risk Management function, the current function, the operational compliance function and the financial management function. Risk Management function and responsibility for the development and maintenance of the Risk Management systems, their provision, all risks and proper supervision without the parties of the first level of protection - in daily work, as well as in decision-making, as well as in the future risk profile assessment. Relevant functions provide feedback to the Company's Management Board and / or Audit Committee on the effectiveness and compliance of Risk Management systems from the first level of protection;

8. Risk register of the Company

- 8.1. All identified risks in the process of the Risk management are registered in the Risk register of the Company.
- 8.2. The Risk register includes the following information about each risk:
 - 8.2.1. the Risk group;
 - 8.2.2. the Risk itself;
 - 8.2.3. description of the Risk;
 - 8.2.4. the Risk impact scope (Company level or Structural unit level)
 - 8.2.5. description of the existing control measures;
 - 8.2.6. action plan for mitigation;
 - 8.2.7. action plan for mitigation implementation deadline;

- 8.2.8. responsible person for risk existing control measures and mitigation plan implementation;
- 8.2.9. the Probability;
- 8.2.10. the Impact;
- 8.2.11. the Risk level;
- 8.2.12. the Probability after the Risk mitigation Plan execution;
- 8.2.13. the Impact after the Risk mitigation Plan execution;
- 8.2.14. the Risk level after the Risk mitigation plan execution.

8.3. the Probability is estimated and assigned in the Risk assessment process, using the following Probability scale:

Figure 2. Probability scale.

Probability	Description
Frequent (5)	Highly likely to occur
Probable (4)	Likely to occur
Occasional (3)	Possible to occur
Remote (2)	Will most likely not occur
Improbable (1)	Highly unlikely to occur

8.4. the Impact is estimated and assigned in the Risk assessment process, using the following Impact scale:

Figure 3. Impact scale.

Objective/Relative value	Catastrophic (4)	Critical (3)	Marginal (2)	Negligible (1)
Cost	> 30% increase	10–30% increase	5-10% increase	< 5% increase
Time	> 30% increase	10–30% increase	5-10% increase	< 5% increase
Scope (the extent of the area or subject matter that the Risk is related to or to which it is relevant)	End result effectively useless	Major areas affected	Significant areas affected	Minor areas affected

Quality	End result effectively useless	Unacceptable quality reduction	Quality reduction requires sponsor approval	Barely noticeable quality degradation
----------------	--------------------------------	--------------------------------	---	---------------------------------------

8.5. the Risk level is determined using the following Risk level matrix:

Figure 4. Risk level matrix.

Probability/Impact	Catastrophic (4)	Critical (3)	Marginal (2)	Negligible (1)
Frequent (5)	Intolerable (20)	Intolerable (15)	Substantial (10)	Moderate (5)
Probable (4)	Intolerable (16)	Intolerable (12)	Substantial (8)	Moderate (4)
Occasional (3)	Intolerable (12)	Substantial (9)	Moderate (6)	Tolerable (3)
Remote (2)	Substantial (8)	Moderate (6)	Moderate (4)	Tolerable (2)
Improbable (1)	Moderate (4)	Moderate (3)	Moderate (2)	Tolerable (1)

8.6. The Company Risk tolerance is defined based on the Risk level:

Figure 5. Risk tolerance of the Company.

Risk level	Control of the risk to be considered
Intolerable (12-20)	Unacceptable risk. Risks of this level need an immediate mitigation plan prepared for implementation and immediate, effective, temporary risk mitigation measures to be applied.
Substantial (8-10)	Unacceptable risk. Risks of this level need a mitigation plan prepared for implementation and if possible immediate, effective, temporary risk mitigation measures applied.

Moderate (3-6)	Acceptable risk. Reduction of the risk within the defined timeframes should be attempted whilst keeping control of the prevention costs. If this medium risk involves potentially serious consequences, consider an additional assessment to determine its probability and determine the need for better control measures.
Tolerable (1-2)	Acceptable risk. No additional control of the risk is required. Target a more economical solution or an improvement without additional cost. Ensure monitoring that the risk is kept under control on a long-term basis.

8.7. The Risks of Intolerable and Substantial Risk level that may significantly adversely affect the Company's ability to provide the services or to achieve the strategic goals set by the Company, events, which may cause significant financial loss or damage to the Company's reputation, or events which may have an adverse effect on the health and / or life of natural persons are to be considered as Significant risks by the Management board of the Company.

8.8. Management Board of the Company ensures the Risk mitigation plans for The Risks of Intolerable and Substantial Risk level and monitors implementation of these plans.

9. Responsibility for policy maintenance

9.1. The Management Board is responsible for maintaining this Policy and updating the Policy at least every 5 years.