APPROVED

at the Council meeting of
the Joint Stock Company “Latvijas Gāze”
held on November 30, 2023,
minutes No.8 (2023)

JSC “LATVIJAS GĀZE” RISK MANAGEMENT AND GOVERNANCE POLICY

1. Purpose of the Policy

1.1. The purpose of the Company's Risk management and governance policy (hereinafter – the Policy) is to lay down the Company's risk governance structure, the common basic principles of risk management, and the division of responsibilities in order to timely identify and manage the main adverse factors towards the Company's operation, ensuring the accomplishment of the Company's strategic objectives and a successful development, and mitigating the potential losses and/or reputational harm.

1.2. The principles set out in the Policy are in conformity with the best international practice of risk management and governance and the external regulatory enactments.

2. Definitions of terms

2.1. **Company** – the Joint Stock Company "Latvijas Gāze".

2.2. **External regulatory enactments** – the regulatory enactments of the Republic of Latvia and foreign countries that are binding to the Company's operations.

2.3. **Internal regulatory enactments** – the Company's internal regulatory enactments, including regulations, policies, rules, procedures, resolutions, orders and other documents that govern the Company's operation and are binding to all structural units and employees.

2.4. **Incident** – a risk event that has actually occurred.

2.5. **Risk** – an event that may adversely affect the Company's ability to accomplish the operational objectives and effectively pursue the strategy.

2.6. **Risk management system** – a set of tools, methods and events with the purpose of ensuring an effective management of the Company's risks in line with the best practice.

2.7. **Risk management process** – risk identification, risk analysis and assessment, risk mitigation and control, risk reporting.

2.8. **Risk appetite** – the amount of risk that the Company is ready to take in order to accomplish the strategic objectives.

2.9. **Risk identification tool** – a document (MS Excel) through which the Company identifies and assesses risks, describes the control measures implemented towards mitigating the risks identified, and designates the persons and structural units in charge thereof.

2.10. **Risk manager** – a person designated by the Board of the JSC "Latvijas Gāze" in charge of risk management at the Company.

2.11. **Internal control system** – a set of measures introduced in order for the Company to operate as securely, effectively and well-organised as possible. The elements of the internal control system are control environment, risk management, control measures, information and communication, monitoring.

3. Risk management levels – division of duties and responsibilities

3.1. **The Council of the JSC "Latvijas Gāze"** approves the Company's Risk management and governance policy and once pear year reviews a report by the Board of the JSC "Latvijas Gāze" on the effectiveness of risk management and the major risks.

3.2. **The Board of the JSC "Latvijas Gāze"** is responsible for the implementation of the risk management policy and strategy at the Company, the running of the risk management process, and the approval of internal regulatory enactments/documents.

3.3. **The Risk management committee** ensures a uniform risk management on a Company level, reviews the current risks and their assessment, picks out and analyses the major risks, and gives recommendations for the improvement of internal regulatory enactments.
The members of the Risk management committee are designated by the Board of the JSC "Latvijas Gāze". The Risk management committee at least once per year reports to the Board of the JSC "Latvijas Gāze" on the Company's major risks and the measures to be taken for their mitigation.

3.4. **The Risk manager of the Company** ensures the establishment and improvement of comprehensive risk management system in line with the best practice, the development of relevant internal regulatory enactments, and the implementation of the risk management process, supports the heads of structural units and employees in its implementation, provides regular updates to the Risk management committee, and reports to the Board of the Company.

3.5. **The heads of structural units of the Company** keep track of the processes and operational environment of the functions / structural units under their management in order to properly and timely identify and manage existing and potential risks, including the implementation of the necessary controls. The heads of structural units immediately notify the Risk manager of risk incidents and events that may adversely affect the functions/structural units under their management and/or the operation of the entire Company.

3.6. **The employees of the Company** assess day-to-day operational risks, take the necessary control measures in line with the internal regulatory enactments, and immediately notify the management of events or incidents that may adversely affect the course of processes.

3.7. **The internal auditor of the Company** is responsible for an independent supervision of the internal control system, including the risk management system, ensuring the planning and performance of audits appropriate to the level of the Company's risks.

4. Basic principles of risk management

4.1. The purpose of risk management is to protect the Company from the materialisation of risks that might hinder the continuity of business, the accomplishment of the objectives set forth, the implementation of plans and a successful development, and adversely affect financial stability and reputation.

4.2. Risk management is an integral part of the Company's day-to-day management, business activities, functions and processes, and the division of responsibilities therein follows the principle of three lines of defence.

4.3. Risk management is based on a culture of risk awareness that is binding across all management levels of the Company. The employees are regularly and systematically educated and advised, developing a culture of risk awareness at the Company and raising awareness of risks and their management and each employee's responsibility for a successful risk management in his/her area of activity.

4.4. The Company abides by the following risk management principles:
4.4.1. Risk management is integrated in and coordinated with the strategy development and implementation processes as well as the day-to-day operational activities, the planning and implementation of investment projects, and other processes;
4.4.2. The risk management process is adapted to the Company's needs and the specifics of the risks inherent to its operation;
4.4.3. The risk management system is designed so as to respond timely and appropriately to changes and events in the external and internal environment;
4.4.4. The risk management system is based on information of past, current and possible future events;
4.4.5. A successful risk management enables ensuring operational continuity in the lines of activity critical to the Company;
4.4.6. Under the principle of separation of duties, the responsibility for risk management in operational activities and for control thereof is separated to the extent possible;
4.4.7. In risk management, the principle of materiality applies, and all risks inherent to the Company's operation are split into two categories: significant risks and insignificant risks.
4.4.7.1. By **significant risks** the Company understands risks whose initial risk level (the product of probability of risk and impact of risk) exceeds 13 and which result in one or several of the following criteria being met:
4.4.7.1.1. There may be an adverse impact on the Company's ability to do business and/or to accomplish its strategic objectives;
4.4.7.1.2. There may be substantial losses and/or substantial reputational harm incurred;
4.4.7.1.3. There may be an adverse impact on human health and/or life.
4.4.7.2. By **insignificant risks** the Company understands risks whose initial risk level (the product of probability of risk and impact of risk) does not exceed 13, whose results does not leave a substantial adverse and lasting impact on the Company's operation, and whose possible consequences can be eliminated swiftly and without substantial resources.
4.5. The Company uses the following approaches to reduce the risk level, aligning them with the risk assessment and ensuring reasonable assurance of the result achieved in risk mitigation:
4.5.1. Risk aversion – if possible, the Company does not take actions that may cause an unacceptably high and difficult-to-control risk;
4.5.2. Risk transfer or distribution – if possible and considered beneficial, the Company insures (through direct insurance or risk distribution among subcontractors, suppliers, counterparties, etc.) lines of activity that may cause a risk to materialise and bring losses.
4.5.3. Risk level reduction – the Company makes and maintains an internal control system that reduces risks to an acceptable level.
4.6. The control methods used to reduce the level of the Company's risks may be:
4.6.1. Preventive, i.e., applied to prevent the materialisation of the possible risk, such as division of duties and responsibilities, coordination of

decisions, authorisation, planned or extraordinary inspections, automated controls, deviation analyses, physical control, etc.;

4.6.2. Corrective, i.e., applied to mitigate the consequences of the materialisation of the risk if it could not be prevented, such as harm elimination measures, incident analyses, availability of backup systems, etc. Corrective controls should be supplemented with activities aimed towards preventing the materialisation of a similar risk in future.

4.7. The risk management system and processes are continuously improved based on the best practice and experience.

5. Risk management system

5.1. In order to manage the risks inherent to the Company's operation, a common system is set up that combines elements of the risk management process with other measures that ensure a timely identification, assessment and mitigation of risks. The risk management system is:

5.1.1. Risk identification, analysis and assessment – the identification and assessment of risks of the Company's lines of activity, processes and systems, the assessment of effectiveness of the existing controls, and the analysis of the necessary risk limitation measures takes place at least once per year using the risk identification tool;

5.1.2. Development of a plan of risk mitigation measures and improvement of the internal control system – a plan of measures is drawn up at least once per year specifying the necessary control measures, the persons in charge, and the deadlines for the reduction of the remaining risk level;

5.1.3. Registration and analysis of risk incidents – a risk database is set up where all operational, financial and compliance risk incidents or events that may harm the Company are registered, and the causes and consequences of such incidents are analysed;

5.1.4. Risk assessment in development projects – new services/products are introduced and changes to existing services/products are made only after a comprehensive risk assessment;

5.1.5. Determination of key risk indicators (KRIs) – the use of statistical, financial and other indicators that reflect the risk level in various lines of activity of the Company;

5.1.6. Business continuity planning – the Company conducts a business impact analysis and develops a business continuity plan (The Company's risk manager and heads of structural units);

5.1.7. The employees are trained on risk management matters as necessary based on personnel changes in structural units and requests by heads of structural units;

5.1.8. Reporting – risk summaries and reports are presented at the Company at least once per year. The Risk managers report to the Board of the Company which, in turn, reports to the Council. The Risk committee at least annually reports on risks to the Board of the JSC "Latvijas Gāze" which notifies the Council of the JSC "Latvijas Gāze" of the significant risks.

5.2. The risk management system covers all risk groups inherent to the Company's operation as listed in Section 7 of the Policy. The Risk management committee is responsible for implementing the measures of the risk management system and its overall performance.

6. Risk management process

6.1. The Company's risk management process includes the following elements: risk identification, risk analysis and assessment, risk control and decision-making, risk monitoring and reporting.

6.2. The Risk manager organises the implementation of the risk management process and is responsible for its course, but all structural units of the Company are involved in the process.

6.3. Risk identification envisages a periodic identification and documentation of the risks inherent to each of the Company's activities using the following methods:

6.3.1. Identification of internal and external risk sources;

6.3.2. Analysis of problems and scenarios;

6.3.3. Analysis of the industry and collection of expert opinions.

6.4. As part of risk identification, the Company also identifies the opportunities presented by the external or internal circumstances associated with potential risks and the actions that the Company should take in order to take advantage of such opportunities.

6.5. Risk analysis and assessment envisages analysing and assessing the probability of materialisation of all the risks identified and their possible impact on the Company's operation using risk level rating criteria where 1 means low probability/impact and 5 means very high probability/impact – see Appendix No. 1 Risk identification tool.

6.6. Risk control and decision-making envisages identifying the existing controls and deciding on additional control measures, as well as allocating duties and responsibilities to set up an internal control system that reduces the level of the risk identified to acceptable (based on the risk appetite factor set by the Board of the JSC "Latvijas Gāze").

6.7. Risk monitoring and reporting envisages a risk level revision at least once per year by the Risk manager of the Company and submission of risk management reports to the Board pursuant to the procedure described in Section 3 of the Policy.

7. Risk groups at the Company

7.1. The risks inherent to the Company's operation are divided into the following risk groups:

7.1.1. Strategic and external environment risk – a possibility of various circumstances (incl. external) and events resulting in the Company being unable to accomplish its strategic objectives and fulfil its plans and tasks.

7.1.2. Operational risk – a possibility of suffering losses due to a non-compliant, incomplete or ineffective course of internal processes, employee mistakes, incompetence, operational issues of information technologies and systems.
Operational risk encompasses process risk, personnel risk, information technology and system risk.

7.1.3. Financial risk – a possibility of suffering losses due to erroneous financial calculations or projections, lack of resources, or market conditions.
Financial risk encompasses credit risk (incl. concentration risk), market risk (incl. price risk, interest rate risk, currency risk), liquidity risk.

7.1.4. Compliance risk – a possibility of suffering losses or reputational damage and the further activity being adversely affected due to a failure to comply with the legislative requirements, standards or contracts which may result in punitive sanctions or legal proceedings. Compliance risk encompasses money laundering and terrorism financing risk as well as fraud and corruption risk.

7.1.5. Reputational risk – a possibility of customers, counterparties, shareholders, supervisory authorities and other stakeholders developing a negative impression of the Company or the services provided by it, with an impact on the subsequent operation.

7.2. The groups of the risks inherent to the Company's operation may be periodically revised based on the results of risk identification and assessment.

8. Strategic and external risk management

8.1. The purpose of strategic and external risk management is to establish a system that allows for a timely prediction of and due response to both changes in the external environment circumstances and market events that pose threat to the Company's operation and other circumstances and events that might jeopardise the Company's operation and adversely affect the accomplishment of strategic objectives and business development.

8.2. The process of identification and assessment of strategic and external risk weighs the probability of threat to the Company's long-term development and the availability and quality of its services, decrease in revenue, or occurrence of unforeseen losses due to:

8.2.1. Unforeseen changes in the market circumstances, legislation, business environment;

8.2.2. The Company's inability to timely respond to external events;

8.2.3. Unreasoned and ill-considered decisions on the directions of future development;

8.2.4. A failure to implement the decisions and plans adopted.

8.3. The Company carefully monitors political, social and external events in order to timely respond to changes in the external environment and has implemented and maintains high security standards for protection from crisis situations and external threats.

8.4. The Company has implemented a strategic planning process designed to maintain a proper balance between the long-term objectives and the risks that the Company is willing to take in order to minimise the negative impact of the possible risks on the Company's operation and financial stability. As part of strategic planning, the following approaches are used to minimise strategic and business risk:

8.4.1. The strategy is based on the business environment and market circumstances;

8.4.2. An analysis of strengths, weaknesses, opportunities and threats (SWOT) is conducted, on which basis there are strategic objectives and operational priorities set out to ensure an effective utilisation of the Company's capabilities;

8.4.3. An analysis of development scenarios is conducted, including an assessment of exposure to external circumstances;

8.4.4. Action plans for unforeseen events and changes are drawn up;

8.4.5. The Company's market positions are monitored, as are the strategic objectives, operational plans and financial figures.

9. Operational risk management

9.1. The purpose of operational risk management is to keep the level of operational risk as low as possible whilst maintaining an effective and economically sound internal control system for risk level reduction.

9.2. The following sources of operational risk are subject to appropriate control measures:

9.2.1. Personnel risk – employee mistakes, negligence, incompetence, insufficient number of employees, lack of experience, etc.;

9.2.2. Process risk – regulatory non-compliance of internal processes, ineffective course of processes, lack of regulatory documents, organisational faults, inappropriate division of duties, responsibilities or powers, poor circulation of information, lack of control, etc.;

9.2.3. Information technology and system risk – insufficient IT functionality, information system malfunctions, issues with data availability, integrity and confidentiality, disruptions, lack of automated controls and reports, etc.

9.3. In order to limit operational risk, the Company has divided responsibilities, duties and powers, introduced control measures, and developed internal regulatory enactments governing processes, the decisions adopted are documented, and there is a reporting and performance monitoring process in place.

9.4. Since operational risk may materialise in any line of activity, process, system and service of the Company, all employees of the Company are responsible for its identification and elimination in their day-to-day work.

9.5. It is an obligation of every employee of the Company to immediately report operational risk events or incidents and control system faults found to the Risk manager in order for the necessary risk mitigation and control improvement measures to be timely taken. The reports submitted by employees are registered in the risk database as confidential and only used for the purposes of risk management.

10. Financial risk management

10.1. The purpose of financial risk management is to set up a finance planning and management system that allows for a timely identification of any threat that may adversely affect the Company's profitability and ability to settle its liabilities.

10.2. The risks deemed as major financial risks by the Company are credit risk (incl. concentration risk), market risk (incl. price risk, interest rate risk and currency risk), and liquidity risk.

10.3. The purpose of credit risk management is to ensure an effective and quality limitation of customer and counterparty risk in order to protect the Company from financial losses that may be incurred due to a deterioration of a customer's or counterparty's creditworthiness that makes them uncapable or unwilling to timely settle accounts.

10.4. In order to limit credit risk, the Company assesses the creditworthiness and reputation of business clients, regularly monitors debtors, and sets customer and transaction limits.

10.5. In order to limit concentration risk, particular attention is paid to the financial standing and reputation of the Company's key customers.

10.6. The purpose of market risk management is to establish a system that allows for a timely response to external events that result in changes in market prices, foreign currency rates, interest rates and share prices and may adversely affect the Company's revenue and value.

10.7. In order to limit market risk, the Company regularly keeps track of the market circumstances and prices, currency rate and interest rate fluctuations, and takes risk limitation measures, including closing of financial instrument transactions. The principles of market risk limitation are detailed in the Market risk limitation policy.

10.8. The purpose of liquidity risk management is to establish a system that allows for planning and foreseeing the necessary liquidity level, maintaining an optimum balance between yield and cost and reducing the probability of the Company not being able to timely settle its liabilities.

10.9. In order to limit liquidity risk, the Company assesses the maturity structure of assets, liabilities and off-balance sheet items, keeps the outgoing and incoming cash flow under control, and sets and controls transaction limits.

11. Compliance risk management

11.1. The purpose of compliance risk management, including that of money laundering and terrorism financing risk and fraud risk, is to prevent the possibility of the Company's operation being non-compliant with the regulatory requirements, such as laws, regulations, standards, which may result in threat to the Company's future operation and reputation and in a legal obligation or punitive sanctions.

11.2. The following sources of compliance risk are subject to appropriate control measures:

11.2.1. Fraud risk – internal fraud, theft, deliberate violation of regulatory enactments, data and document forgery, confidential information leaking, corruption, etc.;

11.2.2. Personnel risk – dishonest or unethical conduct, dependency on key people.

11.3. The following approaches are used for compliance risk management:

11.3.1. Regular monitoring of regulatory enactments, changes and amendments, fulfilling the relevant requirements in the Company's operation and updating the internal regulatory enactments as appropriate;

11.3.2. Coordination of cooperation agreements and regular performance monitoring;

11.3.3. Timely preparation and submission of summaries and reports, fulfilment of requests from supervisory authorities and other external institutions;

11.3.4. Updating of the Company's internal regulatory enactments and assessment of the actual compliance, monitoring of performance of Board resolutions and orders, elimination of faults found during internal and external inspections;

11.3.5. Whistleblowing system – reporting of violations that extend beyond infringements of personal interests and concern the Company and the interests of its employees or general public;

11.3.6. Situations of conflict of interests are timely identified and eliminated;
11.3.7. Tax risks are managed pursuant to the principles described in the Tax risk management guide.

12. Reputational risk management

12.1. The purpose of reputational risk management is to reduce the probability of the Company's customers, counterparties, shareholders, supervisory authorities and other stakeholders developing a negative impression of the Company which might adversely affect the ability to maintain existing or build new business relationships with customers, counterparties and other persons.

12.2. Reputational risk is closely linked (interacts) with other risks. The level of reputational risk may increase as a result of materialised operational or compliance risk, and increased reputational risk may, in turn, increase the level of strategic risk, with an adverse effect on profitability and further development.

12.3. The following approaches are used for reputational risk management:

12.3.1. Information monitoring in mass media – a regular monitoring of information in mass media regarding events in the business environment and market circumstances that might affect the Company's reputation, including monitoring of information on the major customers and counterparties;

12.3.2. Review of customer and counterparty complaints – a register of customer complaints has been set up and allows for a timely identification of problem situations and prevention of harm to the Company's reputation;

12.3.3. There have been rules of procedure and a code of conduct drawn up that lay down the principles, provisions and standards of professional conduct and ethics to ensure that the employees of the Company carry out their duties in good faith, be unbiased in the performance of professional duties and decision-making, abide by laws, regulations and standards, respect and keep the confidentiality of customer and transaction information and business secret, and their conduct and behaviour be held up to high ethical standards;

12.3.4. Analysis of reputational risk and possibilities of its materialisation – when developing procedures and action plans for managing crisis situations, the possible events that may entail increased reputational risk are identified, the causes and possible consequences of such events are identified, and the actions to be taken to protect the Company's reputation in a crisis situation are set out.

13. Supervision and updating of the Policy

13.1. The Board of the Company supervises the implementation and performance of the Policy at the Company.

13.2. Once per year, when reporting on major risks to the Risk management committee, the Risk manager of the Company delivers proposals as to the necessary amendments to the Policy and the internal regulatory enactments related to it.

13.3. The Risk management committee reviews the Risk manager's proposals and, if necessary, puts amendments to the Policy up for review at the Board. Amendments to the Policy are approved by the Council.

13.4. At least once per three years, the internal audit of the Company conducts an independent inspection of the implementation and performance of the Policy and the compliance of the internal processes with the Policy requirements.

13.5. At least once per six years, the Company conducts an external independent assessment of the compliance of the Policy with the best practice and the external requirements.

14. Appendix

14.1. Appendix No. 1 – Risk identification tool

***

APPENDIX NO. 1

Risk assessment scale and explanations

Risk rating	PROBABILITY of risk occurrence		
	Likelihood	Probability	Explanation
5	Almost certainly	90-100%	The risk is likely to occur several times a year.
4	Very likely	66-90%	The risk is likely to occur within the next 12 months.
3	Possibly	33-66%	The risk is likely to occur within the next 12-24 months.
2	Rarely	10-33%	It is possible that the risk will occur in the next 2-3 years.
1	Very rare	0-10%	The risk is unlikely to occur within the next 3 years.

Control effectiveness	Control effectiveness	
	Explanation	
5	Very effective control	Reduces 81-100% of risk
4	Effective control	Reduces 61-80% of risk
3	Adequate control	Reduces 50-60% of risk
2	Partial control	Reduces 21-49% of risk
1	Insufficient control	Reduces 0-20% of risk

IMPACT of risk				
Risk rating	Impact	Impact on goals / plans / processes	Impact on finances / assets / values	Impact on reputation / customers / employees
5	Critical	Significant problems that threaten the achievement of goals and plans. It can have a long-term negative impact on operations.	Possible financial losses may exceed EUR 3 million. Significant damage to material assets/values is possible.	Widespread long-term negative publicity in the mass media, negative impact on a large number of customers/cooperation partners/employees.
4	High	Serious problems, but with a temporary impact on the fulfillment of goals and plans, the progress of processes	Possible financial losses are from 100 thousand to 3 million EUR. Significant damage to tangible assets/values is possible.	Negative news in the mass media. Problems negatively affect some customers/cooperation partners/employees.
3	Medium	Small problems that can negatively affect the execution of plans and the progress of processes	Possible financial losses that do not exceed 100 thousand EUR. Minor damage to tangible assets/values is possible.	Temporary publicity in the mass media is possible. Problems may negatively affect individual customers/partners/employees.
2	Low	Individual problems that can be quickly eliminated, which do not hinder the achievement of goals and do not affect the course of processes	Possible financial losses that do not exceed 10 thousand EUR. Minor damage to tangible assets/values possible.	No impact on reputation and customers. Possible impact on individual employees.
1	Very low	Individual problems that can be quickly eliminated, which do not hinder the achievement of goals and do not affect the course of processes	No anticipated financial loss or damage to assets.	No impact on reputation, customers and employees.

SOURCES of risk origin	
Source of risk	Explanation
Employees	Internal fraud or malfeasance
	Lack of knowledge and skills
	Insufficient number of employees
	Dependence on key employees
	Errors made by employees
	Health and safety at work
Processes	Process errors
	Insufficient or inadequate controls
	Lack of procedures, rules and instructions
	Inappropriate division of duties and responsibilities
	Late or faulty management decisions
Systems	Deficiencies or interruptions in information systems
	Insufficient or incorrect data
	Data protection and confidentiality issues
	Systems design errors
	Insufficient or inadequate IT support
External conditions	External fraud, theft, malfeasance
	Problems of customers and cooperation partners
	Legislation, standards, market conditions, etc. changes
	Crisis situations, natural disasters, pandemic

Risk level	Residual risk	Initial risk	Responding to risk
	Residual risk / Controls	Probability * Impact	
Critical	15.0 - 25.0	20.0 - 25.0	The risk is not acceptable
High	6.1 - 14.9	13.0 - 19.0	Mostly not acceptable
Average	3.0 - 6.0	7.0 - 12.0	Mostly acceptable
Low	1.1 - 2.9	4.0 - 6.0	The risk is acceptable
Very low	0.2 -1.0	1.0 - 3.0	The risk is acceptable