

APPROVED BY
Resolution No. 9-26 of the Board of Joint
Stock Company Lietuvos Paštas of 5
September 2025

RISK MANAGEMENT POLICY

Version 4

Effective from 05-09-2025

Policy owner: Business and Technology Development Division

Objective:	To establish a risk management strategy and principles to implement the strategic objectives of the Group of Companies of Joint Stock Company Lietuvos Paštas, ensure uninterrupted operations and quality of services, compliance with legal acts, maintain a good reputation and meet the needs of stakeholders.
Scope of application:	The Group of Companies of Joint Stock Company Lietuvos Paštas.

CONTENT

1.	GENERAL PROVISIONS	3
2.	REGULATORY SCOPE	3
3.	TERMS AND ABBREVIATIONS	3
4.	BASIC PRINCIPLES AND COMMITMENTS.....	4
5.	RISK CLASSIFICATION	4
6.	RISK APPETITE	7
7.	RISK MANAGEMENT PROCESS	7
8.	RESPONSIBILITY, ACCOUNTABILITY AND CONTROL	10
9.	SUPERVISION AND CONTROL OF POLICY IMPLEMENTATION	13

DOCUMENT HISTORY

Date of signing	Version	Essential description of document change	Document owner	Document developer
17-12-2020	1	Risk management policy is being approved.	Strategy and development department	Risk analyst
18-08-2021	2	The policy is being changed because the concepts have been clarified, risk categories have been detailed, risk appetite has been determined for each risk category, a risk matrix, risk probability and impact assessment scales have been included, and the risk management process and its stages and responsibilities have been clarified.	Business and Technology Development Division	Risk manager
27-09-2023	3	The policy is being changed regarding the updated document format and the requirements of the Bank of Lithuania, the concepts have been clarified, the principles and risk categories have been supplemented, the 3-line model has been updated, and responsibilities have been clarified.	Business and Technology Development Division	Risk manager
05-09-2025	4	Policy changes: revised concepts; revised and updated principles, changed names of risk levels and impact levels, changed risk probability assessment scale, updated risk impact descriptions, revised responsibilities.	Business and Technology Development Division	Risk manager

1. GENERAL PROVISIONS

1.1. The risk management policy of the Group of Companies of Joint Stock Company Lietuvos Paštas (hereinafter - the Policy) establishes the risk management strategy, main principles and responsibilities of the Group of Companies of Joint Stock Company Lietuvos Paštas (hereinafter – Group of companies), to ensure a unified risk management process that helps to identify potential risks in a timely manner and make risk-based decisions that reduce the negative impact on operations.

2. REGULATORY SCOPE

2.1. The policy has been prepared under the requirements set out in the ISO 31000:2018 standard "Risk Management Guidelines" and the description of the requirements for the management system and protection of received funds of electronic money institutions and payment institutions, approved by the Board of the Bank of Lithuania in its version No. 03-33 as of March 6, 2025.

3. TERMS AND ABBREVIATIONS

3.1. The following terms and abbreviations are used in this Policy:

Company	Joint Stock Company "Lietuvos paštas".
Group of companies	The Joint Stock Company Lietuvos Paštas and its subsidiaries (including subsidiaries registered and operating abroad).
Risk	The impact of uncertainty on the achievement of the objectives of the Company's group of companies, which may be positive and/or negative. Risk can affect various objectives – financial, safety, business continuity, legal and other objectives, set at different levels: strategic, organizational, project, product or process.
Risk appetite	The scope of risk that the Company's shareholder expressing his will through a board decision, allows us to be assumed to achieve strategic goals.
Risk matrix	A visual tool used during risk assessment to determine the level of risk significance, regarding the probability and impact values of the risk occurrence.
Risk owner	The head of a structural division or other employee responsible for managing the risks falling within his area of responsibility and having the authority to manage these risks.
Risk management	In light of the risk, actions have been coordinated to direct and control the activities of the Company's group of companies. The basis of management is the analysis of risk factors, response planning and implementation, and information dissemination.
Risk management committee	A committee established by order of the Company's director general, which makes risk management decisions, performs risk management supervision and control functions.
Description of risk management procedures	A document detailing the implementation of the risk management strategy and principles set out in this Policy defining the risk management process, participants and responsibilities.
Risk register	A document that records records of relevant risks, risk analysis and assessment results, risk management measures and the results of monitoring their implementation.

Risk manager	An employee responsible for risk management coordination (collection of risk management information from risk owners, updating the risk register, organizing risk management decision-making, preparing reports), control (monitoring the implementation of risk management plans) and improvement of the risk management process (formation of risk management practices, consulting employees, organizing training, continuous review and updating of the process).
Stakeholders	Individuals or organizations that can influence, be or feel influenced by a decision or activity (customers, the public, employees, trade unions, partners, creditors, shareholders, investors, opinion leaders, media, etc.).

4. BASIC PRINCIPLES AND COMMITMENTS

4.1. Basic principles of risk management:

4.2. **Creating and preserving value** - risk management helps to implement the strategic goals of the Company's group of companies, increase operational efficiency, prepare for unexpected events and reduce their likelihood and/or impact.

4.3. **Integrity** – risk management is an integral part of all processes and decision-making within the Company's group of companies. It is integrated into daily operations, strategic and operational planning, and change management. Risk management is part of every employee's responsibility and contributes to the formation of culture.

4.4. **Relevance and reliability of information** – risk management is based on reliable data, observation, experience and expert assessment. Risk management properly and in a timely manner anticipates, discloses, confirms and responds to changes in risk. Risk management activities are properly documented and maintained.

4.5. **Involvement** – management bodies, managers and employees are involved in risk management, and they are provided with timely and appropriate information about risks, thus strengthening the awareness of the importance of risk management, responsibility and quality of decisions.

4.6. **Transparency** – risk management information is provided to the Company's audit and risk management committee and the Board at established intervals, and if necessary, to other interested parties. This helps to justify decisions made and strengthens trust in the Company's group of companies.

4.7. **Continuous improvement** – the risk management process is continuously improved based on experience gained, changes in the external and internal environment, and consistent risk monitoring, to ensure effectiveness and adaptability to changing conditions.

4.8. The risk management principles are applied in the management of the Company's group of companies, in daily operations, decision-making and in the management of all types of risks. They contribute to the formation and improvement of the culture of the Company's group of companies.

5. RISK CLASSIFICATION

5.1. Risk categories based on the causality:

5.1.1. **Strategic/business risk** – the risk arising from the establishment and implementation of a strategy that is insufficiently defined, based on incomplete or inaccurate data, or related to changes in the operating environment (for instance, political, economic, social, technological, legal) and the organization's ability to prepare for or take advantage of them. Timely identification and proper management of these risks is of particular importance for the implementation of the goals set out in the strategic planning documents of the Company's group of companies. To achieve success and sustainable development, the implementation of strategic goals and the management of the most significant risks are presented and monitored by the board.

5.1.2. **Financial risk** – the risk arising from the management of financial assets and financial liabilities resulting in low investment returns, failure to properly manage assets/liabilities or failure to obtain the highest economic value from the resources used, and financial reporting that does not meet the requirements.

The main financial risks that may have a significant impact on the activities and financial results of the Company's group of companies:

Settlement risk – the probability of incurring losses due to a customer not paying on time or failing to fulfill their contractual financial obligations. Overdue customer payments are managed in accordance with the procedures for managing receivables from customers and using external providers of pre-trial and judicial debt collection services.

Liquidity risk – the risk that the Company's group of companies will not have sufficient funds to meet its financial obligations on time in the current period. Long-term and short-term forecasts of direct cash flows are prepared indicating the need for funds and expected sources of financing. Short-term and long-term financing needs are determined by assessing the planned scope of activities, funds required for investments in long-term assets, and the likely risks associated with them. When forecasting cash flows, the potential need for borrowed funds is assessed, the maturity of agreements with credit institutions is monitored, the probability of defaulting on obligations to credit institutions and the possible consequences thereof are assessed. The company provides financial services based on an electronic money institution license; therefore, all third-party funds are protected under the applicable procedure for the protection of funds of payment service users.

Market risk – the risk that the Company's group of companies will suffer losses due to fluctuations in market variables. The most relevant market risks are exchange rates and interest rates. Currency risk – the risk of incurring losses due to adverse changes in exchange rates. The main transaction currency in the activities of the company's group of companies is euros - when concluding any transactions, the aim must be to ensure that settlements are made in euros. Risk is managed by trying to ensure that as much of the Company's group costs as possible (to the extent economically reasonable) are incurred in the same currency in which revenue is generated. Interest rate risk is the risk that the interest rate on loans and credits of the Research Company's group of companies will change unfavorably. In cases where specific investment projects or activities are financed, for the payback of which even a small increase in the financing interest rate may be of critical importance to the Company's group of companies, a fixed interest rate is chosen, if possible. Given the upward trend in EURIBOR, the possibility of reducing the balance of indebtedness to credit institutions is being assessed. The use of excess account balance is constantly effectively managed by controlling and forecasting payments to suppliers.

Customer funds protection risk – the risk that the Company will not be able to properly protect customer funds, which may result in their loss. This risk is managed using the mechanism of holding customer funds in deposit accounts, insurance, guarantees or surety bonds established by law. The concentration risk of customer funds to be held is managed by holding customer funds in credit institutions with a high credit rating.

Counterparty credit risk is not relevant because the Company's group of companies does not provide credit on its own behalf but acts as a consumer credit intermediary and the counterparty credit risk is assessed by the consumer credit provider (creditor).

5.1.3. **Operational risk** – risk arising from internal environmental factors: insufficient, improperly defined or ineffective (not result-oriented) internal processes, insufficient internal control, which may lead to fraud, errors, deterioration of customer service quality (quality and/or quantity of services suffer), failure to ensure compliance and/or low economic benefits. Operational risk may also arise from external environmental factors: natural disasters, cyberattacks, etc.

Operational risk may have a significant impact on the activities of the Company's group of companies. When performing an impact analysis on operations, the risks inherent in significant activities, services and products provided, processes and information systems, and ensuring their continuity are assessed. The main sources of this risk are analyzed: the adequacy of established

processes and procedures, the functioning of information systems, the influence of the human factor (illegal actions of employees, errors, illegal actions of other persons). Operational risk is managed by ensuring a properly functioning internal control system, which includes the implementation of ethical standards, the implementation of corruption prevention measures, the identification and management of conflicts of interest, and the security of information and information systems. The functions of employees are clearly separated, rights, duties and responsibilities are established, the activities of structural units are controlled, and a management information system is established.

To ensure an optimal balance between operational needs and the establishment of information security requirements and the implementation of measures, the Information Security Policy and Personal Data Processing Rules have been approved. On their basis, an information security management system is being developed and implemented within the Company's group of companies, which includes continuous risk assessment and management in areas that have an impact on information security – cybersecurity and personal data protection – as well as in processes and resources related to the areas (technology, employees, customers, third parties, etc.). Information system control and security measures are assessed at set intervals, and system recovery plans are tested and updated.

Given the requirements imposed on financial market participants regarding the financial services provided by the Company, the Outsourcing Policy establishes the main principles and responsibilities aimed at ensuring the management of risks related to the outsourcing of operational functions. Among others, operational concentration risk is assessed, i.e. the potential impact of the transfer of operational functions to the same area, dependence on the same service providers, etc.

5.1.4. Compliance risk – risk related to the regulatory and legal environment and its changes, arising from insufficient measures to comply with a legal or regulatory requirement, which results in legal liability and sanctions, and a negative impact on the reputation of the Company's group of companies. Internal control procedures to manage this risk are provided for in the Compliance policy and internal documents detailing its provisions. The Company's group of companies determines priority areas of compliance based on an assessment of the most significant compliance risks. The planning of risk management measures in these areas is based on both the established risk materiality level and the compliance risk appetite, ensuring appropriate risk management in priority areas.

Compliance risk management regarding the financial services provided by the Company is subject to the requirements of the Anti-Money Laundering and Terrorist Financing (hereinafter – AML/CFT) implementation legislation. Money laundering and terrorist financing risk (hereinafter - the ML/TF risk) – the risk that the Company's activities related to the provision of financial services, including its internal documents and the operational processes established by them, will not comply with the requirements of legal acts regulating the field of AML/CFT. The main provisions regarding the management and control of this type of risk significant to the Company are regulated in the Anti-Money Laundering and Terrorist Financing Prevention Policy, based on which the Company's internal documents elaborate on the ML/TF requirements, including the AML/CFT risk management process, responsible persons, and internal control and monitoring procedures.

5.1.5. Reputational risk – risk arising from decisions made or situations that arise and their management, including violations of ethics, data protection, lack of sustainability, systematic or recurring failures, insufficient quality of services or lack of innovation, which damage the reputation and image, relationships and/or destroy trust in the Company's group of companies.

Reputational risk includes the risk of customer behavior that determines the likelihood of losses and arises from conflicts of interest, improper handling of customer complaints (due to likely violations of personal rights or legitimate interests related to services provided by the Company's group of companies and contracts concluded), and data security violations. This risk is relevant because damage to the reputation of the Company's group of companies may result in loss of trust, significant financial impact, and loss of customers. The system of measures for creating a corruption-resistant environment, managing corruption risks, and balancing public and private interests of the Company's group of companies is formed and implemented based on the principles established in

the Anti-Corruption Policy. Sustainable business culture and practices are created and developed based on the Sustainability Policy, which defines priority areas of sustainable development in the areas of environmental protection, social responsibility and good governance, and also provides measures to ensure their implementation.

6. RISK APPETITE

6.1. The risk appetite is determined and reviewed annually by the Company's Board.

6.2. Risk appetite is determined for each risk category regarding the culture of the Company's group of companies, areas of activity, the nature of the goals pursued, financial capacity, and competitive environment.

6.3. The scale used to determine risk appetite¹:

	5 Open 20-25	4 Flexible 15-16	3 Cautious 8-12	2 Minimalist 4-6	1 Averse 1-3
General description	Innovative approach, choosing solutions with higher risks to achieve greater potential benefits	All possible solutions are evaluated, and the most likely beneficial one is chosen, given the acceptable risk	Safe solutions are preferred, which have a low level of risk and may have limited potential for benefit	Only extremely safe, low-risk solutions are chosen, even if the expected benefits are minimal	Risk-averse, uncertainty-averse
Philosophy	Reasonable risk is taken	Extremely reasonable risk is taken	Preference for safe options	Extremely conservative approach to risk-taking	The main goal is risk avoidance.
Tolerance for uncertainty	Quite likely	Likely	Limited	Low	Extremely low
Approach to choosing solutions	A solution with the highest possible benefit is chosen, assuming the probability of failure	A beneficial solution is chosen if the impact of the risk can be managed	A decision is made only if the risk is limited and the benefit is significantly greater	A decision is made only when necessary and the probability of failure is low	Decisions with the lowest risk are always preferred, even if the potential benefits are lower
Compromise to achieve other goals	Risks are accepted to achieve other important goals	Risk is accepted if a level of control is ensured and the benefits are clear	Risk avoidance is sought, may be tolerated in exceptional cases	Risk is accepted only if there are no other alternatives, to a minimal extent	Risks are never taken, even if they interfere with achieving other goals

6.4. Employees must ensure that decisions made do not result in risks greater than the established risk appetite.

7. RISK MANAGEMENT PROCESS

7.1. Risk is a natural part of everyday life. The Company's group of companies cannot avoid risk, but actively, using available means, seeks to analyze and assess the circumstances that may lead to the occurrence of risk, and to manage the probability and/or impact of the occurrence.

7.2. Stages of the risk management process:

¹ The risk appetite level estimates indicated in the risk appetite scale correspond in terms of points to the risk significance scores indicated in the risk matrix, which are equal to the product of the risk probability and maximum impact estimates.

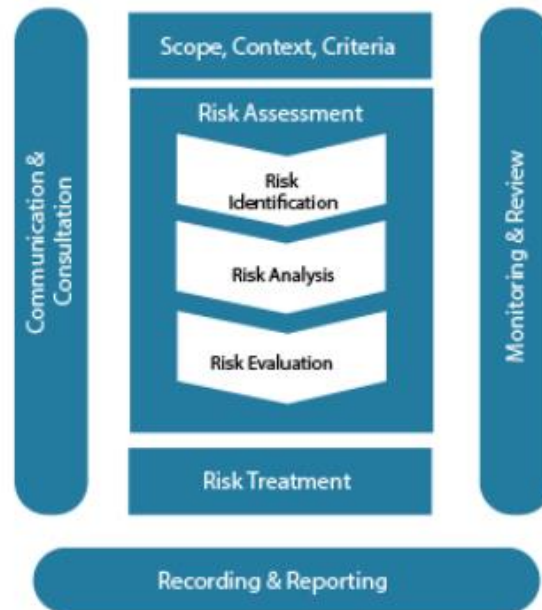


Fig. 1 Risk management process

7.2.1. Determining the scope, context and criteria: defining the scope of risk management activities (at what level, in what scope of activities are risks identified); determining the factors of the internal and external environment, in which the activity is carried out; determining the criteria, under which risks will be assessed.

7.2.2. Risk assessment: risks are regularly identified, analyzed and assessed.

7.2.2.1. Risks are identified in all areas of activity during systemic risk reviews, change management and operational incident investigations. Risks are registered and information is documented in risk registers.

7.2.2.2. During risk analysis, the risk significance level is determined (the product of the risk probability and the maximum impact estimates). The analysis considers the effectiveness of risk management measures already in place, i.e. the residual risk is assessed at the time of assessment.

7.2.2.3. Risk probability assessment scale, assessing how often a risk may occur:

PROBABILITY		
5	Very high	More than 1 time per year
4	High	1 time per year
3	Average	1 time in 1-3 years
2	Low	1 time in 3-5 years
1	Very low	Less than every 5 years

7.2.2.4. Risk impact assessment scale:

IMPACT					
		HEALTH AND SAFETY	FINANCIAL CONDITION	BUSINESS CONTINUITY	REPUTATION
1	Insignificant	Health impairment that prevents the employee from continuing to work the next day;	The expected impact is less than EUR 250,000	A minor disruption in one of the processes is quickly restored. There is no impact on customers.	The events are not expected to attract media or social media attention.

		affects no more than 1 person.			
2	Low	Health impairment that requires outpatient treatment for an employee; or health impairment for 2-5 people that allows employees to continue working the next day.	The expected impact is greater than 250001 but less than 500000 EUR	A disruption in one of the processes is recovered without significant consequences for other processes. Slight functionality limitation for customers.	Individual events or topics attract regional (city and district) media or small-audience social media groups.
3	Average	Health impairment resulting in hospitalization of an employee; or health impairment of 5-10 people as specified in descriptions 1-2.	The expected impact is greater than 500001 but less than 1 million euros.	Recovering from a disruption in several processes. Significant disruption of functionality for customers, restored within the terms specified in the contracts.	Individual events or topics attract the attention of national media or are "raised" by opinion leaders through national media or social networks.
4	High	Health impairment that results in hospitalization of the employee and requires long-term rehabilitation; or health impairment specified in descriptions 1-3 for 10-50 people.	The expected impact is greater than 1,000,001 but less than 2,500,000 EUR.	A disruption of operations that significantly affects many processes but does not interrupt the Company's core operations. Significant disruption of functionality for customers, restored after exceeding the terms specified in the contracts.	Negative public opinion or critical assessment attracts the attention of all types of media.
5	Critical	A health disorder where the employee can no longer continue working; or a health disorder specified in descriptions 1-4 affecting more than 50 people; or there are fatalities.	The expected impact is greater than 2,500,001 EUR.	At least one of the Company's main activities is interrupted; there is no possibility of serving customers.	Continued negative assessment of the Company's group of companies, affecting the continuity of operations and attracting the attention of national and international media.

7.2.2.5. Each identified risk is assessed according to a risk matrix:

Impact	Critical	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Average	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Insignificant	1	1	2	3	4	5
			1	2	3	4	5
			Very low	Low	Average	High	Very high
			Probability				

Critical	urgent actions
High	necessary actions
Average	possible actions
Low	monitor
Insignificant	no actions

7.2.3. Risk management: a risk management decision is made (regarding the significance of the risk and whether the risk does not exceed the established risk appetite. If necessary, a decision may be made to reduce risk and for risks that do not exceed the risk appetite; a risk management plan is prepared; after the measures provided for in the plan are implemented, an assessment of the effectiveness of the plan is carried out;

7.2.4. **Monitoring and review:** continuous monitoring and regular review of the implementation of risk management processes, identified risks, their assessment and management plans are carried out;

7.2.5. **Communication and consultation:** there is ongoing regular two-way information sharing with process participants and stakeholders throughout the process;

7.2.6. **Recording and reporting:** assessing stakeholder needs; preparing and submitting quarterly, semi-annual and annual reports.

7.3. The risk management process applies to all types of risk management, which is regulated in detailed internal documents and integrated into routine business processes and daily management.

7.4. Effective risk management is based on fostering a risk management culture, which is based on constantly updated information available to employees about the risks inherent in the activity and their management experience.

7.5. The aim is to maintain and develop the risk management qualifications of employees through periodic training.

8. RESPONSIBILITY, ACCOUNTABILITY AND CONTROL

8.1. Risk management is based on the Three Lines Model, which has created a system of responsibilities that helps strengthen the Company's group of companies management and risk management:

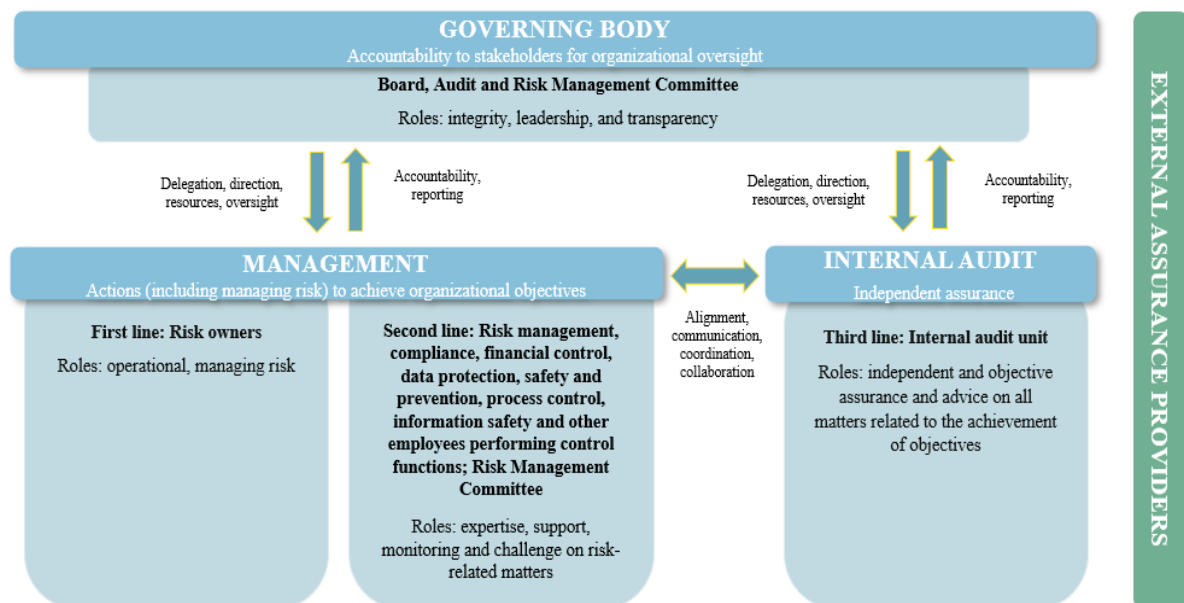


Fig. 2. Three Lines Model

8.2. Responsibilities of participants in the risk management process:

Process		I line	II line			III line	General Director	Heads of subsidiaries	Audit and Risk Management Committee	Board
		Risk owner	Employees performing control functions	Risk manager	Risk management committee	Internal audit department				
Scope, context and criteria	Risk management policy			Prepares, reviews, updates	Considers, makes suggestions	Conducts an independent assessment of the effectiveness and efficiency of the risk management system and individual measures	Ensures implementation in the Company's activities	Ensures implementation in the activities of the Subsidiary	Considers, makes suggestions	Approves
	Risk management system			Develops, improves and coordinates implementation	Makes risk management decisions, performs risk management supervision and control functions, assesses the effectiveness of the risk management system, and makes proposals for changes and improvements		Responsible for operations within the Company	Responsible for operations at the Subsidiary	Provides opinions, comments, suggestions for change and improvement	Provides suggestions for change and improvement
	Risk appetite			Prepares	Considers, makes suggestions				Considers, makes suggestions	Approves
	Description of risk management procedures		Prepares, reviews, and updates documents that implement the provisions published in the Policy	Prepares, reviews, updates	Considers, makes suggestions		Approves		Familiarizes with internal documents regulating risk management and provides recommendations	

15 (19)

	Risk management culture	Contributes to the formation of a risk management culture	Contributes to the formation of a risk management culture, consults, and organizes training for risk owners	Contributes to the formation of a risk management culture, consults, and organizes training for risk owners	Contributes to the formation of a risk management culture		Forms a risk management culture, encourages employees to manage risks and communicate about them openly and honestly within the Company	Forms a risk management culture, encourages employees to manage risks and communicate about them openly and honestly within the Subsidiary	Provides opinions, comments, suggestions for change and improvement	Sets expectations for risk management culture
--	--------------------------------	---	---	---	---	--	---	--	---	---

8.3. Employees are encouraged to participate in risk management activities by providing information about identified risks to the management.

9. SUPERVISION AND CONTROL OF POLICY IMPLEMENTATION

9.1. The implementation of the policy provisions is detailed in documents prepared by the Company's divisions within the limits of their competence.

9.2. The Business and Technology Development Division is responsible for the preparation and timely updating of the Policy.

9.3. The policy is approved by the Company's Board.

9.4. The policy is reviewed at least every two years and updated if necessary

9.5. The policy applies to the entire Company's group of companies.

9.6. This Policy is public and published on the Company's website.

9.7. The heads of departments whose employees must follow this Policy in their activities are responsible for familiarizing their subordinate employees with this Policy.
