CORPORATE RISK MANAGEMENT POLICY

ALLOS

Approval date: 09/27/2023	Responsible body: Board of Directors
Version: 01	Responsible for Policy: Compliance
Classification: Corporate Governance Policy	Review: 5 years

The company strives for integrity, ethics, and transparency in business, basing its activities and business decisions on the highest standards of conduct, aligned with international guidelines and best practices.

1. Objective

This Corporate Risk Management Policy, which was prepared in line with COSO ERM and ISO 31,000, having observed the guidelines outlined in CVM Instruction 522/2014, CVM Instruction 586/2017, the Brazilian Code of Corporate Governance, the Novo Mercado Regulation, and the Three Lines Model of the IIA/ 2020, establishes the principles, guidelines, methodology, and process for identifying, analyzing, and handling risk. It also defines the responsibilities of the governance agents that are part of the company's corporate Risk Management process. The policy is, therefore, an instrument that facilitates the dissemination of the corporate Risk Management culture by the company, as it seeks to establish a common language on the subject.

2 Scope

Applicable to all employees, third parties, and companies directly and indirectly controlled by the company, except malls managed where the company has no participation.

3 Definitions

Mitigating Action – Actions and controls adopted by the company to minimize or eliminate exposure to corporate risk and reduce the probability and/or impact of such materialization.

Risk Appetite – The level of risk a company is willing to accept in the pursuit and realization of its strategy, expressed in the Impact x Probability gauge.

Internal Audit – Independent and objective evaluation of processes and internal control environment. It helps the organization to achieve its objectives, from the application of a systematic approach to evaluate and improve the effectiveness of Risk Management processes and internal controls.

Risk Category – Events that, having materialized, may affect the achievement of the company's objectives, survival, sustainability, longevity, and profitability, reducing or destroying its respective value.

Staff – Employees, administrators, superintendents, shopping center managers, and representatives of the company.

COSO - Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework.

Compliance - Compliance with laws, laws, contracts and standards, procedures, guidelines, and internal policies that apply to the business.

Risk Dictionary – Tool used to classify Risk Categories by typology. e.g.: Strategic, Operations, Financial, Compliance, Technological, Climatic, Systemic, Environmental, and Image.

Risk Owner – Employee appointed by the company responsible for the treatment, monitoring, and reporting of the corporate risk they are responsible for. The Risk Owner represents the first line of governance for Risk Management.

Facilitator – Employee appointed by the Executive Director of the department related to risk, which aims to establish strategies to identify, analyze, evaluate, treat, monitor, and communicate potential events that may affect the objectives and results, in the face of the materialization of a risk/risk category.

Risk Factor – Individual and/or combined causes with the potential to contribute to the eventual materialization of a risk.

Risk Management – Process conducted by the Board of Directors, Audit and Risk Management Committee, Executive Board, Risk Management Department, and other business departments to identify, analyze, evaluate, treat, monitor, and communicate potential events or situations that may affect the achievement of the company's objectives and results.

Risk Impact – Consequences of the materialization of a risk, which can be expressed quantitatively / qualitatively.

Key Risk Indicator (KRI) – Metric used to verify and monitor exposure to corporate risk, based on analysis of the company's internal and external environments. It should, preferably, be related to the Risk Factor and should be measured promptly to identify changes in trends that may result in the materialization of a risk.

ISO 31,000 – An international standard that provides principles and directives related to Risk Management.

Risk Map – Graphical representation/plot of the criticality result of the identified Risk Categories represented by the Impact versus Risk Probability.

Risk Matrix – A risk management tool that evaluates the Inherent Risk, existing controls, and Residual Risks, to ensure the proper classification and prioritization of existing risks and review of existing risks.

The IIA's Three Lines model – The Institute of Internal Auditors' model, which helps organizations identify structures and processes that best assist in achieving the objectives and facilitate strong governance and risk management.

Action Plan – Measures adopted to reduce the probability and/or impact or the inherent risk and its consequent criticality. These measures may be adopted to avoid increasing the criticality of the risk, depending on the company's risk appetite.

Climate Transition Plan – The document responsible for the analysis of scenarios and impacts of potential climate change on the business and sector.

Risk Portfolio – The document that consolidates risks identified. For each risk, it presents Risk Factors, mitigating actions, the inherent and residual assessment of the respective Risk Factors, the person responsible for their treatment (owner(s)), response(s), action plan(s) and/or contingency plan(s)), and the respective KRIs.

Risk Probability – Qualitative and/or quantitative level that measures the chance of corporate risk materializing.

Impact x Probability gauge – Document that formalizes the description and criteria considered for each of the dimensions analyzed and the classification of the level of impact and probability of the identified corporate Risk Categories.

Risk Response – Definition of the treatment the company will attribute to the risk factor. In response, one can choose to avoid, reduce, share, or accept it.

Risk - Any event that may affect the company's ability to achieve its objectives.

Inherent Risk - Risk an organization is exposed to without any actions and/or controls that may reduce the probability of its occurrence or impact.

Residual Risk – Risk remaining after considering all existing actions and/or controls (and their effectiveness) to mitigate it.

Prioritized Risk – Risks selected by management (according to established criteria) to which treatment and/or monitoring strategies should be applied, monitored, and reported as a priority, promptly.

Risk Tolerance – Acceptable level of variation in the performance of an action and/or process aimed at achieving a certain objective.

4 Responsibilities

The Board of Directors is responsible for:

- Ensuring the appropriate structure and resources for the corporate Risk Management process;
- Supporting the promotion of the Risk Management culture;
- Approving the Corporate Risk Management Policy, as well as its future reviews;
- Approving the Corporate Risk Matrix and accompanying evaluation and periodic monitoring – supported by the Audit and Risk Management Committee; and
- Approving the degree of Risk Appetite and Tolerance acceptable, and the Impact x Probability gauge.

The Audit and Risk Management Committee is responsible for:

- Ensuring the authority, autonomy, independence, and responsibility of the Risk Management Department;

- Accompanying the periodic monitoring of the activities of the Risk Management Department and the results of the process;
- Evaluating and recommending for deliberation by the Board of Directors the guidelines of the corporate Risk Management process (methodology, processes, systems, policies, standards, and reporting mechanisms, among others) and ensuring the company's practices and good market practices are aligned;
- Evaluating and recommending for deliberation by the Board of Directors, the Corporate Risk Matrix, the Corporate Risk Management Policy, and the Impact x Probability gauge;
- Monitoring changes in the criticality assessment in the Corporate Risk Portfolio, reporting variations in Prioritized Risks and those that the Committee deems necessary to the Board of Directors;
- Receiving communication from the Board of Directors about possible new unidentified Risks, and, promptly, communicating this to the Risk Management Department; and
- Advising the Board of Directors on Corporate Risk Management performance and results.

The Executive Board is responsible for:

- Supporting and fostering the promotion of the Risk Management culture;
- Participating in deciding the degree of the company's Risk Appetite and Acceptable Risk Tolerance;
- Valuate and recommend for review by the Audit and Risk Management Committee the Corporate Risk Matrix, the Corporate Risk Management Policy and the Impact x Probability Ruler, for the purposes of deliberation by the Board of Directors;
- Defining the Owners of Corporate Risks;
- Approving Risk Responses (avoid, reduce, share, or accept);
- Evaluating the action plans suggested by the risk owners; and
- Informing the Risk Management Department about unidentified risks, whether new or not, promptly.

The Legal Executive Board is responsible for:

- Analyzing/validating the Corporate Risk Management Policy, as well as any reviews;
- Accompanying the periodic monitoring of the activities of the Risk Management Department and the results of the process;
- Informing the Risk Management Department whenever there are updates to strategic planning or the occurrence of material facts;
- Evaluating the adequacy of human, financial, and technological resources for corporate Risk Management;
- Supporting and fostering the dissemination of the Risk Management culture; and
- Receiving a report from the Risk Management Department for periodic evaluation of the Corporate Risk Matrix and established mitigation actions.

The Risk Management Department is responsible for:

- Fostering and disseminating Risk Management culture throughout the company, ensuring that all business departments have access to, and can consider, the objectives of Risk Management;
- Structuring and providing regular training to promote acculturation to all agents involved in the corporate Risk Management process;

- Developing, suggesting, and reviewing guidelines for the company's corporate Risk Management process (methodology, processes, systems, standards, and reporting mechanism, among others);
- Coordinating and monitoring the process of identification, evaluation, and classification of the company's risk with the company's governance agents and business departments;
- Developing and updating the Corporate Risk Management Policy;
- Preparing and executing the work plan, including budget, resources (human and technological), and deadlines, to enable the execution of the corporate Risk Management process in an efficient manner
- Annually reviewing the criteria defined in the Impact x Probability gauge and proposing alterations when significant changes occur;
- Providing methodological support for business departments to manage their own risks;
- Making suggestions to the Executive Board in defining the owners of the company's risks;
- Supporting and assisting the risk owners in the definition of the action and contingency plan, and the definition of KRIs and risk exposure levels;
- Receiving and consolidating the report on new corporate risks and any changes in criticality and reporting them to the Audit and Risk Management Committee and the Executive Board;
- Monitoring and consolidating the risks related to the company and/or its sector of operation, the status of the action plans and KRIs, sent by the risk owners, and issuing periodic reports to the Executive Board and the Audit and Risk Management Committee;
- Proposing updates to the Risk Portfolio and the criticality of the existing risks whenever there are updates in the strategic plan, also updating the company's risk appetite (when necessary);
- Developing the risk quantification and valuation methods;
- Providing methodological support for Risk Management in the supply chain; and
- Supporting internal and/or external audits to evaluate the Corporate Risk Management Policy.

The Risk Owners are responsible for:

- Promoting the culture of Corporate Risk Management;
- Indicating the professional to be the facilitator of its business department (if applicable), this person having technical knowledge about the corporate risk and being chiefly responsible for updating the information map, the effectiveness of the initiative, and the internal direction of the action plans
- Providing technical support regarding the risk factor, the action plan, risk, and criticality;
- Elaborating, suggesting, and implementing action and/or contingency plans for the mitigation of risks (involving the other business departments if necessary);
- Reviewing the technical details of the risk and its factors, the Risk Assessment and the risk response, promptly, considering changes arising from mitigating actions and/or existing controls related to the risk, and implementation of the action and contingency plans;
- Defining the KRIs, supported by the Risk Management Department, to monitor the variation and results of the corporate risks under their responsibility; and
- Making periodic reports to the Risk Management Department on the monitoring of the risk under their responsibility (possible change of Probability and/or Impact) and possible new risks identified.

The Internal Audit Department is responsible for:

- Preparing the annual internal audit plan based on the result of the risk assessment and processes/topics considered relevant; and

- Assessing the quality and effectiveness of the company's risk management, control, and governance processes.

Staff are responsible for:

- Informing the Risk Management Department if they identify any risk that may impact the values, objectives, decision-making and/or organizational structure of the company.

5 Guidelines

- Risk Management must be independent;
- Risk Management must be integrated and aligned with the company's culture and strategic planning, considering its values, objectives, decision making, business model, operation, and organizational structure;
- Risk Management must be dynamic and formalized through methodologies, standards, manuals and procedures, permeating the entire company and establishing internal and external partnerships to promote and maintain the corporate Risk Management environment;
- Risk Management must be continuous, and the Risk Map must be updated annually and/or in the event of internal or external events that affect the company's strategic objectives;
- All professionals involved in the company's Risk Management process must be trained in an appropriate and timely manner to fulfill their duties;
- The Board of Directors, the Audit and Risk Management Committee, and the Legal Executive Board shall promote corporate Risk Management and its guidelines to all the company’s hierarchical levels and assets, to ensure the application and execution of its procedures;
- The Risk Management Department reports to the Legal Executive Board, which will report the Risk Management process and structures, including the implementation and evolution of the Corporate Risk Management Policy, to the Audit and Risk Management Committee;
- The company has an independent Internal Audit Department, linked to the Board of Directors through the Audit and Risk Management Committee, with an adequate structure and budget to carry out its activities;
- Risk-based decision-making must be part of the company's management, to preserve and create value;
- Corporate risks must be identified, evaluated, treated, communicated, and monitored to mitigate the impacts on the strategies, fulfill their objectives, and comply with external regulatory demands. For such identification, external (economic, business, environmental, political, regulatory, social and technological) and internal (infrastructure, people, processes and technology) factors must be considered;
- The corporate risks identified should be investigated in-depth through analysis of their factors, the identification of mitigating actions, the evaluation of criticality (Impact x Probability gauge), the prioritization and establishment of treatment and monitoring strategies, and the definition of the respective Risk Owners and the deadline for implementation;
- The assessment of actual and potential risks must consider the possible negative impacts on sustainability;
- Risk Management must interface with the Internal Audit process, combining with efforts for the early identification of risks and conservative and timely management;

- The assessment of actual and potential risks must consider the possible negative impacts on sustainability, governance, climate, and environmental aspects;
- The definition of the responses attributed to the Risk Factors must consider the company's willingness to expose itself to the risks, considering their effects and cost-benefits, and prioritizing investment for the implementation of treatment strategies;
- Corporate Risk Owners must be elected according to the criteria established by the company. However, executive positions are recommended, since it requires articulation with different business departments for the implementation of treatment strategies and the meeting of deadlines;
- The structure and process of Corporate Risk Management must be customized and updated to remain adequate as the internal and/or external context of the company changes, ensuring the achievement of its objectives;
- The corporate Risk Management process must ensure the identification and mitigation of vulnerabilities and externalities of systemic risks (those arising from the large-scale weakening or collapse of natural or human systems on which society and the economy depend) in a systematic manner;
- The Corporate Risk Management Policy shall be evaluated independently and annually either by the Internal Audit Department, or an independent audit, as to its effectiveness, including, but not limited to, its operational and socio-environmental aspects; and
- The continuous improvement of the Risk Management process must be achieved through continuous monitoring, allowing adequate management of the risks and the improvement of the process through frequent evaluation and review cycles.

6 The Risk Management Process

6.1. Corporate Risk Management

The process of managing corporate risks begins with the identification of Risk Categories and Risk Factors associated with strategic planning or inherent to the company's business and sector. It is the responsibility of the Risk Management Department, with each department responsible for the organizational processes, to identify the respective Risk Categories. The Risk Categories mapped in the Corporate Risk Dictionary are classified, but not limited to, the following types: Strategic, Operations, Financial, Compliance, Technology, Climate, Systemic, Environmental, and Image. Subsequently, the existing mitigating controls/actions aimed at reducing the criticality of the risks (Impact and/or Probability of materialization) are identified and mapped, considering the short-, medium-, and long-term aspects.

It is important to emphasize that as new strategic objectives are outlined, the internal or external scenario changes, requiring a review of the Risk Management process. Finally, at least annually, the corporate Risk Portfolio must be reviewed to ensure that events that may threaten the business as a whole and/or the fulfillment of its objectives are identified and properly addressed.

From the consolidation of such information, inherent and residual risks are evaluated for each Risk Factor and Risk Category, based on the criteria established in the Impact x Probability gauge for materialization. This information must be recorded formally in a Portfolio and Corporate Risk Matrix.

Subsequently, the responses to the Risk Factors, treatment, and monitoring strategies to be implemented for the respective Risk Factors are defined, and the Risk Categories are prioritized. If the response is to "reduce" the Risk Factor, action plans will be established for treatment and/or monitoring. If the decision is to "avoid,"

the strategy/operation/activity that generates the Risk Factor should be discontinued. When the decision is to "accept," no action is taken, the option being just to monitor the factor. Finally, if the answer is to "share," the company must find ways to share the Risk Impact with third parties, in the scenario of its materialization.

Risks must be continuously monitored by the Risk Management Department through Key Risk Indicators (KRIs) and reported periodically to the Executive Board, the Audit and Risk Management Committee, and the Board of Directors. The report should also consider the Action Plan implementation status, including justifications or any suggestions/needs for change in the strategy to treat and/or monitor the risks, as well as any changes in the characteristics of the risks.

6.2. Climate Transition Risk and Opportunity Management

The mapped Climate Transition Risks are classified into two types (Transition Risks and Physical Risks) and seven categories (Current and Emerging Regulation, Technology, Legal, Market, Reputation, Acute and Chronic). After categorization, the Risks are prioritized based on the history and/or potential of materialization in one or more of the company's malls versus the financial impact caused by this materialization.

In addition to the verification of Climate Transition Risks, the opportunities arising from the climate transition scenario for the Company are verified and prioritized. The opportunities mapped result in sustainable actions that corroborate the Company's strategic planning and strengthen the company's brand before the market and customers.

Risks must be continuously monitored by the Risk Management Department through Key Risk Indicators (KRIs) and reported periodically to the Executive Board, the Audit and Risk Management Committee, and the Board of Directors. The report should also consider the Action Plan implementation status, including justifications or any suggestions/needs for change in the strategy to treat and/or monitor the risks, as well as any changes in the characteristics of the risks.

7 References

- COSO-ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework
- ISO 31,000
- Brazilian Code of Corporate Governance
- CVM Instruction 552/2014
- CVM Instruction 586/2017
- IIA 2020 Three Line Model
- Novo Mercado regulations

8 Ethics and Consequence Management Channel

Failure to comply with the guidelines expressed in this policy will result in the adoption of sanctions.

If they have any questions about these guidelines, employees should email the Compliance Department at compliance@allos.co.

If any employees are aware of non-compliance with this policy's guidelines, they must report it to the Ethics Channel (telephone 0800 591 8825, or at www.canaldeetica.com.br/allos).

All reports made through the above channels are confidential and may be anonymous. The company guarantees that retaliation against anyone who makes a report or raises suspicions of violations through the Ethics Channel, reports a violation, or in any other way brings to the company's attention a situation that may constitute a violation of this policy or the law, or which deserves to be investigated or analyzed, will not be tolerated.