Raízen Policy – PLT.29

RISK MANAGEMENT POLICY

Purpose

This Risk Management Policy ("Policy") aims to establish principles, guidelines and responsibilities to be observed in the Enterprise Risk Management (ERM) process of Raízen S/A ("Company" or "Raízen") to help identify, assess, respond to, monitor and communicate the risks that may impact the Company in its sector of activity.

Raízen's Risk Management Framework has been established according to a governance model that helps the Company achieve its strategic objectives while fulfilling its commitments to different stakeholders (shareholders, customers, suppliers, employees, society, government, investors, etc.).

We believe that the risk management process must be transparent and communicated throughout the Company, ensuring full knowledge of this Policy and the responsibilities of each individual in the different levels of the organization. The continuous improvement of this process must reflect organizational changes and maintain alignment with the Company's other management processes, supporting decision-making aimed at protecting and generating value for Raízen.

In situations where specific business areas have a risk management role at a tactical or operational level, they must adhere to the methodology and guidelines established by this Policy. Exceptions must be presented to and approved by the Executive Leadership Team.

Table to Contents

1. Definitions

The terms and expressions listed below will be defined as follows:

Audit Committee – An advisory body to the Company's Board of Directors. As established by the Company's bylaws, its mission is to oversee the operationalization of internal and external audit processes, and the mechanisms and controls related to risk management, and to ensure that the financial policies are consistent with the Company's strategic guidelines and risk profile.
Board of Directors – As established by the Company's bylaws, this body acts as the guardian of the Company's principles, values, corporate purpose and governance system.
Consequence – The effect of the materialization of a risk, whether it had been previously identified or not.
Criticality – The classification of a risk based on impact and likelihood assessments.
Current Residual Risk – The risk remaining after the implementation of mitigating actions and control activities at the time of risk identification and assessment.
Executive Leadership Team – The group made up by the Company's CEO (L1) and Vice-presidents (L2).
IBGC – *Instituto Brasileiro de Governaça Corporativa*, or Brazilian Institute of Corporate Governance.
Impact – The consequences of a risk materializing, which can be measured qualitatively or quantitatively.
Impact Scale – The criteria and scales used to assess impact, defined according to the unique characteristics of the business.
Inherent Risk – A risk associated with the business before any action, control or countermeasure is taken. An organization's raw exposure to risk.
Internal Audit – The area responsible for assessing the effectiveness of the Company's risk management and processes, risk mitigation actions, internal controls and compliance with the standards and legislation of the markets where the Company operates, in accordance with its principles and guidelines.
Internal Controls – The area responsible for developing and implementing controls to reduce the Company's exposure to risks, ensuring compliance with standards and legislation in the markets where the Company operates, and guaranteeing the reliability of financial and management reports.
Likelihood – The probability of a risk materializing, which can be assessed qualitatively or quantitatively.
Likelihood Scale – The criteria and scales used to assess likelihood, defined according to the unique characteristics of the business.
Mitigating Actions (action plan) – An action (or set of actions) that is aimed at reducing risk exposure and is linked to the factors that cause such exposures, in addition to having an individual who is responsible for its implementation and a deadline for its completion.
Projected Residual Risk – The risk projected into the future after the full implementation of mitigating actions and control activities. The projected risk determines the minimum degree of criticality of the risk according to how the Company is willing to treat it.
Risk – The possibility of an event happening that could negatively affect the achievement of an organization's goals, preventing the creation of value or even destroying existing value.
Risk Appetite – The level of exposure to loss that the Company is willing to accept to achieve its short-, medium- and long-term strategic objectives.
Risk Capacity – The maximum risk tolerance—higher than the risk appetite—that the Company is willing to accept to achieve its strategic objectives and ensure business continuity.
Risk Dictionary – A document that records the main risks identified based on the analysis of business strategies and context. It is a key tool in the definition of a common risk language and in the risk management process, as it ensures alignment within the organization and creates a process free from interference.
Risk Factors – A specific set of circumstances that contribute to the occasional materialization of a risk. Any given risk may be associated with one or more risk factors.
Risk Form – A document that consolidates all information related to the process of identifying, assessing and responding to a risk.
Risk Management – The area under the Risk, Assurance and Internal Controls director that is responsible for conducting the risk management process within the Company.

Risk Management Process – A set of coordinated activities for identifying, analyzing, treating and reviewing business risks, performed in accordance with the approved policy and methodology for assessing, classifying and reporting risks.
Risk Matrix – A graphical representation of the assessment of the Company's criticality levels considering impact and likelihood analyses.
Risk Owner – The manager responsible for managing a risk, or risk factors, as well as implementing mitigation actions and internal controls.
Risk Response – The way through which a risk is addressed.
Risk Tolerance – A risk limit, lower than the appetite, after which senior management must be alerted to take mitigating actions and reduce risk exposure.
Risk Treatment – A set of initiatives to address the response to risks, including, but not limited to (i) mitigating actions, (ii) internal controls, (iii) project execution, (iv) development/acquisition of systems or (vi) creation of normative documents.

2. Scope

This Risk Management Policy ("Policy") applies to Raízen and its subsidiaries.

3. References

- Bylaws
- ABNT NBR ISO 31000:2018 Standard
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- *Instituto Brasileiro de Governança Corporativa* (Brazilian Institute of Corporate Governance, IBGC)
- The IIA's Three Lines Model (The Institute of Internal Auditors)
- PR.FIN.A04 – Risk Matrix Review
- Raízen S.A. – Audit and Integrity Committee Charter
- Raízen S.A. – Internal Rules of the Board of Directors

4. Guidelines

Corporate risk management is a process conducted jointly by the Executive Leadership Team and the Corporate Risk Management area, and assessed by the Company's Audit Committee. It establishes strategies for identifying and monitoring, throughout the Company, potential material events that can negatively affect it.

Corporate risks are grouped according to the following categories:

(i) **Strategic Risks**: Risks associated with the strategic decisions of senior management and that can lead to a substantial loss in the economic value of the organization or a negative effect on its reputation in the market.
(ii) **Operational Risks**: Risks associated with the possibility of loss (of production, assets, customers, revenues) resulting from failures, deficiencies or inadequacy of internal processes involving people, systems or unexpected external events (e.g.: natural disasters).
(iii) **Financial and/or Market Risks**: Risks associated with the exposure of the organization's commercial and financial operations.

(iv) **Regulatory, Legal or Compliance Risks**: Risks associated with non-compliance with or changes in laws and regulations issued by federal and/or local governments, regulations issued by regulatory agencies or even normative documents issued by the Company itself.

(v) **Information Risks**: Risks associated with the loss, misuse, unauthorized access or disclosure of information or personal data from internal or external stakeholders, which may threaten the Company's business or harm its image.

Corporate risk management is an integral part of the Company's corporate governance processes and must be used as a source of relevant information for strategic decision-making and for setting strategic goals, in addition to being considered in the Company's management cycles. It must be conducted in such a way as to maintain the Company's risk exposure on par with its risk appetite while enabling it to achieve its goals and targets.

The Company's risk management follows the IIA's Three Lines Model, as described in a position paper published by The Institute of Internal Auditors in September 2024, summarized as follows:

- **1st Line of Defense**: The Company's business areas, including its affiliates and subsidiaries. They are responsible for the risks they manage, as well as for their respective mitigating actions and associated internal controls.
- **2nd Line of Defense**: Risk Management and Internal Controls. They must equip first-line managers to properly manage risks by organizing and establishing processes, defining methodologies, and providing training and guidance, in addition to reporting information to the appropriate governance bodies.
- **3rd Line of Defense**: Internal Audit. Provides independent oversight to confirm the effectiveness of and compliance with the model and report its recommendations to the appropriate governance bodies.

Additional roles and responsibilities of each line of defense regarding risk management are detailed in item 5. Roles and Responsibilities.

4.1. Risk Management Process

Raízen recognizes that managing risks effectively is essential to achieving business objectives. Each business or function must assess its environment, set clear goals and:

- Identify the risks that may impact the achievement of these goals.
- Assess the impact and likelihood of these risks materializing.
- Implement effective actions to mitigate the identified risks.

Raízen also requires all businesses and functions to monitor, communicate and report changes in the risk environment, as well as the effectiveness of actions taken to manage identified risks on an ongoing basis.

The methodology adopted by Raízen is based on the integrated risk management framework suggested by COSO and IBGC, as well as the principles established by ISO 31000. Effective risk management enhances the value of the Company's business decisions, since conscious choices are made regarding the risks that may impact or result from these business decisions. The objective of risk management is therefore not to arbitrarily reduce or eliminate risk, but rather:

- Standardize concepts related to risk within the company
- Share information related to risks within the Company

- Support decision-making
- Align the Company's organizational activities with its management cycles
- Ensure that the Company's corporate governance processes reflect best practices
- Assist the 1st Line of Defense in risk management and reduction, when applicable
- Define roles and responsibilities related to risk management
- Increase transparency in the Company's interactions with stakeholders, including, but not limited to financial institutions, investors, shareholders, market analysts, credit agencies, regulatory bodies, and external auditors.

4.1.1. Steps of the Risk Management Process

The steps of Raízen's risk management process are based on ISO 31000:2018 as shown in the figure below.

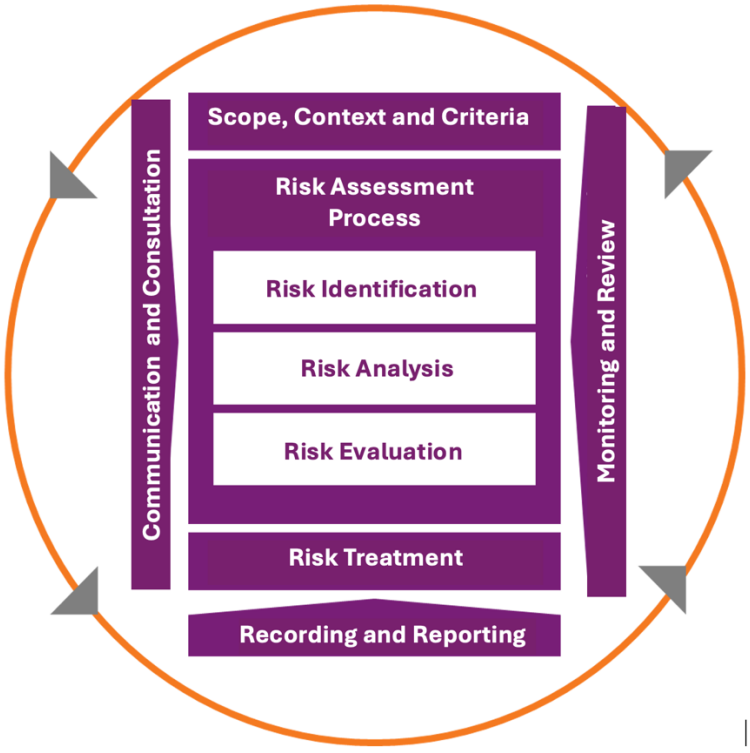

Figure 1 – Risk Management Process

SCOPE, CONTEXT AND CRITERIA

When planning for any activity, realistic and measurable goals are set according to the business context. The first step of the risk management process involves understanding the Company's strategic objectives considering internal and external factors.

RISK IDENTIFICATION

Risk identification will be more valuable when directly linked to the strategic objectives of the business. Different approaches may be adopted to identify risks, and the choice of approach will depend on the size and complexity of the business/operation or opportunity/project, and the volatility of the risk environment. Risk identification, including for emerging risks, will involve meetings or workshops dedicated to discussing risks in each Raízen business or may also occur through the materialization of a significant event with potential to reoccur.

This step involves creating a list and description of risks and associated factors, including internal ones, that may divert the Company from achieving its strategic objectives or from complying with standards and regulations.

RISK ANALYSIS

The risk analysis step must consider the impact and likelihood of a risk materializing, as well as its associated factors.

The impact must not only take into account the immediate consequences of the materialization of a risk, but also the indirect effects. Not all risks can be quantified in financial terms, and qualitative criteria may be a more appropriate option for the assessment or certain risks. Qualitative criteria may include, but are not limited to, environmental, social, compliance, health and safety, institutional image, product quality or technology criteria. The assessment of likelihood must consider the history of the risk materializing, the existing controls to address the risk, the existence and effectiveness of mitigating actions and the technical opinion of experts in the field, including risk owners.

A risk assessed before the effect of any mitigating action or associated control is called Inherent Risk. Current Residual Risk is the risk remaining after the partial implementation of countermeasures. Projected Residual Risk is the risk remining after the full implementation of mitigating actions.

RISK EVALUATION

In this step, we consider the criteria established in the previous step to evaluate the risks, which involves classifying them and their associated factors in the Company's Risk Matrix.

The Risk Matrix then becomes a prioritization tool, considering the evaluation of the risks compared with the established risk appetite, to direct efforts and mitigate the most relevant risks according to the business context.

Risks are classified according to four levels of criticality, considering the likelihood and impact scores in decreasing order:

- Very High – highest criticality in terms of business value
- High
- Medium
- Low – lowest criticality in terms of business value

RISK TREATMENT

Risk assessments support the allocation of resources and the prioritization of actions based on a comprehensive overview of all significant risks considering the Company's objectives. This step includes the planning and implementation of mitigating actions and/or internal controls to respond to each risk and associated risk factor.

It is worth emphasizing that the decision regarding the appropriate treatment of a risk or associated factors depends on its assessment considering the Company's risk appetite. Risks can be treated as follows:

- *Mitigate* – Reduce the likelihood and/or impact through internal controls or mitigating actions.
- *Accept* – Accept the impact of residual risks and all the consequences of its eventual materialization. We must maintain existing controls, if there is any, to prevent an increase in criticality and ensure that the risk will remain managed.
- *Transfer* – This requires a third party that is willing to accept some of the risk together with the Company. This could include, for example, contracting insurance or forming a joint venture.
- *Avoid* – Completely eliminate the source of a specific risk or risk factor. Examples of how to avoid a risk include the interruption of an activity, refraining from operating in a given region or market, or the sale/divestment of assets. However, it is important to note that not all risks can be avoided.

COMMUNICATION AND CONSULTATION

Business risk must be communicated quickly and continuously to the various stakeholders to ensure that the risk management process remains aligned with the implementation of the Company's strategy. This enables the identification of relevant information that can continuously increase the Company's knowledge regarding the risks identified.

Transparent communication regarding risks is also recommended, to ensure that decisions are made based on the full understanding and with consideration of the risks and opportunities involved, and how they will be managed.

The risks must be periodically reported to the Company's Executive Leadership Team and other governance bodies in an integrated and consolidated manner.

MONITORING AND REVIEW

Changes in the internal and external business contexts and the decisions taken during the implementation of the strategy will continually change the Company's risk profile. These changes must be identified in a timely manner, followed by the classification of new risks or changes in the classification of risks already identified, and the review of the Company's Risk Matrix, together with the appropriate governance bodies.

RECORDING AND REPORTING

Risk owners must periodically analyze and report their risks—using the standard Risk Matrix, as per the methodology followed by Raízen—as well as any risk materializations and their actual consequences for the Company. In this way, we can measure the actual progression of the identified risk and the efficiency of the mitigating actions and internal controls. Lessons learned must be recorded to continually improve processes

and mitigate the consequences of a new materialization. In cases of significant incidents, Raízen's Executive Leadership Team and/or the Audit Committee must be involved in the discussion.

5. Roles and Responsibilities

Board of Directors

- Oversee the execution of activities related to general strategy planning and execution, in line with the business objectives.
- Review and approve the general developments of risk management strategies, including this Policy and its implementation.
- Support the activities related to the development of the Risk Matrix, as well as the definition and approval of the Company's risk appetite.
- Periodically assess whether corporate risk management processes enable the Company to achieve its strategic objectives, as reported by the Audit Committee.

Audit Committee

- Monitor the quality and integrity of the Company's internal audit mechanisms and Internal Controls area.
- Assess the effectiveness and sufficiency of the control and risk management systems, including legal and regulatory risks in any judicial or administrative spheres.
- Assess the Risk Management Policy and the effectiveness of its implementation.
- Assess and monitor the Company's risk exposures through periodic review of the Risk Matrix.
- Assess the Company's risk appetite proposed by the Executive Leadership Team.
- Keep the Board of Directors informed about the effectiveness of the risk management processes.

Executive Leadership Team

- Evaluate and approve policies for establishing the Company's internal control and risk management system.
- Recommend the level of risk appetite for approval by the Board of Directors.
- Periodically review and evaluate the risks identified by the Company through the Risk Matrix, as well as their associated factors, responses, treatments, mitigating actions and controls, when applicable, to maintain them on par with the Company's risk appetite.
- Inform the Risk Management area about potential risks not yet identified or about important information about identified risks.
- Steer the focus of risk management toward the most relevant topics for the Company's strategy and continuity.
- Foster and sponsor the development of a risk management culture aimed at strategic decision-making.

Risk Management Area (2nd Line of Defense)

- Develop policies and procedures for establishing the Company's internal control and risk management system.
- Coordinate the Company's risk management process following the guidelines set forth in this Policy.
- Develop and implement the risk management strategy and methodology in compliance with applicable

laws and regulations, internal policies, standards and procedures, and best practices in management.
- Ensure that the governance process and roles and responsibilities established by this Policy are being followed.
- Keep this Policy, the Risk Management Procedure, and the Company's Risk Matrix up to date.
- Monitor the risk exposure levels periodically in accordance with the guidelines of this Policy.
- Report on the levels of potential exposure to the main risks identified to the Executive Leadership Team and the Audit Committee.
- Comply with the recommendations of the Audit Committee and the Executive Leadership Team regarding the risks identified or the risk management process.
- Promote a culture of corporate risk management within the organization.
- Assist risk owners in the risk management process.
- Support and challenge business areas and risk owners in the development of mitigating actions and internal controls.
- Monitor the implementation of mitigating actions by managers to, when applicable, confirm their effectiveness in mitigating or reducing risks, reporting it to the Executive Leadership Team and the Audit Committee.

Corporate Controls Area (2nd Line of Defense)
- Maintain the methodologies and best practices related to the risk management process and the Company's internal control environment.
- Assist the integration of risk management and internal control processes.
- Continuously identify and evaluate internal controls based on risks inherent to the business.
- Report the results of the evaluation of the Company's control environment to those responsible for controls, the Executive Leadership Team and the Audit Committee.
- Support the business areas in the development of risk controls and mitigating actions.
- Promote the culture, guidelines and methodology of internal controls throughout the Company.

Business Areas and Functions (1st Line of Defense and Risk Owners)
- Identify, assess, respond to and monitor the risks under their responsibility, according to the procedures set by this Policy.
- Inform the Risk Management area about potential or materialized risks to be incorporated into the Company's risk management process.
- Report changes—organic or caused by significant events—in the internal or external context of the identified risks that can change their assessments and require responses to be adjusted.
- Provide updated and complete information about the risks during the process of identifying them and creating the Risk Matrix.
- Determine and implement the treatment for the identified risks, when applicable.
- Report the status of the treatments determined for the identified risks under their management.
- When requested, report the status of the risks under their responsibility to the governance bodies.
- Ensure the execution and effectiveness of the existing internal controls to treat risks.

Internal Audit Area (3rd Line of Defense)
- Assess the quality and effectiveness of the Company's risk management processes, periodically monitor the risk mitigating actions and the weaknesses recorded in audit reports, and share information to

inform the risk management model.

- Identify and point out risks that may not yet have been identified by the organization through an independent assessment of the internal control environment.
- Assist the Chief Executive Officer and the Board of Directors, through the Audit Committee, by examining, assessing, reporting and recommending ideas to improve the internal environment and the effectiveness of the risk management process.
- Develop a work plan in line with the Company's strategy and prioritize activities using, among other tools, the most current Risk Matrix.
- Submit the audit work plan for assessment and approval by the Board of Directors and Audit Committee.

6. Annexes

Not applicable.

Area	Risk Management
Responsible Party	Jorge Manoel Daltio Meneghelli
Approver	Audit Committee, Carlos Alberto Bezerra de Moura, Sonia Maria de Sá