

Raízen's Policy – PLT.29

Risk Management Policy

This Risk Management Policy ("Policy") aims to establish the principles, guidelines, and responsibilities to be observed in the process of managing risks inherent to the business activities of Raízen S/A ("Company" or "Raízen"), in order to identify and monitor risks related to the Company or its sector of operation.

Raízen's Control Structure is designed to provide reasonable assurance regarding the achievement of the Company's business objectives and compliance with its external obligations and commitments.

The Structure consists of 3 (three) types of components, namely: (i) foundations, (ii) organization, and (iii) processes. This Policy provides guidance on the application of the Risk Management Process, as one of the foundations.



Definitions:

The terms listed below shall have the meanings assigned to them as follows:

Risk Appetite – The level of Risk exposure that the Company is willing to accept in order to achieve its short-, medium-, and long-term business objectives.

Corporate Controls – The area responsible for assessing the quality and effectiveness of the Company's Risk management processes.

Company's Board of Directors – Acts as the guardian of the Company's principles, values, corporate purpose, and governance system.

Audit Committee – An advisory body to the Company's Board of Directors, whose mission is to oversee the operationalization of internal and external audit processes, the mechanisms and controls related to Risk management, and the alignment of financial policies with the Company's strategic guidelines and Risk profile.

COSO (Committee of Sponsoring Organizations of the Treadway Commission) – A private, nonprofit organization created in the United States in 1985, dedicated to improving the reliability of financial reporting, especially through the application of ethics and effectiveness in the fulfillment of Internal Controls. The entity is sponsored by five of the leading professional associations in the financial field in the United States.

Risk Matrix – A graphic representation of the Company's exposure levels along two axes of analysis (Impact and Probability).

Action Plan – An action (or set of actions) aimed at reducing Risk exposures. An action plan must be aligned with the factors causing the exposures. It must also have parties responsible for its implementation and completion deadlines.

Probability – The possibility of an event occurring. In Risk management terminology, the word "probability" is used to refer to the chance of something happening, regardless of whether it is defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, or described using general or mathematical terms (such as probability or frequency over a given period of time).

Risk – The possibility of an event occurring that could adversely affect the achievement of the organization's objectives, preventing the creation of value or even destroying existing value.

Inherent Risk – The risk associated with the business before the effect of any action or countermeasure. It is the Company's gross exposure to Risk.

Residual Risk – The risk remaining after the implementation of mitigating actions and control activities.

1. PURPOSE OF THE POLICY

Raízen recognizes that managing risks effectively is fundamental to achieving its business objectives. Each Business and Function shall analyze its environment, define clear objectives, and:

- identify the risks to achieving these objectives;
- assess the impact and probability of risks materializing;
- implement effective actions designed to:
 - achieve business objectives;
 - protect the Company's assets against misuse, loss, or fraud;
 - facilitate economical, effective, efficient, and secure operations; and
 - enable compliance with the limits set forth by the Control Structure.

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

2. GENERAL RISK MANAGEMENT GUIDELINES

Corporate risk management is a process conducted jointly by the Company's Audit Committee (the body that advises the Company's Board of Directors) and the Company's Executive Board, which establishes the strategies for identifying and monitoring, across the entire Company, potential material events capable of affecting it.

Corporate risks are grouped into six categories:

(i) Strategic Risks: associated with decision-making by senior management and may result in substantial loss in the organization's economic value. They are caused by changes in the external environment;

(ii) Operational Risks: associated with the possibility of losses occurring (in production, assets, customers, revenues) resulting from failures, deficiencies, or inadequacies in internal processes, people, and systems;

(iii) Financial and/or Market Risks: those associated with the organization's exposure through its financial operations;

(iv) Regulatory, Legal, and Compliance Risks: those associated with exposure to non-compliance with laws and regulations issued by central and local governments, as well as regulations issued by regulatory bodies or of an internal nature. These are associated with the prevention of money laundering, integrity, etc.;

(v) Information Risks: those consisting of the loss, misuse, unauthorized access, or disclosure of information or personal data belonging to internal or external stakeholders, which may threaten the business or harm the Company's image; and,

(vi) Image Risks: the risk of events occurring, frequently associated with the materialization of other risks, that cause reputational damage and affect the

Company's credibility.

Corporate risk management must be carried out in such a way as to keep risks at levels compatible with the Company's risk appetite, allowing for reasonable assurance of the fulfillment of its objectives.

The management of the Group's Risks and opportunities follows the concept of the three lines of defense:

- **1st Line of Defense:** comprised of the Group's business areas, including its affiliates and subsidiaries, responsible for the Risks and opportunities they manage.
- **2nd Line of Defense:** comprised of the Company's control structures, which must equip first-line managers for the proper management of Risks and opportunities.
- **3rd Line of Defense:** comprised of the Company's Internal Audit, acting with an independent perspective to verify the effectiveness of the model.

The methodology adopted by Raízen uses as a reference the integrated Risk management framework proposed by COSO (Committee of Sponsoring Organizations of the Treadway Commission).

The broader roles and responsibilities of each line of defense with respect to Risk management are detailed in the Roles and Responsibilities section below.

3. THE RISK MANAGEMENT PROCESS

Risk is defined as a potential future event that could influence the achievement of the Company's objectives. This includes "upside" and "downside" risks. Effective risk management increases the value of the Company's business decisions, since conscious choices are made regarding the risks that impact, or result from, those business decisions.

The purpose of risk management is therefore not to arbitrarily reduce or eliminate risk.

The Risk Management Statement applies to all Businesses and Functions, as well as to all activities carried out by Raízen. This includes the development of opportunities, project execution, and daily operations.

3.1. Risk Management Boundaries

The Control Structure establishes limits for Raízen's activities. This includes Raízen's General Business Principles and Standards, which provide standards on risks that require common treatment across all Raízen's companies, businesses, and functions. These Standards are risk-based (as is the entire Control Structure), which means that their application does not eliminate these risks. For example, the Treasury element of the Financial Standards includes standards on foreign exchange risk management and the

use of insurance. HSSE (Health, Safety, and Environment) Standards include standards on the management of operational and safety hazards, and other HSSE activities. When a business objective cannot be achieved without compromising elements of the Control Structure, management will take measures to ensure compliance or the discontinuation of the activity.

3.2. Risk Management Process Steps

- DEFINITION OF CLEAR OBJECTIVES:

During the planning phase of any activity, realistic and measurable objectives are defined within the context of the relevant business environment. These objectives are defined during the Company's business planning process. For a new business opportunity, objectives may be defined during the identification and evaluation phases and may be further refined when a negotiation mandate is requested. At the individual level, objectives are defined as part of the annual performance evaluation process. Regardless of the level or terminology, clear objectives are defined so that it is clear what must be achieved, when, and by whom.

- RISK IDENTIFICATION

Risk identification can only have value or meaning when explicitly linked to objectives. Different approaches are adopted to identify risks, and the approach adopted will depend on the size and complexity of the business/operation or the opportunity/project, and the volatility of the risk environment. Risk identification will involve meetings or workshops dedicated to risk in each Raízen Business and Function. Sources of risk include economic, political, commercial, technical, financial, and operational risks. However, risks rarely originate from a single dimension and almost never affect only one factor. For example, an accident causing damage at a manufacturing site as a result of a technical risk affects not only the individual and their family, and the site (through the temporary closure of the site by the authorities), but may also lead to project delays, with possible defaults under a supply contract, potentially harming our reputation.

Risks are managed in 3 categories (High, Medium, and Low):

- Quadrants classified as "High" have greater criticality to business value, requiring prioritization and follow-up, as well as priority action plans to eliminate or reduce their severity and/or frequency.
- Quadrants classified as "Medium" have moderate criticality to business value, requiring regular monitoring to continuously guide mitigation strategies and/or contingency plans.
- Quadrants classified as "Low" have lower criticality to business value, requiring focus on defining acceptable levels of loss from events and actions that prevent the level of impact from increasing over time.

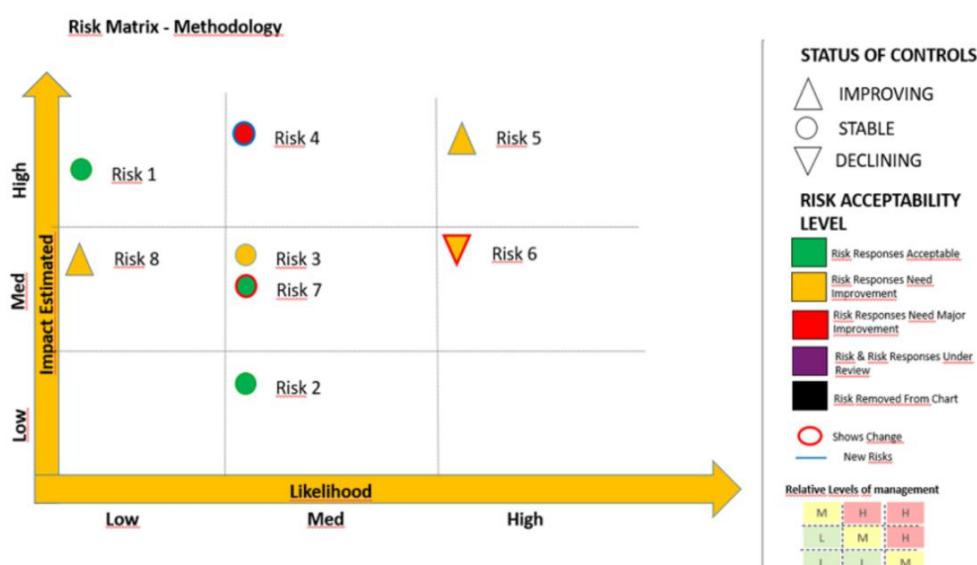
- ASSESSMENT OF RISK IMPACT AND PROBABILITY

Impact must consider not only the immediate consequences of a risk materializing, but also its indirect effects. Not all risks can be quantified. For certain types of risk, such as reputational risk or HSSE (Health, Safety, Security, and Environment) risks, a qualitative assessment will be necessary.

The assessment of probability must consider the risk management track record. For example, if a given business's track record in credit management is poor, then there is a greater probability of credit default occurring. An assessment of risk exposure without any actions in place is referred to as the gross risk assessment. Residual risk is defined as the risk that remains after considering the existing actions being taken.

- IMPLEMENTATION OF EFFECTIVE ACTIONS

Risk assessment assists in the allocation of resources and prioritization of actions, based on a comprehensive overview of all significant risks within the context of the relevant company's objectives. For each risk, acceptability is determined, which involves an assessment of the residual risk level compared to the amount of risk that management is willing to accept. When risk management requires significant improvement before the risk can be considered acceptable, this is indicated by the color code red. For risks requiring improvement, but of a less fundamental nature, the color yellow is used. Green is used to denote risks that management considers acceptable, and blue where the risk and/or responses to it are under review. For risks that are not acceptable, time-bound actions are required that will result in the acceptance of the risk (the "get-to-green plan"). Raízen will use the following standard risk matrix to assist management in this process ("Risk Matrix"). The position on the Risk Matrix represents the residual risk.



It is important not to confuse risk acceptability with impact. A risk with high impact and high probability may be acceptable if adequate controls and safeguards are in place and operating to manage the risk. The most obvious example is commodity price risk. In this

regard, 3 (three) generic actions can be taken to manage risks, as follows:

1. Accept and control the risk: accept the risk and put in place appropriate controls (preventive and detective) to manage the risk and maximize value.
2. Transfer and/or share the risk: some risks are transferred (for example, to an insurance company) or shared (for example, with contractors or joint venture partners).
3. Terminate or renounce the activity: risks are avoided, for example, by discontinuing an activity or withdrawing from a region or market. Some risks are eliminated in part through sale or divestment. However, it is important to establish whether all risks will be eliminated or whether some will remain with the business (for example, environmental liabilities).

In general, risks are retained and managed when a company (e.g., Business or Function) has the capacity to manage them better than others and is sufficiently rewarded for doing so. Alternatively, risk is transferred or shared when others are better able to manage the risk at an acceptable cost. An important element in risk management is assessing what the cost of risk transfer would be and what opportunities would be lost through the transfer of risk. An example of risk transfer at a fixed price is the purchase of insurance to cover physical damage to assets. It is also important to understand the consequences of risk transfer for the Company as a whole, since it may have an offsetting position for the specific risk elsewhere.

The implications of transferring risks to third parties are evaluated as part of this decision. For example, in most projects, contractors are involved in providing goods and services. The assessment of contractors' capacity and their selection is therefore a key factor in commercial risk management. The decision to transfer risk to a contractor considers the contractor's ability to manage that risk. The implication of a contractor entering liquidation can be significant and is considered at an early stage in the contractor prequalification process. It is obvious that great care must be taken in assuming that risk transfer is effective, both in terms of legally watertight provisions and, in many cases, the transferee's financial soundness and creditworthiness.

The impact of actions taken and/or changes implemented in the risk environment will change the acceptability of the risk. For example, if a risk is assessed as "yellow" and "improving" over several consecutive periods, a reassessment of its acceptability level will be necessary, which may lead to a change in acceptability to "green". On the Risk Matrix, an upward-pointing triangle indicates an improvement in risk or environment management in the period immediately preceding the assessment. If there is no further improvement, a circle is used. Similarly, a downward-pointing triangle indicates a decline in risk or environment management in the period immediately preceding the assessment.

- RISK COMMUNICATION AND MONITORING

Changes in business conditions and decisions made while conducting business will continuously alter a company's risk profile. This makes it important to have frequent and explicit conversations about risk to maintain ongoing awareness of which risks are

significant.

It also requires transparent communication regarding significant risks to decision-makers, so that decisions are made with a full understanding of the risks and opportunities involved, and how they will be managed. For example, standard investment proposals include a transparent and comprehensive description of the risks (advantages and disadvantages).

The Company's Audit Committee considers identified risks and adjusts process review plans and resource allocation. To facilitate this process, Businesses and Functions appoint owners for each risk. Risk owners are responsible for ensuring that a clear definition and assessment of the risk is maintained, and for considering the effectiveness of existing actions to manage the risk. They are not necessarily responsible for managing the risk themselves. At the Senior Management level, Raízen's Executive Board and the Audit Committee review the risks that affect Raízen's objectives.

- **RISK REPORTING**

The leadership teams of Businesses and Functions are required to review and report their risks annually using the standard Risk Matrix. This facilitates the aggregation of Raízen's risks and Raízen's mitigation plan by its Controlling Area to support management discussion at Raízen's Audit Committee.

Submission dates will be published by the Controller in accordance with the Audit Committee's schedule.

3.3. Roles and Responsibilities

Board of Directors

- Review and approve the general definitions of Risk management strategies, including this Policy;
- Establish Raízen's Risk Appetite levels based on the Company's strategic objectives;
- Monitor critical alignments: strategy, Risks, controls, compliance, incentives, and people;
- Periodically assess whether corporate Risk management processes enable the Board of Directors to achieve its Risk oversight objectives.

Audit Committee

- Oversee the adequacy of processes related to risk management and the internal control system, in line with the guidelines established by the Board of Directors;
- Assess and monitor the Company's Risk exposures through annual approval of the Risk Matrix;
- Monitor the evolution of the management of identified risks, as well as compliance with applicable legislation, the Group's policies, standards, and

- procedures, and the effectiveness of controls and response actions taken;
- Assess the adequacy of human and financial resources allocated to Raízen's corporate Risk management process;
- Keep the Board of Directors duly informed regarding the effectiveness of Risk management processes and, when necessary, recommend changes to concepts and risk appetite levels.

Internal Audit Area (3rd Line of Defense)

- Assess the reliability of information, review the effectiveness and efficiency of operations, and asset safeguarding, ensuring compliance with laws, regulations, and contracts;
- Advise the CEO and the Board of Directors, through the Audit Committee, by examining, evaluating, reporting, and recommending improvements to the adequacy of the internal environment and the effectiveness of the Corporate Risk Management process;
- Identify and flag Risks not yet mapped within the organization through independent assessment of the internal control environment;
- Assess the quality and effectiveness of the Company's Risk management processes, periodically monitor Risk mitigation actions and weaknesses recorded in audit reports, and feed information back into the Risk management model;
- Prepare its work plan and prioritize its activities based on the Risk Management Process.

Corporate Controls Area (2nd Line of Defense)

Holds various responsibilities regarding its Risk Management and Internal Controls structures. Specifically for Risk management, its main responsibilities are:

- Develop and apply the Risk management strategy and methodology in compliance with applicable laws and regulations, internal policies, standards, and procedures, and management best practices;
- Together with the Internal Audit Area, align risk, impact, and probability measures, so that the same concepts are used to classify Risks in both activities;
- Keep this Policy, the Risk Management Procedure, and the Risk Matrix Template up to date;
- Promote a culture of corporate Risk management within the organization;
- Equip and train all managers in business areas and functions to ensure the correct and timely identification, analysis, and assessment of Risks and the development of action plans;
- Support managers in formulating the concepts and methodologies used in corporate Risk management, as well as the Risk Map and the Risk Scale, which establishes the classification of Risks by the severity of their potential impacts;
- Periodically monitor Risk exposure levels in accordance with this Policy's guidelines;

- Report to the Vice-Presidencies through the Governance Committees, and to the Audit Committee, on the potential exposure levels of the main identified Risks;
Monitor the implementation of action plans with managers to verify, where applicable, their mitigation or reduction, reporting to Executive Leadership and the Audit Committee.

Business Areas and Functions (1st Line of Defense)

- Identify, assess, mitigate, and monitor the Risks of the processes and businesses under their responsibility, based on the criteria established in this Policy;
- Define and implement action plans for the mitigation of identified risks;
- Ensure the execution and effectiveness of existing Internal Controls for Risk mitigation.

3.4. General Provisions

This Policy may be supplemented by specific procedures (standards, procedures, and work instructions) when applicable and required.

This document was approved on June 1, 2021, by the Company's Board of Directors and is effective immediately, for an indefinite period, from the date of its publication and disclosure.