1. OBJECTIVE

Establish the guidelines and responsibilities for Risk Management at Cosan S.A. ("Cosan" or the "Company"), as well as guide the processes of risk identification, assessment, treatment, monitoring, and communication, incorporating a risk perspective into strategic decision-making and promoting a Risk Management culture at all organizational levels, in accordance with market best practices.

2. APPLICATION AND SCOPE

This Risk Management Policy ("Policy") covers Cosan and shall serve as a reference to its subsidiaries and/or co-controlled companies, as from the date of its approval and consequent publication.

3. DEFINITIONS

The terms listed below shall have the meanings assigned below:

Mitigating Actions (action plan) - An action (or set of actions) aimed at reducing risk exposures that must be connected to the factors causing the exposures. It must also have those responsible for its implementation and a deadline for completion.

Risk Appetite - Level of exposure to loss, financial or non-financial, quantitative or qualitative, that the company is willing to assume in order to achieve its short, medium and long-term strategic objectives.

Internal Audit - The area responsible for assessing, in accordance with its principles and guidelines, the effectiveness of the Company's Risk Management and processes, risk mitigation actions, internal controls and compliance with the rules and legislation of the markets in which the Company operates.

Risk Capacity - Maximum Risk Tolerance Limit, higher than the appetite, which the Company can withstand in order to achieve its strategic objectives, while maintaining the continuity of its business.

Cosan Risk Committee - A committee made up of company executives and the Risk Management Department, responsible for identifying, reviewing, discussing and monitoring risks that may affect the business.

Audit Committee - A permanent advisory body linked and subordinate to the Company's Board of Directors, responsible for (i) advising the Board of Directors on internal control and risk management processes; (ii) supervising the activities of the Internal Audit; and (iii) supervising the activities of the Cosan Group's independent audit firms, among other functions described in the Company's Bylaws.

The Company's Board of Directors - This is the Company's highest governance body. The Board of Directors, among other duties, is responsible for electing managers, approving the work plans, investments and budget of the Company and its subsidiaries. The Company's main guidelines and policies are approved by the Board of Directors.

Consequence - Effect of the materialization of Risks, whether identified or not.

Internal Controls - The area responsible for designing and implementing controls to reduce the company's level of exposure to risks, maintaining compliance with the rules and legislation of the markets in which the company operates, as well as maintaining the reliability of financial and management reports.

Criticality - Risk classification according to its impact and probability assessments.

Risk dictionary - A document that records the main risks identified from the analysis of strategies and the business context. It is a fundamental part of defining a common risk language, enabling better understanding across the organization.

Executive Board (Diretoria) - Cosan's Executive Board is the body responsible for the internal organization and day-to-day running of operations, implementing the general policies and guidelines established by the Board of Directors.

Risk Owner - Manager responsible for managing risks, or Risk Factors, as well as implementing the respective mitigating actions and/or internal controls.

ESG (*Environment, Social and* Governance) - Concept that assesses a company's sustainability considering environmental, social and governance aspects.

Risk Factors - A specific set of circumstances that contribute to a risk eventually materializing. The same risk may contain one or more related factors.

Risk Sheet - Document that formalizes all the information relating to the process of identifying, assessing and treating risk.

Risk Management - Area, subordinate to the Risk Management, Internal Controls and Internal Audit Department, responsible for conducting the Risk Management Process within the Company.

IBGC - Brazilian Institute of Corporate Governance. It is a civil society organization and a collaborative network of ideas dedicated to exploring important governance themes and issues that have a positive impact on society.

IIA - *The Institute of Internal Auditors*. International professional association based in the United States. Its main objective is to promote and develop the practice of internal auditing and corporate governance worldwide.

Impact - The impact refers to the Consequences that will be generated if the risk materializes and can be measured qualitatively or quantitatively. In general, it is the categorization and measurement of the consequences of the risk materializing.

ISO 31000 - The 2018 ABNT NBR ISO 31000 standard, which is the international standard that provides principles and guidelines for risk management and is applicable to any type of organization, regardless of its size or sector.

Risk Matrix - Graphical representation of the assessment of the Company's degrees of Criticality considering the impact and Probability analyses.

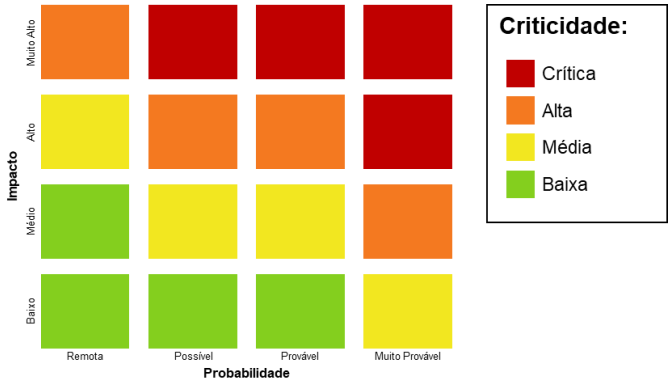

Figure 1- Cosan Risk Matrix

Strategic Planning - A management tool that defines goals, actions and resources for an organization to achieve its objectives. At Cosan, strategic planning is carried out through the RPA (Annual Planning Meeting).

Probability - Chance of a risk materializing. It can be assessed qualitatively or quantitatively.

Risk management process - Set of coordinated activities for identifying, analyzing, treating and reviewing business risks, carried out in accordance with the policy and methodology approved for evaluating, classifying and reporting risks.

Impact Ruler - Criteria and scales, defined according to the specifics of the business, for analyzing Impact.

Probability Ruler - Criteria and scales, defined according to the specifics of the business, for Probability analysis.

Risk Response - Definition of how to deal with risk.

Risk - Possibility of the occurrence of an event capable of adversely affecting the achievement of the organization's objectives, preventing the creation of value or even destroying existing value.

ESG Material Topics - The ESG topics most relevant to the company and its stakeholders, considering their financial and strategic impact.

Risk tolerance - This is a risk threshold, lower than the appetite, at which senior management should be alerted to take mitigating actions and reduce exposure to risk.

Risk treatment - A set of initiatives, which can be documented using a Risk Sheet together with all the information relating to a given risk, including but not limited to (i) mitigating actions, (ii) internal controls, (iii) project execution, (iv) systems development/acquisition or (vi) the creation of regulatory documents, to address the Response to risks.

4. GENERAL GUIDELINES

Corporate Risk Management is an integral part of the Company's corporate governance and must be used as a source of relevant information for strategic decision-making and defining strategic objectives, as well as being present in the Company's management cycles such as budget management and Strategic Planning. It must be carried out in such a way as to maintain exposure to risk at levels compatible with the Company's Risk Appetite, making it possible to guarantee its objectives and targets.

The company's risk management complies with the Three Lines of Action Model set out in the IIA opinion of September 2024, represented as follows:

- **1st Line of Action:** is made up of the Company's business areas, including its subsidiaries and co-controlled companies, which are responsible for the risks they manage, as well as for the execution and effectiveness of their respective Mitigating Actions and their associated internal controls.
- **2nd Line of Action:** this is made up of the structures that must equip first line managers to correctly manage risks by organizing and structuring processes, defining methodologies, developing training and guidance, as well as reporting information to the competent governance bodies. The 2nd Line can be made up of (i) the Risk Management, Internal Controls, Compliance and related areas; and also (ii) internal governance bodies such as executive committees, commissions, forums and/or working groups.
- **3rd Line of Action:** is made up of the Company's Internal Audit, acting with an independent eye to verify the effectiveness and compliance of the model and report its recommendations to the competent governance bodies.

The broader roles and responsibilities of each line of action in relation to risk management are detailed in item 4.3 (Roles and Responsibilities) below.

In order to define the criteria contained in this Policy, the Company's Risk Management area uses the following definitions for risks in their different stages of identification.

- **Inherent Risk -** Risk associated with the business before the effect of any action, control or countermeasure. It is the company's gross exposure to risk;
- **Residual (Real) Risk -** Risk remaining after the implementation of some mitigating actions and control activities at the current moment of risk identification and assessment; and
- **Projected Risk -** Risk, in its future form, after the full implementation of mitigating actions and control activities. The projected risk determines the minimum degree of Criticality of the risk according to the treatment the Company is willing to carry out.

4.1. Risk Management Process

The organizational structure proposed for Risk Management is based on the parameters and guidelines established by the IBGC and ISO 31000, especially with regard to the stages of risk management, which have the following objectives:

- Ensure that Risk Management is integrated into all of the Company's organizational activities;
- Define roles and responsibilities for risk management;
- Standardize concepts and practices;
- Influence decision-making;
- Provide a dynamic and efficient information routine;
- Ensure that the Company's corporate governance is followed and critically analyzed; and
- Provide greater transparency for the company's various stakeholders: shareholders, market analysts, credit agencies, regulatory bodies, among others.

Below are the stages of the Risk Management process, based on ISO 31000:

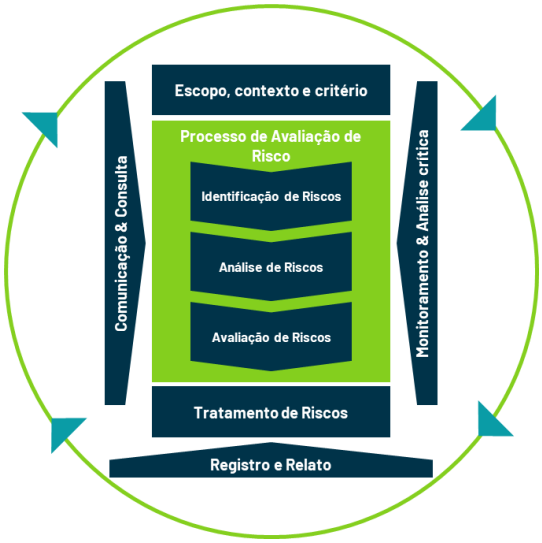

Figure 2- Risk Management Process

4.1.1. Scope, Context and Criteria

In the planning phase of any activity, realistic and measurable objectives are defined in the context of the business environment. In the first stage of the risk management

process, an understanding of the strategic objectives is captured, taking into account the internal and external contexts in which the company operates.

4.1.2. Risk identification

Risk identification is an ongoing management process and is most valuable when it is directly linked to the business's strategic objectives. Different approaches are adopted to identify risks and the approach taken will depend on the size and complexity of the business, the opportunity/project and the volatility of the risk environment. The identification of risks will involve meetings, interviews or workshops dedicated to risks, or it may also occur through the materialization of a significant event with the possibility of new occurrences.

This stage involves creating a list and description of risks and their respective factors that could divert the company from achieving its strategic objectives or from non-compliance with rules and regulations, including internal ones.

As it is a *holding company*, the company must also seek to identify systemic risks through the risk matrices of its investees or any processes, events or factors that belong to transversal structures in the companies. Risks of this nature can lead to the total or partial discontinuation of one or more of the investees' operations at the same time.

4.1.3. Risk analysis

In the risk analysis stage, the Impact and Probability of the risk materializing, as well as their respective factors, must be taken into account.

Impact should not only take into account the immediate consequences of a risk materializing, but also the indirect effects. Not all risks can be quantified in financial terms, and for some risks qualitative criteria are more suitable for analysis. Qualitative criteria can be, but are not limited to, environmental, social, compliance, health and safety, institutional image, product quality or technology.

The Probability analysis must take into account the history of the risk materializing, the existing controls that address the issue, the existence and effectiveness of Mitigating Actions and the technical opinion of experts in the field, including the risk owners.

4.1.4. Risk assessment

In this stage, we compare the level of risk classified during the analysis stage, taking into account the criteria established in the previous stage. In the assessment, we classify the risk in the Company's Risk Matrix.

The Risk Matrix then becomes a prioritization tool, according to the assessment of risks in comparison to the determined Risk Appetite, for directing efforts and mitigating the most relevant risks according to the business context. As shown in Figure 2, the risks are assessed in 4 degrees of Criticality, according to the vector composed of the Probability and Impact scores in descending order:

- Very High - highest Criticality to business value;
- High;
- Medium; and
- Low - least critical to business value.

4.1.5. Risk treatment

Risk assessment helps to allocate resources and prioritize actions, based on a comprehensive overview of all significant risks in the context of the company's objectives. At this stage, Mitigatory Actions and/or internal controls will be defined and implemented in order to respond to each respective risk or risk factor. It is worth emphasizing that the decision on the appropriate treatment of the risk, or its respective factor, depends on its assessment in comparison to the company's risk appetite. We can treat risks as follows:

- **Mitigate -** Reduce exposure to Probability and/or Impact using internal controls or Mitigating Actions;
- **Assume -** Accept the Impacts of the risk in its residual form and all the Consequences of an eventual materialization. We must maintain existing controls, if they exist, so that the risk does not increase in Criticality and remains managed;
- **Transfer -** Requires a third party to be willing to assume part of the risk together with the company. For example, taking out insurance, forming joint ventures, among others; or
- **Avoid -** Completely eliminate the source of a risk. For example, stopping an activity, withdrawing from a region/market, or selling/divesting assets.

4.1.6. Communication & Consultation

It is necessary to communicate quickly and continuously with the different stakeholders about business risks in order to keep the risk management process and the implementation of the company's strategy aligned. In this way, relevant information can be identified that allows for the continuous improvement of information on the risks identified.

Transparent communication about risks is also recommended, so that decisions can be made with a full understanding and consideration of the risks and opportunities involved, and how they will be managed.

Periodic reports on risks should be made in an integrated and consolidated manner to the Executive Board and other company governance forums.

4.1.7. Monitoring & Critical Analysis

During the risk monitoring process, changes in the internal and external context should be detected, identifying emerging risks and changes in risks that have already been formalized, as well as monitoring the execution of Mitigating Actions/internal controls defined by the Risk Owners and the respective areas of the Company, updating the risk classification in the matrix and reporting to the Board of Directors and other Company Governance forums.

4.1.8. Registration and Reporting

Risk Owners must report any materialized risks and their real consequences for the company. In this way, we can measure the real adherence of the identified risk and the efficiency of the Mitigating Actions and internal controls. Lessons learned must be recorded in order to maintain the continuous improvement of the processes involved and mitigate the Consequences of a new materialization. In significant cases, the Company's Board of Directors and/or Audit Committee should be involved in the discussion.

4.2. Dictionary of Risks

The company is subject to various risks that can adversely affect its business. Therefore, in order to define a common language and enable better understanding within the organization, risks can be classified according to the following categories:

- **Strategic Risks** are those associated with senior management decision making and can generate a substantial loss in the company's economic value or have a negative effect on its reputation, credibility or brand in the eyes of the market and the communities in which it operates.
- **Financial risks** are those associated with
  i. The exposure of the organization's financial operations;
  ii. The issue of incomplete, inadequate, inaccurate or untimely financial, management, regulatory, tax, statutory and sustainability reports;
  iii. The company's counterparties who may fail to honor their commitments and obligations (credit risk);
  iv. The alteration or extinction of regional and/or sectoral tax incentives;
  v. the possibility that cash flows are not managed effectively to maximize operating cash generation, manage the specific risks and returns of financial transactions (liquidity risk);
  vi. The devaluation of credit agreements due to a deterioration in the borrower's risk rating;
  vii. A reduction in financial results;
  viii. The volatility of interest rates, exchange rates and other macroeconomic indicators; and
  ix. Raising and investing funds in disagreement with established policies.
- **Compliance, Legal or Regulatory Risks** are those associated with non-compliance with laws and regulations issued by central and local governments as well as regulations issued by regulatory bodies or even of an internal nature. They are also associated with the prevention of money laundering, anti-bribery issues or the occurrence of changes in regulations and actions by regulatory bodies which could significantly affect the company's ability to manage its business with integrity.
- **Operational Risks** are those associated with the possibility of losses resulting from failures, deficiencies or inadequacy of internal processes, people and systems, as well as external events such as natural disasters, fraud, strikes and terrorist acts.

- **Technological and Information Risks** are those associated with cyber attacks, attempts to compromise the confidentiality, integrity or availability of data or computer systems, as well as failures, unavailability or obsolescence of equipment and facilities, computerized control, communication, logistics and operational management systems, which impair or make it impossible to continue the organization's regular activities. They may also be associated with the loss, misuse, access or unauthorized disclosure of information or personal data of internal or external stakeholders, which could threaten business or damage the company's image.

In addition, risks can also be classified, not obligatorily, to the Company's ESG Material Themes. Classifications of this nature can be

- **Transition Risks** are those related to regulatory, technological, market and reputational changes resulting from the transition to a low-carbon economy. This includes factors such as carbon pricing, new environmental legislation and changes in consumer and investor preferences.
- **Emerging Risks** are newly identified risks that could impact the company's business in the long term and, in some cases, already have initial effects. Unlike other risks, they are unprecedented and unprecedented, which implies greater uncertainty and a lack of preparation for their management.
- **Physical risks** are those related to the direct impacts of climate change on operations, assets and production chains. They can be acute (extreme events such as storms and droughts) or chronic (gradual changes such as rising temperatures and changes in rainfall patterns).

4.3. Roles and responsibilities

The company has a specific Risk Management area, which works together with the Risk Management, Internal Controls and Internal Audit Board, with the support of the Financial and Investor Relations Vice-Presidency and the Audit Committee, as shown in the image below:

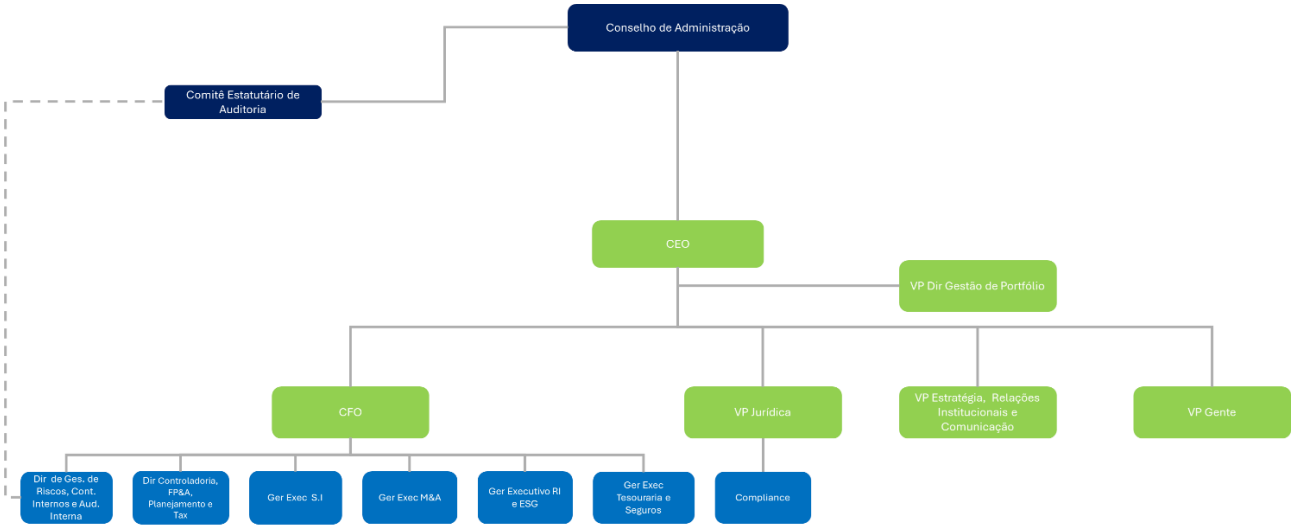

Figure 3- Cosan structure

4.3.1. Board of Directors

- Approve the strategy adopted for the Company's Risk Management;
- Approve the Risk Management Policy and monitor its implementation;
- Approve, every 3 (three) management cycles or upon the occurrence of significant events, the Company's Risk Appetite proposed by the Executive Board;
- Validating the Company's identified risks, as well as their respective Responses, Mitigating Actions and controls, when applicable;
- Supervising the Risk Management Process based on the information presented by the Executive Board and other governance bodies; and
- Ensuring the periodic assessment of the Risk Management process, policies and systems.

4.3.2. Audit Committee

- Evaluate the Risk Management Policy, its methodology and the procedures established by the Company for this process and recommend its approval to the Board of Directors;
- Periodically monitor and evaluate risk management, as well as the execution of the process and its results;

- Annually assessing the effectiveness and sufficiency of the business risk management systems in accordance with this Policy and reporting these results to the Board of Directors;
- Advising the Board of Directors on the supervision of the Company's Risk Management Process; and
- Analyzing and recommending approval of the risk appetite and the Risk Management Process to the Board of Directors.

4.3.3. Executive Board

- Recommend, at least every 3 (three) management cycles or as soon as significant events occur, the degree of Risk Appetite for approval by the Board of Directors;
- Point out to the Board of Directors the risks involved in implementing the Company's strategy at each Strategic Planning cycle or upon the occurrence of significant events;
- Validating the Response and Mitigation Actions for each risk based on the recommendation of the Risk Owners and the Risk Management Department;
- Ensure the implementation of Risk Management in all business areas;
- Define guidelines, resources and targets to ensure the smooth running of Risk Management and promote the integration of Risk Management with the management and planning cycles;
- Evaluate, on an annual basis, the effectiveness and sufficiency of the business risk management systems in accordance with this Policy;
- Approve the Internal Regulations of the Company's Risk Committee, if applicable; and
- Informing the Risks and Internal Controls area about the identification of new risks or events that are relevant, and their respective evolution.

4.3.4. Cosan Risk Committee (CRC)

- Identify, review and manage risks that may affect the business;
- Discuss with leadership the level of exposure to the main risks and the actions taken to monitor and control such exposures; and
- Acting in the management and monitoring of Risk Appetite.

4.3.5. Risk Management Department

- Implement and manage the Risk Management process, in accordance with the Risk Management Policy approved by the Board of Directors, as well as complying with the recommendations and determinations of the Audit Committee, Risk Committee and/or Executive Board;
- Proposing the Internal Regulations of the Risk Committee and ensuring that they are complied with and updated, if applicable;
- Developing and applying the Risk Management strategy, methodology and culture, in accordance with current regulations and best market practices;
- Follow up and monitor the risks reported by the areas, allocating them in the Risk Matrix and the status of implementation of their respective Mitigating Actions;
- Presenting and reporting risks and the level of exposure to risks to the Executive Board, the Risk Committee, the Audit Committee and the Board of Directors;
- Search for best market practices and make the connection with the business;
- Providing training to disseminate the culture and methodology used in Risk Management;
- Advising the areas on the identification, analysis and assessment of the Impact and Probability of risks and their respective Mitigating Actions;
- Submit an annual assessment of the effectiveness and sufficiency of the business risk management systems in accordance with this Policy to the Audit Committee and the Executive Board;
- Identify new risks or events that are relevant, and their respective evolution.

4.3.6. Business Areas (Risk Owners)

- Identify and manage the risks that may affect the Company and recommend the Response/Treatment;
- Informing the Risk Management, Internal Controls and Internal Audit Board of the identification of a materialized or potential risk, whether in their area

or others that they may observe, as well as suggesting its allocation in the Risk Matrix;

- Suggest changes to the risk mapping and validate all the information provided, at least quarterly;
- Report periodically to the Risk Management Department on the status of Mitigating Actions; and
- When requested, report and respond to the governance bodies (Executive Board, Risk Committee, Audit Committee, Board of Directors, etc.) on the risks for which it is responsible.

4.3.7. Internal Controls Management

- Develop and maintain the methodology and good practices for assessing the risks and the internal control environment of business processes related to business risks;
- Advising the Executive Board and Business Areas on the preventive identification of risks, and suggesting measures for their prevention and minimization;
- Manage the process of identifying and evaluating the controls and risks inherent in their respective processes based on qualitative and/or quantitative criteria of the Impact and Probability Rules of the risks;
- Structuring the internal control system in a way that is compatible with the Company's activities, guaranteeing the segregation and controls necessary to mitigate any conflicts in the conduct of its business;
- Report the results obtained in the assessment of the internal controls environment to the process owners, the Board of Directors and the Audit Committee and other forums, when applicable.
- Aligning the internal control structure with the objectives of the company's processes, internal regulations, business strategies and the complexity and risks of operations;
- Support managers and employees in drawing up the action plans needed to implement an adequate internal control environment and mitigate risks; and

- Making managers aware of the importance of integrated risk management and their responsibilities for maintaining and preserving the internal control environment.

4.3.8. Internal Audit

- Provide independent opinions to the Audit Committee, which will assess materiality and report to the Board of Directors, on the Risk Management Process, the effectiveness of internal controls and corporate governance, recommending improvement actions where applicable; and
- Verify compliance of the Risk Management Process with the policies and standards adopted by the Company.

4.3.9. REFERENCES

- Bylaws - Cosan;
- Internal Regulations of the Board of Directors - Cosan;
- Internal Regulations of the Audit Committee - Cosan;
- Internal Regulations of the Executive Board - Cosan.

REVIEW AND APPROVAL HISTORY

This Policy was approved by the Board of Directors on May 23, 2025 after evaluation by the Statutory Audit Committee as provided for.