



# CORPORATE RISK MANAGEMENT POLICY



## **SANTOS BRASIL**

### **1. PURPOSE**

The purpose of this policy is to set out principles, guidelines, and responsibilities for Corporate Risk Management, based on the identification, analysis, prioritization, treatment approach, monitoring and communication of risks that may affect the scope and execution of the planned strategy, for Santos Brasil's decision-making. Thus, the vision of corporate risks is now embedded into the decision-making process, adapting Governance to good market practices, and enabling the fulfillment of the strategy, as well as the creation and preservation of value for Santos Brasil.

This document also seeks to facilitate the dissemination of knowledge and the incorporation of a risk management culture at Santos Brasil, defining a common language on the subject and considering its values, history, decision-making processes, business model, operations, and organizational structure.

### **2. SCOPE**

This Policy applies to all Santos Brasil employees, as well as members of the Board of Directors, Audit Committee and shall automatically apply to new subsidiaries and affiliates.

### **3. REFERENCES**

**ABNT NBR ISO 31000:2018** - Risk Management - Guidelines;

**ABNT NBR ISO/IEC 270005:2019** - Information Technology - Security Techniques - Information Security Risk Management;

**COSO - ERM:** Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management Framework;

**Brazilian Corporate Governance Code (CBGC);**

**Santos Brasil Code of Conduct;**

**IIA** - The Institute of Internal Auditors: Three-line defense model;

**CVM Instruction 552;**

**CVM Instruction 586;**

**LAW No. 6.404/76** - It provides for Publicly-held Corporations;

**Santos Brasil Internal Controls Policy; Novo Mercado Rules.**

### **4. CONCEPTS**

**Mitigating action:** Actions and controls adopted by Santos Brasil to minimize or eliminate exposure to corporate risks and mitigate their eventual materialization.



**Risk Appetite:** Level of risk that an organization is willing to accept in the pursuit and achievement of its strategy and objectives, expressed through the Impact and Probability Ruler and the "Approval Level for Corporate Risk Taking" matrix.

**Criticality of the Risks:** Result of the combinatorial analysis of the impact and probability axes. The criticality of the risk can be defined in five levels: High, Significant, Moderate, Low, Minimal.

**Risk Owner:** An employee appointed by Santos Brasil in charge of handling and monitoring the corporate risk under his/her responsibility. He/she shall be preferably an Officer.

**Enterprise Risk Management (ERM):** A process conducted by the Board of Directors, including through its Advisory Committees, and the Executive Board, which aims to outline strategies to identify, analyze, assess, deal with, monitor and communicate potential future events that could affect Santos Brasil's results.

**Facilitator:** Employee with technical expertise of corporate risk who assists the risk owner in updating information on the effectiveness of initiatives and the internal direction of action plans.

**Corporate Risk Factor:** Causes contributing to corporate risk materialization. A risk may have different interfaces responsible for one or more related causes.

**Key Risk Indicator (KRI):** Measure to obtain exposure to corporate risk. Preferably, it should be related to the cause of the risk and should be measured on a regular basis to help detect changes in trends and anticipate an eventual materialization of the risk in question.

**Impact:** Consequences resulting from the materialization of a corporate risk, which can be expressed quantitatively and/or qualitatively.

**Corporate Risks Matrix:** Graphical representation of the corporate risks identified by Santos Brasil, positioned according to the criticality of each risk, which is defined by assessing its impact and probability.

**Action plan:** Actions aimed at creating, correcting, or enhancing the performance of treatment initiatives. They shall have a single person in charge and a completion date.

**Corporate Risks Portfolio:** Corporate risk catalog and respective risk factors.

**Probability:** Qualitative and/or quantitative level that characterizes the chance of corporate risk materializing.

**Impact x Probability Ruler:** Document that formalizes the description and criteria to be considered for each of the dimensions analyzed in classifying the level of Impact and Probability of the corporate risks identified, generating the Inherent/Residual Relevance in the Corporate Risk Matrix.

**Risk Response:** Definition of how Santos Brasil will treat the risk factor. In response, it can choose to avoid, reduce, share, or accept.

**Risk:** Any event that may affect Santos Brasil's ability to achieve its objectives and business strategy.

**Corporate Risk:** Risks that could impact the achievement and execution of the planned strategy or the business as a whole.

**Inherent Risk:** Risk intrinsic to the business operation or activity, without considering the actions and controls that mitigate it.

**Residual risk:** Remaining risk after considering all the actions and controls in place to mitigate it.



## 5. PRINCIPLES

### 5.1. SANTOS BRASIL'S COMMITMENTS TO RISK MANAGEMENT

- I. Provide a healthy and safe environment for people, assets, the environment, and operational processes by fostering Santos Brasil's risk management process and internal controls;
- II. Meet legal, operational and customer requirements, reducing the likelihood and impact of significant risks inherent in the Company's activities;
- III. Promote continuous improvement in risk management performance within Santos Brasil;
- IV. Train, raise awareness and develop competence in risk management and a culture of internal controls for all employees, suppliers, and service providers;
- V. Promote the preparation of reports on the status of risk management and internal controls, to be analyzed and approved by Santos Brasil's Board of Directors.

### 5.2. RISK MANAGEMENT COMMITMENTS AT SANTOS BRASIL

- I. Have its independent performance assured;
- II. Be embedded into Santos Brasil's culture and business areas, considering its values, strategic pillars, decision-making, business model, operation, and organizational structure;
- III. The Board of Directors, the Audit Committee, the Compliance Committee, and the Board of Executive Officers shall foment risk management at all hierarchical levels and assets of Santos Brasil, also ensuring the application, execution, and adhesion to its procedures;
- IV. The decision-making process shall consider current and potential risks to objectives and strategies, with a view to preserving and creating value for Santos Brasil;
- V. Corporate and operational risks shall be identified, assessed, treated, communicated, and monitored to mitigate the impacts on Santos Brasil's strategies and the fulfillment of its objectives. This identification shall consider external factors (economic, business, environmental, political, social, and technological) and internal factors (infrastructure, people, processes, and technology);
- VI. The corporate and operational risks identified shall be detailed by analyzing their factors, looking at current mitigating actions, assessing their criticality (impact and probability), prioritizing, and setting out treatment and monitoring strategies, as well as defining the respective Risk Owners in charge and deadlines for implementation;
- VII. The definition of the responses assigned to the risk factors shall consider Santos Brasil's willingness to expose itself to the risks, envisaging their effects and cost-benefit, prioritizing investments for the implementation of treatment strategies;
- VIII. The Corporate Risk Management structure and process shall be customized and updated to remain appropriate as Santos Brasil's internal and/or external context changes, ensuring the achievement of its objectives;
- IX. Continuous improvement of the corporate risk management process shall be fostered through evaluation cycles and independent reviews.

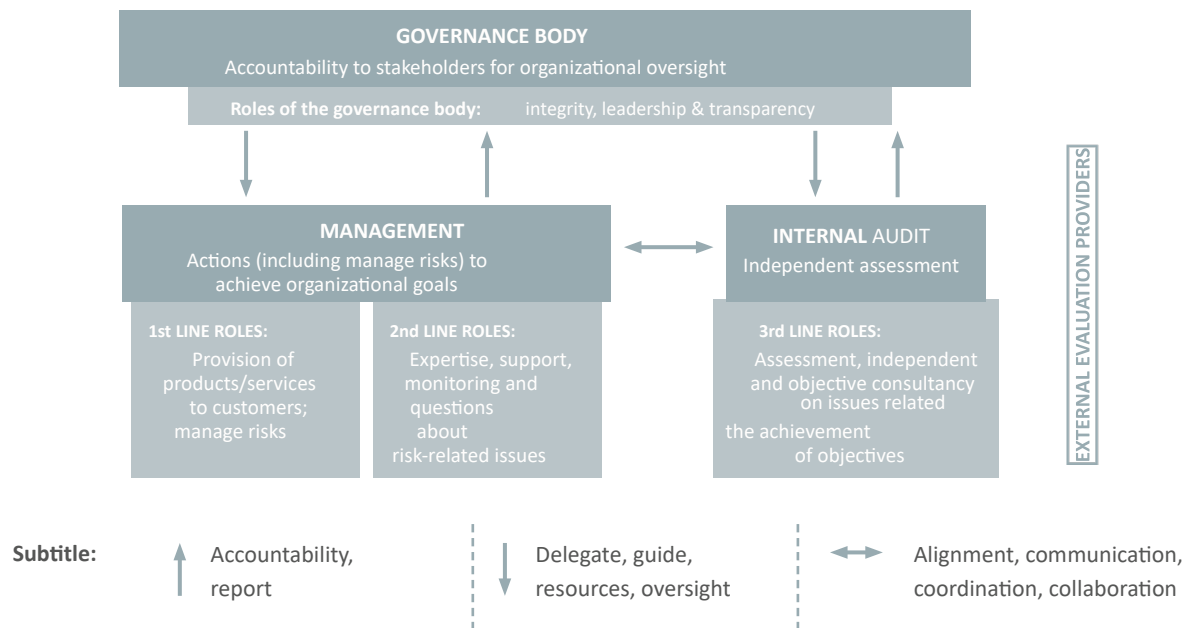
## 6. DEFINITIONS



## 6.1. RISK MANAGEMENT

The risk management model adopted by Santos Brasil is built on the three-line defense concept, in which each entity of the organization has defined roles in their risk management process, as illustrated below.

### IIA THREE-LINE MODEL



**Source:** Institute of Internal Auditors (IIA) Position Statement - the three lines of defense in effective risk management and controls (January 2013).

**Governance Body:** It is composed of Santos Brasil's management, ensuring that structures and processes are in line with effective corporate governance and that organizational objectives and activities are consistent with the prioritized interests of stakeholders.

**1st Line of Defense: Duties/areas that manage and hold ownership over risks** – It is composed of the operational management control level, responsible for maintaining effective internal controls and for routinely conducting procedures to manage its risks and controls.

As a first line of defense, the managerial areas (business/support) are liable for managing the risks related to their processes, and in charge of implementing corrective measures to respond to these risks.

**2nd Line of Defense: Duties/areas that oversee risks** - represented by support areas, these are responsible for setting out risk management and compliance policies and/or procedures for the development and/or monitoring of first-line defense controls.

**3rd Line of Defense: Duties that provide independent analysis/assessments** - The Internal Audit is liable for the independent review of risk management, supporting the organization in achieving its objectives and presenting a systematic and disciplined approach to evaluating and enhancing the effectiveness of risk management, controls, and governance processes. The employees of the Internal



Audit Area provide the Board of Directors through the Audit Committee and directly to this Committee, with assessments based on a high degree of independence and objectivity within Santos Brasil.

Control activities shall be constantly assessed, taking as a reference the good practices established by the COSO (Committee of Sponsoring Organization of Tradeway Commission) standards.

### 6.2. RISK MAPPING

The purpose of this stage is to identify the risks to which Santos Brasil is exposed and which could affect its strategy, objectives, and/or operations. To support this process, Santos Brasil relies on biannual support from an external consultancy, so that the model adopted internally is in line with good market practices and adopts an unbiased analysis.

The mapping of these risks can take place through various activities conducted at the most diverse levels of the organization, such as meetings of understanding with various levels of the Company's professionals, Compliance and internal and external audits, management or process evaluations, due diligence, significant external changes such as changes/entry of applicable legal/regulatory requirements; changes in or new compliance obligations (including integrity), mergers and acquisitions (if applicable), strategic changes in the Organization; significant non-compliance results, among others. At this stage we can also consider internal factors (people, processes, technology, etc.) and external factors (economic, political, social, environmental, etc).

Santos Brasil has categorized its risks into the following categories set out in its Corporate Risk Portfolio:

**Compliance:** risk of losses and sanctions due to failure to comply with regulations, compliance obligations and legislation that may cause or cause damage to the Company's reputation and image. This category also includes accounting failures in terms of recording and publishing accounting information.

**Strategic:** risk of loss resulting from the failure of the strategies adopted, considering the dynamics of business and competition, political and economic changes in the country and abroad, as well as environmental, social and governance issues.

**Operational:** risk of loss resulting from failures in our processes and operations, contracts, information technology, the environment and related to our People and Management processes.

**Financial** risk of losses resulting from market fluctuations that impact the organization's assets, as well as risks related to the creditworthiness of customers and paying sources and the Company's liquidity in relation to its financial obligations.

If any new potential risks and/or factors are identified, these shall be reported to the Corporate Risks role performed by the Compliance Area by e-mail, at [compliance@santosbrasil.com.br](mailto:compliance@santosbrasil.com.br), so that due treatment is provided.

In addition, the results of the Internal Audit and Independent Audit work will periodically be reported to the Compliance area, so that together they can serve as a basis for new risks and/or factors.

New factors will be included in the Risk Map and will be forwarded to the business area for analysis, while the new risks will be included in the next revision of the Strategy Map.

### 6.3. RISK CLASSIFICATION

Risks and risk factors related to Santos Brasil's strategic objectives are identified and prioritized to ensure that any materialization that may occur is known in advance and managed at an acceptable level.



The risks identified by the Corporate Risks role performed by the Compliance Area, supported by external consultancy and through meetings, are analyzed in relation to their impact of materialization and probability of occurrence, resulting in each risk's exposure level.

The impact analysis considers qualitative and quantitative criteria, such as Financial, Operations, Compliance, Image & Reputation, Continuity & Sustainability, Health & Safety, Environment & Community. The analysis of the probability of occurrence is measured based on the recurrence of risks materialization and the reliability of their mitigating actions.

It shall be incumbent upon the Risk Owners to carry out the impact and probability analyses. The result of this assessment, as well as the risk classification criteria, are represented by the Risk Matrix and Risk Map.

All areas of Santos Brasil shall, as standard, adopt the corporate risk management methodology outlined herein, and the use of parallel methodologies is prohibited.

#### 6.4. TREATMENT OF MAPPED RISKS

This stage requires management to define a response to the risks identified to bring exposure to a certain risk to an acceptable level for the organization, which can vary according to Santos Brasil's risk appetite.

You can choose between four responses to risk: avoid, reduce, share, or accept.

**Avoid:** the strategy/operation/activity that generates the risk factor shall be discontinued.

**Reduce:** reduce the impact and probability of materialization of the risk to the maximum and/or up to the level of risk appetite acceptable to the Company.

**Share:** the Company shall look for ways to share the impact of the total or partial risk considering the scenario of its materialization.

**Accept:** no action is taken and the Company assumes this risk, leaving the option of only monitoring the factor.

#### 6.5. RISK-TAKING SCOPE

The process involves the Risk Owner, Compliance Committee and Board of Directors accepting the level of exposure to a risk, considering any potential justifications for this (such as the unfeasibility of implementing mitigating actions) and thus accepting the potential consequences of this situation in the future.

All risk-taking processes shall be sent to the Audit Committee's previous acknowledgment.

CRITICALITY OF THE RISK	ASSUMPTION OF RESPONSIBILITY
Critical and meaningful	Board of Directors
Moderate	Compliance Committee
Low	Risk Owner
Minimum	

#### 6.6. MONITORING AND CRITICAL ANALYSIS

When the action plan is defined by the "Risk Owner", it shall be monitored and reported monthly to the Compliance and Audit areas liable for the Internal Controls and on demand to the Committees and/or Boards.



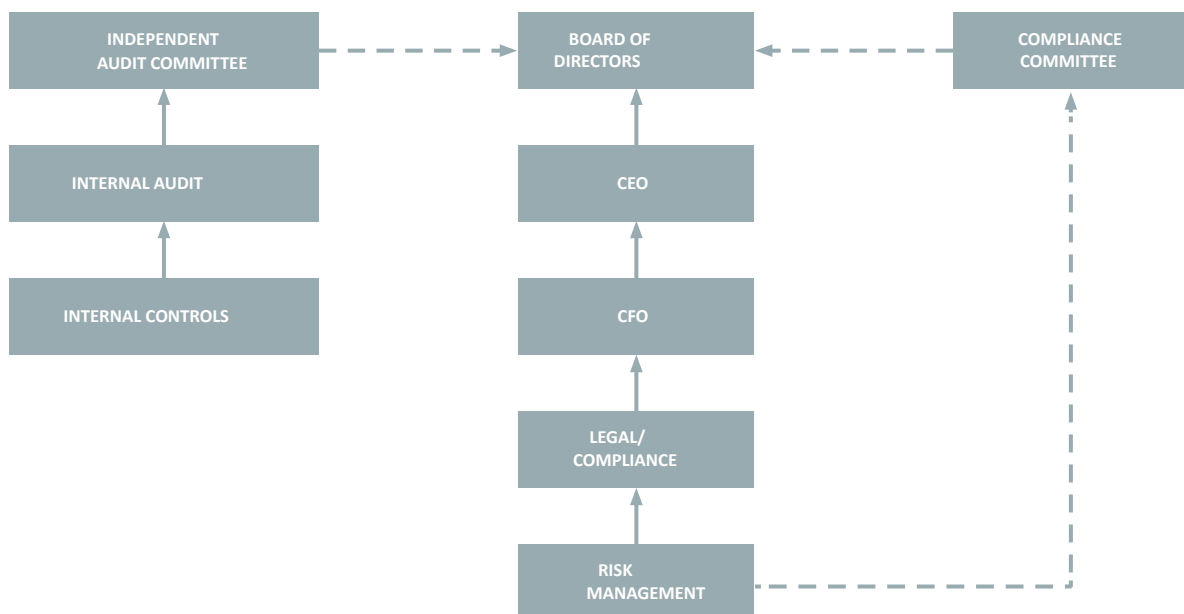
The plans may have a long-term implementation approach, similar to the fulfillment of strategic planning. It is therefore necessary to reach conclusions in phases for long-term actions.

The final deadline for implementing the action plan shall be agreed between the Risk Owners and the Compliance and Internal Audit areas, liable for the Internal Controls. Any postponement of the deadline shall only be accepted at the Risk Owners' request. The new deadline shall have to be agreed with the Compliance and Internal Audit areas.

## 6.7. COMMUNICATION AND CULTURE OF RISKS

Santos Brasil shall continuously disseminate information about the development of all phases of the risk management process to its employees. It is, therefore, the responsibility of everyone to provide, share and obtain information that contributes to the acculturation of the corporate environment in the field of corporate risks.

## 6.8. CORPORATE RISK MANAGEMENT STRUCTURE



## 7. RESPONSIBILITIES AND DUTIES

### 7.1 . BOARD OF DIRECTORS

Approve the Corporate Risk Management Policy, as well as any amendments arising from revisions;

- Agree with the Assumption of Responsibility process for significant and critical risks;
- Approve Santos Brasil's risk management, internal controls, and internal audit duties;
- Ensure the authority, autonomy, independence and responsibility of the Risk Management, Internal Controls, and Internal Audit duties;

Ensure the allocation of adequate financial and non-financial resources to enable the Compliance Area to perform its risk role and

- the Internal Audit to perform its internal controls and audit roles properly, annually reassessing the sufficiency and adequacy of the budget and resources allocated; Support the dissemination of the risk management, controls, and audit culture at Santos Brasil.





## 7.2 ■ . AUDIT COMMITTEE

Oversee the performance and results of Santos Brasil's Corporate Risk Management, Internal Controls, and Internal Audit duties process;

- Annually approve the Internal Controls and Audit work plan;
- Report on internal audit activities, corporate risks, and internal controls to the Board of Directors;
- Analyze the annual independent assessments of the Risk Management process in line with the opinions of the Internal and External Audit and report the results and action plans to the Board of Directors;
- Support the dissemination of the risk management, controls, and audit culture at Santos Brasil;
- Assess, monitor, and recommend to management the correction or improvement of the Internal Controls Policy, as well as any revisions.

## 7.3 ■ . COMPLIANCE COMMITTEE

Assess, monitor, and recommend to management the correction or improvement of the Corporate Risk Policy, as well as any

- revisions, submitting it to the Board of Directors' approval;

Monitor the performance and results of Santos Brasil's Corporate Risk Management, Internal Controls, and Internal Audit duties;

- Approve Assumption of Responsibility processes for risks mapped as moderate;
- Receive reports from the Compliance Area liable for the Corporate Risk Management to periodically assess the corporate risk matrix and mitigation actions established;

Annually approve the Corporate Risk Management work plan;

- Present to the Board of Directors matters considered relevant to the effective monitoring of corporate risks;
- Validate the risk maps and their respective degrees of impact and probability of the risks incurred by Santos;
- Assess and decide on eventual conflicts of interest in the Risk Management process; Support the
- dissemination of the Risk Management, Controls, and Internal Audit culture.

## 7.4 ■ . BOARD OF EXECUTIVE OFFICERS

Participate in the Corporate Risk Management process (observing the duties, methodology, processes, among others) and ensure

- that it is aligned with Santos Brasil's practices and good market practices;

Inform the Compliance Area liable for the Corporate Risk Management whenever there are updates to strategic planning or the

- occurrence of relevant facts;

Ensure sufficient resources for the implementation of effective internal controls and corporate risk mitigation strategies;

- Support the dissemination of the Risk Management, Controls, and Internal Audit culture;
- Ensure the execution of the Corporate Risk Management work plan;
- Get to know the impact and probability ruler (risk appetite);
-



Participate in the process of building and updating the corporate risk portfolio;

- Contribute to the risk assessment, according to the established impact and probability criteria;
- Support the definition of corporate Risk Owners;
- Approve the portfolio and indicate the risks to be prioritized;
- Approve risk responses (to avoid, reduce, share, or accept);
- Promote evaluation cycles and reviews of the risk management process (through internal or external agents) on an annual basis, to
- ensure the effectiveness and independence of the process;

Communicate unidentified risks, whether new or not, to the risk management role as soon as possible.

## 7.5 • CORPORATE RISK MANAGEMENT

Develop, suggest, and review guidelines for Santos Brasil's corporate risk management process (methodology, processes, systems, standards and reporting mechanisms, and others);

- Draw up and keep up to date the Corporate Risk Management Policy;
- Draw up and execute the work plan, including budget, resources (human and technological) and deadlines, so that to make feasible
- the effective execution of the Corporate Risk Management process;

Promote the interface between the risk management process and update the business strategy;

- Annually review the criteria defined for the Impact and Probability Ruler and propose changes when significant changes occur;
- Promote communication of the Corporate Risk Management process;
- Provide methodological support for Risk Management to the areas of Santos Brasil;
- Elaborate a conceptual and methodological training plan to be applied to all agents involved in the risk management process, as
- well as to other employees;

- Coordinate and monitor the process of identifying and assessing corporate risks with Santos Brasil's executive and operational management, including those related to social and environmental aspects;

Assist in the definition of Risk Owners;

- Support the Risk Owner in defining the action and contingency plan, as well as in defining indicators (KRIs) and risk exposure levels;
- Monitor the implementation of action plans, as well as any deadline extensions;

- Receive and consolidate any changes in the criticality of corporate risks and report them to the Executive Board, Compliance
- 

Committee, Audit Committee, and the Board of Directors;

- Monitor and consolidate the status of the action plans and risk indicators (KRIs) sent by the Risk Owners and issue periodic reports to the Executive Board, the Compliance Committee, the Audit Committee, and the Board of Directors;

- Propose a review of the risk portfolio whenever there are updates to the strategic plan, within two years, whenever material changes occur in circumstances or in the context of the organization or, lastly, at shorter intervals if necessary;



Disseminate the Risk Management culture throughout Santos Brasil, ensuring that all areas have access to and can consider the

- objectives of corporate risk management;

Submit the corporate risk matrix and mitigating actions to the Compliance Committee on a regular basis.

## 7.6 ■ . CORPORATE RISK OWNERS

Be the facilitator or appoint someone from your business area (if applicable), who has the technical expertise of corporate risk and

- will be primarily responsible for updating the mapping information, initiative effectiveness and internal direction of action plans;

Draw up, suggest, and implement action and/or contingency plans to mitigate risks (with the involvement of other areas, if

- necessary);

Define risk indicators (KRIs) to monitor the variation and results of the corporate risks under his responsibility;

- Periodically review the technical detail of the risk, its factors, the risk assessment (impact and probability) and the response to the
- risk, considering changes to the mitigating actions and existing controls (considering the results of the process assessments) related to the risk and completion of the implementation of the action and contingency plans;

Record the data relating to the action plans and the results of the corporate risk monitoring indicators (KRIs);

- Issue regular reports to the Compliance Area liable for the Risk Management and the Internal Audit Area liable for the Internal
- Controls, on the monitoring of the risk under their responsibility (significant changes in the probability and/or impact of the risk or in any other characteristic and if they identify unmapped risks).

Disseminate the culture of Risk Management;

- Approve the Assumption of Responsibility process for low and minimal risks.

## 7.7 ■ . INTERNAL CONTROLS MANAGEMENT

Draw up the Controls Matrix;

- Support areas in risk self-assessment (CSA - Control Self-Assessment);
- Analyze, Evaluate, Test and Control the operation of existing controls aiming at ensuring that they are effective in mitigating
- identified risks;

Issue periodic internal control reports, in accordance with current legislation;

- Support the Audit Committee in promoting ethical standards, integrity, and an organizational culture that evidence to all employees the importance of internal controls and the role of each one in the process.

## 7.8 ■ . INTERNAL AUDIT

Carry out the actions and duties provided for in this Policy for the Audit Area;

- Monitor the activities of the Internal Controls Area maintained by Santos Brasil's operational and support units;
-



Measure the quality and effectiveness of the Company's risk management, control and governance processes and to promote an

- independent evaluation of the activities carried out by Santos Brasil's areas, so that to allow the Board of Directors to analyze the adequacy of controls, the effectiveness of risk management, governance processes, the efficiency of the controls supporting the issue of financial statements and compliance with rules and regulations;

Monitor the implementation of action plans, as well as any deadline extensions;

- Report its activities to the Board of Directors, through the Audit Committee;
- Set out the planning of Internal Audit activities to be shared and reviewed by the Audit Committee, as well as share the most
- relevant results of the work executed for acknowledgment and any suggestions for improving internal controls;

Submit the Internal Audit work plan annually for approval by the Audit Committee and the Board of Directors' acknowledgment.

### 8. FINAL PROVISIONS

Any breach of the provisions herein may represent serious misconduct in relation to the link or relationship that any of its members have with the Company, besides characterizing a civil and/or criminal unlawful act.

This Policy may only be amended by decision of the Company's Board of Directors. Cases not covered by this Policy shall be decided by the Board of Directors.

This Policy shall be reviewed on an ongoing basis, either to ensure the continuous improvement of corporate governance practices or due to statutory, legislative, or regulatory changes, and shall be reviewed, approved, and recorded in the minutes of the Board of Directors. Any review of this policy shall be communicated to addressees, with a copy of the latest version approved by the Board of Directors being sent concurrently.

### 9. RECORDS

IDENTIFICATION	STORAGE	PROTECTION	RETRIEVAL	RETENTION	PROVISION
Strategic/Corporate Risk Management Policy	Electronic means	Cloud storage	Record retrieval path	Not determined	Not applicable



[www.santosbrasil.com.br](http://www.santosbrasil.com.br)