RISK MANAGEMENT AND INTERNAL CONTROLS POLICY

Year - 2022

1. GENERAL PROVISIONS

Reviewed at the 21st Extraordinary Meeting of the Board of Directors, held on December 7th, 2022 (Version 5).

2. INTRODUCTION

Sanepar stresses and establishes governance rules and general guidelines for its integrated corporate risk management and internal controls process to reiterate its commitment to a culture of integrity in which risks are assessed and used as a decision-making instrument to help the Company understand the scenarios in which it operates and the impact it has on stakeholders. This helps the Company achieve its strategic goals in its constant search for improvement and through an ever-increasing adherence to the principles of good governance and social and financial sustainability to preserve and generate value.

3. PURPOSES

Incorporate the risk management and internal controls vision and practice into Sanepar's decision-making process. Establish principles, guidelines, rules, responsibilities and concepts to enable the identification, assessment, treatment, monitoring and communication of risks and internal controls in the Company's processes.

4. SCOPE

This Policy is prepared and based on the Company's Management and applies to all employees, managers, governance agents, third parties, partner institutions and all parties related to Sanepar.

5. DEFINITIONS

Key terms referenced in this corporate policy include:

I. **First Line**: Performance level where the objects of the processes foreseen and mapped by the Company are carried out and the respective controls applied;

II. **Second Line**: The various corporate roles that check the effectiveness of internal controls, risk management and compliance supervision related to the first line;

III. **Third Line**: The independent assessment carried out by the Internal Audit that checks the adherence and effectiveness of the controls and processes on the second and first lines;

IV. **Mitigation Action**: Measure adopted by the Company to reduce its exposure to risk, seeking to mitigate the possibility of risk materialization;

V. **Focal of Process**: Employees appointed by their managers to support internal control activities of the processes;

VI. **Risk Appetite**: Maximum level of risk impact exposure for triggering risk governance;

VII. **Evaluation of internal control systems**: Assessment of the business process that allows identifying risks and the internal controls necessary to mitigate them;

VIII. **Internal Control:** A process conducted by the organization's governance structure, management and other professionals, designed to provide reasonable assurance with respect to the achievement of objectives related to operations, disclosure, and compliance;

IX. **COSO:** (Committee of Sponsoring Organizations of the Treadway Commission) A private, non-profit institution that aims to provide documents and/or financial reports with the highest possible level of accuracy, therefore applying principles such as organizational ethics, transparency, internal controls, risk management and corporate governance. This Committee established the methodologies known as COSO ERM (Enterprise Risk Management), a market reference in the subject, and COSO IF (Internal Controls/Integrated Framework);

X. **Cost-Benefit:** It consists of reducing the risk of failures in terms of meeting objectives and goals of an activity based on the concept that costs should not exceed the benefits provided;

XI. **Risk Owner:** The Company's chief executive officer who will have the role and treat the corporate risks assigned to him;

XII. **Risk Facilitator:** Professionals appointed by Risk Owners to advise them on their roles and activities related to corporate risks;

XIII. **Risk Factor:** An isolated or combined condition that may increase the probability of risk materialization;

XIV. **Board Focal of Process:** Professionals appointed by their officers to act in the evaluation of internal control systems of the board processes;

XV. **Risk Impact:** The qualitative and/or quantitative analysis of risk materialization effects on the Company;

XVI. **Risk Indicator:** A metric used to monitor and assess the variation of corporate risks mapped from data obtained in the Company's internal and external environment;

XVII. **Risk Matrix:** A graphic representation of the exposure to corporate risks identified by Sanepar according to the criticality of each risk, which is established by assessing its impact versus its probability;

XVIII. **Risk Profile:** The Company's willingness to incur risks. Examples of risk profiles: conservative, moderate, and aggressive;

XIX. **Integrated Risk Management Planning:** A document prepared by the risk management and internal controls area containing the periodic planning of activities to be performed, reported and presented, deadlines, the necessary resources, and the people in charge;

XX. **Risk Portfolio**: A catalog presenting the characteristics and information of each risk, such as description of the risk and its factor(s), criticality of gross and residual risks, existing mitigation actions, risk response(s) and action and contingency plans, if applicable;

XXI. **PYIP:** Pluri-annual Investment Plan;

XXII. **Risk Response:** Definition of how the Company will treat the residual risk. As a response, it can choose to avoid, reduce, share, or accept the risk;

XXIII. **Risk:** It is the uncertainty about the possibility of losses or gains in the course of events related to the Company's strategic objectives;

XXIV. **Corporate Risk:** Risks that may interrupt the achievement of objectives and the execution of the planned strategy;

XXV. **Gross Risk:** It is the probability and impact of a risk event before any control measures are implemented;

XXVI. **Residual Risk:** The risks remaining after the adoption of measures to mitigate the probability assessments and the impact of gross risks materialization;

XXVII. **Segregation of Duties:** Prohibition to the appointment of the same person to work simultaneously in roles more susceptible to risks, seeking to reduce the possibility of error masking and fraud in the respective processes;

XXVIII. **Risk Tolerance:** A percentage of the risk appetite established by the Company that, when reached, calls upon the governance for risk management;

XXIX. **Risk Materialization:** It occurs when a risk, whether subject to control and treatment or not, materializes in an event or fact and impacting the Company's goals, continuity, feasibility or business sustainability.

6 REVISION

This policy must be reviewed every two years, at any time upon regulatory or market request or as required by the Risk Management Committee, the Executive Board, the Audit Committee or the Board of Directors.

Changes made to this document must be forwarded for approval by the governance bodies mentioned above.

7 GUIDELINES

I. To disseminate, within the scope of the Integrity Program, the need for risk management and internal controls among employees to internalize this culture during the development and performance of activities and routines of the Company's processes;

II. To adopt rules of structures and mechanisms to encompass managers' and employees' actions through the daily implementation of internal control practices in accordance with Article 9, Item I, of Law 13303/2016;

III. To ensure that the area responsible for verifying compliance with obligations and risk management and corporate internal controls (Second Line) is in line with the provisions of Paragraph 2, Article 9, of Law 13303/2016;

IV. To ensure compliance with rules and regulations and adherence to internal policies and procedures;

V. To establish internal controls for the Company's risks, goals, and strategic planning;

VI. To ensure the application of the Segregation of Duties principle to avoid conflicts of interest and fraud;

VII. To present the report to the governance agents through periodic reports of critical analysis and monitoring of the Company's risks and controls;

VIII. To adopt the line approach, which includes integrated action between: (i) process management, (ii) internal controls, risk management and compliance and (iii) Internal Audit;

IX. To ensure that the process management in the First Line is responsible for implementing actions that ensure compliance with its processes and adequate risk management and respective controls;

X. To ensure that the Second Line assists and monitors the first line in fulfilling its responsibilities toward effective risk management, internal controls and process compliance;

XI. To ensure that the Third Line provides the governance bodies with assessments of the effectiveness of processes in relation to risk management and internal controls;

XII. To encourage the presence of risk management in all management, planning, Internal Controls and Internal Audit processes, thus promoting the early identification of risks and their timely management;

XIII. To ensure that the risks identified are assessed, classified, prioritized, and their responses defined;

XIV. To ensure the promotion of continuous improvement of the risk management process and internal controls through assessments and reviews cycles to ensure the effectiveness of risk management and monitoring; and

XV. To ensure that all process management areas provide all the information necessary, in a timely manner, for the work carried out by the Risk Governance and Compliance area.

8 RISK MANAGEMENT PROCESS

Risk management activities will be based on good Corporate Governance practices established by the standards and methodology of the Committee of Sponsoring Organizations of the Treadway Commission – COSO and make up the second pillar, Risk Analysis and Control Environment, of Sanepar's Integrity Program.

The Risk Management Process is conducted to ensure, with reasonable certainty, that the Company's objectives are achieved in its strategic and operating aspects:

I. In the identification and mapping of corporate risks that may affect the achievement of the Company's strategic objectives. The starting point is the strategic planning that subsidizes the capture of these risks to allow the assessment of their criticality (impact and probability), the identification of existing mitigation actions, internal controls, definition of new treatment actions, monitoring and reporting;

II. The information above must be recorded in a risk portfolio, reviewed every year, considering the course of events related to the strategic objectives and the change in impact worsening or risk probability;

III. Continuous monitoring of prioritized corporate risks uses indicators that must be evaluated monthly by the Risk Management Committee, quarterly by the Executive Board, Audit Committee and Board of Directors, or at any time in relevant cases; and

IV. To promote process mapping and evaluation of internal control systems by preparing flowcharts, risk matrixes, internal controls, control testing, delivering handling plans to mitigate risks with reasonable certainty, and improve process efficiency.

8.1 Exposure Limits

The Company considers the risk exposure limits (appetite and tolerance) established within the conservative profile[1], which are established according to the nature of each risk.

8.1.1 Corporate Risks

a) The appetite for this type of risk is measured in financial value and represents the maximum impact, over a one-year horizon, that the Company is willing to assume to achieve its objectives;

b) The appetite must be calculated according to an established methodology, consisting of two (2) approaches: the *quantitative*, in which the accepted deviation resulting from the materialization of risks is calculated, and the *qualitative*, in which the value defined in the first approach is weighted by means of the analysis of the Company from the perspective of variation in relevant indicators, the capital structure, control environment, reputation, and compliance;

c) Tolerance is a percentage of the established risk appetite that, when reached, calls upon the Governance for risk management;

d) Appetite and tolerance must be updated annually or when relevant facts occur; and

e) If the sum of the financial impacts estimated for the prioritized corporate risks exceeds the defined tolerance, Governance must be called upon to reassess the existing mitigation plan.

[1] Conservative profile, considering (i) the type of Business, where the Company has Agreements with the municipalities, in accordance with what was disclosed in the 2Q2022 - 75% of the revenue arises from agreements with maturity after 2033; (ii) Debt Profile with low leverage within the covenants metrics; (iii) Contracting of hedge against foreign exchange exposure; (iv) That it has a Risk, Treasury, and Market Management Policy.

[1] Financial risks are addressed in the Risk, Treasury, and Market Management Policy, available on Sanepar's Investor Relations Portal.

8.1.2 Operational Risks

a) The appetite for operational risks is established based on the criticality of the risks identified in the assessment of the processes internal control system;

b) For risks assessed as “Significant” and “Critical”, it is mandatory to establish handling plans to mitigate the materialization probability and impact;

c) For risks assessed as “Moderate”, it is advisable to draw up handling and monitoring plans for existing actions and controls to maintain or reduce this level;

d) For risks assessed as “Low”, existing actions and controls must be maintained and monitored to maintain this level; and

e) For the Compliance risks identified in the assessment of the processes, there must be defined action plans, regardless of their criticality, in order to mitigate them. Other exceptions must be discussed by the Executive Board and approved by the Board of Directors.

9 STRUCTURE

a) The area responsible for verifying the compliance with obligations and managing corporate risks and internal controls (Second Line), must be subordinated to the CEO and led by an officer. The Internal Regulations of the Executive Board must define the duties of the area and establish structures and mechanisms that ensure independent action, as established in paragraph 2 of article 9 of Law No. 13303/2016.

b) The Governance, Risks, and Compliance Deputy Board is responsible for ensuring the enforcement of this policy. To this end, managers of processes affected by risks must provide, in a timely manner, all the information necessary for the development of the work carried out.

c) The budget and structure of the Risk Management and Internal Controls processes must be analyzed by the Internal Audit to certify whether they are suitable for the activities and size of the Company.

10 RESPONSIBILITIES

10.1 Board of Directors

a) To approve guidelines for Sanepar's integrated risk management and internal controls process (methodology, processes, systems, policy, standards, and reporting mechanisms, among others);

b) To approve risk appetite and tolerance;

c) To approve prioritized corporate risks and their respective response and contingency plans;

d) Periodically, to assess the corporate risks portfolio and their mitigating actions;

e) To monitor the results of risk management and internal controls processes by means of executive reports;

f) To evaluate and validate the internal controls and risk management framework established to ensure the handling of risks; and

g) To approve the risk management work plan.

10.2 Audit Committee

a) To advise the Board of Directors on the approval of corporate risks to be prioritized and their respective mitigation and contingency plans, as well as changes in the assessment of risks criticality, risk appetite, and the definition of guidelines and policies for the process of risk management integrated with internal controls;

b) To advise the Board of Directors on the analysis of the annual independent assessments relating to risk management and internal controls processes;

c) To monitor the results, action and contingency plans of risk management and internal controls processes and report any recommendations to the Board of Directors; and

d) To monitor the quality and integrity of risk management mechanisms and internal controls.

10.3 Executive Board

a) To promote Sanepar's risk management and internal controls process (methodology, processes, systems, policy, standards, and reporting mechanisms, among others) and ensure that they are aligned with good management practices, including the Company's strategic planning;

b) To ensure the enforcement of guidelines and compliance with the risk management and internal controls procedures;

c) To decide on the risk management and internal controls procedures and their updates;

d) To review and validate the risk appetite and tolerance value;

e) To assess the risk management work plan and submit it for approval by the Board of Directors;

f) To review and approve the corporate risk portfolio;

g) To monitor and manage all corporate risks in the portfolio;

h) To define risk owners;

i) To analyze the action plans suggested by the risk owners and approve any postponement of deadlines;

j) To submit to the Board of Directors, for approval, the prioritized corporate risks and their respective action and contingency plans;

k) To decide on the results of the risk management processes and internal controls;

l) To indicate the need for independent assessments of the risk management process and internal controls (internal or external agents), so as to ensure their effectiveness;

m) To ensure the continuous development of professionals working in the Company’s risk management and internal controls;

n) To ensure the autonomy of Sanepar's internal controls agents in the exercise of their activities, guaranteeing access to documents, information systems, and people, as well as other elements necessary for the exercise of their activities;

o) To ensure the alignment among the business plan, strategic and investment planning, and Risk Management and Internal Control, aiming at the adequate handling of risks; and

p) To designate focal of process of the executive board, considering the appropriate skills and profile to perform the duties.

10.4 Risk Management Committee

a) To evaluate variations in the criticality of risks, and, when these are significant, report them to the Executive Board, the Audit Committee, and the Board of Directors;

b) To analyze, propose, and decide on guidelines and strategies for risk management processes and internal controls;

c) When necessary, to analyze and present points for improvement in the risk management process and internal controls (methodology, processes, systems, policy, standards, and reporting mechanisms, among others);

d) To support the Executive Board in defining risk appetite and tolerance;

e) To evaluate and decide on the risk management work plan for the executive board;

f) Monthly, to monitor the outcome of mitigation actions and risk indicators proposed for the handling of prioritized corporate risks;

g) On a quarterly basis, to monitor the outcome of assessments of the processes internal control systems;

h) To analyze and recommend necessary resources for the execution of risk management processes and internal controls;

i) To ensure compliance with the Risk Management and Internal Controls Policy;

j) To report on the Committee's activities when requested by the Executive Board, Audit Committee, and Board of Directors;

k) To analyze and make recommendations regarding the corporate risk portfolio and handling plans whenever there are updates;

l) To analyze and propose prioritization of corporate risks; and

m) To analyze and make recommendations regarding handling plans resulting from the assessments of the processes internal controls systems.

10.5 Risk Management and Internal Controls Area

a) To propose and review guidelines for Risk Management and Internal Control processes (methodology, processes, systems, policy, risk portfolio, standards, and reporting mechanisms, among others);

b) To disseminate knowledge about risk management and internal controls to employees to strengthen this culture in the Company;

c) To prepare and periodically review the risk management work plan;

d) To coordinate and monitor the corporate risk portfolio review process, as well as the evaluation of internal control systems;

e) To act together with the Executive Board, Audit Committee, and Board of Directors in the discussion on the definition of the Company's risk appetite and tolerance;

f) To monitor the alignment among the Business Plan, strategic and investment planning, and Risk Management and Internal Control, aiming at the adequate handling of risks;

g) To prepare, review, and update the risk portfolio whenever there are updates to the Company's Strategic Map or when relevant events occur;

h) To assist in defining risk owners;

i) To assist the owner and facilitator in defining risk indicators, treatment actions, and contingency plans;

j) To monitor changes in the criticality of corporate risks and report them to the Risk Management Committee and the Executive Board;

k) To prepare reports with the results of the risk management processes and internal controls;

l) To report the results to the Risk Committee monthly, and, quarterly, to the Executive Board, Audit Committee, and Board of Directors;

m) Ensure alignment between operational and corporate risks;

n) To monitor the implementation of handling plans resulting from the evaluation of internal control systems;

o) To assist managers, focal of process, and agents of internal controls in the development of the evaluation of internal control systems;

p) To ensure that recommendations related to risks and internal controls, coming from the Internal Audit, External Audit, Supervisory Bodies, and External Controllers, are incorporated into the mapping of processes and handling plans.

10.6 Corporate Risk Owners

These are professionals appointed by the Company to monitor and handle corporate risks.

a) To appoint the risk facilitator, considering the appropriate skills and profile for the roles and for assisting in the guarantees below;

b) To ensure the preparation of risk sheets and their updates, whenever necessary;

c) To develop indicators to monitor the changes and the results of the risk under their responsibility;

d) To ensure the implementation of actions necessary to mitigate risks, along with the involvement of other areas;

e) To monitor the monthly transfer of the necessary data and critical analysis to the Risk Management area, as well as the updating of the financial impact, for the preparation of risk reports;

f) To inform the Risk Management area of any significant changes in the probability and/or the risk impact or in any other characteristic, and, if identified, unmapped risks;

g) When required, to report to the governance bodies on the development of action plans to mitigate risks and contingency plans;

h) To promote systematic debates and discussions developed in its areas of operations and with its managers to ensure the effectiveness of the risk management and monitoring;

i) To carry out a technical review of the risk, its factors, the risk criticality (impact versus probability), considering changes in existing mitigation actions, completion of action and contingency plans; and

j) To identify and define responses to risks (avoid, mitigate, share, or accept).

10.7 Corporate Risk Facilitators

a) To support the Risk Owners in their duties and activities;

b) To provide information to the Risk Owners for technical review of the risk, its factors, the risk criticality (impact versus probability), and the response, considering changes in existing and proposed mitigation actions and contingency plan;

c) To prepare systematic reports for the Risk Owner to present to the Risk Management and Internal Controls Area and to the Risk Management Committee the monitoring of the risk under their responsibility;

d) To support the Risk Owner in the reporting to the Risk Management and Internal Controls area of any significant changes in the probability and/or the risk impact or in any other characteristic, and, if identified, unmapped risks;

e) To participate in periodic meetings held by the Risk Management and Internal Controls Area;

f) To act with the Risk Owner in the implementation of the actions necessary to mitigate the risks, ensuring the involvement and adequate deliveries of the intervening areas; and

g) To monitor and report to the Risk Owner, for validation, the results and critical analyzes of risk indicators, mitigation actions, and the updating of the financial impact, according to a schedule predetermined by the Risk Management and Internal Controls area.

10.8 Process Managers

To work with the Risk Owners and/or Corporate Risk Facilitators in implementing the actions necessary to mitigate these risks, ensuring their involvement and adequate deliveries as an intervening area;

a) To designate the focal of the process, considering the skills and profile appropriate for the performance of the duties;

b) To provide support and conditions for carrying out the evaluation of internal control systems related to the processes under their responsibility;

c) To validate the risk matrixes, internal controls, and the handling plan generated in the evaluation of internal control systems;

d) To implement handling plans to mitigate the risks included in the processes under their responsibility, always complying with the levels of authority and employing measures proportional to the risk, observing the cost-benefit ratio in order to add value to the Company; and

e) To communicate the risk management and internal controls area in the event of changes in the legislation or procedures, in the process in which it is inserted, aiming at corporate action.

10.9 Board Focal of Process

a) To act with process managers and focal of process, with support from the Risk Management and Internal Controls area, in carrying out the mapping and evaluation of internal control systems;

b) To align the strategic demands, relevant to its board, to the operational activities of internal controls in the company, based on the training received on the methodology to be applied; and

c) To participate in periodic meetings held by the Risk Management and Internal Controls Area.

10.10 Focal of Process

a) To support the process manager in his duties and responsibilities, reporting relevant facts regarding the internal control activities;

b) To implement or update internal controls and normative documents (including flowchart) in the event of changes in the legislation or procedures, in the process in which it is included, mitigating risks and ensuring Compliance;

c) To align the demands, relevant to its process, to the operational activities of internal controls in the company, based on the training received on the methodology to be applied;

d) To monitor and report to the manager, for validation, the results and critical analyzes to support the monitoring of the internal controls action plans; and

e) To participate, when necessary, in meetings held by the Risk Management and Internal Controls area.

11 ACCOUNTABILITY

Non-compliance with the responsibilities set forth in this Policy must be examined by the Risk Management and Internal Controls Area and submitted for analysis by the Risk Management Committee, which will submit it to the Executive Board for the adoption of measures to determine any possible responsibilities in accordance with the Disciplinary Regulation.

12 FINAL PROVISIONS

This Policy becomes effective on the date of its final approval by the Board of Directors.

13 REFERENCES

BRASIL (BRAZIL). Office of the President of the Republic Law No. 13303 of June 30, 2016, addresses the articles of association of state-owned companies, government-controlled companies, and their subsidiaries, in the Federal, State, Federal District, and Municipal levels. Brasília, Federal Official Gazette of July 1, 2016.

BRASIL (BRAZIL). CVM (Brazilian Securities and Exchange Commission). *Instrução Comissão de Valores Mobiliários 552 de 2014*.

_____. CVM (Brazilian Securities and Exchange Commission). *Instrução da Comissão de Valores Mobiliários 586 de 2017*.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. Internal Control – Integrated Framework. New York: AICPA, 1992.

_____. Committee of Sponsoring Organizations of the Treadway Commission – Internal Control - Integrated Framework. 2013.

Guide to the CICS Common Body of Knowledge (CBOK). Internal Control Institute, Edition III, v.1. 2017.

IIA. The IIA Research Foundation. *IIA DOCUMENTO DE EXPOSIÇÃO Três Linhas de Defesa*, 2019. Available at > https: //global.theiia.org/translations/PublicDocuments /3LOD-IIA-Exposure-Document-Portuguese.pdf> Accessed on July 23, 2020.

14 HISTORY

Risk Management and Internal Controls Policy		**Release**	5th	
Management Area		Governance, Risk, and Compliance Management		
Confidentiality		External Audience		
Release	**Date**	**Person in Charge**	**Approved by**	**Change Description**
1st	11/07/2017	Internal Control and Audit Management - GCIA	Board of Directors	First Issue
2nd	05/07/2019	Governance, Risk, and Compliance Management - GGRC	Board of Directors	Inclusion of reference Corporate Internal Control Policy
3rd	07/23/2020	Governance, Risks, and Compliance Deputy Board - DAGRC	Board of Directors	Change of structure and inclusion of the topic related to risk appetite
4th	08/12/2021	Governance, Risks, and Compliance Deputy Board - DAGRC	Board of Directors	Adjustment of internal control terminology and alignment with the Company's new articles of incorporation.
5th	12/07/2022	Governance, Risks, and Compliance Deputy Board - DAGRC	Board of Directors	Terminology adjustment and policy review for biannual.