PO-GN.01-002	*Edition* 7.0	*Duration* 06/20/2024
RISK MANAGEMENT AND INTERNAL CONTROLS	*Revalidation*	

ELABORATION:

Vice-Presidency of Governance, Risks, Compliance and Sustainability
Executive Risk Management Department
Internal Controls Management

REVIEW/SUPPORT:

Regulations Division
Corporate Governance Executive Management

APPROVAL:

Eletrobras Board of Executive Officers (BEO) - RES-308/2024, of 06/11/2024
Eletrobras Board of Directors (BOD) - DEL-114/2024, of 06/20/2024

TERM: 5 years

Summary

1 INTRODUCTION

1.1 OBJECTIVE

To establish principles, guidelines and responsibilities for guiding the processes of identification, assessment, treatment, monitoring and communication of risks and internal controls inherent to Eletrobras' activities, incorporating the vision of risks into its strategic planning and decision-making and the vision of internal controls into its processes, in compliance with applicable regulations and best market practices.

1.2 SCOPE

This policy applies to Eletrobras.

2 REFERENCES

2.1 Federal Law No. 12.846/2013 (Anti-Corruption Law) - Provides for the administrative and civil liability of legal entities for the practice of acts against the public administration, national or foreign, and makes other provisions.

2.2 Federal Decree No. 11.129/2022 - Regulates Law No. 12.846, of August 1, 2013, which provides for the administrative and civil liability of legal entities for the practice of acts against the public administration, national or foreign.

2.3 Foreign Corrupt Practices Act (FCPA), 1977.

2.4 Sarbanes-Oxley Act of 2002, with emphasis on sections 302 and 404.

2.5 CVM Instruction No. 480 of December 7, 2009 (with emends introduced *posteriori*) - Provides for the registration of issuers of securities admitted to trading on regulated securities markets.

2.6 COSO 2013 (Committee of Sponsoring Organizations of the Treadway Commission*)* - Internal Control - Integrated Framework.

2.7 COSO ERM 2017 (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management).

2.8 Code of Best Corporate Governance Practices of the Brazilian Institute of Corporate Governance - IBGC, 2023.

2.9 Corporate Governance Booklets - Corporate Risk Management - Evolution in Governance and Strategy - IBGC, 2017.

2.10 Standard ABNT NBR ISO 31000:2018 - Risk management - Guidelines.

2.11 IIA 2020 Three Lines Model (Institute of Internal Auditors).

3 CONCEPTUALIZATION

3.1 Risk appetite - Limit of exposure to risks that the company is willing to accept in order to achieve its strategic objectives and create value for shareholders.

3.2 Control owner - Organizational unit that has responsibility for internal control, including its adequacy, execution and documentation of evidence.

3.3 Risk owner - Organizational unit that has authority and responsibility for risk management.

3.4 Internal Controls - a set of actions and procedures to manage risks and increase the probability that the objectives and targets set by the company will be achieved.

3.5 Deficiency or "gap" in internal control - Absence or failure of control that does not allow the associated risk to be mitigated.

3.6 Eletrobras - Holding, its wholly owned subsidiaries and companies in which it has direct and indirect corporate control.

3.7 Risk event - An event or situation, generated by an internal or external source, which negatively affects, or has the potential to affect, the achievement of a company objective.

3.8 Integrated risk management and internal controls - Architecture implemented at Eletrobras for risk management and internal controls, under a common methodology and language, aligned with the other lines; integrated management, through a structured approach and a better understanding of the interrelationships between risks and internal controls, aligns strategy, processes, people, technology and knowledge, with the aim of preserving and creating value for the company and its shareholders.

3.9 Impact - The result of the materialization of a risk that affects the company's business, processes and operations, being expressed qualitatively and/or quantitatively.

3.10 Uncertainty - State, even if partial, of deficiency of information related to an event, its understanding, its knowledge, its consequence, or its probability, which can become a threat to the company.

3.11 Risk indicator - Measurement that, in conjunction with the assessment of the context, is used to evaluate how the risk behave itself and provide alerts regarding exposure or its potential for future loss.

3.12 Risk Matrix - A set of risk events identified by the company, described and classified into pillars and categories.

3.13 Three Lines Model - A set of principles and guidelines drawn up and published by IIA Global, The Institute of Internal Auditors, which aims to clarify and organize the responsibilities and roles of the organization's professionals in risk management and internal controls.

3.14 Probability - The chance of something happening, regardless of whether it is defined, measured, or determined objectively or subjectively, qualitatively or quantitatively.

3.15 Deficiency Remediation - Action plan documented by the area responsible for the deficiency with the aim of addressing the inconsistencies identified during internal and external audit tests.

3.16 Risk response - Action to reduce, maintain or avoid the company's exposure to risk by acting on the probability and/or impact, including, but not limited to, internal controls.

3.17 Risk - The negative effect of uncertainties on the company's objectives.

4 PRINCIPLES

4.1 Risk appetite statement

Creating value is essential for Eletrobras. Leadership in our market, through investments in generation, transmission and commercialization focused on clean energy, is part of our proposal for sustainable expansion. We do not tolerate decisions that could compromise profitability, financial discipline, corporate sustainability, ethical and compliance standards, the operational safety of our assets and the health and safety of our employees and outsourced workers.

We seek to be innovative, considering the relevance of investing in other segments, diversifying our portfolio of businesses and services, in synergy and in line with Eletrobras' strategy.

4.2 Generating value for Eletrobras

Eletrobras recognizes that integrated risk management and internal controls are directly related to the company's strategic guidelines of sustainable growth, profitability, and value creation, as they allow for the preventive identification of threats to business objectives, weaknesses in processes and risk-based decision-making.

4.3 Adoption of good corporate governance practices

Eletrobras adopts the best corporate governance practices, in terms of risk management, internal controls and anti-fraud and anti-corruption policies and practices, in a systematic, structured and timely manner, in order to improve and maintain the transparency and quality of its information, disclosed internally and externally, seeking a better reputation in the market and a differential in generating value for its shareholders and other stakeholders.

4.4 Definition of a common language between the holding company and its companies

The adoption of a standard language for risk management and internal controls is essential to the process, enabling better understanding between the parties and interference-free communication.

4.5 Use of standards and methodologies recognized by the market

With a model based on formalized methodologies and standards, recognized by the market and disseminated at Eletrobras, the integrated management of risks and internal controls is aligned with the strategies, initiatives and organizational structures, in addition to meeting the sector's requirements and those of the regulatory and inspection bodies. In order to support risk management and internal control activities, Eletrobras adopts, in an integrated manner, a single systemic solution that has functionalities for the assessment and continuous monitoring of the risks inherent to its businesses, as well as allowing for the self-assessment of design and effectiveness tests for internal controls, thus allowing for the reliability of information and security for the businesses in which Eletrobras operates.

4.6 Establishment of roles and responsibilities

Eletrobras formally defines and communicates the roles and responsibilities of each of the employees involved in the risk management and internal control processes.

4.7 Involvement of governance bodies

The work of the Eletrobras Board of Directors (BOD), the Audit and Risks Committee (ARC), the Fiscal Council (FC) and the Eletrobras Board of Executive Officers (BEO) plays a key role in the success of the risk management and internal control processes, since they are the main people involved in decision-making on strategic company issues.

4.8 Establishment and maintenance of the necessary infrastructure for integrated risk management and internal controls

To manage risks and internal controls efficiently, Eletrobras has an adequate and integrated infrastructure of processes, people and technology, establishing clear and objective communication mechanisms.

4.9 Integration of risk management and internal controls into organizational processes

Integrated risk management and internal controls permeate Eletrobras' organizational practices and processes, so as to:

a) ensure the identification of risk events inherent and residual to its business

areas, whether individual or corporate in scope; and

b) ensure the effectiveness of its processes by periodically mapping, self-assessing and testing the effectiveness of internal controls.

4.10 Periodic analysis of risk management and internal controls at Eletrobras

The areas of risk management and internal controls play a critical role for Eletrobras and must ensure the effectiveness of risk management and internal controls through frequent reviews, favoring the fulfillment of its objectives. Eletrobras assesses its maturity in risk management, using a model adapted from the Corporate Governance Booklets - Corporate Risk Management, by the Brazilian Institute of Corporate Governance (IBGC), and evaluates the control environment by testing the effectiveness of its internal controls.

4.11 Adoption of the Three Lines Model

Eletrobras adopts a risk management and internal control model based on the concepts of the Three Lines, which is:

a) First line: Vice-presidents, directors, managers and business areas, as well as project and process managers. This line is responsible for providing products/services to clients and managing risks and internal controls.

b) Second line: Risk and internal control areas. This line has expertise in risk management and internal control processes and is responsible for supporting, monitoring and questioning risk-related issues.

c) Third line: Internal Audit. This line conducts independent and objective assessment and advice on issues relating to the achievement of objectives.

5 GUIDELINES

In order to achieve the objectives, set out in this policy, Eletrobras must carry out the macro-steps of the risk management and internal control processes described in the sub-items below.

5.1 Identifying risks and mapping internal controls

5.1.1 Risk identification must recognize and describe the main risks to which Eletrobras is exposed, whether of a strategic or operational nature, including considering possible changes in its business environment.

5.1.2 For risks of a strategic nature, a corporate Risk Matrix must be defined with events, their respective descriptions, and the risk owners.

5.1.2.1 The identification of risks of a strategic nature must be conducted with the participation of the BEO and those responsible for the business areas.

5.1.3 For risks of an operational nature, inherent to Eletrobras' processes, internal controls must be mapped and designed to operate in accordance with the activities carried out by the management area, with the aim of guaranteeing operational efficiency, accurate reports and compliance with laws, regulations and policies in force.

5.1.3.1 The documentation of internal controls is a guideline and an essential tool for implementing independent tests, whose work role and planned activities are based on the controls described therein.

5.2 Assessment of risks and the internal control environment

5.2.1 In the case of risks of a strategic nature, once they have been identified, causes and consequences must be identified and qualitative and/or quantitative analyses carried out in order to define the attributes of impact and probability, which will be used to prioritize the risks to be dealt with.

5.2.1.1 When assessing strategic risks, consideration should also be given, including, to surveying and analyzing existing responses and internal controls, thus determining residual risks.

5.2.2 In the case of risks of an operational nature, the internal control environment must be periodically assessed by means of tests carried out by Administration, complementing in its scope the key controls, which must be determined based on their relevance to the results of the processes and the achievement of Eletrobras' objectives and targets.

5.2.2.1 Administration´s tests are aimed at assessing the effectiveness of controls and identifying any ineffective controls, as well as recommending improvements to improve the internal control environment.

5.2.2.2 The external auditor conducts independent tests in accordance with auditing standards and presents the results of his work in the form of an internal control report in connection with the financial statements.

5.3 Treatment of risks and remediation of internal control deficiencies

5.3.1 After the assessment, the BEO's positioning in relation to a strategic risk must be aligned with the risk appetite defined by the Board of Directors. The positioning options are:

a) Avoid - the company chooses not to start or continue in businesses, processes and activities that could generate risks or cause them to be exposed.

b) Live with/accept - the company believes that its exposure to the risk is in line with its appetite; or it believes that the effort to mitigate or transfer it would be greater than the value of the impact caused by its materialization; or, because the risk is of external origin but inherent in its activities, it has no way of reducing its exposure. Coexistence presupposes monitoring the company's exposure to risk.

c) Mitigate/transfer - the company seeks to minimize its exposure to risk, either by reducing the impact and/or probability with responses to risks and/or the design of internal controls, or by transferring/sharing the impacts of the risk with other agents.

5.3.1.1 If the position is to avoid, mitigate or transfer, Eletrobras must execute responses, including through internal controls, that pursue a risk exposure in line with the appetite approved by the Board of Directors.

5.3.2 Deficiencies identified in the internal control environment, whether through management testing or the Independent Auditor's assessment, must treated and remedied through specific action plans per deficiency.

5.3.2.2 Whenever deficiencies are formally identified, action plans must be created by the areas that own the controls, with the support of the internal controls area, to adapt ineffective controls and/or create necessary controls.

5.4 Monitoring risks and the internal control environment

5.4.1 In the monitoring process, one should:

a) supervise the implementation and maintenance of risk responses and action plans to remedy internal control deficiencies;

b) verify the achievement of response objectives and established remediation plans through ongoing management activities and/or independent assessments;

c) ensure that responses and remediation plans are assertive, effective and efficient;

d) detect changes in the external and internal context, identifying emerging risks; and

e) analyze changes in risk events, processes, trends, successes and failures, and learn from them.

5.4.1.1 In periodic assessments of strategic risks, the areas that own the risks should make an effort to additionally define metrics and/or proactive monitoring models, or even risk indicators, so that, where defined by the Board of Directors, the *status of* risk exposure can be monitored in a more specific format and detail in comparison to the limits and tolerances determined by the Board itself.

5.5 Communicating risks and internal controls

5.5.1 Communication, during all stages of the risk management and internal control processes, must reach all interested parties, being carried out in a clear and objective manner, respecting the good governance practices required by the market.

6 RESPONSIBILITIES

6.1 Board of Directors (BOD)

6.1.1 Ratify the approval of this policy.

6.1.2 Approve the reporting schedule, as well as its revisions, on the proposal of the BEO and the opinion of the ARC.

6.1.3 Determine the risk appetite, with a proposal from the BEO and the ARC opinion.

6.1.4 Supervise the risk management and internal control processes, through regular reports from the BEO, evaluated by the ARC, with a focus on the assertiveness of the process, the responses to risks and the results of internal control tests.

6.2 Audit and Risk Committee (ARC)

6.2.1 Monitor risk management and internal control processes, bringing the most relevant findings to the attention of the BOD.

6.2.2 Analyze all the material submitted to the BD on the company's risk management and internal controls, giving its prior opinion.

6.3 Fiscal Council (FC)

6.3.1 Contribute to the issues, including in its minutes any additional information it deems necessary or useful for the risk management and internal control processes.

6.4 Board of Executive Officers (BEO)

6.4.1 Evaluate the assertiveness of the risk management and internal control processes through periodic reports, discussing and validating, at the collegiate level or by vice-presidency, the evaluations presented by the proprietary risk areas and defining the positioning in relation to the risks, in accordance with the appetite approved by the Board of Directors.

6.4.2 Periodically monitor the results of the tests of controls executed by internal and external audits.

6.4.3 Ensure the implementation of risk management and internal controls in companies, allocating the necessary resources to the process and defining the appropriate infrastructure for the activities.

6.4.4 Approve specific rules on risk management and internal control processes.

6.4.5 Approve the corporate Risk Matrix.

6.4.6 Define proprietary risk areas.

6.4.7 Evaluate the deficiencies reported by internal and external audits, according to their degree of criticality.

6.4.8 Approve the Risk Management and Internal Controls Policy, propose the risk appetite and the schedule for risk and internal controls reports, as well as their reviews, forwarding them to the ARC for its opinion and, subsequently, to the BoD for approval.

6.5 Risk management and internal control areas

6.5.1 Acting as a second line, coordinating and defining the standards to be followed in terms of risk management and internal control processes, their support systems and the forms and frequency of their reports.

6.5.2 Support and guarantee the identification, assessment, treatment and monitoring of risks and internal controls by the proprietary areas, as well as consolidating and reporting on the status of risks in the corporate Risk Matrix and the results of control tests to the BEO and the BoD.

6.5.3 Disseminate the culture of risks and internal controls at Eletrobras.

6.5.4 Propose the Risk Management and Internal Controls Policy, specific rules on risk management and internal controls processes and the corporate Risk Matrix for approval by the BEO.

6.6 Risk owner areas

6.6.1 Act as the first line, managing the risks inherent in their activities, identifying, assessing, treating and monitoring them.

6.6.2 Provide the risk area with all the necessary information, with solidity and reliability.

6.7 Proprietary internal control areas

6.7.1 Act as the first line, ensuring the correct execution of controls and documenting the necessary evidence.

6.7.2 Inform the internal controls area, in suitable time, the need to update the controls for which it is responsible.

6.7.3 Implement the action plans defined to remedy the deficiencies identified by the internal and external audits.

6.8 Internal Audit

6.8.1 Evaluate the effectiveness of the risk management and internal control processes, interacting with the responsible areas regarding the verifications conducted.

6.8.2 Evaluate the adequacy of the responses to risks, recommending improvements to the area that owns the risk when necessary.

6.8.3 Conduct management tests verifying that the internal controls are appropriate and capable of mitigating the associated risks, as well as that they are operating correctly.

6.8.4 Periodically report their evaluations to the BoD and ARC.

7 GENERAL PROVISIONS

7.1 This policy is in line with Eletrobras' other policies.

7.2 The legal and regulatory provisions relating to the subject and the company's specific legal determinations and agreements must be observed.

7.3 This policy can be broken down into other specific normative documents, always in line with the principles and guidelines established here.

7.4 Normative documents and provisions contrary to this policy are hereby revoked.

8 EDITION HISTORY

Edition	Code and name	Doc. and date of approval
1.0	Eletrobras Companies' Risk Management Policy	RES-1279, of 12/08/2010 and DEL-059/2011, of 04/29/2011
2.0	Eletrobras Companies' Risk Management Policy	RES-509/2014, of 07/28/2014, and DEL-132/2014, of 10/30/2014
3.0	Eletrobras Companies' Risk Management Policy	RES-521/2016, of 08/23/2016, and DEL-170/2016, of 09/23/2016
4.0	Eletrobras Companies' Risk Management Policy	RES-639/2019, of 09/16/2019 and DEL-204/2019, of 09/26/2019
5.0	Eletrobras Companies' Risk Management Policy	RES-381/2021, of 06/07/2021, and DEL-135/2021, of 06/18/2021
6.0	Eletrobras Companies' Risk Management Policy	RES-539/2022, of 11/14/2022, and DEL-167/2022, of 12/01/2022
Main changes		
Expansion and updating of the scope, inserting and relating internal control activities to the risk management process; and review and adjustments to the References, Conceptualization and Responsibilities sections.		