CEMIG
RISK MANAGEMENT AND INTERNAL CONTROLS POLICY

**Replaces NO–02.19,
of December 10, 2021**

1. INTRODUCTION

Companhia Energética de Minas Gerais – CEMIG considers integrated management of the risks associated with its activities to be an essential function, involving identification and implementation of the internal controls that are necessary for creation of value for clients, stockholders, employees, suppliers, the public and other stakeholders.

Commitment to efficient management of corporate risks is one of the foundations of sustainable growth and of achieving the objectives of the Company's Strategic Plan. This commitment is one of Cemig's Values, and as such must be adhered to and put into practice at all times by all those working at Cemig or in its name, including suppliers.

2. OBJECTIVES

2.1 To establish the principles, guidelines, concepts and responsibilities involved in the processes of management of risks and internal controls in the corporate environment. These provide the basis for planning, identification, analysis, evaluation, treatment, monitoring and communication of Cemig's risks and internal controls, and propagation of the culture and good practices at all levels of the Company.

2.2 To enable the vision of risks to be incorporated as an integral part of the Cemig's Strategic Plan, supporting the taking of decisions, in accordance with the applicable regulations and best market practices.

3. RANGE AND COVERAGE

3.1 This Policy applies to: Companhia Energética de Minas Gerais – CEMIG ('**Cemig**' or '**the Company**'), Cemig Geração e Transmissão S.A. ('**Cemig GT**'), and Cemig Distribuição S.A. ('**Cemig D**').

3.2 This Policy is recommended to the suppliers of Cemig, Cemig GT and Cemig D, and to the companies in which any of these three companies have stockholding interests, subject to their corporate procedures, and in proportion to the importance and materiality of the risks of the businesses in which they operate.

4. REFERENCES

• The Brazilian **'State Companies Law':** Law 13.303, of June 30, 2016.

• **Minas Gerais State Decree 47.105** – of December 16, 2016.

• **COSO – ERM:** The *Enterprise Risk Management Framework* (2004) of COSO – *the Committee of Sponsoring Organizations* of the *Treadway Commission* – and its document *Enterprise Risk Management – Integrating with Strategy and Performance* (2017).

• **COSO Framework:** The COSO document *Internal Control – Integrated Framework* (2013).

• **COBIT:** The *Cobit* IT governance management model, designed by ISACA. The current version, created by ISACA, is ***Cobit 2019*.**

• Audit Procedures Committee of the American Institute of Certified Public Accountants (ACIPA);

• The *Sarbanes-Oxley Act*, of 2002, in particular Sections 302 and 404;

• ABNT Standard NBR ISO 31000:2018 – *Risk Management: Principles and Guidelines*.

• ABNT Standard ISO GUIA 73:2009 – *Risk Management: Vocabulary.*

• The *IIA 2020 Three Lines of Defense Model*, published by the Institute of Internal Auditors (IIA): Updated version (2020) of the IIA's *The Three Lines of Defense.*

• The *Code of Best Corporate Governance Practices* of the Brazilian Corporate Governance Institute (IBGC), 6th Edition, 2023.

• Cemig Policy NO–02.51: Internal Controls (SOX) Consequences and Accountability Policy.

5. CONCEPTS

For the purposes of this Policy the following concepts are adopted:

5.1 Risk appetite: The level of exposure to risk that Cemig is prepared to accept in seeking to achieve strategic objectives and create value for stakeholders.

5.2 Risk Factors: Situations which, when not effectively controlled by Cemig, can lead to the occurrence of an adverse event.

5.3 Internal control: The process conducted by Cemig's governance structure, management and other professionals, comprising the plan of organization and the coordinated operation of the methods and measures adopted by Cemig to protect its assets, check and confirm the accuracy and trustworthiness of its accounting data, promote operational efficiency, and encourage alignment with the policy set out by senior management.

5.4 The Committee of Sponsoring Organizations (COSO): A private, non-profit organization dedicated to establishing guidelines that aim to protect an organization from risks. Its recommendations are considered to be a reference for implementation of the internal control systems of organizations, increasing the reliability of financial reports, through ethics, effectiveness of internal controls and corporate governance.

5.5 Impact: A generic word for the consequence of an event, that affects Cemig's strategic

objectives, and can be measured qualitatively or quantitatively.

5.6 Key Risk Indicators (KRIs): Indicators of possible exposure to the risk being monitored, enabling preventive corrective action to be taken.

5.7 Materiality: A risk is described as material when the decided level of risk appetite has been reached or exceeded.

5.8 Action Plan: A group of actions that are necessary to ensure the responses to risks, after a decision on the treatment to be given to a risk. They have a defined start and end point.

5.9 Corporate risk management methodology: The structured process for planning, identification, analysis, assessment, treatment, monitoring and communication of corporate risks, with the intention of standardizing and orienting their mapping and monitoring. It can be adapted to align with the existing risk classifications.

5.10 Internal control methodology: The set of procedures and actions designed to manage the risks inherent to the organization. It includes: analysis of the company's internal controls environment; assessment of the risks that have been mapped; the activities of controls, information and communication carried out with and to the agents who are involved in and responsible for the management of risks and internal controls; and the processes and activities of monitoring for maintenance and effectiveness of the control environment.

5.11 Probability: The chance that a risk may materialize, at different degrees of intensity, which may be measured qualitatively and/or quantitatively.

5.12 Remediation: Actions taken or to be taken, to correct deficiencies identified in controls.

5.13 Risk: A factor or event which, if it occurs, could cause a negative impact or damage, inhibiting or preventing achievement of Cemig's objectives – or which could provide input for decision-making, thus representing an opportunity.

5.14 Control Owner: The qualified professional responsible for executing a control, documenting the evidence and performing one or more business processes.

5.15 Action Plan Owner: The qualified professional whose responsibility is to execute and be responsible for activities defined as treatment of a risk, updating information on the completeness and perception of mitigation, and documenting the evidence of its execution.

5.16 Risk Owner: The professional whose responsibility is to map and manage a risk, and indicate the actions for treatment of it, based on the risk appetite decided by the appropriate level of authority.

5.17 Focus Person: A person appointed by the Risk Owner or by a Director, with professional responsibility to: help in the process of mapping risks and internal controls; provide support in any actions for treatment or remediations; ensure that within the area of his/her activity planned time limits and the quality of treatment are complied with; and submit the results obtained for approval by the Risk Owner.

5.18 Treatment: Decision on a treatment should be taken on the basis of the level of exposure to a risk, comprising a cost-benefit analysis in relation to the risk appetite decided by Cemig. The

following decisions are possible:

- avoid the risk, by deciding not to begin, or to discontinue, the activity which gives rise to it;
- accept the risk, assuming the current exposure;
- increase the risk, with the intention of seeking an opportunity;
- mitigate the risk, minimizing the impact and/or probability;
- share the risk with, or transfer it to, an outside party, avoiding the exposure.

5.19 The Three-Tier model, created and published by the Institute of Internal Auditors ('IIA Global'), supports communication about management of risks and internal controls, by describing the essential roles and responsibilities of each tier. These are as follows:

- **First Tier:** The managers and executives of Cemig's operational and business processes.
- **Second Tier:** The areas of risk management, internal controls and other governance areas.
- **Third Tier:** The Company's Internal Auditing unit.

5.20 The Risks Heatmap: A visual tool that illustrates the positioning of risks in terms of levels of exposure, probability and impact.

6. PRINCIPLES AND GUIDELINES

6.1 Achieve and maintain transparency and quality of information published internally and externally, always aiming to improve the Company's reputation with the market, and a differential in generation of value for its shareholders and other stakeholders, adopting best corporate governance practices, in a systematic, structured and timely manner.

6.2 Keep the systems of internal controls and risk management aligned with best market practices, seeking ever-improving compliance with the demands of the operational sectors, and the regulatory and inspection bodies.

6.3 Ensure access to information on risk management and internal controls, through Cemig's communication channels.

6.4 Assist decision-making by the competent bodies, aiming to ensure conscious and appropriate decisions on Cemig's internal controls and risk management environment that are directly related to the strategic guidelines for sustainable growth, profitability and value creation for the Company.

6.5 Standardize and automate the mechanisms of risk management and internal controls, aiming to enhance synergy between the three Tiers and the competent bodies of Cemig.

6.6 Ensure compliance with the applicable laws and regulations, aiming always for transparency

and adherence to the internal policies, rules and procedures.

6.7 Ensure that the structure of risk management and internal controls results in understanding of the principal risks arising from internal and external events affecting Cemig, adapting to any changes in the context, ensuring that they are identified, analyzed, assessed, treated, monitored and tested efficiently and effectively.

6.8 Promote the culture of management of risk and internal controls, demonstrating the importance of these subjects in Cemig to all employees, so as to achieve a significant degree of guarantee throughout its operations.

6.9 Ensure that each role, during the risk management process, is formally defined and assigned, with the responsibilities described, disclosed and clearly understood by all those involved.

6.10 Give timely support to the Board of Directors, the Board of Directors Risks Committee, the Audit Board, the Audit Committee, the Executive Board and other governance bodies of Cemig, in relation to the situation of the Company's risk management and internal controls environment.

7. RESPONSIBILITIES

7.1 The Board of Directors

- To establish general guidelines, and to integrate the practices of risk management and internal controls into the decision-making process.
- To evaluate and approve the Top Risks Matrix, and the general guidelines for setting the Company's acceptable levels of risk (Risk Appetite).
- To assess and approve the Risk Management and Internal Controls Policy.
- To ensure implementation of, and to supervise, the systems for management of risks and internal controls established for the prevention and mitigation of the principal risks to which the Company is exposed, including the risks related to safety and security of accounting and financial information and the occurrence of corruption or fraud.
- To monitor the results of the processes of risk management and internal controls, through executive reports.

The Board of Directors Risks Committee

- To monitor, periodically, the process of risk management and internal controls, reporting the most important points to the Board of Directors.
- Advising the Board of Directors, to assess and evaluate the decision on the Top Risks Matrix, and the general guidelines for establishment of the Company's limits for acceptable levels of risk (Risk Appetite).
- To analyze all material submitted to the Board of Directors about management of the Company's risks and internal controls, and give prior opinion on it.

7.3 The Executive Board

- To ensure application of the principles and directives of this Policy, and alignment with it in terms of efficacy in management of risks and internal control procedures.
- To disseminate the culture of risk management and internal controls in the Company, and to strengthen the roles of the First and Second Tiers.
- To submit to the Board of Directors, for assessment and validation: (a) the Top Risks Matrix, and (b) the general guidelines for establishment of the Company's risk appetite (acceptable limits for exposure to risk).
- To submit the Risk Management and Internal Controls Policy to the Board of Directors for assessment and validation. To participate in the process of identification, prioritization and validation of the risks in the various Chief Officers' Management Units, monitoring the treatment of business risks, during the execution of the Strategic Plan.
- To guarantee timely and satisfactory execution of the internal controls relating to the risks inherent to the processes that are under the management of each Chief Officer's Management Unit.
- Through periodic reports, to assess the assertiveness of the risk management process, based on discussion and validation, in the Executive Board as a whole or in each Chief Officer's Department, of the assessments presented by each Risk Owner, in accordance with the appetite approved by the Board of Directors.

7.4 The Corporate Risks Management Committee (CMRC)

- To evaluate and approve the Top Risks Matrix, and the general guidelines for establishment of acceptable limits for risk appetite.
- To submit the Company's Risk Management and Internal Controls Policy to the Board of Directors for assessment and validation.
- To disseminate the culture of risk management and internal controls within the Company.
- To support the Executive Board in monitoring of risks and internal controls, and to submit preventive recommendations for potential risks evaluated in meetings of the Committee.
- To support the First Tier in any requests for human, financial or any other type of resources, to assist in the management of Cemig's risks and internal controls.
- To recommend revisions to policies, rules and procedures, with the objective of enhancing management of risks and internal controls.
- To report to the Executive Board a consolidated panorama on exposure to potential risks in Cemig.

7.5 The First Tier

The First Tier comprises the Owners of risks and internal controls in the various business units, management units and processes. The First Tier is responsible for managing risks and internal controls,

assisting in identification of risks, and providing timely communications on the progress and status of risks and controls, and on any alterations that might impact Cemig's internal controls environment. It also has the following responsibilities:

- to ensure timely and sufficient execution of the internal controls that are under its responsibility;
- to provide support during the evaluation of Cemig's risk management and internal controls environment;
- to assess and validate the mapping of risks and the description of controls, and the individuals responsible for each one, as presented in Cemig's Risks and Internal Controls Matrix;
- to assess and validate the Action Plans arising from the evaluations of the risk management and internal controls environment;
- to propose emerging or emergency risks, in good time, as and when they occur;
- to report occurrences to the interested publics, jointly with the Second Tier, for treatment of the related risks;
- to advise the Second Tier whenever there is any alteration in the legislation or procedures related to any process, if it might result in need for review of a related control; and
- to provide timely communication of any need for adaptation of internal controls, and/or any adverse events, to guarantee the reliability of Cemig's internal controls environment.

This Tier has three important, principal agents: Risk Owners, Control Owners, and the Focus Person. The main activities for each of these are:

7.5.1 Responsibilities of Risk Owners

- to identify, analyze, evaluate, treat, prevent and monitor risks in an overall integrated manner;
- to ensure timely implementation of plans of action proposed for treatment of risks, with the support of the Owners of each plan of action;
- to obey the directives and decisions set by the Second Tier;
- to continuously monitor the scenario of risks, with a view to revision or identification of potential risks that create a need for implementation of preventive or mitigatory controls;
- to monitor compliance in dealing with risks, to ensure that internal and external regulations are obeyed;
- to monitor KRIs regularly, to ensure effectiveness of the controls and Action Plans;
- to analyze proposals for improvements of controls and recommendations for implementation of new controls, suggested by Control Owners, aiming to enhance risk management;
- to guarantee the resources necessary for management of risks in the Company, in accordance with its budget directives; and

- when mapping risk, to fill out and validate the relevant information, using the Risk Management support tool, provided by the area responsible for support to the process.

- When there is a threat that any risk will materialize, Risk Owners should immediately, proactively, implement the actions for mitigation or prevention they deem to be appropriate, evaluating the level of risk appetite that has been decided; and subsequently advise the responsible body of Cemig if any support or validation from higher levels of authority is necessary.

- Whenever Risk Owners feel it to be necessary, they should ask the Second Tier and the CMRC for support in implementing any mitigation or prevention actions for the risks under their responsibility.

7.5.2 Responsibilities of Control Owners

- to execute the controls under their responsibility, in accordance with the procedures and frequencies that have been decided, documenting all the necessary evidence and steps taken, for submission, whenever requested, to the internal and external auditors and/or the Company's governance areas;

- to notify the Risk Owner of any deficiencies identified in the tests, especially in the case of critical controls, to warn of possible impacts on mitigation of the risk associated with the control;

- where controls are ineffective or insufficient, or absent, to monitor the Action Plans for remediations, setting deadlines and specifying the people responsible;

- to monitor the execution and timeliness of Action Plans for controls, updating them whenever they deem this to be necessary; and

- if the deadline for implementation of a plan is no longer viable, to decide, together with the Second Tier, on a new deadline.

7.5.3 Responsibilities of the Focus Person

This is the person appointed by the Risk Owner or the Chief Officer as the focal point for all subjects of risk management and internal controls in his or her specific Chief Officer's Department, Senior Management unit, or line management unit. Their responsibilities are:

- to disseminate the culture of risks and internal controls in the Company, maintaining and strengthening an environment of operational controls that is adequate for the effectiveness and continuity of the related business area;

- to ensure risks and internal controls are mapped, providing support in any actions to treat risks or address remediations; and

- to monitor, and act to ensure compliance with, deadlines and quality in the actions taken within the sphere of activity, for approval by the Risk Owner.

7.5 The Second Tier:

The second tier in management of risks and internal controls comprises the Risks and Internal Controls Management Unit, which is responsible for supporting the process of management of risks and internal controls**.** This tier also has the following main responsibilities:

- to decide the methodology, processes and infrastructure necessary for uniform and efficient management of risks and of internal controls;
- to develop and implement policies, rules and procedures that orient the areas of Cemig on the method of action and communication, and the roles and responsibilities relating to the procedures of management of risks and internal controls;
- to propose actions to be taken by the First Tier to promote awareness, and disseminate the culture of management of risks and internal controls in the Company;
- to establish a timetable of corporate training sessions to be executed by all of Cemig's publics;
- to support the First Tier with orientations and recommendations on the procedures of Cemig's internal controls and management of risks;
- to provide support for external dissemination of official information on management of corporate risks and internal controls;
- to establish a regular agenda for reporting to the Executive Board and to the Board of Directors on the current status of the processes of management of risks and internal controls, highlighting the most critical items and those which require decisions to be taken;
- to prepare reports on internal controls, to assist in management of risks and operational efficiency of the business areas;
- to plan allocation of financial, human and technological resources for management of risks and internal controls;
- periodically, to update and revise the Top Risks Matrix, to keep it aligned with Cemig's Strategic Plan or any significant changes in the Company's environment, and to submit this to analysis by the Executive Board and the Board of Directors;
- periodically, to update and revise the Risks and Internal Controls Matrix, to keep it aligned with any changes in Cemig's Strategic Plan or significant changes in the Company's environment, and to submit this to analysis by the Executive Board;
- to implement and monitor the KRIs, to ensure efficacy in the processes of management of risks and internal controls; and
- whenever necessary or requested, to report the state of the risks and internal controls management environment to the Board of Directors, the Audit Board, the Audit Committee, the Executive Board and the other governance bodies of Cemig.

7.6 The Third Tier

The Third Tier consists of the Internal Audit Senior Management Unit, responsible for carrying out assessments and inspections by executing tests of controls, and audits, to provide independent analysis of aspects including the effectiveness of the management and prevention of risks, and management of internal controls and compliance. It is also responsible for:

- deciding a plan for revisiting the risks that Cemig considers to be the most critical;
- assessing the effectiveness of the corporate governance process, and of the system for management of corporate risks and internal controls;
- reporting to the Governance Forums the result of all audit work, with emphasis on any action plans that have not been completed and on any gaps and failures in controls;
- auditing the internal controls system, and issuing periodic reports to those responsible, in order to evaluate the structure of internal controls on financial statements, in compliance with the Sarbanes-Oxley Law – SOX;
- to hold discussions aimed at diffusing the culture of internal controls, risk mitigation and compliance through rules applicable to companies in the Cemig Group; and
- to carry out tests of effectiveness of controls related to risks.

8. THE PROCESS OF CLASSIFICATION AND MANAGEMENT OF CORPORATE RISKS

8.1 Classification of risks

Risks in Cemig are classified by level, and type.

8.1.1 Classification by level:

- *Top Risks*:

– Risks measured, on the Heatmap, in the worst case scenario (WC) – considering all the 5 dimensions when positioned in the red band; and in the financial dimension (F), considering the positions of high and very high impacts;

– Macroprocess Risks indicated by the Corporate Risk Monitoring Committee (CMRC), Executive Board, Risk Committee of the Board of Directors and the Board of Directors, through consultation or express decision, as being significant and in need of priority treatment.

- *Macroprocess Risks:* These are risks associated with more than one process of the organization.
- *Process Risks:* Risks associated with one of the processes of the organization.

8.1.2 Classification by type:

Type	Description
External	Associated with changes in the external context, such as significant political and economic changes (national or international), which can result in failure of strategies adopted.
Strategic	Risks associated with decisions of a strategic character, or changes in the general internal conditions of the Company, that have a significant impact on its business model and strategy.
Economic / financial risks	Risks associated with inefficacious management or control of the organization's financial resources, or with market variations (e.g. availability of credit, exchange rates, and movements in interest rates).
Legal and Regulatory Compliance	Risks associated with non-compliance with external legislation applicable to the business, especially regulation of the sector, and/or failure to prepare or publish required reports, or to comply with internal rules and procedures. This category includes penalties for non-compliance with legislation, environmental rules or policies, or Cemig's Sustainability Guidelines.
Compliance risks	Risks related to the directives of the Company's Compliance Policy – this refers to unethical behavior that could lead to fraud, corruption and/or conflict of interests, leading to financial losses, and/or damaging the Company's image.
Operational risks	Risks related to deficiencies in or inappropriate management of internal processes, or arising from influence of external events, resulting in loss of quality, performance, clients, assets or security (including information technology, information security and telecommunications data). This also includes deficiencies in the process of management of people, succession, union relationships, organizational climate, workplace safety, and resistance to new market practices.
Social–environmental risks	These are risks associated with deficient or inappropriate environmental or social management, causing impact on the environment and/or the general public. They also include potential effects on the business arising from climate change, which may prevent new projects or expansion of production capacity from being feasible.

8.2 Methodology of Cemig's Corporate Risks Management

The process of management of risks is structured in five phases, as follows:

8.2.1 Planning

The Corporate Risks Matrix is identified, taking as its starting point the strategic directives approved in the multi-year Strategic Plan and the decisions in the Work Plan for Management of Risks and Internal Controls, and is classified into Levels of Risk.

8.2.2 Identification of Risks

Risks are identified through assessment of the processes of the business, in a process of search for, recognition of and description of risks – ascertaining and listing the causes, impacts and scope, which are then validated by Risk Owners.

8.2.3 Analysis of Risks

This phase comprises decision on attributes of probability, and quantitative and/or qualitative impact, in an analysis considering the effects of the existing controls (residual risk).

8.2.4 Assessment of Risks

This comprises comparison of the results of the risk analysis with the established risk criteria, to determine whether additional action will be required. If there is a need for action in relation to a risk, the options for treatment of the risk should be considered, with a view to establishing action plans and controls.

8.2.5 Treatment of Risks

This involves identification of actions to respond to risks, such as controls and Action Plans. The type and level of response, and priorities, depend primarily on the materiality and level of risk, taking the decided risk appetite as a starting point.

8.2.6 Monitoring of Risks

Action plans, assessments of mitigating controls and risk indicators (KRIs) are monitored and subjected to critical analysis, with a view to improving the quality and effectiveness of the design, implementation and results of the process. Accompaniment and monitoring should be continuous, throughout the universe of Cemig's risks.

This phase also comprises communication and reporting to the competent forums. The process of communication should be structured in three segments:

- Promotion of Cemig's culture of risks.
- Addressing the points of decision-making at the competent instances.
- Periodic reports on the universe and scenario of corporate risks and internal controls.

8.3 Methodology of Management of Cemig's Internal Controls

8.3.1 The Internal Controls process is based on the following structure:

a) The Controls Environment

The internal controls structure identifies the control environment within which the organization exists, assessing the internal controls as a whole. This assessment makes possible a better adaptation of the company's view, its objectives, the processes and activities that support it, and the risks linked to the business.

(b) Risk assessment

Measurement of the risks identified, and preparation of a strategy for implementation or extension of the controls already existing, so as to mitigate the organization's exposure to risks that have been mapped.

(c) Control activities

These are the policies and procedures adopted that help to ensure that the responses to risks are executed.

(d) Information and communication

This covers the collection and dissemination of information to ensure that all agents involved understand about the risks existing in each process, and their responsibilities in the management of risks and controls.

(e) Monitoring activities

These are activities that provide for the controls to continue to be efficacious, and for the control environment to continue to be effective over time.

9. FINAL PROVISIONS

All new procedures related to Management of Corporate Risks and Internal Controls must be stated in specific instructions, and be in accordance with this Policy. Upon publication they become an integral part of this Policy.

COMPLIANCE DIRECTORATE (DCI)

*** Policy approved by the Board of Directors on November 9, 2023.**