

CEMIG POLICY ON MANAGEMENT OF CORPORATE RISKS AND INTERNAL CONTROLS

**Replaces NO-02.19, of
December 12, 2019**

1. INTRODUCTION

Companhia Energética de Minas Gerais – CEMIG considers management of the risks associated with its activities to be an essential function, involving identification and implementation of internal controls 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 must be practiced at all times by all those working at Cemig or in its name, including suppliers.

2. OBJECTIVE

The objective of this Policy is to establish the principles, guidelines, concepts and responsibilities in the processes of management of risks and internal controls in the corporate environment. These provide the basis for planning, identification, analysis, 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.

3. RANGE AND COVERAGE

This Policy applies to Companhia Energética de Minas Gerais – CEMIG, Cemig Geração e Transmissão S.A. ('Cemig GT'), and Cemig Distribuição S.A. ('Cemig D'), and serves as orientation to their suppliers, and to all the companies in which Cemig has an equity interest, including wholly-owned subsidiaries (herein referred to for the purposes of this Policy, jointly, as 'Cemig').

4. REFERENCES

- 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).
 - Brazilian Standards Association (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 Model*: Updated version (2020) of *The Three Lines of Defense* published by the Institute of Internal Auditors (IIA).
 - The *Code of Best Corporate Governance Practices* of the Brazilian Corporate Governance Institute (IBGC), 2015.
-

5. CONCEPTS

The following concepts are adopted for the purposes of this Policy:

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

5.2 Causes (Risk Factors): Situations which can cause occurrence of an adverse event when not effectively controlled by Cemig.

5.3 Internal control: A process conducted by the governance structure, management and other professionals of the entity, to provide secure achievement of objectives in terms of efficacy and efficiency in operations, reliability of reporting, and compliance with laws and regulations.

5.4 COSO – The Committee of Sponsoring Organizations: A nonprofit entity dedicated to improvement of financial reporting through ethics, effectiveness of internal controls, and corporate governance. It studies the factors that can lead to generation of fraudulent reports, and creates recommendations for listed companies, their auditors, educational institutions, the Securities and Exchange Commission of the USA, and other regulators. COSO's recommendations are regarded as a benchmark for risk management and internal controls.

5.5 Impact: Any qualitatively or quantitatively measurable consequence of an event that affects Cemig's strategic objectives.

5.6 Key Risk Indicators (KRIs): Metrics associated with the causes that have been mapped, enabling preventive corrective action to be taken.

5.7 Materiality: Degree of severity of the probable result of materialization of a risk at its lowest envisaged level. A risk is said to be material when the defined level of risk appetite has been reached.

5.8 Action Plan: Description of actions that have been decided for elimination or mitigation of a risk, and/or the principal actions to be taken, after decision on the treatment to be given to a risk.

5.9 Corporate risk management methodology: The structured process for planning, identification, analysis, 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 Probability: The chance that a risk may materialize – different degrees of intensity are attributed.

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

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

5.13 Control Owner: The qualified professional responsible for executing controls, documenting evidence and carrying out one or more business processes.

5.14 Action Plan Owner: The professional whose responsibility is to execute the measures decided to deal with the risk, update their completeness and efficacy, and document the evidence.

5.15 Risk Owner: The professional whose responsibility is to map and manage a risk, and indicate the actions for dealing with it, based on the risk appetite decided by the person with the competent level of authority.

5.16 Focal Point: A professional nominated by the Risk Owner or by a Director, to be responsible for ensuring risks and internal controls are mapped, and actions for dealing with them and remediation are supported, and for monitoring to ensure that measures taken within his/her activity are in compliance with specified deadlines and quality, subject to approval by the Risk Owner.

5.17 Treatment: Decision to 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; or
- share and/or transfer the risk, for example by insurance and/or other contractual instruments.

5.18 The Three Lines: A model aims to improve communication about management of risks and internal controls, through clear exposition of the essential roles and responsibilities within Cemig. The following are the responsibilities of each Line:

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

6. PRINCIPLES AND DIRECTIVES

6.1 Achieve and maintain transparency and quality of information, at all times seeking enhancement of reputation in relation to the market, and a differential in terms of generation of value for stockholders, adopting best corporate governance practices, in a systematic, structured and timely manner.

6.2 Keep the systems of internal controls and risk management in accordance with best market practices, seeking to ensure enhancement in compliance with the demands of the operational sectors, and the regulatory and inspection bodies.

6.3 Guarantee 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.

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

6.6 Ensure compliance with applicable laws and regulations, seeking 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, and that they are identified, analyzed, treated, monitored and tested efficiently and efficaciously.

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

6.9 Give timely support to the Board of Directors, the Fiscal Council, 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 Responsibilities of the Board of Directors

- To establish general guidelines, and to achieve integration of the practices of risk management and internal controls with the decision-making process.
- To evaluate and approve the Top Risks Matrix, and the general guidelines for establishment of acceptable limits for risk appetite.
- To evaluate and approve the Cemig Policy on Management of Corporate Risks and Internal Controls.
- To monitor, by means of executive reports, the results of the processes of risk management and internal controls.
- To supervise the activities of risk management and internal controls, to be executed by the CEO and the other members of the Executive Board.

7.2 Responsibilities of the Executive Board

- To ensure application of the principles and directives of this Policy, with commitment to efficacy in management of risks and in the procedures of internal controls.
 - To disseminate the culture of risk management and internal controls in the Company, and to strengthen the roles of the First and Second Lines.
 - To submit the Top Risks Matrix, and the general guidelines for establishment of the Company's acceptable limits for exposure to risks (Risk Appetite), to the Board of Directors for assessment and validation.
 - To submit the Cemig Policy on Management of Corporate Risks and Internal Controls to assessment and validation by the Board of Directors.
 - 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 execution of the Strategic Plan.
-

- To guarantee timely and satisfactory execution of the internal controls related to 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 and/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.

7.3 Responsibilities of the Corporate Risk Management Committee (CMRC)

- To disseminate the culture of risk management and internal controls in Cemig's business.
- To support the Executive Board in monitoring business risks and internal controls, and to submit preventive recommendations for potential risks evaluated in meetings of the Committee.
- To support the First Line in any requests for human, financial, and 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 for enhancement of risk management and internal controls.
- To report to the Executive Board a consolidated panorama on exposure to potential risks in Cemig.

7.4 The First Line

The First Line comprises the Owners of risks and internal controls in the various business units, management units and processes. It 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 give support during 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, presented in Cemig's Risks and Internal Controls Matrix;
- to assess and validate the Action Plans arising from evaluations of the risk management and internal controls environment;
- to advise the Second Line whenever there is any alteration in the legislation or procedures related to any process, that could result in a need for review of the control.
- to provide timely notification of the need for adaptation of internal controls, and/or any adverse events, to ensure effective maintenance of Cemig's internal controls environment.

It is important to emphasize that the First Line has three important principal agents: **Risk Owners**, **Control Owners**, and **Focal Points**. Their main activities and responsibilities are:

7.4.1 Responsibilities of Risk Owners

- to identify, evaluate, deal with, prevent and monitor risks in a complete and integrated manner;
- to implement Action Plans proposed for treatment of risks, with the support of the Owners of each measure taken;
- to obey the directives and decisions set by the Second Line;
- to continuously monitor the scenario of risks, with a view to revision or identification of potential risks that create a need for implementation of controls for prevention or mitigation;
- to monitor compliance, ensuring that internal and external regulations are obeyed in dealing with risks;
- to monitor KRIs regularly, to ensure effectiveness of controls and Action Plans;
- to analyze proposals for improvements of controls, and recommendations for implementation of new controls, suggested by Control Owners, to enhance risk management;
- to guarantee the resources necessary for management of risks, in accordance with the Company's budget directives;
- when mapping risk, to fill out and validate the Corporate Risks Registry Spreadsheet, provided by the area responsible for support to the process;
- when there is a threat that any risk will materialize, to immediately and proactively implement actions for mitigation or prevention that they deem to be appropriate, taking into consideration the level of risk appetite that has been decided; and subsequently, if any support or validation from higher levels of authority is necessary, to advise the responsible body of Cemig; and
- whenever they consider it to be necessary, to ask the Second Line and the CMRC for support in implementing mitigation or prevention actions for the risks under their responsibility.

7.4.2 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 tests, especially for critical controls, to warn of possible impacts on mitigation of the risk associated with the control;
 - to monitor Action Plans arising from remediations for any ineffective or insufficient controls, or any absence of controls, deciding deadlines and specifying the people to be responsible; and
 - to monitor the execution and timeliness of Action Plans relating to controls, updating them whenever they deem this to be necessary; and if any deadline for implementation of a plan is no longer viable, to decide, together with the Second Line, on a new deadline.
-

7.4.3 Responsibilities of Focal Points

- to be the central point, appointed by the Risk Owner or the Chief Officer, for all matters relating to risk management and internal controls in a Chief Officer's Department, Senior Management unit, or Management unit.
- to ensure risks and internal controls are mapped, providing support in any actions to deal with them or to address remediations; and
- to monitor, and act to ensure compliance with, deadlines and quality in the actions taken within the Focal Point's sphere of activity, for approval by the Risk Owner.

7.5 The Second Line:

The second line in management of risks and internal controls is the Risks and Internal Controls Management Unit, responsible for providing support to the process of management of risks and internal controls. This Line also has the following main functions and 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, communication, and the roles and responsibilities relating to the procedures of management of risks and internal controls;
 - to propose actions for promoting awareness to be taken by the First Line to disseminate the culture of management of risks and internal controls in the Company; and to establish a timetable of corporate training sessions to be executed by all of Cemig's publics;
 - to support the First Line 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 the management of risks and promote operational efficiency of the business areas;
 - to assess the technical effectiveness of recommendations proposed in Action Plans put forward by the First Line, the CMRC and other bodies;
 - to plan allocation of financial, human and technological resources for management of risks and internal controls;
 - periodically to update and revise the Corporate Risks Matrix, to keep it aligned with any changes in Cemig's Strategic Plan or significant changes in the Company's environment, and to submit it 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 it to analysis by the Executive Board;
- to implement and monitor 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 environment of Cemig's risks and internal controls management to the Board of Directors, the Fiscal Council, the Audit Committee, the Executive Board and the other governance bodies of Cemig.

7.6 The Third Line

The Third Line consists of the Internal Audit management unit, responsible for assessment and inspection by tests and audits, providing independent analysis of aspects including the effectiveness of risk management and prevention, internal controls and compliance. It is also responsible for:

- deciding a plan for revisiting the risks that Cemig considers to be the most critical;
- recommending improvements to enhance the business processes assessed;
- preparing reports of audits, and formalizing Action Plans that are established, setting deadlines and specifying the parties responsible;
- monitoring the Action Plans established by the business areas, to ensure that non-compliances are dealt with; and
- advising the First and Second Lines, and the governance bodies, of the results of tests, and on exposure to significant risks.

8. CLASSIFICATION AND MANAGEMENT OF CORPORATE RISKS

8.1 Classification of risks

Risks in Cemig are classified by Hierarchy, and by Type.

8.1.1 Classification by Hierarchy:

- *Top Risks*: These are the macro process risks that are indicated, by the Corporate Risks Monitoring Committee (CMRC), the Executive Board and the Board of Directors, by consultation or by express decision, as directly affecting achievement of the strategic guidelines and objectives and needing priority treatment.
 - *Macro Process Risks*: 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 of risks by Type:

Type	Description
Business risks	Risks associated with decisions of a strategic character, or changes in the general situation of the Company, that have a significant impact on its business model and strategy.
Economic / financial risks	Risks arising from ineffective management or control of the organization's financial resources, or from external factors (e.g. availability of credit, exchange rates, and changes in interest rates).
Legal and regulatory risks	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 and/or policies, and Cemig's Sustainability Guidelines.
Compliance risks	Risks related to the directives of the Company's Compliance Policy – involving unethical behavior that can lead to fraud, corruption and/or conflict of interests, resulting in financial losses, and/or damage to 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 processes of management of people, succession, relationships with unions, organizational climate or 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 on the general public. They also include potential effects on the business arising from climate change, which may hinder or prevent feasibility of new projects or expansion of production capacity.

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

The risks to which the Company is exposed are identified and described – ascertaining and listing the causes, impacts and scope defined and validated by Risk Owners.

8.2.3 Analysis of Risks

This phase comprises attribution of probability, and quantitative and/or qualitative impact, in an analysis considering the effects of the existing controls (Residual Risk).

8.2.4 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 type of risk, taking the risk appetite that has been decided as a starting point.

8.2.5 Monitoring of Risks

Monitoring of Action Plans, and assessment of mitigatory controls and risk indicators (KRIs). This 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.

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, CORPORATE RISKS AND INTERNAL CONTROLS MANAGEMENT UNIT (DCI)

Policy approved by the Board of Directors on December 10, 2021.
