	POLICY **- PO -**	CODE **PO-GE-EBE-0003** REVISION **04** APROVAL **ADE-958-0004 of 27/07/26** **Minutes of the 301ª BDM of 05/08/26**

TITLE

ENTERPRISE RISKS & OPPORTUNITIES MANAGEMENT (ERM)

1. OBJECTIVE

ENGIE Brasil's Enterprise Risks and Opportunities Management Policy establishes the principles, guidelines, and responsibilities for structured management of enterprise risks and opportunities within the scope of the companies.

The purpose of Enterprise Risks and Opportunities Management (ERM) is to continuously maintain and improve the value, reputation, and strategy implementation of the companies, encouraging reasonable risk-taking in legal terms, and that is considered acceptable and economically viable. Achieving this objective requires adequate knowledge of the risks to which the companies are exposed, as well as the ability to identify, evaluate, and manage them in a structured manner. The goal is to strengthen the management of risks and business opportunities as part of organizational culture and contribute to the resilience, continuity, and sustainability of the companies' businesses.

2. DEFINITIONS

2.1 ACTION PLAN
Set of measures adopted to reduce the impact and/or probability of risk materialization, with the objective of aligning it with the risk appetite defined by the Company.

2.2 ADMINISTRATORS
Members of Executive Committee of ENGIE Brazil (COMEX), members responsible for GBUs, Management of operating companies, and in the case of publicly listed companies listed, the Board of Directors and other governance bodies.

2.3 BUSINESS PARTNER
Internal consultant who integrates risk management with the Company's business objectives, actively collaborating with leaders and managers to identify, evaluate, and mitigate threats that may arise from strategic changes, new projects, or business environment.

2.4 COSO ERM - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION
International framework that guides the identification, evaluation, management, and monitoring of business risks to increase company value, aligning risk management with strategy and performance. It aims to protect assets, improve decision-making, and ensure that strategic objectives are achieved.

2.5 ENTERPRISE RISKS AND OPPORTUNITIES MANAGEMENT (ERM)
Structured and multidisciplinary exercise, with the objective of identifying, analyzing, evaluating, treating, monitoring, and communicating the risks and opportunities that may impact the Company's strategic objectives. ERM is a continuous process, with annual cycles and short, medium, and long-term vision, aligned with the ENGIE Group methodology and based on international standards such as ISO 31000 and COSO ERM.

2.6 ENTERPRISE RISKS AND OPPORTUNITIES MATRIX
Document that synthesizes the result of the analysis of enterprise risks and opportunities management, containing identification of risks and opportunities, causes, consequences, risk evolution, scenarios, mitigation plans, and the graphic representation (matrix of rows and columns) of risk exposure, based on the combination between impact and probability, used for prioritization and treatment, which is the Heat Map.

2.7 ERM

Cópia não controlada

English acronym for Enterprise Risk Management.

2.8 GBU – GLOBAL BUSINESS UNIT
Corresponds to an operational segment whose operational and financial performance is regularly reviewed by the Group's Executive Committee.

2.9 IMPACT
Quantitative and/or qualitative representation of the positive or negative effect that the materialization of the risk/opportunity brings in relation to what was projected in the financial base case (MTP V1), or in achieving business objectives.

2.10 ISO 31000
International standard that focuses on dealing with uncertainty in a structured way to increase organizational resilience. Its objective is to provide structured guidelines for organizations of any size to integrate risk management into all activities, strategies, and operations, aiming to protect value, improve performance, increase confidence in decision-making, and ensure business continuity.

2.11 OPPORTUNITY
Any uncertain event with the probability of having a positive impact on the company's sustainability or reputation, or the achievement of its strategic, financial or operational objectives.

2.12 PRM
English acronym for Project Risk Management which means Risk Management in Projects. Project Risk Management is a systematic and interactive approach to the identification, evaluation, mitigation, and review of risks involved in a project, which enables achieving project objectives with awareness and acceptance of random factors that may occur. Risk management in projects aims to coordinate the individual stages of risk management, regardless of their nature, and the ways these stages interact, considering project objectives.

2.13 PROBABILITY
Chance of occurrence of a risk event, which should be expressed quantitatively, according to criteria defined by the ENGIE Group.

2.14 RISK
Any uncertain event with the probability of having a negative impact on the company's sustainability or reputation, or the achievement of its strategic, financial or operational objectives.

2.15 RISK APPETITE
Degree of risk that companies are willing to accept to achieve their strategic objectives and results, serving as a reference for decision-making at all levels.

2.16 RISK CATALOG
Document that brings the relationship of main risks, organized into risk families and numbered to allow consolidation by the controller, ENGIE S.A.

2.17 RISK OFFICER
Professional responsible for managing enterprise risks and opportunities, aligned with the ENGIE group's methodology and applicable standards.

2.18 RISK OWNER
All ENGIE managers are owners of risks related to their duties or authorities and assume responsibility for the risk exposure incurred by their decisions. Every manager is a Risk Manager.

Cópia não controlada

2.19 RISK REGISTER
Structured compilation of risks that have been identified and managed throughout the project lifecycle (in PRM) and/or during corporate risk review (in ERM). It should be created at the beginning of the project, in the Business Development phase and should be kept updated throughout the duration of the project and delivered at each milestone, whenever there is a change of participants. For each corporate risk, a specific risk register should be developed.

2.20 THREE-LINE MODEL
Created by the Institute of Internal Auditors - IIA, it is a governance framework that establishes roles and responsibilities for risk management at three levels: business areas (1st line), risk management functions, internal controls and compliance (2nd line) and internal audit (3rd line).

3. DISPOSALS

3.1 APPLICATION AND SCOPE

This policy applies to all operational companies, controlled and suggested for ENGIE´s non-controlled companies in Brazil.

It covers all types of risks to which ENGIE Brasil is exposed, regardless of their origin or nature. It must be observed in any activity or decision that may impact the Company's strategic, operational, financial, environmental, social, reputational or compliance objectives.

4. PRINCIPLES

4.1 GENERAL

4.1.1 Confidentiality

4.1.1.1 The identification, risk assessment, mitigation strategies and action plans are highly strategic and sensitive information are classified as "restricted/internal" according to ENGIE Group rules, as they highlight vulnerabilities that may be explored by competitors and actions that generate competitive advantages.

4.1.1.2 This information is subject to controlled communication and must comply with legal obligations, especially in the context of financial disclosures.

4.1.1.3 The implementation of ERM respects the governance obligations and legal obligations of Group entities. Correct implementation of protection for this information should be consistent with the specific dissemination of information among managers so they can implement risk management actions.

4.1.2 Framework

4.1.2.1 ENGIE Brasil's enterprise risks and opportunities management is aligned with the ENGIE Group's methodology, which is based on internationally recognized best practices, such as ISO 31000 and COSO ERM, considering applicable legislation. The methodology includes supporting documentation (risk catalog, manuals, etc.) and management tools (corporate systems).

4.1.2.2 ENGIE Group's values are considered in the enterprise risk and opportunity management at ENGIE Brasil, as well as compliance with legal and regulatory obligations.

Cópia não controlada

4.1.2.3 *Risk-taking is intrinsic to any business:* conducting business implies taking a reasonable level of risk and must consider the long-term sustainability of the business, through continuous identification and monitoring of risks.

4.1.2.4 *There is no zero risk:* it is not economically viable to mitigate a risk to the point where its impact is zero. However, it is essential to implement management procedures and mitigation plans that control risks within the risk appetite defined by the ENGIE Group, balancing cost and benefit.

4.1.2.5 *Better manage our risks, in order to ensure our performance:* managing risks provides greater assurance that strategic and operational objectives will be achieved, in the context of changing business environment. This approach promotes a deeper understanding of risks, fostering conscious and reflective decisions for safer choices.

4.1.2.6 *The worst risk is the one that you don't know:* a risk that is not identified is not mitigated.

4.1.2.7 The culture of enterprise risk and opportunity management should be continuously promoted through training, guidance, and engagement of leadership, ensuring adequate capacity building for those involved in their responsibilities.

4.1.2.8 This Policy should be reviewed in accordance with the Enterprise Risks and Opportunities Management Policy of the ENGIE Group.

4.2 STRUCTURE OF ENTERPRISE RISK AND OPPORTUNITY MANAGEMENT

4.2.1 ENGIE Brasil adopts the Three Lines Model, in accordance with the guidelines of the Institute of Internal Auditors (IIA):

a) **1st line** – composed of managers of business areas, responsible for identifying, assessing, and managing risks related to their scope of operations. They must implement action plans for adequate risk mitigation, as well as monitor the effectiveness of these initiatives;

b) **2nd line** – composed of Compliance, Internal Controls, and Enterprise Risk and Opportunity Management areas. The Enterprise Risk and Opportunity Management area is responsible for supporting and guiding the 1st line in the application of the corporate risk management methodology, promoting adherence to policies and procedures, consolidation of information, and risk culture in the organization;

c) **3rd line** – composed of the Internal Audit area that operates with functional independence to assess the effectiveness of enterprise risk and opportunity management, internal controls, and governance. In publicly listed companies, Internal Audit reports directly to the Statutory Audit Committee and Board of Directors, contributing with recommendations for the continuous improvement of these practices.

In the process of enterprise risk and opportunity management, action plans and controls defined within the Group's Internal Control Program (INCOME) are risk mitigators. The Enterprise Risk and Opportunity Matrix guides the annual work plan of internal audit. Enterprise Risk and Opportunity management works in a coordinated manner with other functional lines, such as Ethics and IT, among others.

4.3 PROCESS OF ENTERPRISE RISK AND OPPORTUNITY MANAGEMENT

4.3.1 Enterprise risk and opportunity management at ENGIE Brasil should be implemented in a structured, systematic, and continuous manner, with biannual issuance of the Enterprise Risk and

Cópia não controlada

Opportunity Matrix (preliminary and final version), aligned with international best practices, including ISO 31000 and COSO ERM guidelines, as presented below:

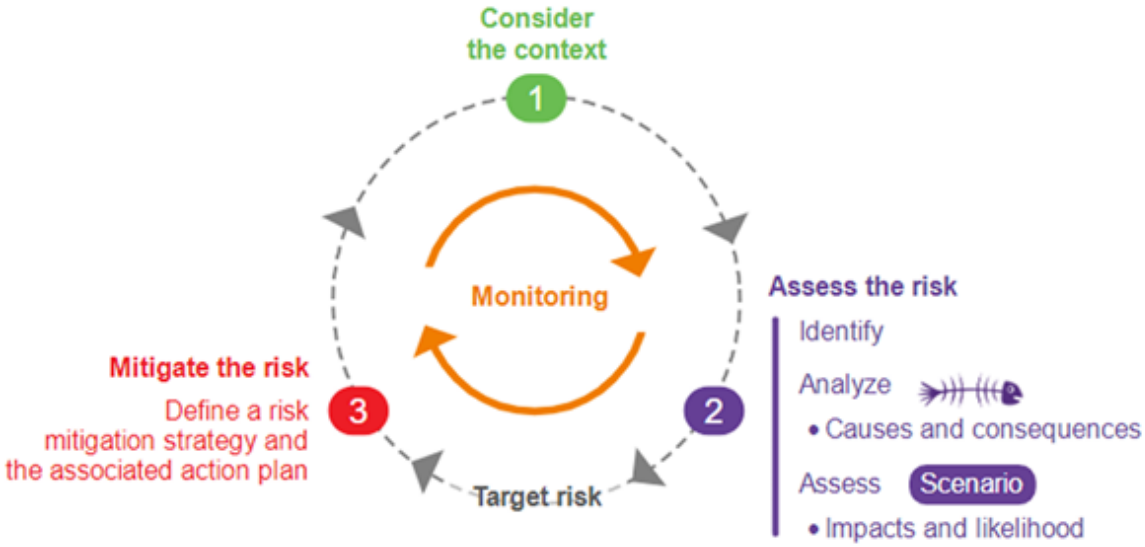


Figure 1: Enterprise Risk and Opportunity Management Cycle

a) Context consideration
Analysis of the business environment in which the Company operates.

b) Risk Analysis
Comprises the identification, analysis of causes and consequences, scenario assessment, with quantification/qualification of impact and probability of inherent risk (raw risk) and residual risk (risk after mitigation). Companies may establish a Risk Management Forum to promote and expand discussion on the topic.

c) Mitigation
Risk mitigation through continuous action plans and specific action plans with defined periods (start date and end date).

d) Monitoring
Identified risks, relevant materializations, and established mitigation plans are monitored by risk owners with the support of the enterprise risk and opportunity management area.

e) Approval
The enterprise risk and opportunity management process follows the schedule defined by the ENGIE Group each year. The Enterprise Risk and Opportunity Matrix must be approved in applicable instances: operational companies (Executive Board), ENGIE Brasil (Executive Committee with participation of GBU representatives). Furthermore, in publicly listed companies, the Enterprise Risk and Opportunity Matrix must be discussed in the Statutory Audit Committee and must be presented to the Board of Directors and the Fiscal Council.

f) Communication
The Enterprise Risk and Opportunity Matrix must be communicated to appropriate management levels of operational companies, GBUs, the ENGIE Group, Internal Audit, Legal

Cópia não controlada

area, and Internal Controls area. Enterprise risks and opportunities will also be communicated to other stakeholders in accordance with applicable legislation and ENGIE Group guidelines.

4.3.2 Enterprise Risk and opportunity management in project development must observe the PRM (Project Risk Management) methodology defined by the ENGIE Group. When projects are approved and move into the implementation phase, their risks are managed in accordance with the ERM methodology.

4.4 RESPONSIBILITIES AND ASSIGNMENTS

4.4.1 ENGIE Brasil maintains an organized structure responsible for the application of enterprise risk and opportunity management described in this Policy, at different levels of the organization, as detailed in the subsequent items.

4.4.2 **Risk Owner/Manager**

4.4.2.1 These are the responsibilities of the Risk Owner/Manager:

a) Identify, assess, and monitor risks associated with their activities and processes;
b) Develop, monitor, and regularly update action plans;
c) Keep risk information updated with the Enterprise Risk and Opportunity Management area;
d) Act as a reference in risk management in their area, promoting communication and prevention.

4.4.3 **Enterprise Risk and Opportunity Management Area**

4.4.3.1 These are the responsibilities of the Enterprise Risks and Opportunities Management Area:

a) Coordinate, monitor, and report corporative risks to the Administrators in order to support strategic decision-making;
b) Act in the preparation of the Risk Register for expansion projects, in accordance with ENGIE Group guidelines;
c) Contribute to reports related to enterprise risks and opportunities management for external stakeholders;
d) Serve as secretary to the Risk Management Forum, in the case of publicly listed companies;
e) Provide support to Executive Board in strategic decision-making related to risks;
f) Disseminate knowledge about risks and best practices in risk management, contributing to the strengthening of a culture of prevention and corporate responsibility.

4.4.4 **Risk Management Forum** [1]

4.4.4.1 These are the responsibilities of the Risk Management Forum:

a) Analyze and propose contributions to the draft of Enterprise Risks and Opportunities Matrix prepared by the enterprise risks and opportunities management area based on proposals submitted by business areas that own the risks;
b) Contribute to the identification of other risks and opportunities;

[1] Not mandatory, but recommended

Cópia não controlada

c) Validate the proposed Enterprise Risks and Opportunities Matrix (draft) to be submitted for approval by Executive Board;
d) Promote a culture of risk management, reinforcing conduct aligned with the Company's values.

4.4.5 **Executive Board**

4.4.5.1 These are the responsibilities of Executive Board:

a) They are responsible for managing the risks of their areas of activity or over which they have authority. They are the risk owners of their companies and may delegate ownership and management to other managers. "Every Manager is a Risk Manager";
b) Define the overall level of risk (risk appetite) that should be achieved within a specific period of time based on ENGIE Group guidance;
c) Ensure the execution of the Enterprise Risks and Opportunities Management Policy;
d) Integrate risk analysis into strategic and operational decision-making;
e) Ensure adequate resources, structure, and training for the enterprise risks and opportunities management in the areas under their responsibility;
f) Promote a culture of risk management and reinforce conduct aligned with organizational values;
g) Approve proposed changes regarding risk treatment and monitoring of mitigation plans.

4.4.6 **Statutory Audit Committee** [2]

4.4.6.1 These are the responsibilities of the Statutory Audit Committee:

a) Monitor the effectiveness of the enterprise risks and opportunities management process, compliance with laws and regulations;
b) Confirm whether the risk disclosed in external communication is based on risk assessment methodology and is in compliance with applicable standards and laws;
c) Advise the Board of Directors on the supervision of enterprise risks and opportunities management and on the continuous improvement of governance practices;
d) Evaluate and monitor the Company's risk exposures;
e) Be aware of and supervise the enterprise risks and opportunities management matrices, as well as their reviews.

4.4.7 **Board of Directors**[3]

4.4.7.1 These are the responsibilities of the Board of Directors:

a) Approve the Enterprise Risks and Opportunities Management Policy and its revisions;
b) Monitor the effectiveness of the enterprise risks and opportunities management process;
c) Be aware of and supervise the enterprise risks and opportunities management matrices, as well as their revisions;
d) Ensure that management has mechanisms and internal controls to identify, assess, prioritize, mitigate, report and monitor risks, in order to maintain them at levels compatible with the organization's risk appetite;
e) Promote a culture of enterprise risks and opportunities management, integrity, accountability and prevention at the highest level of the Company.

[2] In the case of publicly listed companies
[3] In the case of publicly listed companies

Cópia não controlada

4.4.8 **Executive Committee (COMEX)**

4.4.8.1 These are the responsibilities of the Executive Committee (COMEX):

a) Approve the Enterprise Risks and Opportunities Management Policy and its revisions;
b) Be aware of and supervise the enterprise risks and opportunities matrices, as well as their revisions.

4.4.9 **Enterprise Risks and Opportunities Management Support** (ERM functional line)

4.4.9.1 These are the responsibilities of the Enterprise Risks and Opportunities Management Support (ERM functional line):

a) ERM functional line is composed of all Risk Officers of the entities;
b) ERM functional line is supervised by the Risk Officer of ENGIE Latam and by the Chief Risk Officer (CRO) of each entity;
c) Chief Risk Officer (CRO) is a member of the Executive Committee (COMEX) of each entity and is responsible for risk management within its scope, for defining risk appetite and supporting the achievement of action plans.

4.4.10 **Risk Officer**

4.4.10.1 These are the responsibilities of the Risk Officer:

a) Conduct the annual risk review of its scope of action in accordance with the ERM methodology, under the supervision and validation of the CRO;
b) Implement Group guidelines in coordination with support areas;
c) Advise on the identification, analysis and assessment of risks and action plans;
d) As a Business Partner, must advise managers on how to reduce or increase risk-taking, both in daily operations and in projects, in compliance with Group laws, regulations and policies;
e) The Risk Officer includes in the annual risk review of its scope of action an assessment of the consistency between the evaluations of enterprise risks and opportunities management and those presented in the risks section of the MTP;
f) Act in the review of project risks (PRM);
g) Interact with the Internal Audit area to support it in establishing an Annual Audit Plan based on risks;
h) Interact with the Internal Control area to define the action plans of the Group's Internal Controls Program (INCOME), which serve as risk mitigation measures for Enterprise Risk Management (ERM);
i) Contribute to improving knowledge of the risks of its entity, thus increasing credibility, improving risk-taking assessment and, therefore, maintaining and creating value, acting to support strategic and operational decision-making;
j) Ensure that the Policy, procedures and methodologies are implemented correctly.

Cópia não controlada