1. PURPOSE

Define principles and guidelines for the Integrated Corporate Risk Management, within the operating framework of Companhia Paranaense de Energia - Copel (Holding), its wholly-owned subsidiaries (SIs), and controlled companies, respecting its corporate procedures

This Policy is applicable, on an indicative basis, to its jointly-owned companies, affiliated companies and other companies in which it holds equity interests.

For the purpose of this Policy, all the companies listed in the previous paragraph will hereinafter be referred to as Copel.

2. CONCEPTS

2.1 – INTEGRATED CORPORATE RISK MANGEMENT

A structured and continuous process designed to proactively identify and respond to potential events that are likely to affect Copel's objectives, seeking to maintain risks at appropriate levels. The process is divided into five macro steps: Identification, Assessment, Treatment, Monitoring and Communication. At COPEL, this model is based on the COSO - ERM (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management) and the Code of Best Corporate Governance Practices of the Brazilian Corporate Governance Institute (IBGC).

2.2 – RISK

Possibility of an event occurring and adversely affecting the ability to reach objectives, which may lead to negative impact, positive impact, or both. It will be a risk if the effect is negative or an opportunity if the result is positive. Risk is measured in terms of impact (or consequences) and probability and the following types of risk are considered:

a) inherent risk: risk existing before measures are taken to alter its probability or impact if the risk materializes; and

b) residual risk: risk remaining after measures have been taken to treat inherent risk.

2.3 - EVENT

Incident or occurrence caused by internal or external sources and affecting the achievement of the objectives.

2.4 - PROBABILITY

Indicates the possibility of a given event occurring.
Probability may be expressed in quantitative terms, such as percentage, frequency of occurrence, or another numerical metric, or in qualitative terms such as: high, medium, low.

2.5 - IMPACT

Outcome or effect of an event that affects objectives. Impacts (or consequences) may be expressed qualitatively or quantitatively. The impact of an event may be positive or negative in relation to the organization's objectives.

2.6 - INCIDENT

Unforeseen and undesirable event that may disrupt and prevent objectives being reached, cause financial loss, reputational damage and operational impacts.

2.7 - INTERNAL CONTROL

Set of policies and procedures developed and deployed to ensure reasonable certainty in relation to reaching

organizational objectives for operations, disclosure and compliance. Cope uses the COSO's Internal Control Integrated Framework.

2.8 - RISK APPETITE

Risk level that Copel is willing to accept in order to fulfill its mission and vision and generate shareholder value.

2.9 - RISK TOLERANCE

The acceptable variation for the achievement of Copel's objectives.

2.10 - RISK MANAGEMENT ROLES

2.10.1 - BOARD OF DIRECTORS - BoD

A collegiate resolution body responsible for:

- establishing the general orientation of Copel's businesses;
- defining the degree of risk appetite;
- establishing roles for the Executive Boards regarding risk management;
- approving the annual strategic risk plan;
- approving the Integrated Corporate Risk Management Policy;
- evaluating the effectiveness of the risk management process at Copel; and
- reviewing, every six months, the Risk Matrix and the resulting mitigation plans.

2.10.2 - STATUTORY AUDIT COMMITTEE - SAC

An Independent advisory and permanent body that reports to the Board of Directors and is responsible for:

- reviewing and supervising the accounting and financial reporting processes;
- evaluating the effectiveness of the risk management process at Copel;
- supervising the activities of the internal auditors and the independent external auditors;
- periodically reviewing the Corporate Risk Integrated Management Policy; and
- analyzing, on a quarterly basis, the Risk Matrix and the resulting mitigation plans.

2.10.3 - THREE LINES OF DEFENSE

- 1st line of defense: Comprised by the Executive Boards, department superintendents and managers, as well as project and process managers. This line is responsible for identifying and assessing risks and conducting routine control procedures to mitigate the vulnerabilities of their activities.
- 2nd line of defense: Provides risk management structures, internal controls and compliance, assisting the 1st line of defense in the development of effective processes and controls. The Governance, Risk and Compliance Departments are part of the 2nd line of defense
- 3rd line of defense: Conducts independent assessments for the effectiveness of governance, risk management, and internal controls, including how the 1st and 2nd lines of defense achieve risk and control management objectives. The Internal Audit is part of the 3rd line of defense.

2.10.3.1 – Executive Boards (1st Line of Defense)

These Boards are responsible for:

- sponsoring the implementation of risk management within the scope of their activities;
- defining the managers responsible for identifying and evaluating the risks inherent in their activities;

- supporting risk managers in establishing treatment actions and control mechanisms for identified risks; and
- supporting the Governance, Risk and Compliance Department - GRC in the preparation of the annual strategic risk plan.

2.10.3.2 - Risk Manager (1st Line of Defense)

The individual at Copel responsible for:

- identifying risks, their causes and how they impact Copel;
- establishing appropriate treatment actions and control mechanisms for each risk;
- conducting periodic monitoring of risks under his/her responsibility; and
- reporting, in accordance with the defined methodology and standards, all risks to the Governance, Risk and Compliance Department.

2.10.3.3 - Governance, Risk and Compliance Department - GRC (2nd Line of Defense)

The organizational structure at Copel (Holding) responsible for:

- defining and coordinating the implementation of guidelines, policies, methodologies and internal control and corporate risk management practices at Copel;
- ensuring the effective dissemination and proper application of policies and methodologies;
- preparing, along with the Executive Boards, the annual strategic risk plan;
- managing Copel's corporate risk portfolio;
- monitoring treatment actions and control mechanisms for identified risks; and
- periodically reporting risk management activities to the Statutory Audit Committee and the Board of Directors.

2.10.3.4 - Internal Audit (3rd Line of Defense)

The independent organizational structure responsible for:

- evaluating the effectiveness of the risk management process at Copel;
- evaluating the appropriateness of the treatment actions and internal control mechanisms, recommending, when necessary, improvements to the risk manager; and
- conducting periodic reports of its assessments to the Board of Directors and the Statutory Audit Committee.

2.11 - RISK MATRIX

A document in which risks, causes, impacts, exposure levels, risk managers, processes, treatment actions and other relevant information is recorded in order to monitor the identified risks. The graphic representation of this document is done through the Heatmap.

3. PRINCIPLES

3.1 - PROTECTION AND VALUE GENERATION FOR COPEL

Risk management is directly related to Copel's sustainable growth, identifying threats and providing information for risk-based decision making.

3.2 - RISK MANAGEMENT INTEGRATION WITH DEFINED STRATEGIES AND PERFORMANCE MONITORING

Risk management must support Copel's Management during the process that defines the Company's strategies and performance monitoring, ensuring the alignment of strategic objectives with Copel's mission, vision and

values.

3.3 - FORMAL ESTABLISHMENT OF ROLES AND RESPONSIBILITIES

Each risk management process role needs to be formally defined and the individuals involved must be communicated and state that they clearly understand their duties and responsibilities.

3.4 - CONSTITUTION AND MAINTENANCE OF ADEQUATE STRUCTURES

It is essential that an integrated risk management structure for processes, technology and people is periodically constituted and assessed by the governance bodies, so that such structure remains efficient.

3.5 - DEFINITION OF A COMMON METHODOLOGY FOR THE COMPANY

A common language should be adopted in risk management process, using recognized methodologies and standards and adapted to Copel's business profile and organizational structure.

4. GUIDELINES

4.1 - Maintain the risk management policy in line with Copel's objectives and strategies.

4.2 - Maintain effectiveness and compliance for the internal controls environment.

4.3 - Ensure the existence of risk monitoring for corruption and fraud in the internal controls environment.

4.4 - Integrate the risk management process into business relationships with suppliers and business partners.

4.5 - Adopt corporate performance indicators for the monitoring of the Integrated Corporate Risk Management.

4.6 - Ensure that severe risks with very low likelihood of occurrence are also considered when defining strategies.

4.7 - Consider socio-environmental, business sustainability, health and safety aspects, seeking to anticipate, evaluate and reduce the short, medium and long-term impacts of the Company's operations on society.

4.8 - Integrate and maintain levels of risk appetite that are aligned with Copel's strategy, business and financial dimensions.

4.9 - Adopt practices for reporting and controlling incidences.

4.10 - Adopt risk appetite criteria that, on a timely basis, must be submitted for awareness by the Board of Directors - BoD.

4.11 - Direct all identified opportunities to the responsible areas for analysis and implementation of necessary actions for their accomplishments.

4.12 - Ensure that associated risks and controls are reviewed at least annually, in accordance with the criteria related to the exposure of their associated risks.

4.13 - Ensure that the processes and activities involving the Integrated Corporate Risk Management are carried out by the three lines of defense.

4.14 - Ensure that approval authority and duty responsibilities is clearly segregated and maintained within activities.

4.15 - Ensure that the overall process for risk identification and analysis is monitored and continuously improved to identify potentially unknown risks.

4.16 - Promote a risk management corporate culture, especially in subsidiaries, jointly controlled companies and affiliates.

5. RISK CATEGORIES

Copel defined its risk category classification according to the four classes of objectives set by COSO - ERM, the

nature of its operations and the relationship with its activities:

5.1 - STRATEGIC RISK

- Strategic - risks associated with senior management decision-making and strategic planning, which could generate a substantial loss in Copel's economic value.
- Reputational - the possibility of losses resulting from the deterioration of Copel's brand with the market, customers and regulators, due to negative publicity.

5.2 - FINANCIAL RISK

- Market - risks associated to the fluctuation in fair value or future cash flows of a financial instrument due to changes in market prices, such as exchange rates, interest rates and stock prices.
- Liquidity - the possibility of not having sufficient resources, cash or other financial assets, to settle obligations on their due dates.
- Credit - the risk of incurring losses arising from the difficulty of receiving amounts invoiced to its clients or a counterparty in a financial instrument, resulting in the lack to comply with its contractual obligations.
- Disclosure - risks associated with the possibility of issuing incomplete, inaccurate or untimely financial, managerial, regulatory, tax, and statutory. reports, exposing Copel to fines, penalties or other sanctions.

5.3 - OPERATIONAL RISK

- Processes - risk related to the effectiveness and efficiency of Copel's operations, including financial and operational performance targets and the safeguarding of asset loss and the possibility of losses resulting from failure, deficiency or inadequacy of internal processes, people and systems, or external events.
- Information Technology - risks of unauthorized access to company data and information, resulting from vulnerability in access control mechanisms, segregation of duties and/or violation of policies that cause external attacks, interruptions to the IT environment, alterations or improper disclosure of information.
- Socioenvironmental - risks related to the impacts of Copel's operations on society and the environment, which may affect the Company's reputation and generate sanctions by the regulatory agencies. This risk is also associated to the effect of severe weather, scarcity of natural resources or mobilization of communities, which may cause interruption in services or damage to energy production.
- Projects - risks related to transmission, generation, distribution, telecommunications, research and development projects, among others, which may imply additional costs, delays in project delivery and sanctions by regulatory agencies.

5.4 - COMPLIANCE RISK

- Laws and regulations - non-compliance with environmental, labor, tax and regulatory laws to which Copel is subject to, including internal policies and regulations, exposing the Company to the sanctions by regulatory agencies.
- Fraud and corruption - risks related to physical theft of assets, the passing on of information, misuse of financial resources, conflicts of interest, influence peddling, bribery, collusion with suppliers and customers, among others, resulting in financial losses, fines, penalties and sanctions by regulatory agencies thus deteriorating Copel's image.

6. RELATED LEGISLATION AND REGULATIONS

a) Federal Law 12846/2013 (anti-corruption law);
b) Federal Decree 8420/2015 (regulates anti-corruption law);
c) Federal Law 13303/2016 (State Company Law);
d) Federal Law 8429/1992 (Law on Administrative Misconduct);
e) Sarbanes-Oxley Act of 2002, particularly sections 302 and 404;
f) United States Foreign Corrupt Practices Act (FCPA), 1977;

g) ABNT Standard NBR ISO 26000, 2010;
h) NPC 0101 - Financial Investment Policy;
i) NPC 0103 - Disclosure of Material Information and Preservation of Confidentiality Policy;
j) NPC 0105 - Investor Relations Policy;
k) NPC 0310 - Communications Policy;
l) NPC 0303 - Sustainability Policy;
m) NPC 0301 - Information Security Policy;
n) NPC 0106 - Related Parties Transactions and Conflicts of Interest Policy;
o) NPC 0308 - Corporate Governance Policy;
p) NAC 030901 - Process Management;
q) NAC 030905 - Portfolio and Project Management;
r) COSO - ERM (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management);
s) Risk Management Model published by the National Quality Foundation – FNQ;
t) Code of Best Corporate Governance Practices of the Brazilian Corporate Governance Institute (IBGC); and
u) CVM Instruction 586, dated June 08, 2017.

This document is a updated to NPC 0104 dated 09/19/2016.

This Policy was approved at the 2,284th Executive Board Meeting (“*Redir*”) on 01/22//2018 and at the 174th Board of Directors’ Meeting on 01/23/2018.

Document signed by:

ANTONIO SERGIO DE SOUZA GUETTER
Chief Executive Officer

Change control	
Date	Description
09/19/2016	Inclusions: Positive impact and opportunity in the risk concept, item 2.6 Compliance with internal rules and policies as a compliance risk, item "d" of item 2.10 Risk Profile. Guideline 4.12 to annually submit the risk appetite criteria adopted to the Audit Committee, replacing the risk appetite parameter table.

	Guideline 4.13 on identified opportunities.
03/28/2018	Adequacy to the existing organizational structure. Alterations: • Update of the concepts of Integrated Corporate Risk Management, risk and event to adapt them to COSO ERM, items 2.1 to 2.3; • Adjustment to item 4.5 to define what monitoring is for the integrated management of risks and not just the risk itself; • Inclusion of health and safety aspects in guideline 4.7; and • updating of legislation related to the subject, item 6. Inclusions: • Concepts of Roles for Risk Management, Line of Defense and Risk Matrix, item 2.10 and sub-items; and • Guidelines 4.12 to 4.16. Exclusions: • Concepts of subsidiaries and affiliates; and • Concepts of fraud and corruption.