

**PL-OSPB-00007**

Version B

## **ENTERPRISE RISK MANAGEMENT POLICY**

Approved by Yuri Gama Lopes/BRA/Petrobras (RISCOS) on May 27, 2024 | Managed by RISCOS/GIR

ACTIVE Standard

### **1. APPROVAL MINUTES**

Policy approved by the Petrobras Board of Directors - Minutes CA 1.647, item 12, Agenda nº 183 of 12/16/2020

### **2. SCOPE**

Applies to the Petrobras System, respecting the necessary procedures and approvals, as provided for in article 16 of Petrobras' Bylaws and the Bylaws of other companies.

### **3. PRINCIPLES**

**3.1** Life must be respected in all its diversity, and the rights, obligations, facilities, processes, information, reputation, and image of the company must be protected against threats arising from intentional or unintentional actions.

**3.2** Risk management is aligned and consistent with the company's strategic plan.

**3.3** Risk management is part of the company's commitment to act ethically and in compliance with the legal and regulatory requirements established in the jurisdictions where it operates.

**3.4** Risks are considered in all decisions, and their management must be carried out in an integrated manner, taking into account the inherent benefits of diversification.

**3.5** Actions to respond to risks consider the possible long-term cumulative consequences, the potential impacts on our stakeholders, and should be oriented towards the preservation or aggregation of value and business continuity.

## **4. GUIDELINES**

**4.1** Strengthen the risk management philosophy as part of the company's corporate culture.

**4.2** Seize opportunities and anticipate threats that affect our strategic, economicfinancial, operational, or compliance objectives.

**4.3** Promote uniformity of concepts and integration of methodologies used in risk identification, analysis, evaluation, and treatment to improve the reliability of information and the transparency of the entire risk management process.

**4.4** Proactively and comprehensively manage risks associated with business, management processes, and corporate services to maintain them at an acceptable level of exposure, consistent with Petrobras' risk appetite.

**4.5** Undertake risk management actions effectively, efficiently, economically, and effectively.

**4.6** Align risk management actions with the actions of organizational units responsible for internal controls, compliance, and internal audit of the company.

**4.7** Strengthen autonomy in the risk management process and the segregation of roles between risk takers and those responsible for monitoring them.

**4.8** Allow administrators, investors, and other stakeholders access to a continuous, transparent, and appropriate flow of information associated with key risks and their management process in the company, respecting the degree of confidentiality of information, as well as corporate procedures, policies, guidelines, and other internal corporate security and information standards.

**4.9** Enable employees and service provider companies (through contracts) to continuously and adequately build risk management skills according to their assignments

**4.10** 10 Improve monitoring and critical analysis of risk management as an integral part of a continuous process of improving corporate governance.

## **5. AUTHORITY AND RESPONSIBILITY**

### **5.1 From the Board of Directors (CA) or equivalent governing body of the company**

**5.1.1** Approve the company's risk appetite, proposed by the Executive Board or equivalent body.

**5.1.2** Systematically monitor risk management.

### **5.2 From the Statutory Audit Committee or equivalent**

**5.2.1** Assist the Board of Directors or equivalent governing body in establishing global policies regarding risk management.

### **5.3 From Internal Audit**

**5.3.1** Systematically evaluate the risk management process and recommend improvements.

### **5.4 From the Executive Board (DE) or equivalent**

**5.4.1** Propose the risk appetite.

**5.4.2** Ensure the necessary measures for alignment between risk appetite and risk exposure of the company.

### **5.5 From the Executive Risk Committee or equivalent**

**5.5.1** Monitor actions to treat enterprise risks.

Analyze and issue recommendations regarding:

**5.5.2** risk management policies and processes, as well as actions to mitigate key risks.

**5.5.3** risk monitoring metrics and exposure limits, aiming to provide advice to the DE or equivalent body in matters related to the subject; and

**5.5.4** refer to the Executive Board or equivalent body any risk management topic deemed relevant for knowledge or deliberation by the DE or CA, or equivalent body.

## **5.6 From the organizational unit responsible for corporate risk management**

**5.6.1** Define a corporate risk management methodology based on an integrated and systematic vision that allows for continuous risk monitoring at various hierarchical levels of the company.

**5.6.2** Disseminate knowledge and support the application of risk management practices in organizational units.

**5.6.3** Identify, monitor, and periodically report key risks of Petrobras to the Executive Board and the Board of Directors.

## **5.7 From holders of the company's overall structure**

**5.7.1** Keep their risk database up to date, in coordination with the organizational unit responsible for corporate risk management.

## **5.8 From holders of organizational units (managers)**

**5.8.1** Coordinate, promote, and monitor risk management actions in their area of operation.

**5.8.2** Develop and improve methodologies to enhance the identification, treatment, and monitoring of specific risks, in line with this policy, guidelines, and corporate risk management standards, in coordination with the organizational unit responsible for corporate risk management.

**5.8.3** To provide the organizational unit responsible for corporate risk management, whenever required, with all necessary information for the integrated assessment of risks, monitoring, and reporting to senior management

## **5.9 From employees**

**5.9.1** Act in the risk management process by applying methodologies for risk identification, analysis, treatment, and monitoring.

**5.9.2** Timely communicate to process managers any identified or altered risks.