# RISK MANAGEMENT POLICY
# PETRO RIO S.A.

# Table of Contents

# 1. Purpose

The purpose of this Risk Management Policy ("Policy") is to establish principles, guidelines and responsibilities that must be observed in the Enterprise Risk Management process inherent to PetroRio's activities, from the identification, analysis, prioritization, treatment approach, monitoring and communicating risks that could affect the scope and execution of the planned strategy.

By adapting the company's governance to good market practices, the decision-making process becomes more robust, incorporating the vision of enterprise risks, which enables the creation and preservation of value for PetroRio.

Furthermore, the policy aims to be an instrument to assist in the dissemination of PetroRio's enterprise risk management culture, as it seeks to establish a common language on the subject, as well as determine the responsibilities of each governance agent involved in the process.

# 2. Scope

This Policy applies to all directors, officers, employees, third parties, and to all people who work directly or indirectly for PetroRio, its subsidiaries, companies under common control, consortiums, business and commercial partners with whom PetroRio has business relationship, regardless of the nature of the relationship, whether ongoing or one-off, whether it involves the transfer of financial resources or just knowledge (know-how). It should be noted that the policy will also automatically apply to new controlled and affiliated companies.

# 3. Definitions

- **Mitigating action**: Actions and controls implemented by PetroRio with the objective of mitigating risk exposure, reducing the probability of its materialization;
- **Risk Appetite**: Level of risk that PetroRio is willing to accept in the pursuit and realization of its strategy and purposes. It is noteworthy that not all types of risk are acceptable;
- **Enterprise Risk Management (ERM)**: Process conducted by the different governance bodies of the company, such as the Board of Directors, Ethics and Compliance Committee and business areas, which aims to establish strategies to identify, analyze, assess, treat, monitor and communicate potential events that may affect the execution of the planned strategy;
- **Enterprise Risk Factor**: Situations and/or circumstances that may lead to an increase in the probability of a risk occurring;
- ***Key Risk Indicator*** **(KRI)**: Metric used to obtain exposure to enterprise risk, being recommended that it is related to the cause of the risk and measured in a defined periodicity according to the criticality of the factor, in order to anticipate a possible materialization of the risk;
- **Impact**: These are the consequences resulting from the materialization of an enterprise risk, which can be expressed quantitatively and/or qualitatively;
- **Enterprise Risk Map**: Graphical representation of enterprise risks allocated according to the criticality of each risk through the assessment of its impact and probability;
- **Action plan**: Plan containing the actions to be implemented by PetroRio in order to mitigate the identified risk;
- **Enterprise Risk Portfolio**: Catalog containing the list of enterprise risks and their respective risk factors;
- **Probability**: Chance of enterprise risk materializing;

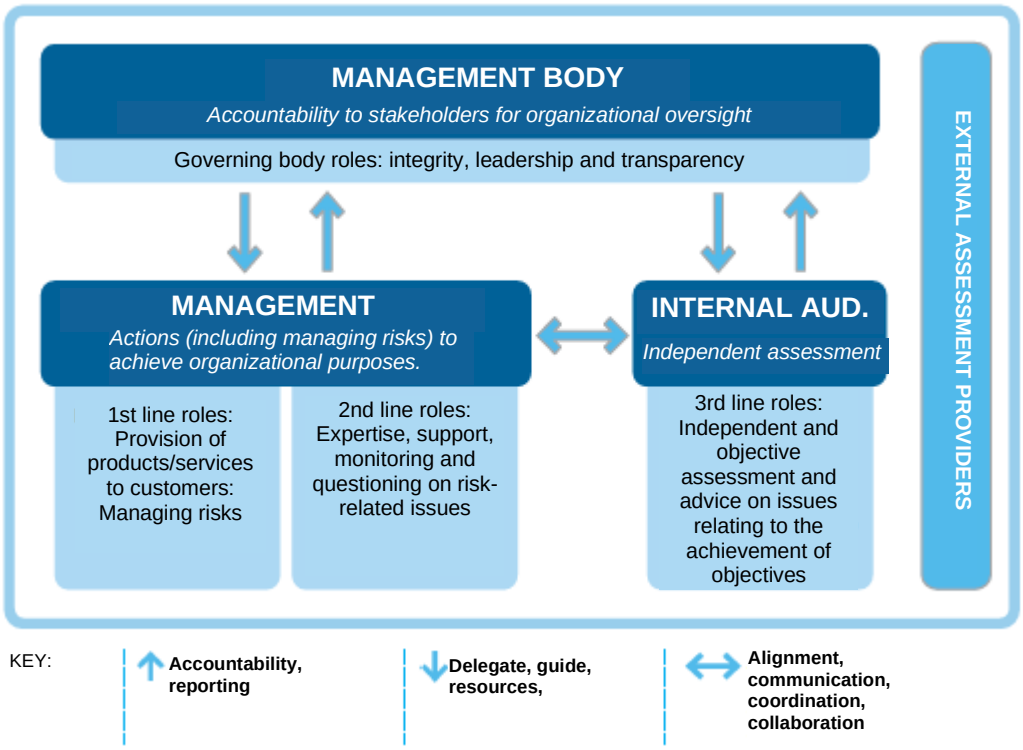
- **Risk Owner**: PetroRio's employee responsible for mitigating and monitoring enterprise risk that is under his/her competence;
- **Impact x Probability Table**: Document that formalizes the description and the criteria to be considered for each of the dimensions analyzed in the classification of the Impact and Probability level of the identified enterprise risks, resulting in the indication of the Inherent and Residual risk;
- **Risk Response**: Definition of the treatment that PetroRio will assign to the risk factor. In response, you can choose to avoid, reduce, transfer or accept;
- **Risk**: Possibility of the occurrence of an event that has an adverse impact, making it difficult or impossible to achieve PetroRio's strategic objectives;
- **Enterprise Risk**: Risks that may impact the scope and execution of the planned strategy or the business as a whole;
- **Inherent Risk**: Risk intrinsic to the operation of the business or activity, not considering the actions and controls existing in the company;
- **Residual Risk**: Risk remaining after considering all existing actions and controls to mitigate it.

# 4. Guidelines

## 4.1 For enterprise risk management

PetroRio is committed to Risk Management and has the practice of constantly analyzing the risks to which it is exposed and that may adversely affect its business, financial situation and the results of its operations.

In this sense, the risk management model practiced at PetroRio is based on the three-line concept of the Institute of Internal Auditors (IIA), where each entity in the organization has defined roles in its risk management process. As stated, the model "helps organizations identify structures and processes that best support the achievement of objectives and facilitate strong governance and risk management".




**Source:** nstitute of Internal Auditors (IIA) Position Statement - the three lines in effective risk management and controls (2020).

This model provides for the following attributions to each instance:

- **Management Body**: Comprised of PetroRio's executive board, they are responsible to the stakeholders for the organization's success, ensuring that the organizational purposes and activities are aligned with the prioritized interests of the stakeholders;
- **1st Line**: Functions/areas that manage and own risks - include both "*front of house*" and "*back office*" activities, they are the areas responsible for maintaining effective internal controls, conducting their day-to-day activities risk management procedures and controls.
- **2nd Line**: Functions/areas that supervise risks - represented by support/technical knowledge areas, they are those responsible for establishing guidelines and procedures related to risk management and compliance for the development and/or monitoring of first line controls.
- **3rd Line**: Functions that provide independent analysis/assessments - Internal Audit is an independent and objective assessment and consultancy activity designed to add value and improve an organization's operations. In this concept, it is responsible for the independent review of risk management, supporting the organization in achieving its objectives and presenting a systematic and disciplined approach to assess and improve the effectiveness of risk management, controls and governance processes.

## 4.2 For the identification of risks

This step aims to identify and map the risks to which PetroRio may be exposed and that may affect its strategy, objectives and operation. That is, the identification of risks involves describing the risks to which the Company is exposed, defining their nature and the causes, consequences and those responsible for each risk.

Risk mapping requires the involvement of the three lines, and can be carried out through interviews with the company's main executives and managers, applied perception surveys, document analyzes from assessments carried out, reports and/or letters of internal controls issued by audits internal and/or external, including inspections, among others. Given the company's performance, risk mapping may also consider factors external to the organization, such as: economic, political, social, environmental, among others.

Based on the theoretical framework proposed by COSO ERM as well as the company's organizational culture, and in order to facilitate the assessment, treatment and monitoring of risks, PetroRio categorized its risks into the following categories set out in its Enterprise Risk Portfolio:

- **Strategic**: risk of losses resulting from the failure of the strategies adopted, taking into account the dynamics of business and competition, achievement of the mergers and acquisitions strategy, political and economic changes in the country and abroad, company image, in addition to environmental, social and governance issues.
- **Financial**: risk of losses resulting from market fluctuations that impact the organization's assets, as well as risks related to the credit capacity of customers and paying sources and PetroRio's liquidity towards its financial obligations;
- **Operational**: risk of losses resulting from failures in processes and operations, third-party management, contracts, information technology, in addition to those related to People and Management processes.
- **Compliance**: risks of losses and legal or regulatory sanctions that the company may suffer as a result of failure to comply with regulations and legislation that may cause or cause damage to PetroRio's reputation and image.

## 4.3 For risk assessment

Once the risks are identified, they must be assessed from the perspective of Impact and Probability, either in the indication of the Inherent risk, or in the indication of the Residual risk. For this, the **Impact x Probability Table** approved by the Ethics and Compliance Committee should be considered.

Based on the analysis of existing controls at PetroRio and its level of exposure, the risks must be prioritized in order to enable an adequate focus on the treatment of risks considered to be of high exposure / greater than the defined risk appetite.

At this stage, the Internal Controls function must be involved to assist in the identification of existing and/or absent internal controls, in order to ensure adequate addressing of residual risk. In order to address the substance of the control, and according to the understanding of the risk owner and its materiality, the techniques of self-assessment and/or walkthrough will be applied.

Furthermore, it is recommended that internal controls be independently assessed by Internal Audit on a periodic basis, with the aim of ratifying and/or rectifying the degree of exposure to a given risk event.

### 4.4 For the treatment of risks

This step involves the management's definition of a response to the identified risks in order to bring the exposure to a given risk to a level that is acceptable to PetroRio, as defined in its risk appetite.

You can choose from four risk responses, namely: accept, avoid, mitigate or transfer

- **Accept the risk:** No action is taken for the identified risk. Risk is generally accepted when its level is within PetroRio's risk appetite ranges. In this situation, there is no need for a new control to mitigate the risk, as the existing controls have been applied effectively and continuously, and may be subject to inspection and/or testing;
- **Avoid the risk:** Discontinue the activities that generate the risk. A risk is generally avoided when there is a probability of a significant impact on PetroRio's purposes and the costs of implementing controls are very high, making its mitigation difficult; whether or not its transfer is possible;
- **Mitigate the risk:** Implement controls that reduce the causes and effects of risk. A risk is generally mitigated when it is likely to have a significant impact on PetroRio's purposes. The implementation of controls, in this case, presents an adequate cost/benefit;
- **Transfer the risk:** Reduce the risk by assigning it to a third party through, for example, taking out insurance, adopting a *hedging* instrument, among others. A risk is transferred when there is a probability of a significant impact on PetroRio's objectives, but the implementation of controls does not present an adequate cost/benefit.

### 4.5 For the assumption of risks

It consists of the analysis and validation by the Risk Owner, the Ethics and Compliance Committee and the Executive Board of the level of exposure to a risk, considering possible justifications for this (such as not being feasible to establish actions for its mitigation) and, thus, accepting the consequences that this situation may bring in the future.

All risk-taking processes must be sent to the Executive Board.

| Risk Criticality | Scope of Acceptance | Scope of Approval |
|---|---|---|
| Critical and Significant | Ethics and Compliance Committee | Executive Board |
| Moderate | Risk Owner | Ethics and Compliance Committee |
| Low and Minimum | Risk Owner | |

## 5. Responsibilities

### 5.1 Board of Directors

- To approve the Enterprise Risk Management Policy, as well as its amendments arising from the revisions;
- To define PetroRio's risk profile;
- To assess the adequacy of the risk function in order to ensure the effectiveness of this Policy.
- To ensure the effectiveness and monitoring compliance with PetroRio's Risk Management process;

- To ensure the authority, autonomy, independence and responsibility of the risk function;

## 5.2 Ethics and Compliance Committee

- To validate and approve the Impact and Probability Table;
- To approve the guidelines for the Enterprise Risk Management process, including the matrix of identified risks;
- To ensure compliance with the authority matrix for risk assumption;
- To support the dissemination of the Risk Management culture;
- To assess the adequacy of human and financial resources for enterprise risk management;
- To follow up on risk treatment action plans;
- To receive a report from the risk function to periodically assess the matrix of prioritized enterprise risks and established mitigating actions;
- To advise the Board of Directors in the periodic assessment and monitoring of the enterprise risk portfolio.

## 5.3 Executive Board

- To participate in the Enterprise Risk Management process and ensure that it is aligned with PetroRio's practices and good market practices;
- To ensure the adequacy of human and financial resources for enterprise risk management;
- To disseminate the Risk Management culture throughout PetroRio;
- To appreciate eventual changes in the provisions of the Enterprise Risk Management Policy;
- To participate in the process of building and updating the enterprise risk portfolio;
- To contribute to the risk assessment, according to the established impact and probability criteria;
- To support the definition of enterprise risk owners;
- To approve the portfolio and indicate the risks to be prioritized;
- To ensure *enforcement* so that risk owners act properly in the assessment, treatment and monitoring of enterprise risks;
- To assess the action plans to be led by the owners of the prioritized enterprise risks;
- To approve the assumption of responsibility process related to significant and high risks after acceptance by the Ethics and Compliance Committee.

## 5.4 Risk Function

- To develop, suggest and review guidelines for PetroRio's enterprise risk management process;
- To develop and keep the Enterprise Risk Management Policy updated;
- To monitor the implementation of the Enterprise Risk Management Policy throughout PetroRio;
- To develop and carry out the work plan, including budget, resources (human and technological) and deadlines, in order to enable the execution of the Enterprise Risk Management process efficiently;
- To assist in adapting areas to PetroRio's risk profile;
- To promote the interface between the risk management process and the business strategy update;
- To develop communication and training actions aimed at disseminating the Enterprise Risk Management culture throughout PetroRio;
- To provide methodological support for the enterprise risk management to PetroRio's areas;

- To receive and consolidate any changes in the criticality of enterprise risks and report them to the Executive Board, Compliance Committee and the Board of Directors;
- To monitor and consolidate the status of action plans and risk indicators (KRIs) sent by the enterprise risk owners and issue periodic reports to the Executive Board, the Ethics and Compliance Committee and the Board of Directors;
- To propose a review of the enterprise risk portfolio whenever there are updates to the strategic planning.

## 5.5 Function of Internal Controls

- To act in the continuous improvement of PetroRio's internal control environment;
- To work together with the Risk Management function to support risk owners;
- To disseminate the internal control culture at PetroRio through training and focused communications;
- To map PetroRio's internal processes according to the degree of exposure to risks, working with risk owners and other managers in the construction of control matrices;
- To assist in the risk assessment process, especially with regard to the identification of existing internal controls;
- To support risk owners in the preparation and implementation of risk mitigation action plans;
- To assist the other areas in the (re)design of their processes, according to the jointly defined action plan;
- To assist risk owners in reporting the progress of implementation of action plans to the Risk Management function;
- To establish controls in order to ensure the effectiveness of the Risk Matrix.

## 5.6 Risk Owners

- To identify, assess, treat and monitor the related risks, in order to fulfill the strategic purposes and in compliance with PetroRio's risk profile;
- To develop, suggest and implement action and/or contingency plans for risk mitigation (with the involvement of other areas, if necessary);
- To develop risk sheets and update them periodically and whenever necessary;
- To act in the continuous improvement of PetroRio's internal control environment;
- To disseminate the culture of risk management and internal controls to the other members of its area;
- To communicate to the risk function in a timely manner when identifying new risks or changes to current risks;
- To implement the action plans defined together with the Risk Management and Internal Controls functions based on each identified risk;
- To define risk indicators (KRIs) to monitor the variation and results of enterprise risks under their responsibility;
- To make periodic reports to the risk function on the monitoring of the risk under its responsibility;
- To make reports to the Executive Board, Ethics and Compliance Committee, and/or Board of Directors when required.

## 5.7 Internal Audit Function

- To act in the continuous improvement of PetroRio's internal control environment;

- To independently and objectively assess PetroRio's risk management process;
- To independently, objectively and continuously assess the internal controls established for prioritized risks and/or exposures greater than PetroRio's risk appetite;
- To establish an audit plan to assess PetroRio's internal processes according to their degree of risk exposure;
- To assess the effectiveness of implemented action plans;
- To contribute to the improvement of PetroRio's internal control environment through interactions with the areas of the audited processes, generating recommendations and improvements;
- To contribute to improvements in the decision-making process by reporting the results of independent audits carried out;
- To make reports to the Executive Board, Ethics and Compliance Committee and/or Board of Directors about the assessments carried out.

# 6. Non-compliance

## 6.1 Suspected Violation of Policy and Disciplinary Measures

All incidents or suspected violations of this Policy will be treated, within reasonable limits, in a confidential manner, unless PetroRio is required by law or court order to disclose the incident or suspicion, and provided that the physical integrity or the lives of PetroRio's employees and any third parties are not at risk, in which case the Company believes it is their duty to promptly report them to the competent authorities.

Failure to comply with the guidelines set forth herein and related laws to which PetroRio is required, including by default, will result in the application of disciplinary measures and penalties provided for by law, in addition to liability for losses and damages caused to PetroRio and third parties.

## 6.2 Reporting Concerns in the Integrity Channel

Any violation of this Policy must be reported through the Integrity Channel or directly to the immediate superior and investigated by the Ethics and Compliance Committee, pursuant to the applicable Law and regulations. Information registered in the Integrity Channel or reported directly to the immediate superior will be treated as confidential, and the identity of the whistleblower will be preserved.

## 6.3 Non-Retaliation

The confidentiality, identity and integrity of those who, in good faith, report a fact or suspected conduct in violation of the rules of this Policy will be preserved at all times.

* * *