Ecopetrol's Risk Management System

2022

All Ecopetrol employees are responsible for understanding and identifying the risks to which they are exposed in the performance of their duties and in the processes in which they participate, and for adequately addressing manageable risks in the performance of their duties. Risk management is performed in alignment with the company´s principles, such as Integrity and Responsibility, and with our cultural statement.

INTEGRATED RISK MANAGEMENT SYSTEM - SRI

The Ecopetrol´ s Integrated Risk Management System is defined as a set of principles, reference frame, and process that allow the organization to manage the effects of uncertainty on meeting objectives, to maximize opportunities, and to assist in establishing strategies and making informed decisions.

Integrated risk management at Ecopetrol adheres to ISO 31000, COSO 2013, and COSO ERM 2017 standards

The Integrated Risk Management System (SRI for its acronym in Spanish) acts as the general regulatory guideline for all risks managed at Ecopetrol and its Group, which are at the strategic, tactical, and operational level.

Each of these levels have different risk typologies, according to the various related regulations and standards. This means that those accountable for risk management in the organization must apply particular risk management methods at the appropriate level of responsibility, keeping them within the risk management principles, framework, and procedures stablished in the Integrated Risk Management System.

RISK MANAGEMENT CYCLE

The risk management cycle / process is systematically applied to all types of risks in the organization at the strategic, tactical and operational levels, through the execution of the following steps:

Risk Management System Cycle

- ***Plan:*** Definition of scope of activities and analysis of internal and external context.
- ***Identify:*** Identification of risks based on the points of view of the people involved and on the analysis of information.
- ***Evaluate:*** Analysis of causes and consequences. Asessment according to probability and impact.
- ***Treat:*** Selection and implementation of options to address the risk.
- ***Communication and inquiry, Record and Report, Monitoring and Review:*** Exchange of information, feedback, continuous monitoring and periodically review of the risk exposure, documentation and reporting of the results of each stage of the cycle, Example: new or modified risks, materialization of risks, potential risks, changes in risk assessments, risk alerts and changes in risk exposure.

Any change in the objectives of the organization and its internal and external environment could result in risk changes, so risk management process at Ecopetrol reflects the dynamics of the organization.

See further details in https://files.ecopetrol.com.co/web/esp/cargas/ecopetrol-rigs-2022-eng.pdf page 161 - 162 .

BUSINESS RISKS

Related to risk directly associated with the company´s strategy, strategic objectives, and/or balanced management dashboard, represented in the business risk map.

Ecopetrol´ s Business Risk Map

1. Unsuccessful protection and incorporation of resources and reserves.
2. Competitiveness of Assets against energy transition.
3. Impact on financial sustainability and value generation.
4. Subordinates that do not fulfill the promise of value.
5. Incidents of operational disruption due to environmental causes.
6. Unsuccessful transition and incorporation of ISA to the Ecopetrol Group.
7. Spread of epidemics that impact the operation.
8. HSE events due to operational causes.
9. Projects that do not meet their value expectation.
10. Breaches of ethics and compliance.
11. Cyberattacks, leak or loss of information.
12. Organizational culture that does not leverage the strategy.
13. Breach of commitments by third parties.
14. Impact on the operation or corporate governance due to geopolitical or regulatory changes or provisions of control entities and the state.
15. Inadequate management against climate change and water.

The construction and updating of the business risk map is conducted collectively, based on internal and external environment analyzes, considering market trends, the specific risks for Ecopetrol Group companies, as well as management standards, benchmarks, and industry risks, which are normally subject to analysis and review by sustainability indices and radars.

The assessment of these risks is performed using the Risk Assessment Matrix, which contains the thresholds of risk acceptance and tolerance, approved by the Board of Directors.

In 2022, 61 KRIs and 85 treatment actions were defined to manage the causes or reduce the consequences of business risks, ensuring that they are measurable over time, quantifiable and verifiable, which ensures their effectiveness.

Additionally, when we have a risk materialization, action plans are defined and executed with the participation of the impacted businesses, maintaining the risks within the tolerance and acceptance levels defined in Ecopetrol.

See further details in https://files.ecopetrol.com.co/web/esp/cargas/ecopetrol-rigs-2022-eng.pdf page 164.
See further details in https://www.ecopetrol.com.co/wps/wcm/connect/474e0c61-7b23-4870-b5bf-fe7f21b5f957/Ecopetrol+Business+Risks+2022.pdf?MOD=AJPERES&attachment=false&id=1685744380014

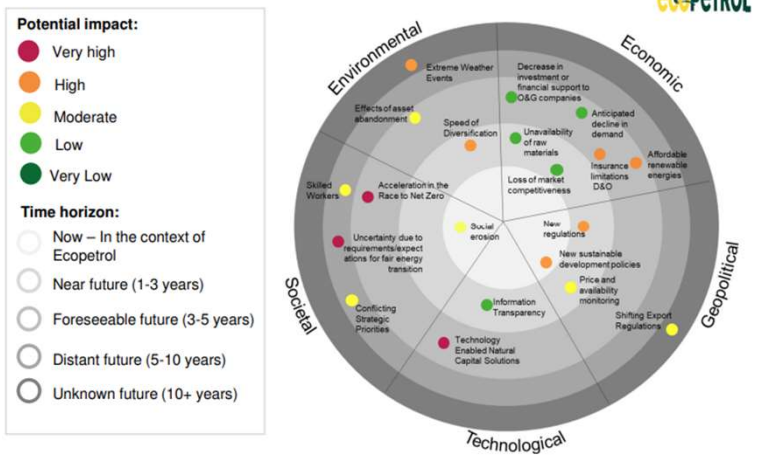
EMERGING RISKS

Ecopetrol defines emerging risks as the that are expected to have a long-term future impact on the company (3-5 years and beyond) or in some instances, they have already begun to impact the company.

According to our definitions and methodologies, emerging risks are considered those that meet some of the following characteristics: i) The risk is new, developing, or significantly increasing in importance. ii) A familiar risk in a new or unfamiliar context or under new context conditions (re-emerging). iii) The potential material financial or reputational impact of the risk is long-term and significant. iv) It is an external risk that arises from events external to the company which are beyond its influence or control. v) The risk and its impact on the company are specific, and vi) Has a high potential impact to Ecopetrol and may require Ecopetrol to adapt its strategy and/or business model.

Emerging risk radar

The following is a graphic representation of the evaluation of emerging risks.



Ecopetrol evaluates each potential risk and defines the treatment plan for each emerging risks which include the following: i) New business risk; ii) Incorporation into existing business risk; iii) Continuous monitoring of emerging risks; or iv) Abandonment of emerging risk.

See further details in https://www.ecopetrol.com.co/wps/wcm/connect/a09b34c6-7c99-4109-b62a-e198f6b83321/ECP+Emerging+risks+2022+Ing.pdf?MOD=AJPERES&attachment=false&id=1685500961733

RISK APPETITE AND RISK TOLERANCE

Our first expression of risk appetite is immersed in the Ecopetrol Group's strategy 2040 and is an element that considers concepts related to reputation, sustainability, environment, compliance, among others.

For the strategic level we have some zero tolerance risks, such as:

- Zero tolerance to fatalities in the exercise of the company's activities.
- Zero tolerance to practices against what is established in the Code of Ethics and Conduct of the Ecopetrol Group.
- Zero tolerance to practices against what is established in the regulations related to the environment, integrity of people, communities and other stakeholders, among others.

In addition, there are some quantitative and qualitative strategic, financial and operational parameters that complement the company's risk appetite:

- ✓ Strategic risk parameters: For example, new products to be introduced, products to be avoided and investment focus for capital expenditures.
- ✓ Financial risk parameters: For example, the maximum acceptable level of loss or variation in performance, including earnings per share variability, free cash flow growth/margin, earnings before interest and taxes growth/margin, return on assets, return percentage of EBITDA.
- ✓ Operational risk parameters: For example, expected sustainability response, existing / projected environmental requirements, safety targets, quality targets and customer criteria and concentrations.

Risk tolerance is linked to the company's risk appetite and is the acceptable variation in business performance. It describes the range of acceptable results in relation to the achievement of a business objective within the risk appetite and is expressed in measurable units.

Risk capacity indicates the maximum amount that our company could bear without affecting its sustainability.

According to that, the tolerance and acceptance zones are represented in **Ecopetrol's Risk Assessment Matrix**.

ECOPETROL´S RISK ASESSMENT MATRIX

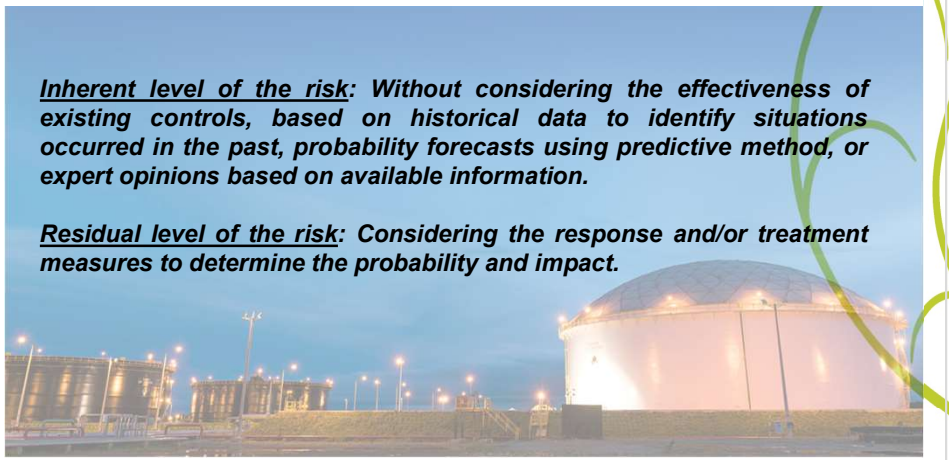
The Risk Assessment Matrix (RAM) contains descriptive scales of probability of occurrence and impacts on dimensions such as **people, environment, economic resources, reputation** and **customers**.

According to the combination of probability and impact, the risk levels are ***Very High, High, Medium, Low and Very Low.***

The RAM stablishes the thresholds by indicating the zones of no tolerance, tolerance with controls and acceptance, as follows:

- ***Non-tolerance zone*** in which the risk must be managed.
- ***Tolerance zone with controls*** in which the risk is being managed through mitigation measures.
- ***Acceptance zone*** in which the risk is assumed by the company.

The risk evaluation considers the magnitude of the consequences and their probability of occurrence, obtaining basic information to prioritize the risks and take decisions regarding treatment. This risk assessment includes the calculation of inherent and residual risk level, according to the scales of probability and impacts, and the tolerance and acceptance levels defined in Risk Assessment Matrix.



Inherent level of the risk: Without considering the effectiveness of existing controls, based on historical data to identify situations occurred in the past, probability forecasts using predictive method, or expert opinions based on available information.

Residual level of the risk: Considering the response and/or treatment measures to determine the probability and impact.

See details of risks identified including a description of the risk, its likelihood and magnitude of the potential impact in Microsoft PowerPoint - Ecopetrol Business Risks 2022

SENSITIVITY ANALYSIS ON FINANCIAL AND NON-FINANCIAL RISKS

REFERENCES FOR ECOPETROL´S SENSITIVITY ANALYSIS 2022 - FINANCIAL RISKS

ECOPETROL performs sensitivity analysis to the financial results that may be sensitive to changes in:

• **Exchange rate variation**: Analyzes the effect of a change -1% and 5%- in the exchange rate of the Colombian peso as compared with the U.S. dollar (See Form 20-F for the fiscal year ended December 31, 2022 note 4.3.2 “Exchange Rate Variation” page 118 and F-101).

• **Interest rate**: Analyzes the effect in the results and other comprehensive income for the next 12 months to variations in interest rate of 100 basis points (See Form 20-F for the fiscal year ended December 31, 2022 section 8 financial statements, note 30.8 Interest rate risk page F-106).

• **Sensitivity analysis over proved reserve balance**: Analyzes the proved reserves as of December 31th, assuming an average price per barrel of ICE Brent price of USD 94.6 per barrel in 2023, USD 88.2 - USD 81.4 per barrel between 2024 and 2030, and between USD 81.2 and USD 77.7 (section 5.2.1 Risk related to our business, page 149 of Form 20-F for the fiscal year ended December 31, 2022).

• **Sensitivity Analysis of the Results**: Analyzes the effect on the Company results due to variations of US$ 1 in the price of ICE Brent crude and of 1% in the COP$/US$ exchange rate (See Form 20-F for the fiscal year ended December 31, 2022 section 4.11 Trend Analysis and Sensitivity Analysis, page 142).

REFERENCES FOR ECOPETROL´S SENSITIVITY ANALYSIS 2022 - NON-FINANCIAL RISKS

ECOPETROL performs sensitivity analysis to the non-financial results that may be sensitive to changes in:

• **Discount rates on pension plan assets and liabilities**: Analyzes the effect of possible changes on the obligation for defined benefits to variations in discount rate, inflation rate, salary growth rate and cost trend (See Form 20-F for the fiscal year ended December 31, 2022, section 8 financial statements, note 22.5 S**ensitivity analysis** page F-84).

• **Sensitivity analysis of reserves volume**: The analysis conducted on our oil and gas reserves as of December 31, 2022, considering ICE Brent crude oil prices that reasonably reflect management’s view of crude oil prices given prevailing market conditions and management portfolio costs (See Form 20-F for the fiscal year ended December 31, 2022 section 4.11 Trend Analysis and Sensitivity Analysis, page 142).

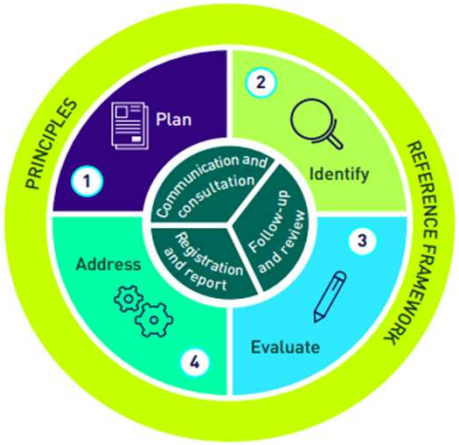
• **Legal Risk**: In the case of the valuation of risks that may result from judicial litigation against Ecopetrol S.A., the "Instructions for the calculation of contingencies for judicial procedures and conciliations" and the "regulations for Ecopetrol's judicial defense and conciliation committee" were established, which defines the criteria to determine the value of the contingencies and provisions derived from judicial litigations, the methodology for such calculation and some rules for the adequate valuation of risks and decision making. The methodology for the valuation of these contingencies includes 6 types of risks and a weighting according to the role in which Ecopetrol acts, i.e. plaintiff or defendant, as well as the rules that must be followed for the valuation of the contingency and its accounting recognition of the provision. (See Form 20-F for the fiscal year ended December 31, 2022, section Risk Factors— 5.2.3 “*Legal and Regulatory Risks - We may incur losses and spend time and money defending pending lawsuits and arbitrations and responding to administrative investigations*” – page 173, and section 8 financial statements, note 23.2 Litigations page F-87).

References:

1. Consolidated Financial Statements - Annual Report under Form 20-F for the fiscal year ended December 31, 2022 with the U.S. Securities and Exchange, (Pages: 118, 119, 142, 143, 144, 148, 149, 173, F101, F-102, F106, F84, F87).
https://www.ecopetrol.com.co/wps/portal/Home/es/Inversionistas/InformacionFinanciera/InformesSEC

https://www.sec.gov/ix?doc=/Archives/edgar/data/0001444406/000141057823000400/ec-20221231x20f.htm

RISK MANAGEMENT CYCLE



- **Plan:** define the scope of the activities and analyze internal and external context.
- **Identify:** identify risks based on the perspectives of the people involved and the analysis of the information.
- **Evaluate:** analyze the causes and consequences. Assess according to probability and impact.
- **Address:** selection and implementation of options to address the risk.
- **Communication, follow-up, and registration:** information exchange, feedback, and continuos monitoring.

The monitoring of business and process risks serves to identify alerts, verify the execution of the mitigants, and ensure actions against the materializations reported by the persons in charge, in order to maintain the risks within defined tolerance and acceptance levels. The relevant results of this follow-up were periodically reported to the Executive and Audit and Risk Committees according to occurrence or criticality thereof, by means of management reports in the monthly sessions.

The objective of reviewing risk is to permanently verify that the identified, assessed and treated business risks are within the company's tolerable levels according to the RAM, in order to provide feedback to the business risk cycle and take actions to ensure their proper management.

The scope of this stage is the monitoring and assurance, carried out permanently, on a monthly basis, to identify risk alerts, verify the execution of mitigating factors, and determine actions against any arising materialization, in order to maintain risks within defined tolerance and acceptance level. This includes:

- ✓ KRIs and alerts generated, as metrics used to provide early signals of increasing risk exposures
- ✓ Follow up of controls and treatment actions
- ✓ Analysis of event materializations
- ✓ Scanning possible changes in the risk context

This analysis is intended to review the risk exposure, regarding:

- Define preventative measures to avoid risk materialization and to maintain the risks within defined tolerance and acceptance levels.
- Reassess the risks based on Risk Assessment Matrix, according to impacts on the business and the probability of occurrence.
- Verify that risk management measures are properly executed and that the expected effects on the risk are achieved.
- Identify alerts relative to potential risk materialization, propose and execute actions.
- Analyze risk materialization events in terms of their causes, impacts as well as measures to reduce the impacts and prevent their recurrence.

See details in https://files.ecopetrol.com.co/web/esp/cargas/ecopetrol-rigs-2022-eng.pdf page 162- 163 .

2022 RISK TRAINING FOR NON-EXECUTIVE DIRECTORS

All nine (9) non-executive members of the Board of Directors are periodically trained on risk management. In 2022, the non-executive members received risk management education regarding:

i)The board as a key player in risk oversight; ii) Navigating U.S. Securities Laws and Regulations: Compliance Programs & Risk Mitigations; and iii) Conscious challenges for business transformation towards a higher purpose (includes different cases study with materialization of risks); and iv) podcast "Learn about the risk landscape of the world of O&G", among others

Please see:

1. Training, Education, and Instruction, Integrated Management Report 2022, page 154
https://files.ecopetrol.com.co/web/esp/cargas/ecopetrol-rigs-2022-eng.pdf

2. Board of Directors in 20F- Report 2022, page 205 - 209
https://www.ecopetrol.com.co/wps/wcm/connect/22a8a7ef-d4ef-46ac-a195-fa7a3acb0e89/22-10205-1_D15.6_ECOPETROL+S.A._20-F.pdf?MOD=AJPERES&attachment=false&id=1650922322313

2022 RISK TRAINING FOR EMPLOYEES

Ecopetrol has performed focused training in risk management, such as: i) ESG risks, ii) Virtual course related to the Integrated Risk Management System available for all employees, iii) anti-corruption related risks, iv) Emerging risks, v) Concepts of the integrated risk management system for Human Rights risks, vi) Risk management concepts - threats and opportunities, vii) HSE risks, viii) Occupational health risks, ix) "What if" for risks analysis, among others.

34.464 participation by workers
To conduct training on risks

65 training actions
On risks themes

661 streaming connections
On Sustainability risks

Our Training Top on risks:

- What is the Integral Management of risks and HSE impacts?
- Matrix of hazards and risks / Barriers and controls to mitigate them.
- Risk Management in occupational health.
- Steps to carry out a risk analysis for a job execution.
- What is a risk analysis for the execution of works?
- The premises of the risk analysis for work execution.
- Roles and responsibilities in risk analysis for work execution.
- Leadership and planning: Risks and controls.
- Methods for comprehensive management of HSE risks and impacts.
- Application practical method "What if" for risk analysis.

"At Ecopetrol we believe in training as a fundamental element to strengthen the risk culture"

See details in https://files.ecopetrol.com.co/web/esp/cargas/ecopetrol-rigs-2022-eng.pdf page 168.

INTERNAL AUDIT OF THE RISK MANAGEMENT PROCESS

2022 MANAGEMENT TESTING

Ecopetrol' s Integrated Risk Management System and Internal Control Management Systems comply with ISO 31000, COSO (Committee of Sponsoring Organizations of the Treadway Commission) and COBIT (Control Objectives for Information and related Technology) standards, as well as SOX (Sarbanes Oxley Act) and FCPA (Foreign Corrupt and Practices Act) laws and is governed by the applicable internal regulations.

SCOPE OF AUDIT

Evaluation of the process risk management cycle by reviewing the adequacy of risks and the design and effectiveness of controls supporting the system of internal control over financial reporting, as established in the COSO 2013 framework.

CONCLUSIONS

Based on the results of the assessment of the effectiveness of our internal control over financial reporting in accordance with the criteria established by COSO 2013 framework, our management concluded that our internal control over financial reporting was effective as of December 31, 2022.

2022 INTERNAL AUDIT PLAN

Ecopetrol's internal audit design risk-based audit plans, in order to determine the priorities of the internal audit activity, consistent with the Organization's goals to reasonably ensure the Company's Internal Control System and to evaluate and propose improvement actions on the effectiveness of the Company's Risk Management System, among others. Here some examples:

Name of audit	Risk Scope	Year
Environmental management audit	Systematic identification and management of potential environmental impacts and risks associated with Ecopetrol S.A.'s activities.	2022
Cybersecurity management audit	Evaluation of risk management, monitoring and compliance with cybersecurity requirements, training and awareness.	2022
Management practices and response to information security incidents audit	Review the status of the practices carried out by the organization to mitigate information security risks.	2022

EXTERNAL AUDIT OF THE RISK MANAGEMENT PROCESS

2022 REINSURANCE RATING

Ecopetrol received risk inspections to the main industrial facility in refining, by a reinsurance team led by external insurance and risk audit firms, in order to identify opportunities for improvement in operational risk management, minimize the materialization of risks that may affect people, assets and operations.

SCOPE OF AUDIT

Review of risk management; standardization, implementation and sustainability of practices such as risk analysis, work control and development of drills, improvement of the reliability of production processes, early and systematic monitoring and follow-up of risks, investment plan and growth projects, training plans for workers on technical issues, and timely intervention to close observations and recommendations from reinsurers.

CONCLUSIONS

The results place Ecopetrol as a benchmark in risk management, aligned with industry best practices. This has a direct impact on the perception of insurance companies and the terms obtained during each renewal of the Ecopetrol Group's corporate insurance program. The rating obtained is a world-class recognition of the risk inspection process.

2022 QUALITY AUDIT

Ecopetrol performs an external audit for its management systems, based on the requirements under ISO standards and through ICONTEC (a Colombia's National Standards Body), considering as scope of certification the Oil and gas exploration and production. Production of refined and petrochemicals. Commercialization of hydrocarbons, Administrative and Business Support Processes, regarding, among others, ISO 9001:2015 with focus is not only on the individual processes of the organization, but also on the interactions of these processes, including its risks and controls.

SCOPE OF AUDIT

The ISO 9001:2015 Standard is oriented towards a preventive approach that is accentuated with the aspects referred to Risk Management, which consist of recognizing the risks (positives as opportunities, negatives as risks) as within an organization and carrying out the necessary actions to prevent them from occurring

CONCLUSIONS

As of 2022, Ecopetrol's external audit concluded about the risk management process, that it had no breaches against the standard.

See details in chapter “Risk Management System” page 160 https://files.ecopetrol.com.co/web/esp/cargas/ecopetrol-rigs-2022-eng.pdf
See details in Form 20-F for the fiscal year ended December 31, 2022, section 7.8 Controls and Procedures, page 226 and 227. EDGAR PDF (ecopetrol.com.co)

USAMOS NUESTRA ENERGÍA PARA
CONSTRUIR UNA **EMPRESA Y UN PAÍS**
DE TODOS, PARA **TODOS**

ecopetrol