	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1


TABLE OF CONTENT

1. OBJECTIVE.....	2
2. GENERAL CONDITIONS.....	2
3. DEVELOPMENT.....	2
3.1. PHASE 1 - PREPARATION OF THE WORK PLAN.....	3
3.1.1. Inputs.....	3
3.1.2. Process.....	3
3.1.3. Outputs.....	4
3.2. PHASE 2 - IDENTIFICATION OF RISKS.....	4
3.2.1. Inputs.....	4
3.2.2. Process.....	4
3.2.3. Outputs.....	8
3.3. PHASE 3 - RISK ASSESSMENT.....	9
3.3.1. Inputs.....	9
3.3.2. Risk Assessment Process.....	10
3.3.3. Outputs.....	10
3.4. PHASE 4 - IDENTIFICATION OF ADDITIONAL MITIGATING FACTORS AND ALERTS.....	10
3.4.1. Inputs.....	11
3.4.2. Process.....	11
3.4.3. Outputs.....	14
3.5. PHASE 5 - RISK MONITORING.....	14
3.5.1. Inputs.....	14
3.5.2. Process.....	14
3.5.3. Outputs.....	18
3.6. PHASE 6 - COMMUNICATION.....	18
3.6.1. Inputs.....	18
3.6.2. Process.....	18
3.6.3. Outputs.....	20
4. CONTINGENCIES.....	20

This is a faithful translation of the original document in Spanish, by Magdalena Rodriguez de Uscategui, Official Translator and Interpreter, with License 0593 conferred by the Colombian Ministry of Justice on March 27, 1994.

****Esta es una fiel traducción y copia del documento original en español.***

MAGDALENA R. DE USCATEGUI
Traductora e Interprete Oficial
Resolución No. 0593

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

1. OBJECTIVE

Provide guidelines for the application of the risk management cycle at the business level in the Ecopetrol Group, in order to ensure proper management of the risks that may generate deviations from fulfillment of each company's strategy and obtaining reliable information for decision making purposes.

2. GENERAL CONDITIONS

Business risks are those implying threats that, in the opinion of the Board of Directors and Senior Management of the companies, could, to a large extent, deviate from the fulfillment of its strategy.

This document includes business risk management guidelines to implement the Business Risk Management Cycle.

It is worth highlighting that the success of the business risk management depends on the application of the cycle in each and all of the stages.


3. DEVELOPMENT

The guidelines for the management of business risks are established by the Corporate Management of Internal Control Assurance for compliance within the Ecopetrol Group. All areas of each company participate in its execution.

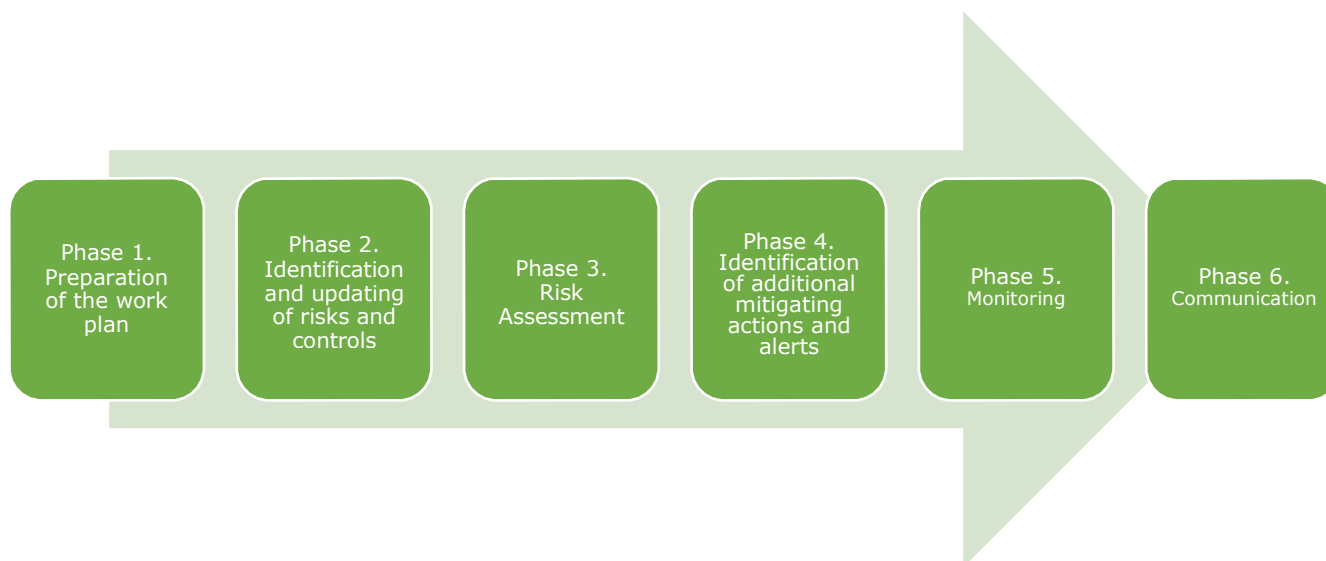
The Business Risk Management Cycle comprises the planning, identification, evaluation, treatment, monitoring and communication stages, as shown below:



Figure 1. Risk Management Cycle

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

The Business Risk Management Cycle is met through the following phases:



3.1. PHASE 1 - PREPARATION OF THE WORK PLAN

In this phase, the scope and objectives of the application of the Business Risk Management Cycle are defined. This phase should include the definition of resources, time, guidelines, processes and tools required to develop the next stages of the cycle.

This planning must be carried out annually, pursuant to the times established by Ecopetrol's Internal Control Assurance Corporate Management for the application of the Business Risk Management Cycle.


3.1.1. Inputs

- Strategic definition of the Company.
- Organizational Structure.
- Company Process Map.
- Other inputs: Organizational guidelines and procedures that can influence risk management planning. These can include authority and decision-making levels, roles and responsibilities of the company's governing bodies, among others.

3.1.2. Process

The plan for the development of the Cycle must be established which must include:

- o The methodologies, tools and activities that must be implemented to develop each of the stages of the cycle.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

o Premises for the creation of work teams that will participate in all stages of the cycle.

In this phase, the work schedule for the application of the Business Risk Cycle is defined.

3.1.3. Outputs

At the end of this phase, there must be a work plan for the application of the Risk Management cycle that includes, among others:

- Schedule where each of the stages of the risk management cycle is registered (phases, activities, start date, end date, responsible).
- Communications: Mechanism for disclosure of Business Risk Management to interested parties, both internal and external, when applicable.

3.2. PHASE 2 - IDENTIFICATION OF RISKS

The identification of risks allows, in a systematic and structured way, to determine the events that may negatively affect the business strategic objectives. These events must be considered, regardless of their being under the control of the organization or not.


3.2.1. Inputs

- Strategic Framework and other definitions of the strategy.
- Methodology and tools defined for planning.
- Context and environment data related to the industry and the company: regulatory reforms, technological changes, initiatives or ongoing projects, etc.
- Business risk map of subsidiaries (when applicable).
- Regulations and other existing inputs in the organization: organizational guidelines, procedures or results that can influence risk management.
- Current Business Risk Map.
- Information on materialized events.
- Self-assessment results and test findings from management and internal and external audits.

3.2.2. Process

To carry out the identification stage, it is possible to start with the previously identified risks and verify their validity and sufficiency vis-à-vis the coverage of business objectives.


To ensure adequate risk identification, activities such as those described below should be carried out, without limitation, in order to have sufficient and adequate sources of information. Some of the activities

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

are optional, as clarified in the explanatory details of each of them.

- Review of the list and descriptive sheet of current business risks.
- Review of the Strategic Framework, Strategic Objectives (or Strategic Pillars) and company Business Plan, without limitation, and the changes derived therefrom.
- Review of the reports published by firms involved in analyzing risks and behavior of companies in the sector: Annually, internationally recognized consulting firms (for example: Price Water House Coopers, Ernst & Young, Deloitte, etc.) publish reports related to risk management in the Oil & Gas sector throughout the world. These reports are one of the main inputs for this stage, as they present and analyze industry risks by segment, and region in some cases.
- Benchmark of other companies in the Oil & Gas industry. As an optional activity, a review of local or international companies can be performed to enrich and analyze the list of typical risks in the Oil & Gas industry.
- Interviews or polls can be carried out with members of the Board of Directors or their alternates, seeking to obtain first-hand their perception of the issues that affect the Company and the environment. Similarly, those responsible for the Operational and Regional Vice Presidencies or for the Company's Directorates and other company staff, whose perception and expert knowledge are deemed important for the analysis, may be included.
- A benchmark that can be used is the list of current risks and the interviewees can be provided with the new topics derived from consulting firm reports, the analysis of the global, national and regional situation of the industry, and the particular conditions undergone by the company and that could integrate the new risk map.
- Review and analysis of strategic risks of the Group companies. This review is conducted to determine the incidence or impact that their risks may have on the business strategic objectives. The review is conducted following the steps described below:
 - i. Identification of strategic risks of the Group companies, which are directly related to the strategic objectives of the analyzed company.
 - ii. Analysis of the risks identified in the previous numeral as regards their relationship with the risks contained in the company's business risk map or their causes. The descriptions and figures associated with these risks will serve as input for documenting figures, data, analysis and preparation of the technical data sheet on business risks.
 - iii. Analysis of impact of risk materialization at Group companies.
- Risk analysis in processes: The risk matrices and controls of the company's processes have useful information for the identification, analysis and management of business risks. The risks of processes

1 For companies that have subsidiaries, this analysis should consider the risks identified in said companies.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1


to be considered or evaluated as possible business risks or causes thereof will be those associated with the company's strategic objectives. An important input for building risk matrices and process controls are the results, findings and recommendations of internal and external audits; therefore, when analyzing the risks in the processes as input for the construction of the business risk map, these results should be incorporated.

- Internal analysis by the Corporate Management Internal Control Assurance (or its equivalent). Throughout the entire Identification stage, an exhaustive review is made of the results of the reports of consulting firms based on interviews, the impact of the risks of the Group companies and their subsidiaries², and of processes and their impact on the business strategic objectives. These sessions take, among others, the decision to submit a new risk for inclusion in the map, and whether a current risk should remain or be removed from the business map. The analysis for making such decisions includes the following:
 - For the inclusion of a new risk: Not all issues identified are reflected as business risks, as they may be included as risk causes or focus, or could be disregarded for having been already addressed and properly managed as process risks. The following should be considered:
 - The significant increase (in frequency or impact) of materialized events related to the risk analyzed.
 - The imminence of its materialization if treatment actions are not carried out in the short, medium and long term³.
 - The weight or relevance given by the participants in the interviews or polls for the construction of the map of the year under review.
 - To remove a business risk:
 - It is deemed that the main causes of risk are properly identified and managed in one of the company's processes.
 - The problem was temporarily considered as a business risk seeking greater visibility due to a specific issue of the company⁴.
 -

² For companies that have subsidiaries, this analysis must include the risks identified in said companies.

³ The imminence of the materialization must be supported with figures and data. For example, Ecopetrol's Business Risk in 2014 "Restrictions on energy capacity for Ecopetrol's operational continuity and growth": The projected energy demand for 2015 amounts to 1,422 MW of electric power to support the development and expected growth of its production, transportation and refining activities. To supply this demand, the planned power supply was 1,256 MW (equivalent to 88.33% of the total required) through self-generation projects, and the remaining energy, that is, around 166 MW (11.67 %) would be achieved through the purchase of unregulated energy in the national energy market. This illustrated two significant issues: high dependence on the execution of generation projects and energy transmission infrastructure and unavailability of energy in the domestic market. If short, medium and long-term actions are not generated, the materialization of this risk would be imminent in view of the expected growth and operation scenarios.


⁴ As an example, we can consider the Risk "major incidents in offshore operations" that was part of Ecopetrol's 2010-2011 corporate risk map, for further visibility of risk exposure such as that materialized in the Gulf of Mexico in April 2010 that, to a great extent, affected the operations, results the operation and results of British Petroleum. Today, the aforementioned risk, although it is not part of the Business Risk Map, it is the focus of another one: Incidents that affect the People, the Environment and the Infrastructure; additionally, it is a specific risk of the Exploration process.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

- As a result of analysis and review, it is concluded that the problem or its associated causes are mostly derived from failures in company management or processes that are not closely associated with events of uncertain occurrence (risks).
- Their KRIs (Key Risk Indicators) and KPIs for related process risks do not show behaviors leading to significant risk exposure.
- To justify the permanence of a risk. The business risk map is dynamic. However, several of the risks remain year after year and their permanence can be explained, among others, by one or more of the following reasons:
 - These are risks inherent in the industry.
 - The reasons for which it was incorporated at the time remain valid.
 - Treatment plans associated with risk have not been finalized and it is not possible to estimate their effectiveness in mitigating or eliminating their cause.
- Structure the final proposal for a business risk map, which must include the preparation of the technical data sheet for each risk and the graphic representation of the map.

The technical data sheet must contain the following items:

- *Name:* It reflects what is meant to be represented with the event. It must be a short name, but ambiguities should be avoided.
- *Strategic pillar/Strategic objective (or its equivalent):* Mention of the strategic pillar that could be affected in the event of materialization of the risk.
- *Description:* Brief characterization that allows foreseeing what could happen. Here you can include the justification of why this risk is relevant to the company.
- *Focus points:* These are the main points of attention among the various causes of risk identified or their treatment alternatives. The purpose is to direct efforts of the management on said focus points.
- *Causes:* This refers to why said event could occur. The analysis of the direct, internal and environmental causes that give rise to the event must be performed. The causes must be concrete and coherent.
- *Consequences:* This refers to the impact of the materialization of the risk event on the business resources (people, environment, economic, reputation, etc.). Direct consequences must be determined.
- *Leverage processes:* these are processes that contribute to risk management in their operations.
- *Accountability and participants:* according to the processes that leverage risk management, the areas involved in said management are defined, whose responsibility, in addition to performing direct actions for the treatment of risk, includes coordinating and monitoring actions that must be carried out by other participating areas with the same purpose.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

- Mitigating factors: These may be process controls, risk treatment actions whose effectiveness has already been known, and other management measures applied across the company, in a cross-cutting manner, or in each of the processes involved in risk management.


The graphic representation must contain the following items:

- Category: The identified risks can be classified according to their generating source, as follows:
 - i. Strategic: These are risks that the company decides to accept to maximize the results of the established objectives that are directly related to the company's strategy. These generate losses associated with the impossibility of properly implementing business plans, strategies, market decisions, allocation of resources and operating models aligned with the strategic direction; they reflect the organization's difficulty to adapt to changes in the business environment, which translates into growth reduction and failure to meet business objectives.
 - ii. Environment: These are generated by external agents. Its causes cannot be prevented, but they can be foreseen and sometimes they are beyond the influence and control of the organization. These are risks associated with factors such as the country where the company is located, its nature, the region and city, as well as the sector, industry and economic, political, social and cultural conditions.
 - iii. Operational: These are risks that arise within the organization and can be controlled. These are risks that can be materialized by the execution of company processes and functions, by failures in processes, systems, procedures, models or people who participate in said processes.
- Validation with members of the management level to define the adjustments required on the proposed risk map.
- Session with members of the Board of Directors Audit Committee (or its representative), to present the risks identified as a result of the analysis performed, making evident changes applicable on the map structure and the content or scope of the risks involved. For this session, each of the risks must be duly supported, that is, they must have sufficient information to support its inclusion in the map, namely: relevant materialized risk events, if any, behavior of the KRI's associated with the risk, and other relevant facts and data to characterize the magnitude of the risk.
- Once the adjustments required by the Board of Directors Audit Committee or whoever substitutes them have been implemented, the risk map is submitted to the Board of Directors for approval.

3.2.3. Outputs

At the end of this phase, there must be:

- Documents with technical data sheets on Business Risks.
- Approved Business Risk Map.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

3.3. PHASE 3 - RISK ASSESSMENT

The risk assessment is based on a semi-quantitative analysis aimed at prioritizing the risks, assigning these values within predefined scales or ranges of probability and impact.

Risks must be prioritized to achieve an effective distribution of available resources to deal with those critical risks. This is achieved by measuring the probability of occurrence of the risk event and the impact on resources (people, environment, economic, reputation, customers, and others, as defined for each of the companies).

The valuation exercise is carried out based on the identified business risks, documenting it in the Risk Valuation Form defined for this purpose⁵, whereby the results of the assessment must be registered, considering two main instances: The inherent and residual values, as shown in the following figure:

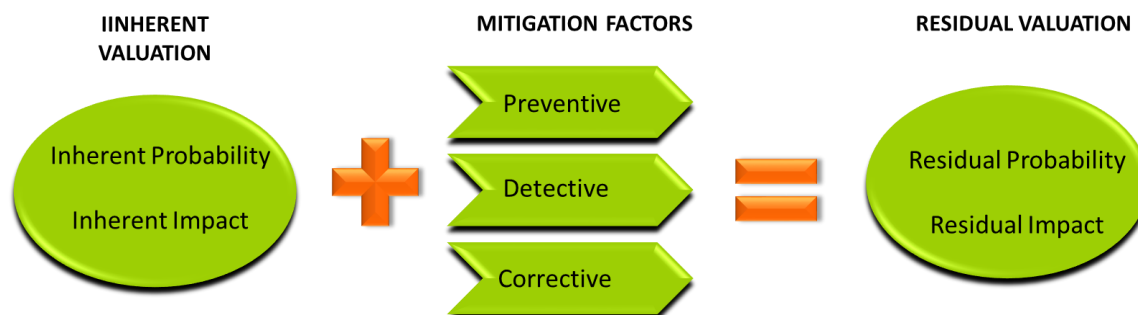



Figure 2. Risk Rating

3.3.1. Inputs

- Identified business risks and mitigation measures.
- Results of strategic objective indicators for last year.
- Company risk assessment matrix (RAM) and assessment format.
- Goals and results of last year's strategic and process objectives and process indicators.
- Matrix of risks and process controls.
- Matrix of risks and cross-cutting controls and multi-executors.
- Results of self-evaluations, preventive monitoring, management's test findings and internal and external audits performed on the processes that feed the evaluation stage, as the detected findings or non-conformities may be risk sources that support impact and probability estimates.
- Context and environment data related to process risks, such as projection of regulatory changes, technological changes, initiatives or ongoing projects, among others.

⁵ The SCI-F-005 form applies for the assessment of process risks in Ecopetrol S.A. Companies that have more or less resources or descriptors must make the pertinent adjustments to said form.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

- Historical information on materialized business incidents or risks that enables the estimation of frequencies of occurrence and impacts: This information includes accident rates, cost and time databases, incidents occurred in the Industry or in the Company, even if they are not registered in formal databases.
- Projection information enabling the estimation of business risks probability or impact. This information includes studies of trends, commercial data and analysis of markets or prices performed by external companies (consulting companies, industry peers, others) or by the company.

3.3.2. Risk Assessment Process

Inherent Valuation

It is the risk assessment based on the probability and impact measurement without taking into account the effect of the mitigating factors.

To perform the probability estimation, based on the probability descriptors defined in the company's RAM matrix, the level of probability of the risk materialization from the causes described must be identified. For such purpose, historical information of events materialized in the process, the company or the industry must be used, or probabilistic data of hypothetically credible events.

The inherent risk assessment depends on the highest level resulting from the combination of the evaluated probability and impact. The levels of these combinations are: VH (Very High - Very high); H (High - High); M (Medium - Medium); L (Low - Low) and N (Null - Null) according to the RAM matrix.

Residual valuation

Once the inherent risk assessment has been obtained, the residual assessment is estimated, starting from the sufficiency and assessment of the effectiveness of the mitigating actions.


The residual valuation is understood as the level of risk resulting once the mitigating actions have been applied to the probability of occurrence of the risk and the impact of its consequences on the resources. This seeks to establish the level of exposure to the identified risks, considering the existence of the mitigating actions in place and their effectiveness in mitigating the risk.

The inherent and residual assessment of business risks must consider the aspects defined in the process risk management procedure of the Ecopetrol Group, GEE-P-005.

3.3.3. Outputs

At the end of this stage, the inherent and the residual assessment of the risks identified in the form set out for this purpose.

3.4. PHASE 4 - IDENTIFICATION OF ADDITIONAL MITIGATING FACTORS AND ALERTS

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

In this stage, the activities intended to prevent the causes or for protection against consequences are defined, and alerts are issued on possible materialization of business risks. If the residual assessment of business risk is "Very High", "High", or "Medium", Treatment Actions or controls must be defined to manage the causes not fully managed by the existing mitigation actions.

3.4.1. Inputs

- Business risk maps.
- Existing corrective or preventive actions.
- Format of Risk Assessment Matrix

3.4.2. Process

In this stage, the causes to be managed for each of the business risks are analyzed and, on such basis, identify the new mitigation measures that allow for reducing the probability. Similarly, the risk consequences are analyzed, identifying additional measures that may reduce the impacts therefrom.


Starting with the definition of treatment options (avoid, accept, transfer, mitigate) this document outlines the steps to be followed for the "Mitigate" option.

a. DEFINITION OF TREATMENT ACTIONS

The Business Risk Treatment Actions are established to eliminate or reduce the causes of the risks or to lessen the impact of their eventual materialization. In this regard, a properly designed Treatment Action must: a) Have a clearly defined structure, and b) Comply with the minimum requirements, according to the type of action required. The defined treatment actions cannot be the normal process activities.

The structure of a treatment action is made up of: Name, Description, Benefits, Work Plan, Plan Advance, Start Date, End Date, and Executor.


AT Elements	Definition	Example
Name	Short name of the action that briefly describes the activity to be carried out.	Design and implementation of the process monitoring structure

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

Description	<p>It must indicate What is going to be done and What for.</p> <p>It includes benefits associated with reducing the probability of the causes occurring or reducing the impacts if the risk materializes.</p>	<p>Design of a Management Control Structure inside the W area, seeking to reinforce the monitoring of process X.</p> <p>An adequate management control structure will allow monitoring alarms on the performance of indicators, reducing the probability of not identifying on time any deviation in the expected results of the process and its potential causes. Consequently, it will enable the reduction of impacts in those cases in which opportunities, corrective actions or remediation are implemented. This may be evidenced in the greater number of alarms managed or in the reduction of impacts generated by the timely management of the causes of the deviation.</p>																									
Work Plan	<p>It is the detailed description of the activities that support the treatment action. It will be made up of the following elements:</p> <ul style="list-style-type: none">• Milestones• Accumulated percentage of planned fulfillment of activities during their execution.• List of deliverables that support the activities performed. <p>Note: The deliverables that are defined must be concrete and evident.</p>	<table><tr><th>ACTIVITY</th><th>CUMULATIVE ADVANCE</th><th>DELIVERABLES</th><th>DATE</th><th>RESPONSABLE</th></tr><tr><td>ACTIVITY 1</td><td>30%</td><td>DELIVERABLE 1</td><td>March</td><td>RESPONSABLE 1</td></tr><tr><td>ACTIVITY 2</td><td>50%</td><td>DELIVERABLE 2</td><td>June</td><td>RESPONSABLE 2</td></tr><tr><td>ACTIVITY 3</td><td>60%</td><td>DELIVERABLE 3</td><td>September</td><td>RESPONSABLE 3</td></tr><tr><td>ACTIVITY 4</td><td>100%</td><td>DELIVERABLE 4</td><td>November</td><td>RESPONSABLE 4</td></tr></table>	ACTIVITY	CUMULATIVE ADVANCE	DELIVERABLES	DATE	RESPONSABLE	ACTIVITY 1	30%	DELIVERABLE 1	March	RESPONSABLE 1	ACTIVITY 2	50%	DELIVERABLE 2	June	RESPONSABLE 2	ACTIVITY 3	60%	DELIVERABLE 3	September	RESPONSABLE 3	ACTIVITY 4	100%	DELIVERABLE 4	November	RESPONSABLE 4
ACTIVITY	CUMULATIVE ADVANCE	DELIVERABLES	DATE	RESPONSABLE																							
ACTIVITY 1	30%	DELIVERABLE 1	March	RESPONSABLE 1																							
ACTIVITY 2	50%	DELIVERABLE 2	June	RESPONSABLE 2																							
ACTIVITY 3	60%	DELIVERABLE 3	September	RESPONSABLE 3																							
ACTIVITY 4	100%	DELIVERABLE 4	November	RESPONSABLE 4																							
Initial Date	Date on which the work plan begins.																										
Completion Date	Date on which the work plan is completed.																										
Executor	Person responsible for the leadership or implementation of the work plan.																										

The actions defined are related to the development of the analysis, the design or modification of processes, the creation of committees, the issuance of guidelines or the fulfillment of training activities, among others. Depending on the type of action defined, the following minimum requirements must be met:

- The analyses, studies or diagnoses can only be considered treatment actions if the implementation of the recommendations resulting from said analyses is included in the Work Plan.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

- If the action intends to change a process, the scope of the treatment action must include the officializing and implementation of said change, that is, the change is already incorporated in the process and there is evidence of its use.
- Actions intended for the creation of committees, working groups or similar, or the modification of their responsibilities or functions must consider the formalization of establishing the committee and the formalization of the responsibilities or assigned functions; there must be evidence of the functioning of said committees.
- If the treatment action is focused on the issuance of a directive or guideline, the scope must include the mechanism for verifying the application thereof.
- The treatment actions associated with training, courses and formation must include the mechanisms that allow to verify knowledge appropriation. (Examples: output tests, certifications, among others).

In cases where the proposed treatment option requires the participation of a different area, its definition must be agreed and approved by the parties involved.

b. DEFINITION OF KRI

The risk alerts or KRI (Key Risk Indicator) are measurement tools for preventive monitoring of the behavior of variables associated with the causes of business risk in order to show changes in the level of exposure to the risks, generating early alerts that lead to reinforcing or focusing management to avoid their materialization.


For the definition of alerts or KRIs, it is possible to select:

- Documented causes of business risk that are most likely to occur ⁶
- The causes that have generated the materialization of the business risk (when applicable).
- Causes related to the external factors of business risks.

Based on the causes analyzed, identify the variables that can be measured and the information necessary for designing the indicator: how, when and where to obtain the information of the variable. Once the availability of the indicator data has been validated, propose a KRI that meets the criteria defined herein, taking into account the following:

- The KRI must be specific, clear and measurable (quantifiable), based on available, recent and reliable data.
- It must have a clear description or intention of that to be measured, considering applicable exclusions or limitations.

⁶ To determine the most likely clauses, use expert judgment.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

- The KRI calculation formula must contain the equation or mathematical expression where the variables and constants are listed to obtain the result.
- It must have a limit, which must be a tolerable numerical value for the generation of the alert that indicates the maximum value (if its trend is negative, indicating good behavior when the KRI result is less than the alert limit) or a value minimum (if its trend is positive, indicating good behavior when the KRI result is greater than the alert limit).
- It must have a specific measurement frequency: weekly, monthly, quarterly.
- It must be different from the result indicators of the Company's strategic map objectives. It can be a means indicator, as long as it is not associated with the selected causes.

All business risks must have at least one "Key Risk Indicator (KRI)" for identifying preventive alerts on the risk behavior, its possible materialization and the deviation from the related strategic objectives. This indicator must be different from related indicators and must have a calculation formula, an alert limit and a trend (positive or negative), so that the monitoring can generate alerts or signals that trigger preventive or corrective actions.

3.4.3. Outputs

- Defined and documented treatment actions.
- Key Risk Indicators KRIs defined for business risks.

3.5. PHASE 5 - RISK MONITORING


The objective of this phase is to verify that the identified, valued and treated business risks are within the tolerable limits of the company to have feedback of the business risk cycle and take actions that ensure their proper management.

The scope of the business risk monitoring stage includes monitoring treatment actions, alerts generated through KRIs and event materialization.

3.5.1. Inputs

- Assessment results
- Risk alarms - KRIs
- Materialized risk events
- Information on Treatment Actions execution
- Information on external changes that may increase exposure to risk.

3.5.2. Process

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

The activities to be carried out for the monitoring stage are described herein below:

a. Monitoring of Treatment Actions

This monitoring ensures systematic feedback on the progress of the Treatment Actions, providing alerts against what is planned to manage the business risk.

To monitor the Treatment Actions, the following must be reported⁷: i) the actual progress of treatment actions, which will be a percentage value according to the fulfillment of the Work Plan activities, and ii) comments or justifications that support the status of execution of the action.

The status of the treatment actions will be defined according to the actual progress, the planned progress, and the start and end dated as follows:

- **Not started:** The start date has not occurred and the action has no associated progress.
- **Execution:** The start date has already occurred, the action has equal or greater progress in accordance with the established Work Plan, and the end date is not yet defined.
- **Delay:** The start date has already occurred and actions have not progressed as planned for the period or the action has no progresses registered, or the action has not been completed on the scheduled date.
- **Closed:** The action progress is 100% on the end date.
- **Canceled:** The action was suspended or canceled before reaching 100% of its progress.

The effectiveness of the Treatment Actions will be determined by the decreased business risk valuation, by reducing the probability of its materialization or the impact of the consequences derived therefrom. Therefore, at the end of each Treatment Action, it is mandatory to report to the Corporate Management Internal Control Assurance (or its equivalent in the companies) the compliance analysis with the expected benefits of each treatment action ⁸.

b. Tracking of warnings generated through KRIs


KRIs can warn about changes in the level of exposure and generate early warnings that lead to reinforcing or focusing actions to avoid risk materialization.

The KRI report must be performed with the established frequency and in accordance with the reporting guidelines defined by each company. The information reported will correspond to:

- Results of the KRI calculation
- Alert status or not, according to the result and defined design parameters (eg measurement unit, trends and alarm limit)
- The analysis of why the alert was generated and the management that will be performed.

⁷ In Bwise for Ecopetrol, and in the form established for this purpose in other Group companies.

⁸ For Ecopetrol, this information must be registered in the Bwise tool, in the field "Progress Observations" and in the case of subsidiaries, it will be registered in the tool defined for such purpose.

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

Monitoring is managed as follows:

- When the result of a KRI is outside its warning limit, the effectiveness of process controls and treatment actions associated with business risks should be reviewed; also, evaluate the need to activate additional prevention measures, implement alternative action plans or focus monitoring on certain risk factors, without limitation, in order to minimize the possibilities of materialized risk events.
- Optionally, produce graphs of the behavior of the historical results to determine if the KRI is moving away or approaching its alarm limit, seeking to identify trends or seasonality in the KRI results.
- Calculate the average and the number of times outside the limit during the last year of measurements, to analyze the KRI results over time.
- When a materialized event occurs, it should be analyzed if there is a KRI associated with the cause that generated the event, and if the respective early warnings were made. Report this analysis in the Risk Materialization Form, GEE-F-044. If no alerts were issued, the KRI design should be reviewed and adjusted to better reflect the risk variables.

c. Materialized risk events


Materialized events are understood as the occurrence of situations whose consequences affected the fulfillment of the objectives defined for the strategy. For the analysis of the materialized events, report the necessary information in the Risk Materialization Management GEE-F-044 Form.

With this information, the sufficiency in the identification of risks, causes and consequences is validated; likewise, the need to adjust existing mitigation factors or defining new mitigation measures is verified, and the assessment of business risk is validated and adjusted.


When feasible, the risk accountant should define actions to mitigate the impact of the materialization of the event, and in every case should define the actions to reduce the probability of occurrence of a new event of associated risk materialization.

In general terms, the follow-up to be carried out is described below for each of the elements associated with business risks:

Item	Scope of the	Analysis	Frequency	Deliverable
Materialized business risk events	Identify any business risk event that has occurred	Analysis of causes of the event. Take into account the typical events contained in the risk description.	Monitoring: Monthly Analysis: Every time an event occurs	Format for Risk Materialization Management in the Ecopetrol Group - GEE-F-044.

	Procedure for Business Risk Management in the Ecopetrol Group			
	Internal Control System Corporate Management of Internal Control Assurance.			
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1	

		<p>Analysis of the consequences of materialization.</p> <p>Identify the changes applicable to the assessment of the business risk.</p> <p>Follow up on actions defined regarding the materialized events.</p>	Monthly	
Treatment Actions	Monitoring the progress of treatment actions.	<p>Review progress with the executor of the treatment action.</p> <p>Compare the actual progress against the planned progress and identify possible deviations.</p> <p>Report deviations for management.</p>	Monthly	<p>Report in Bwise or other tool established in the company.</p> <p>Evidence of meetings or follow-up instances with the business risk leader.</p>
	Verification of effectiveness of closed treatment actions.	Measure the effectiveness of the treatment action in accordance with the provisions of this procedure in section 4.5.2.a	Every time a treatment action is closed.	<p>Report in Bwise or other tool established in the company.</p> <p>Evidence of meetings or follow-up instances with the business risk leader.</p>
KRIs	Monitoring of indicator results	<p>Carry out the analysis of the KRI's behavior in accordance with the provisions of this procedure in section 4.5.2.b.</p> <p>Verify fulfillment of actions established according to the results of the KRI on alert.</p>	Monthly	<p>Report in Bwise or other company established tool.</p> <p>Meeting supports or follow-up instances with the business risk leader -</p>

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

As a result of the monitoring of business risk management, the following must be ensured:

- Adjust the risks in case there are changes in its components (name, description, causes, consequences, focal points, accountable, mitigating actions)
- The identification of new causes of risks, derived from changes in the environment, the strategic objectives or the business situation.
- Changes to treatment actions to include identified improvements or to complement them if they are insufficient or inadequate.
- The identification of risk materialization events and their documentation for future reference and analysis.

The monitoring stage should consider a systematic feedback that provides early warning related to achievement of the expected results or objectives, through the reporting line from the executor of the action to the accountable for the business risk, the risk leader, and the Corporate Management of Internal Control Assurance (or their equivalent in the company) to take appropriate actions for correcting any deficiency detected.

3.5.3. Outputs

Consider the reports in the previous table as output from this stage.

3.6. PHASE 6 - COMMUNICATION

The communication is carried out by developing the business risk management cycle and enabling the socialization of all those involved in the information generated from the analysis and the results of risk management to thus support decision-making for proper management.


The Internal Control Assurance Corporate Management (or its equivalent) defines the communications scheme of the business risk management cycle in the company, to ensure the review by the risk leader and accountable.

3.6.1. Inputs

- Reports and analyses carried in the Monitoring stage.
- Business risks.
- Risk valuation.

3.6.2. Process


Communication is developed through the dissemination of the results of business risk management, through a communication scheme that must contain the following:

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

- Items to communicate or data to be reported.
- Communication channel.
- Sender and receiver of the information.
- Frequency of communication.

For the communication of business risk management, the following scheme is available:

Item	Report	Frequency	Communication Channel	Issuer	Receiver
Risk Management Plan	Schedule of activities for Business Risks	Annual	Email	Internal Control Assurance Corporate Management (or its equivalent in the company)	Business risk accountable.
Execution of Business Risks - Risk Assessment	Business Risk Register	Annual	Bwise or tool established in the company.	Internal Control Assurance Corporate Management (or its equivalent in the company)	Corporate risk accountable and other participants in the construction and management of business risks.
	Summary of the outcome of the cause analysis and definitions of Ats, KRIs and risk valuation	Annual	Memorandum	Business Risks Accountable Vice Presidencies	Internal Control Assurance Corporate Management (or equivalent).
	Summary of relevant issues to be considered by the risk accountable party	Annual	Paper	Internal Control Assurance Corporate Management (or equivalent).	Business Risks Accountable Vice Presidencies
Materialized Risk Events	Form GEE-t F-044	Every time an event occurs.	Completed form sent by email	Business Risk Leader	Internal Control Assurance Corporate Management (or equivalent).

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

Treatment Actions	Execution Report Bwise or tool established in the company.	Monthly	Bwise or tool established in the company.	Executor of the treatment action	Internal Control Assurance Corporate Management (or equivalent).
	Effectiveness report Bwise	Every time that a treatment action is closed	Bwise	Executor of the treatment action	Internal Control Assurance Management.
KRIs	Report Outcome Bwise.	Monthly	Bwise	Responsible for the indicator	Internal Control Assurance Management.

3.6.3. Outputs

Communication scheme implemented for one of the stages of the business risk management cycle.

4. CONTINGENCIES

Not applicable

LIST OF VERSIONS


Previous Document			
Version	Date (dd/mm/yyyy)	Code and Title of Document	Changes
New Document			
Version	Date (dd/mm/yyyy)	Changes	
1	22/05/2019	Document creation. Repeals document PDO-P-022	

For more information contact:

Author(s): Edna Carolina Vargas; Angelica Alaix Martinez
 Telephone: 50559; 52543 Mailbox: edna.vargas@ecopetrol.com.co; angelica.alaix@ecopetrol.com.co;
 Department: Internal Control Assurance Corporate Management

Reviewed electronically by:

Approved electronically by:

	Procedure for Business Risk Management in the Ecopetrol Group		
	Internal Control System Corporate Management of Internal Control Assurance.		
	CODE GEE-P-007	Prepared 22/05/2019	Version: 1

MÓNICA JIMENEZ G. General Secretary ID. No. 52.411.766 General Secretary & Support to Presidency	HELBER ALONSO MELO HERNÁNDEZ Internal Control Assurance Corporate Manager ID. No. 79.862.626 Internal Control Assurance Corporate Management
<p>Document signed electronically, in accordance with the provisions of Decree 2364 of 2012, which regulates article 7 of Law 527 of 1999, on electronic signature and other provisions are issued.</p> <p>To verify compliance with this mechanism, the system generates an electronic report showing the traceability of the review and approval actions by accountable parties. If you need to verify this information, request said report from the Service Desk.</p>	