TABLE OF CONTENTS

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

1. OBJECTIVE

Provide guidelines for the implementation of the risk management cycle at the process level to ensure proper risk management and produce reliable information for decision-making at Ecopetrol S.A. and the Ecopetrol Group companies that consolidate financial statements.

2. GENERAL CONDITIONS

The guidelines for Process Risk Management are established by the Corporate Management of Internal Control Assurance for compliance by Ecopetrol S.A. and the Group companies.[1] These guidelines are detailed in this document and must be executed by complying with the risk management cycle at process level [2].

The procedure for managing process risks is based on the Risk Management Cycle common in all risk management methodologies and reference frameworks and it includes planning, identification, assessment, treatment, monitoring and communication phases, as shown herein below:

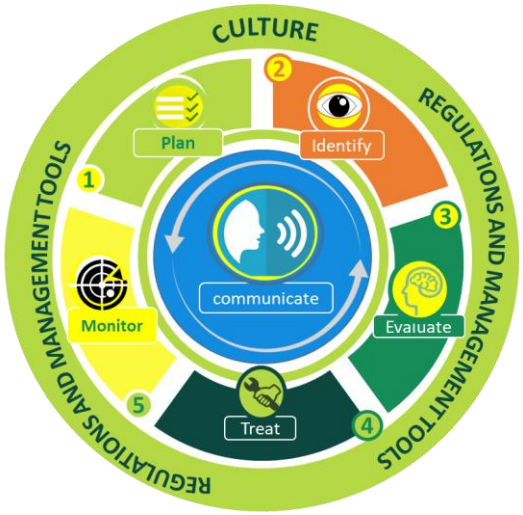


Figure 1. Risk Management Cycle

1 For Group companies, their size and operational situation must be considered.

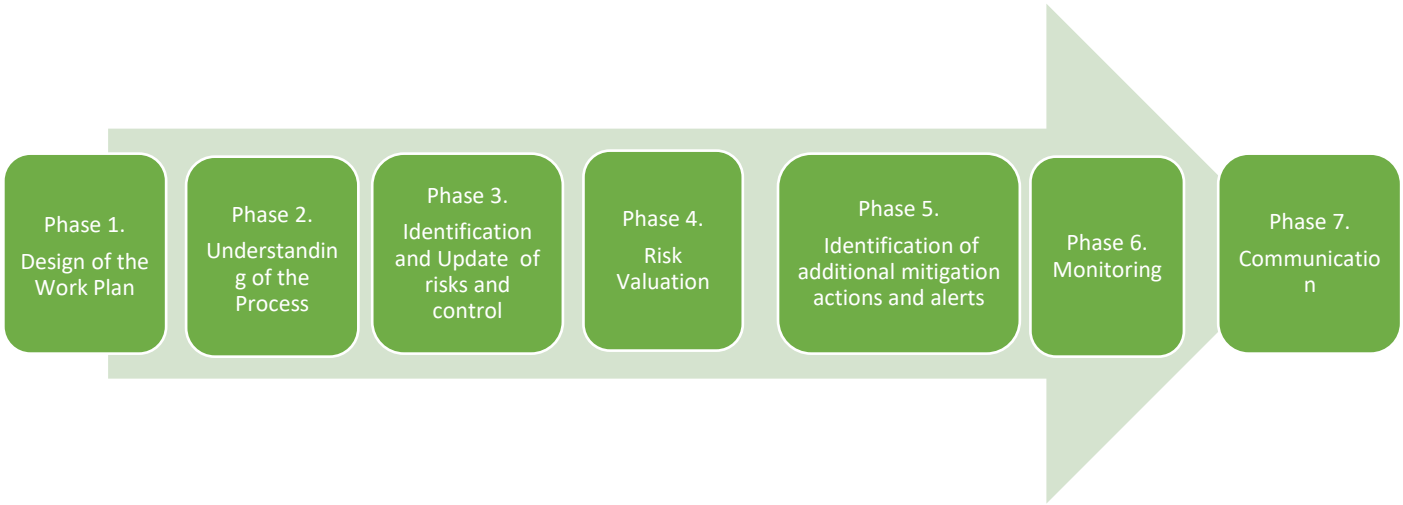
2 In furtherance of this document, Process shall be understood as all that contained in the official Process Map of the Company, including Management Systems.

With regard to the application of the Risk Management Cycle at Ecopetrol S.A. and its Business Group, Risk is any event of uncertain occurrence that, if materialized, could generate a negative impact on the achievement or fulfillment of the company's objectives and processes, and it can be measured in terms of the probability of occurrence of the causes and the impact of the consequences.

The risk management success depends on the application of this procedure, which activities must be carried out at least annually.

3. DEVELOPMENT

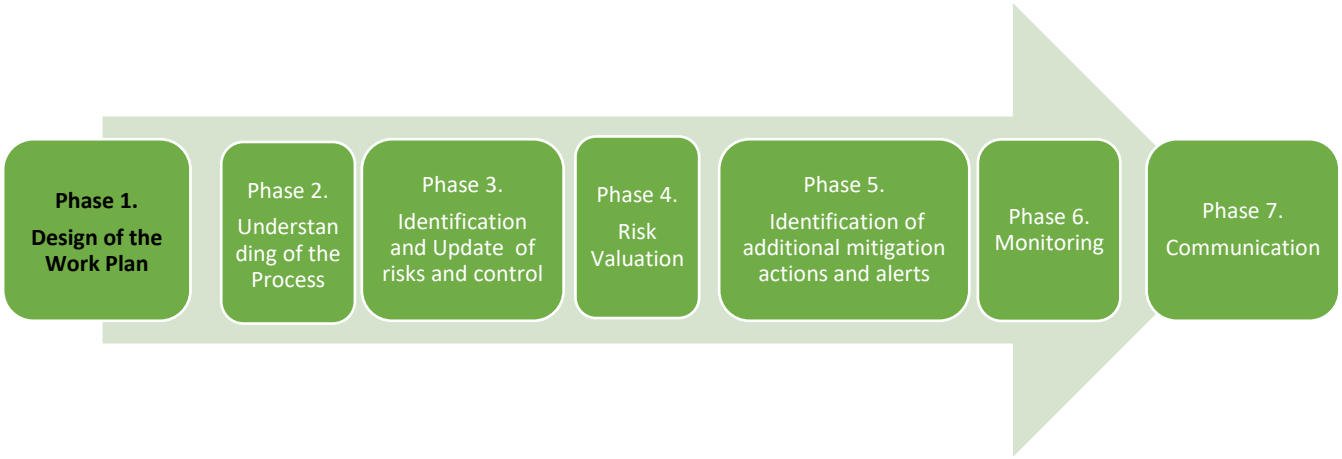
The process risk management cycle is carried out at least once a year and every time it is required according to the nature of the process, and it is accomplished through the following phases:



3.1. PHASE 1 – DESIGN OF THE WORK PLAN

It is required to design an annual work plan with annual and recurring activities to secure an adequate process risk management, intended to define the scope, resources, time, guidelines and tools required to carry out activities related to process risk management.

[3] The positive scope of risk is developed through the processes of defining the strategy, the analysis of taking advantage of opportunities to achieve business goals or processes.



3.1.a. **Inputs**

- *Process Information*: Process map, objective and scope of the process subject to analysis, activity flows of the sub-processes, interaction and attributes (inputs, outputs, documents, indicators, etc.).
- *Lessons Learned*: Experiences, evaluations and opportunities for improvement detected in the previous application of the Risk Management Cycle.
- *Other inputs*: Organizational guidelines and procedures that can influence risk management planning. These may include authority level and decision making, among others.

3.1.b. **Process**

Based on the schedule designed by Ecopetrol S.A.'s Corporate Management Internal Control Assurance, each area/company must define a work plan framed within specific dates.

The activities of this plan must be aligned with those described in this procedure and must include those responsible, starting and ending dates, deliverables, required resources, tools to define how to record and analyze the data in each stage, and how the results will be disseminated among the stakeholders, both internal and external, among others.

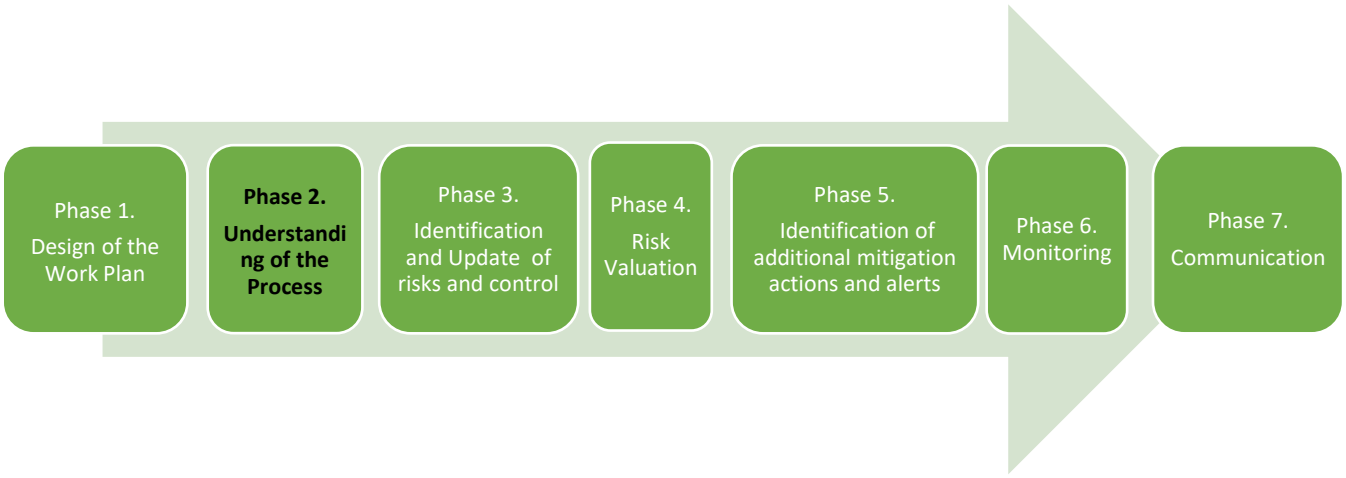
Within the definition of the work team members, there must be expert personnel on the various areas themes to ensure thorough risk identification, mitigation measures and risk alarms. The work team must necessarily include process owners, technical experts and a professional in Risks and Internal Control or their equivalent in the companies.

3.1.c. **Outputs**

At the end of this phase, there must be an annual risk management work plan for each Ecopetrol process and for each company, using the formats set out for this purpose, which must be disclosed in advance and when required to the participants of the risk management cycle in the area (s) involved.

3.2. PHASE 2 – UNDERSTANDING OF THE PROCESS

Whenever it is necessary to identify, document and manage risks and their mitigation measures and alarms, a previous analysis of the process must be carried out, which will be subject to review, in order to fully understand the activities, interaction, results and other relevant information for the period. To document this exercise, the form GEE-F-043 "Work Role Format Construction of Risk and Control Matrix" must be filled out.



3.2.a. Inputs

- *Process Information*: Description of the process and objectives, process operation, scope and limitations of the scope vis-à-vis its objectives, actual or potential changes in the design of the process (transition), activities, internal or external interaction, roles and responsibilities, deliverables, transactions, process data and information systems, events or situations that may cause failures in the process, failures within the operation and scope of the process, relevant third parties of the process, relationship of significant accounts to processes, among others.

- *Objectives Information*: Process objectives and strategic objectives associated with the process (taken from the Balanced Scorecards –BSC- of the areas related to the process), parties involved in achieving the objective, assessment of the fulfillment of the objective, critical success factors vis-à-vis the objectives, critical inputs for process execution, among others.

3.2.b. **Process**

Understand the logical sequence of the process and the information related to its operation: What does the process do? What for? What processes does it interact with?

Review how the process works, understand its objectives and scope, inputs, transformation activities and outputs. Similarly, its interaction with other processes and other input data of section 3.2.a must be identified, and on such basis, analyze at least the following:

- If the process has had significant changes with an impact on the internal control system (namely: scope, roles and responsibilities, critical activities, financial transactions, information systems, among others).
- In the event of having scope limitations, these must be clearly documented in the process due diligence.
- What potential or actual internal or environmental events or situations arise that cause possible process failures.
- What process situations led to having issues identified in self-evaluations, preventive monitoring, management tests and other audits, particularly considering recurring situations and at least the issues detected in the semester preceding the analysis performed.
- Identification[4] of the relevant interacting third parties (contractors that provide relevant services that are part of the processes, which execution could affect the Internal Control System).
- The association of transactions with the process and significant accounts of the financial statements, based on the definitions of accounts and significant processes carried out by the Corporate Management of Internal Control Assurance annually.
- The identification of critical and relevant information systems for process execution and performance.
- The alignment of process objectives and scope with the strategic objectives of the Balanced Scorecard (BSC) of the areas that are related to the respective process.
- The way to measure the fulfillment of the objectives and the critical success factors to achieve the objective.
- Segregation of duties of activities, roles and responsibilities, and information systems related to the process.

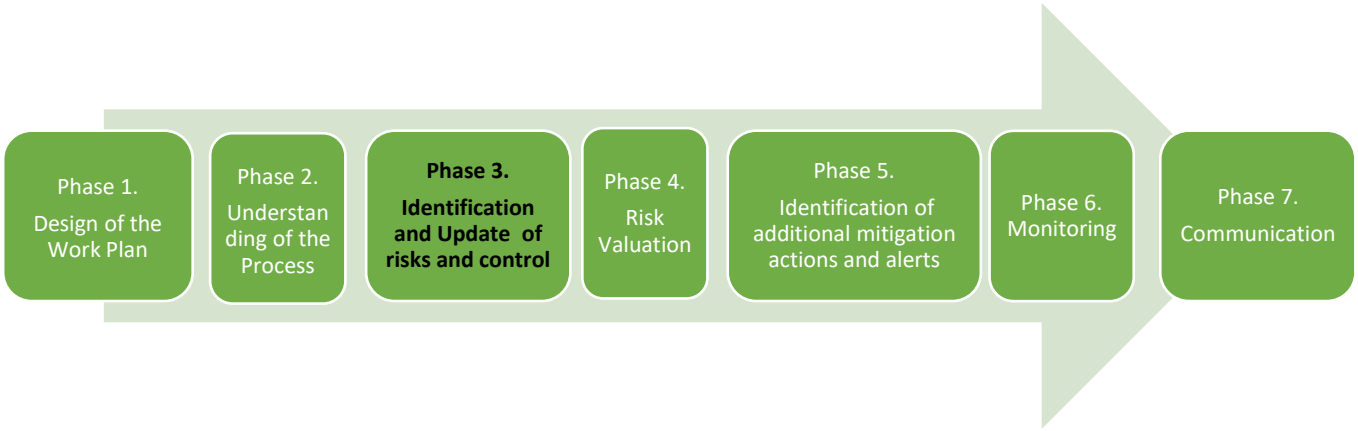
3.2.c. **Outputs**

At the end of this phase, there must be sufficient understanding of the process to perform the risk and control analysis. Also, the complete panorama of objectives (strategic and process) related to the scope of the risk and control matrix must be known.

[4] For the identification of relevant third parties (PAHO Service Provider Organizations) fill out the GEE-F- <043 "Work Role Format Construction of Risk and Control Matrix".

3.3. PHASE 3 - IDENTIFICATION AND UPDATE OF RISKS AND CONTROLS

The identification of risks allows, in a systematic and structured way, to determine the events that may negatively affect the objectives (strategic, operational, reporting, compliance) of the process. These events must be considered, regardless of being or not controlled by the organization. Likewise, the association and updating of controls makes it possible to carry out an assessment and treatment exercise that is closer to the operating reality of the process.



3.3.a. **Inputs**

- *Process Information*: Current Process Map; results of the executed process understanding.
- *Information on objectives*: Alignment of process objectives and strategic objectives of the BSC of the areas associated with the process and its indicators, results of indicators of strategic objectives and of the process in the previous period, environmental factors that may affect the achievement of the objectives.
- *Information on risks and mitigation measures*: Matrix of risks and controls of the processes[5], matrix of deployment of Business Risks in current processes, updated materialized events report, recent results of self-evaluations, findings of management tests, results of issues detected in the last semester from preventive monitoring and internal and external audits affecting the matrix of risks and controls, and the guidelines for the identification and documentation of risks and process controls implemented.
- *Other*: Organizational results, regulatory changes, technological changes, initiatives or ongoing projects, among others, that may influence the risk management of the process / company, regulations that impact risk design and mitigation measures (eg. ISO 37001 - Anti-Bribery Management System).

[5] If there is a Matrix of Risks and Cross-Cutting Controls and Multiple Executors, it should be considered in the exercise.

3.3.b. **Process**

a. IDENTIFICATION / UPDATE OF RISKS

For new processes or processes implying significant changes so that a new risk management exercise is necessary, the risks that may impact the achievement of the previously analyzed objectives must be identified.

On the contrary, if it is an updating exercise, it is necessary to start from the previously identified risks and verify their validity and sufficiency vis-à-vis the coverage of the process objectives.

In both cases, the use of the GEE-F-043 form "Work Role Format Construction of the Risk and Control Matrix" is required to guarantee the traceability of the exercise [6].

b. DEFINITION OF RISKS

The risks must be defined by three elements: Event, causes and consequences[7].

Define the Event: The event should be worded as that situation that, if materialized, would generate a negative impact on the achievement or fulfillment of the process objectives. To identify them, take the analyzed objective and think what situation could lead to deviate from their fulfillment. This should not be worded as denial of the objective, nor as non-management of process activities. Therefore, using terms such as "Inadequate, Insufficient, Not Ensured" should be avoided.

Establish the Causes: This means: why could this event occur? The analysis of the direct causes, both internal and external, which give rise to the event, must be carried out, including those that are directly managed within the scope of the process and those that are not, taking into account that these will be the basis for risk mitigation actions (controls or treatment); therefore, these must be concrete and consistent.

Establish the Consequences: This means, what would be the impact of the materialization of the risk event on the resources? (people, environment, economic, reputation, among others)?
The direct consequences must be determined.

The definition of risks can be performed using the following techniques:

- *Brainstorming*: It consists in bringing together the defined work team for each participant to explain what they consider to be the risks that affect the process objectives, followed by analysis and consolidation.

[6] For Ecopetrol, the identification sheet of this format must be documented. For companies, the format developed by each company for this purpose applies.

[7] For the definition of compliance risks, see Annex 3 of this document.

- *Surveys*: It consists in applying open-ended questionnaires or checklists of previously identified risks. It is practical when the work team is large or scattered and it is difficult to apply different techniques.

- *Interviews*: It consists in a structured dialogue through questions and answers. Its advantage is having access to the opinion of an expert, whose availability is limited, or obtaining higher quality answers by not being biased by a group session. The interview seeks opinions related to process risks. It is useful for obtaining first-hand information from experts.
- *Other tools*: Alternatives such as a list of business-type risks, layout techniques (cause-effect, fishbone, influence diagrams), SWAT analysis, Delphi technique, among others.

Although identification techniques per se do not guarantee absolute identification, a sufficiency analysis of the identified risks should be conducted, based on the objectives and scope of the process.

Therefore, the identification or updating of risks must consider that:

- The risks are significant regarding their possible impact on objectives achievement.
- A risk can be associated with several objectives.
- The risks must be sufficient to cover the scope of the process objective.
- Only the direct causes of the risk event are defined (not the cause of the cause).
- Always include the internal and external causes applicable to the process.
- Observations regarding process risks derived from self-evaluations, monitoring, management tests and other internal and external audits are considered and revised.
- All the objectives (strategic, operational, reporting, compliance) of the processes are covered including the process operation for those cases in which process scope limitations were identified with respect to the objectives.
- Business risks are included according to the business risk matrix versus processes [8]
- Bribery risk factors are included, in accordance with ISO 37000.
- If the risk is within the scope of another process, it must be included in the corresponding process matrix.
- The process areas where there are unidentified risks that can impact the normal operation and the fulfillment of its objectives, which were not been evidenced in the previous steps, must be determined.
- Events of business risks that may impact the objectives of the analyzed process are considered.
- In the event that the process subject to analysis has design or scope limitations (there are differences between what is written and what is done in the process, there are no sufficient activities designed or documented, there is lack of interaction with other processes, it is in the process of documentation or change / transition), make sure to identify the risks that are sufficient in scope to cover the entire process, regardless of their design status.

[8] If the company has developed a link between business risks and process risks.

c. RISK CATEGORIZATION

The identified risks they must be classified according to the category of the event, under the following criteria:

- **Strategic:** Risk associated with the strategic objectives of the area or the company, or those risks identified according to the matrix of business risks versus processes.
- **Financial:** Risk whose materialization directly affects the reliability and reasonability of figures in the financial statements.
- **Compliance:** Risk associated with non-compliance with the laws and regulations applicable to the company, particularly on fraud, misappropriation of assets, corruption, bribery, fraudulent reports, money laundering, terrorist financing, FCPA.
- **Operational:** Risks directly related to the process, due to internal or external causes.

The categories are not mutually exclusive, so a risk can be categorized into one or more categories.

d. IDENTIFICATION / UPDATE OF CONTROLS AND OTHER MITIGATING ACTIONS

In this stage, the causes to be managed for each of the risks are analyzed to thus identify the mitigation measures that reduce the probability. Similarly, the consequences of risk are analyzed and the measures that may reduce the impact are identified.

For a process whose risks are recently established, a new control identification exercise must be carried out, based on the causes of the identified risks.

An update exercise must start from the previously established controls and verify their validity and sufficiency to cover the process risks. This is done by first aligning the direct causes of risk with the existing controls.

In both cases, the use of the GEE-F-043 form “Construction of Risk and Control Matrix Form” is required to guarantee the traceability of the exercise.

e. DEFINITION OF CONTROLS AND OTHER MITIGATING ACTIONS

The definition of controls and treatment actions must be made in accordance with the provisions of the “Procedure for Managing Controls and Mitigation Measures”, GEE-P-006.

An existing mitigation action must be modified, without limitation, when:

- It is not aligned with the direct causes of the associated risk.
- There are changes in the operation of the mitigation action or the associated process.
- It does not mitigate the associated cause.
- There are recommendations derived from self-evaluations, monitoring, management tests and other internal and external audits on its design/operation.
- The mitigation action was not executed or is not effective.
- There are changes in the scope, accountability, start or end dates of the mitigation action.

It should be noted that for existing mitigating actions that are updated, their attributes must also be updated to ensure consistency. This means analyzing if the change to the mitigation action causes changes relative to the executor, frequency, type, classification, among others that may be applicable.

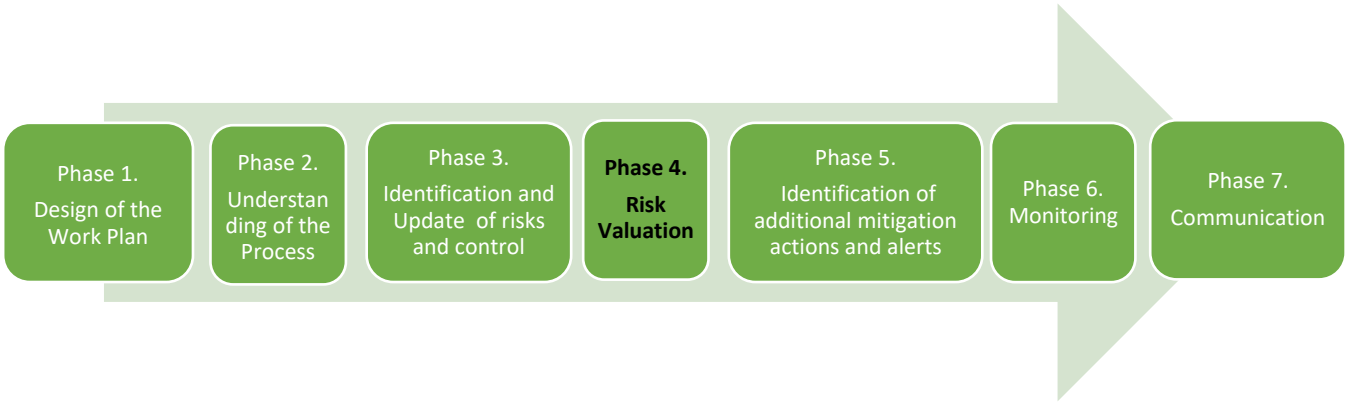
3.3.c. **Outputs**

At the end of this stage, you must have the Form GEE-F-043 "Construction of Risk and Control Matrix Form" reporting the risks associated with the process objectives and the controls and other mitigation actions corresponding to the risks treated, previously validated by the process owners.

3.4. PHASE 4 – RISK VALUATION

The risk valuation implies a semi-quantitative analysis that seeks to prioritize risks by assigning these values within predefined probability and impact scales or ranges.

The risks must be prioritized so as to achieve an effective distribution of available resources to deal with such critical risks. This is achieved by estimating the probability of occurrence of the event and the impact of its consequences on the resources (people, environment, economic, reputation, customers, among others [9]).



[9] As defined for each company.

The valuation exercise is performed based on the risks identified, documenting it in the Risk Assessment Form defined for this purpose[10] whereby the result of the valuation must be recorded, considering two main aspects: The inherent valuation and the residual valuation, as illustrated in the following figure:

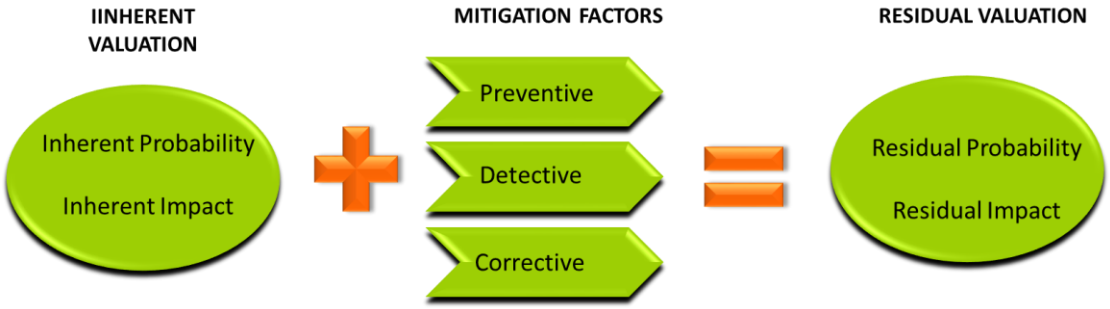


Figure 2. Inherent and Residual Valuation

3.4.a**. Inputs**

- *Information on risks and mitigation measures:* Definition of risk appetite (reflected in the risk assessment matrix – company's RAM), risk assessment format, risk matrix and process controls, risk matrix and cross-cutting and multi-executor controls[11], results of the treatment actions and results of key risk indicators (KRI's) of the last year, links of significant accounts with processes.

- *Information resulting from risk management and controls*: Analysis of self-evaluations, results of control testing carried out through preventive monitoring, findings of Management Tests and internal and external audits performed on processes.

- *Other*: Context and environment information related to process risks such as projection of regulatory reforms, technological changes, initiatives or projects underway, historical information of incidents or materialized risks that allow the estimation of frequencies of occurrence and impact (this information includes databases of accidents, costs and times, incidents occurred in the industry or in the company, even if they are not registered in formal databases).

3.4.b. **Process** [12]

The risk assessment is carried out during the execution of the cycle and must at least be reviewed and, if necessary, repeated each time a materialized risk event occurs, when control failures occur, when the associated treatment actions are ineffective or canceled, and when the mitigating actions are not enough.

[10] The SCI-F-005 format applies to the assessment of process risks in Ecopetrol SA Companies that have more or less resources or descriptors, must make the corresponding adaptation of said format.

[11] If there is a Matrix of risks and Transversal and Multiple Executors controls, it should be considered in the exercise.

[12] Ecopetrol SA must implement the Risk Assessment Matrix format, SCI-F-005.

a. INHERENT VALUATION

The inherent valuation is the assessment of the risk based on the measurement of the probability and impact without taking into account the effect of the mitigating actions.

To perform the probability estimate, based on the probability descriptors defined in the company's RAM matrix, the level of probability of risk materialization must be identified.

To do this, it is necessary to analyze the historical data of materialized events or statistics of the risk that have occurred in the sector, the company or the process, and identity the most critical or representative real situations. If there is not enough information to review a real situation, a credible hypothetical situation must be structured, based on the risk event and the impact of its materialization on the achievement of the related objectives.

The situation must be delimited by numerical data to determine the value of the scenario. Then, the scenario or situation based on which the inherent risk assessment will be carried out is documented, in the format used for risk assessments.

It should be noted that the scenario must preferably be based on the worst known historical situation. To build a hypothetical scenario, it is recommended to review with peers in the industry, and create it jointly with process owners, managers, or heads of the area related to the respective risk, to ensure that the scenario corresponds to critical situations in the opinion of the process expert.

If information is available for building both hypothetical and real scenarios, priority should be given to the real scenario, as long as it provides sufficient information to perform the valuation exercise.

Based on the defined valuation scenario, the probability value that best matches the risk event should be used, considering the available data on frequency or probability. Subsequently, the impacts of the RAM matrix (People, Environment, Economic Resources, Reputation, Clients, according to that defined in the Company Valuation Matrix) are classified according to the impact they generate, taking into account the direct effects on the resources of this matrix. To do this, identify from the descriptors the one that best reflects the impact of the scenario, rating each of the applicable variables according to the scenario.

The inherent risk assessment is derived from the combination of probability and highest impact.

b. RESIDUAL VALUATION

The residual valuation is understood as the resulting level of risk once the mitigating actions have been applied on the probability of occurrence and the impacts on the valued resources. It is intended to establish the level of exposure to the identified risks, considering the existence of the mitigating actions in place and their effectiveness in mitigating them.

Once the inherent risk assessment has been completed, the residual assessment is estimated, based on the sufficiency and effectiveness of the set of mitigation actions associated with the risk (controls and treatment actions with verification of their effectiveness).

The qualification of the controls is based on: a) sufficiency of the mitigating actions, b) control classification, c) type of control, and d) effectiveness of the control.

a) *Mitigating actions sufficiency*: Associate all risk mitigation actions and assess whether they are sufficient to manage the causes, as set out in the Procedure for the management of controls and treatment actions in the Ecopetrol Group, GEE-P-006. If the associated controls are not sufficient, it is understood that they have no incidence in reducing impact and probability.

b) *Control classification*: It is based on the classification of preventive, detective or corrective controls, according to the following association:

Preventive control	Mitigate the causes of risk
Detecting control	Mitigate the causes and/or reduce risk impacts
Corrective control	Mitigate or reduce risk impacts

c) *Control type*: It should be stated if the control is automatic, manual, or manual dependent on IT, in accordance with what has been defined in the risk and control matrix.

d) *Control effectiveness*: To establish the effectiveness for each of the controls based on the results obtained in the Statutory Audit, management tests, internal control self-evaluations, and preventive internal control monitoring and audits, indicating whether the ineffectiveness is associated with operation or design.

Based on the combination of the above factors, a score of maximum 100 possible points is assigned for each associated control according to the following structure:

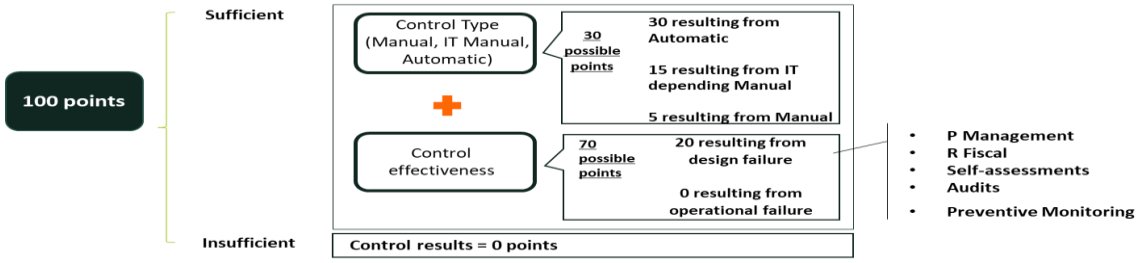


Figure 3. Control scoring scheme

The resulting rating will determine whether the control is weak, moderate, or strong:

- Strong control: Control scored with 90 points onwards.
- Moderate control: Control scored between 75 and 89 points.
- Weak control: Control scored 74 points or less.

To evaluate the control based on the qualification or score obtained, it must be analyzed to what extent it manages the probability or impact of the risk, taking into account the following:

- A control decreases the probability directly if the control activity directly addresses the cause associated with the risk.
- A control does not decrease the probability if the control activity does not mitigate the risk cause.
- A control directly reduces the impact if the control activity is aimed at directly reducing one or more of the risk impacts.
- A control indirectly reduces the impact if the control activity can decrease to a certain extent one of the risk impacts in the event of materialization.
- A control does not lessen the impact if the control activity does not reduce the risk impact.

Finally, according to the evaluation of each control, the inherent risk displacement level should be identified based on the number of columns and rows according to the following table:

Control rating	Helps decrease probability	Helps lessen impact	# Columns in the matrix that move on probability axis	# Columns in the risk matrix that move on the impact axis
Strong	directly	Directly	2	2
Strong	directly	Indirectly	2	1
Strong	directly	does not decrease	2	0
Strong	does not decrease	Directly	0	2
Moderate	directly	directly	1	1
Moderate	directly	indirectly	1	0
Moderate	directly	does not decrease	1	0
Moderate	does not decrease	directly	0	1

In sum, the displacement of the inherent risk in the heat map or in the RAM matrix will depend on the average of the probability and impact levels resulting from the application of the previous analysis to each control, thus obtaining the residual risk.

NOTE: It should be taken into account that if the control being rated is new, resulting from the replacement of a rationalized control on which failures have been identified in the monitoring exercises (internal or external audits, management tests, internal control self-evaluations , etc.), it must be classified as ineffectiveness of the previous control until it operates and its effectiveness is assessed, at which time the assessment of the associated risks should be reviewed.

3.4.c. **Outputs**

At the end of this stage, the inherent and residual valuation of the risks identified in the forms set out for this purpose must be taken at VH levels (Very High - Very high); H (High - High); M (Medium - Medium); L (Low - Low) and N (Null - Very low) according to the company's RAM matrix, and approved by the respective process owner.

3.5. PHASE 5 - DEFINITION OF ADDITIONAL MITIGATING ACTIONS AND RISK ALERTS

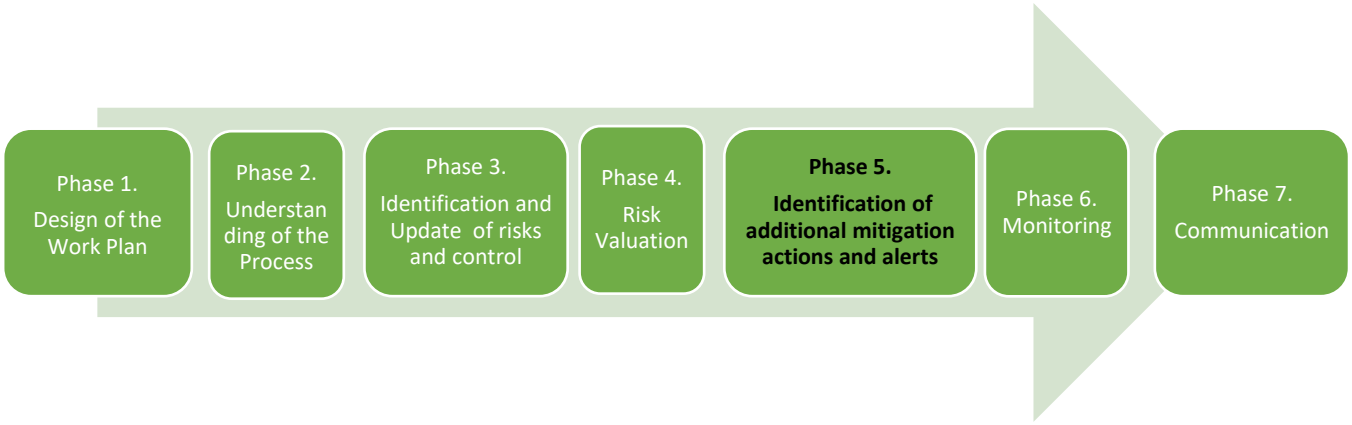
In this stage, additional mitigation activities are defined (controls or treatment actions) intended to prevent the causes or protect against the consequences from risks whose residual value is "Very High", "High" and "Medium"[13], through the analysis of the identified causes and the effectiveness of all associated mitigating actions, in order to select the appropriate option between control activities and treatment actions, which is economically viable to bring the residual risk to an acceptable risk value (“Low" or "Null").

If the residual risk assessment is “Medium”, additional mitigating actions are optional, at the discretion and judgment of the process owner, except in the following cases:

- When the controls associated with risk have had design and operational findings in self-evaluations, management tests, Statutory Audit or preventive monitoring in the last year.
- The risk is of a strategic category.

Risk alerts or KRI (Key Risk Indicator) are also defined as measurement tools that preventively monitor the behavior of variables associated with the risk causes, to indicate changes in the level of exposure to risks, generating early warnings that lead to reinforcing or focusing management to avoid its materialization. KRIs must be identified for those risks with residual values "Very High" and "High" and aligned directly with the strategic process objectives.

[13] According to the levels of the RAM matrices of each company.



3.5.a. **Inputs**

- *Information on risks and mitigation measures*: Results of the risk assessment exercise, risk matrix and process controls, risk matrix and cross-cutting and multi-executor controls[14], reports of internal or external audits on the analyzed process, which can be an input to determine the new mitigation measures, updated materialized events report, etc.

3.5.b. **Process** [15]

a. IDENTIFICATION OF NEW MITIGATION MEASURES

The most appropriate mitigation measure between economically viable control activities and treatment actions (TAs) should be established according to the following options:

- Control activities: Controls are formulated or redefined to mitigate the causes through a systematic and recurring activity in the analyzed process.
- Treatment Actions: If the risk cause cannot be managed with a recurring control activity, in this case a treatment action must be created.
- Cross-cutting Controls: If the cause can be mitigated through a systematic and recurring activity to be carried out by all areas of the company, the cross-cutting mitigation action must be generated, together with the Government process.

[14] If there is a Matrix of Risks and Transversal Controls and Multiple Executors, it should be considered in the exercise.

[15] The guidelines for the construction of controls and treatment actions should be consulted in the "Procedure for managing controls and mitigation measures", GEE-P-006.

- Multiple Executors Controls: If the cause can be mitigated through a systematic and recurring activity to be carried out by some areas of the company, the mitigator of multiple executors must be generated together with the Government process.

b. DEFINITION OF KRI [16]

For the definition of alerts or KRIs, you must select:

- Documented risk causes with the highest probability of occurrence[17].
- The causes that gave rise to risk materialization (when applicable).

From the above selected causes, take at least one and identify what are the variables that can be subject to measurement and determine what information is necessary for the design of the indicator (how, when and where the variable data is obtained). Once the availability of data has been validated, propose a KRI that meets the criteria defined herein.

Please note that a KRI:

- Must be specific and clear, measurable (quantifiable), based on available, recent and reliable data.
- Must have a clear description or intention of what is to be measured, considering applicable exclusions or limitations.
- To obtain the result, the KRI calculation formula must contain the equation or mathematical expression where the variables and constants are related.
- It must have a limit, which must be a tolerable numerical value to generate 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 minimum value (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. To define this frequency, the cycle of the information or input data must be taken into account, as well as the opportunity to generate the alert.
- It must be different from the result indicators of the Company's strategic map objectives and the process indicators, but it can be a medium indicator, as long as it is associated with the selected causes.

[16] There is an example of KRI in the annexes to this document.

[17] To determine which cause is most likely to occur, use expert judgment.

3.5.c. **Outputs**

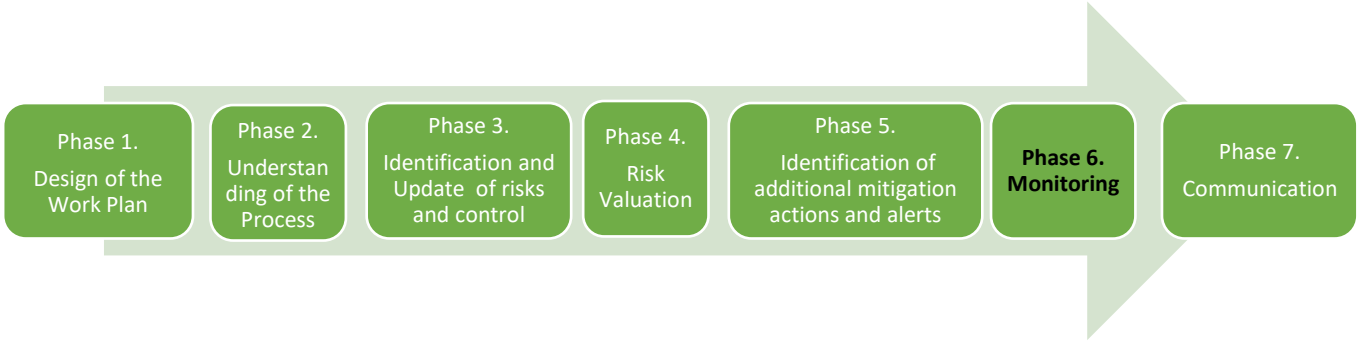
At the end of this phase you should have:

- New or updated mitigation measures (Treatment actions, control activities, Cross-cutting Controls, Multiple Executor Controls, and other Mitigating Actions), which must be documented.
- Designed KRIs.

3.6. PHASE 6 - RISK MONITORING

The objective of monitoring is to verify that the risks identified, valued and treated are permanently within the tolerable limits of the company, for feedback of the risk cycle and to take actions that secure their proper management.

The scope of the monitoring process risks includes monitoring treatment actions, alerts generated through KRIs, event materialization, and measuring the effectiveness of treatment controls and actions through self-evaluations, preventive monitoring of Internal Control, Management Tests and internal and external audits.



3.6.a**. Inputs**

- Risk and control matrices
- Results of the assessment
- Risk alarms - KRIs designed
- Materialized risk events
- Information on the execution of controls and treatment actions
- Information on external changes that may increase exposure to risk
- Results of Internal Control Self-evaluations, Management Tests, Internal and External Audits.

3.6.b. **Process**

a. MONITORING OF TREATMENT ACTIONS

This monitoring[18] ensures systematic feedback on the progress of treatment actions, providing alerts related to that planned for risk management and to assess its final effectiveness.

To monitor treatment actions, the executor (s) of the treatment action (s) must report: i) the actual progress of the treatment actions, which will be a percentage value according to the fulfillment of the activities in the work plan and the defined milestones and dates, ii) comments or justifications that support the state of execution of the action, and iii) measurement of the effectiveness of the final action.

The status of the treatment actions must be updated periodically[19] and it will be defined according to the actual progress, the planned progress, the start and end date, 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 is progressing equal or greater in accordance with the established work plan and the end date has not occurred.
- *Delay*: The start date has already occurred and the progress of the action has not reached the level planned for the period or the action does not show any progress registered or the end date has already occurred and the action has not been completed.
- *Closed*: The end date has already occurred and the progress of the action is 100%.
- *Cancelled*: The action was suspended or canceled before achieving 100% of its progress.

The effectiveness of execution of the treatment actions must be managed in accordance with the provisions of the "Procedure for Management of Controls and Mitigation Measures", GEE-P-006. If it is not effective, it should be understood that the risk has not been managed and, therefore, the risk must be analyzed again within the cycle and its incidence on risk assessment, considering the definition of risk mitigators and alerts, as appropriate.

b. MONITORING MATERIALIZED RISK EVENTS

Materialized events are understood as the occurrence of situations whose consequences affected the achievement of the objectives defined for the strategy, processes or projects. For the analysis of materialized events, at least the following elements should be documented:

- Describe in detailthe materialized event
- Event occurrence date
- Associate the event with a matrix risk
- Determine if the cause of the event was identified in the risk and control matrix
- Establish if the event originated from people, processes or environment

[18] At Ecopetrol, the monitoring of treatment actions is carried out by the professional of the Management of Internal Control Assurance on a monthly basis based on what is reported by the processes.

[19] At Ecopetrol, monitoring or review is carried out on a monthly basis, reporting when applicable according to the defined work plan / milestones. In companies it is carried out according to the calendar or periodicity defined by Ecopetrol's Corporate Internal Control Assurance Management.

- Determine what was the impact of the event on each of the company's resources (eg, people, environment, economic, etc.)
- Identify the mitigation action established for the cause that originated the event
- Analyze the operation and design of the mitigation action
- If the cause or risk was not previously identified, define them
- Establish if the risk has a KRI associated with the cause that defined it
- Identify if the KRI warned about the potential materialization of the event
- Establish if the event occurred modifies the current risk assessment
- Establish if the event occurred involves changes to the mitigating actions
- Document the action to be taken

With this information the sufficiency in the identification of risks, causes and consequences is validated; likewise, the need to adjust existing mitigating actions or define new measures is verified, and the risk assessment is validated and adjusted. These events and their analysis must be registered in the "Format for the management of risk materialization", GEE-F-044. The action plans that arise from the analysis of the materialized event must be reported by those responsible for their execution and monitored by the Corporate Management of Internal Control Assurance [20].

c. MONITORING ALERTS GENERATED THROUGH THE KRI

KRIs can alert about changes in the level of exposure and generate early alerts that lead to reinforcing or focusing management to avoid its materialization.

The KRI report must be carried out at the established frequency and in compliance with the reporting guidelines established by each company. The information reported will correspond to:

- The result of the KRI calculation reported by the process
- Alert status or not, according to the result and defined design parameters (eg unit of measure, trend and alarm limit)
- The analysis of why the alert was generated and the management that will be carried out.

Monitoring is managed as follows:

- When the result of a KRI is outside its alert limit, the Corporate Management of Internal Control Assurance shall carry out a review of the effectiveness of the controls and the treatment actions associated with the risks; as well as evaluating the need to activate additional prevention measures, implement alternative action plans or focus monitoring on certain risk factors, among others, in order to minimize the possibilities of materialized risk events.

- Make graphs of the behavior of the historical results that allow visualizing if the KRI is moving away from or approaching its alarm limit, to identify trends or seasonality in the KRI results (see annexes). The charts apply once two or more KRI reports are available, so that a trend can be established.

[20] At Ecopetrol, monitoring or review is carried out on a monthly basis, reporting when applicable according to the defined work plan / milestones. In companies it is carried out according to the calendar or periodicity defined by Ecopetrol's Corporate Management Internal Control Assurance.

- Calculate the average and the number of times outside the limit during the last year of measurements, in order 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 it presented the respective early alerts. Document this analysis in the Risk Materialization Form. If no alerts were issued, the KRI design should be reviewed and adjusted to better reflect the risk variables.

d. MONITORING THE EFFECTIVENESS OF CONTROLS

The tracking of control activities is carried out through the monitoring of their design and effectiveness, which performed at least through:

- Internal Control Self-Assessments
- Preventive Internal Control Monitoring
- Management Tests
- Internal and External Audits

The effectiveness of the design and operation of the controls must be managed in accordance with the provisions of the "Procedure for the Management of Controls and Mitigation Measures", GEE-P-006.

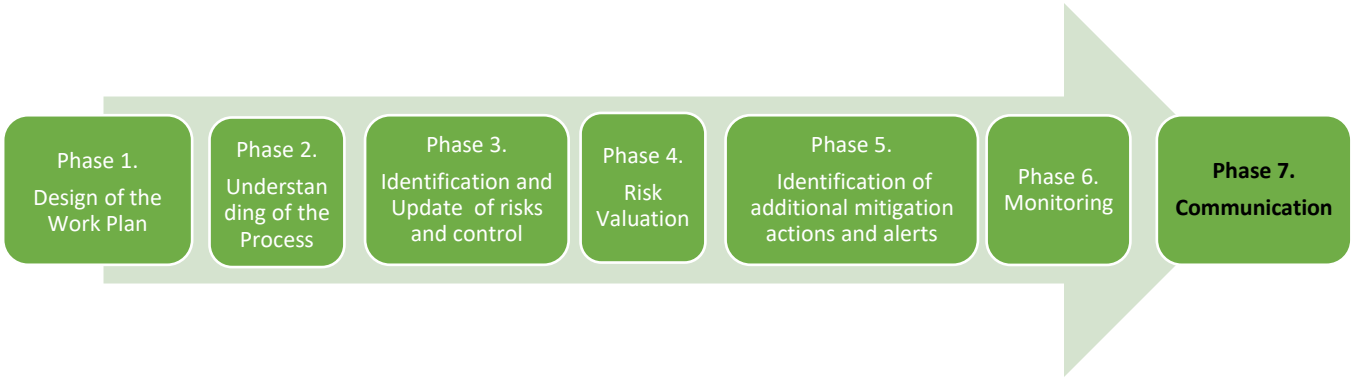
3.6.c. **Outputs**

The result of the monitoring stage should feedback the risk identification, assessment and treatment stages, depending on the issues identified through:

- Report on the status of execution of the Treatment Actions
- Result of KRIs
- Format with materialized risk analysis
- Internal Control Self-Assessment Results
- Internal Control Preventive Monitoring Reports
- Management Tests Observations
- Internal and external audit observations.

3.7 PHASE 7 - COMMUNICATION

Communication is defined as an interactive process of information exchange that allows to socialize the results, share data, opinions and perspectives, facilitate adequate flow of information and dialogue between the stakeholders or involved parties. Communication allows each stage of the risk management cycle to be built together with the Company's areas and processes.



Communication is implemented in each of the phases of this procedure and it must ensure:

- Generation of a risk management common language and culture.
- Feedback on risk management by incorporating the results from each of the phases and the interaction between the process executing areas and the government of the Internal Control System.
- Disclosure of the roles and responsibilities of the participants and stakeholders.
- Disclosure of relevant information on process risk management.
- Identification of synergies among the different areas to strengthen risk management.
- Incorporation of risk management as a strategic variable for decision making.

The following scheme is available for the communication of process risk management:

Phase / Element	Deliverable	Frequency	Communication Channel / Issuer	Receiver
Preparation of the work plan	Schedule	Ecopetrol: At least annually Subsidiaries: According to guide GEE-G-002	Process Owner Email / Compliance Manager of subsidiary	Corporate Management of Internal Control Assurance
Identification and updating of Risks and Controls	Risk and Control Matrix	Ecopetrol: Monthly Subsidiaries: According to guide GEE-G-002	Ecopetrol: BWise Subsidiaries: Risk management report	Corporate Management of Internal Control Assurance
Risk Valuation	Risk Assessment form.	Ecopetrol: Annual minimum or when required Subsidiaries: According to guide GEE-G-002	Process Owner Email / Compliance Manager of subsidiary	Corporate Management of Internal Control Assurance

Identification of additional mitigating actions and risk alerts	Risk and Control Matrix	Ecopetrol: Monthly Subsidiaries: According to guide GEE-G-002	Ecopetrol: BWise Subsidiaries: Risk management report	Corporate Management of Internal Control Assurance
Materialized risk events	Risk materialization format GEE-F-044	Ecopetrol: Every time an event happens Subsidiaries: According to guide GEE-G-002	Email of the owner of the process where the event was detected / Compliance Manager of subordinate	Corporate Management of Internal Control Assurance
Shareholders treatment	Bwise monitoring / effectiveness report for Ecopetrol Risks and Control Matrix for subordinates	Ecopetrol: Monthly And every time a treatment action is closed Subordinates: According to guide GEE-G-002	Ecopetrol: Bwise / Executor of treatment action Subsidiaries: Risk management report	Corporate Management of Internal Control Assurance
Controls	Report of: self-evaluations, management tests, preventive monitoring, internal and external audits	Quarterly Self-Assessments Management tests, preventive monitoring, internal and external audits, when evaluating controls	Self-assessments: Ecopetrol: Bwise Subsidiary: self-evaluations Other monitoring: Ecopetrol: Monitoring reports Subsidiaries: Format of findings according to defined periodicity	Corporate Management of Internal Control Assurance
KRIs	Ecopetrol: BWise Report Subordinates: Matrix risks and controls	Ecopetrol: Monthly Subsidiaries: According to guide GEE-G-002	Ecopetrol: BWise Subsidiaries: Risk Management Format	Corporate Management of Internal Control Assurance

4. CONTINGENCIES

Not applicable

LIST OF VERSIONS

	Procedure for Process Risk Management in the Ecopetrol Group		
	Internal Control System Internal Control Assurance Corporate Management		
	GEE-P-005	Prepared 05/02/2019	Version 2

Last Document			
Version	**Date**	**Old Code Document and Title**	**Changes**
New Document			
Version	**Date**	**Changes**	
1	31/01/2018	Repeals: PDO-P-025 Procedure Cycle Risks Processes PDO-I-027 Instructions for the design and monitoring of Treatment Actions PDO-G-039 Guide for the design, testing and implementation of KRIs PDO-I-017 Instructions for the construction and updating of integral internal control matrices PDO-I-030 Risk assessment instructions.	
2	05/02/2019	Includes analysis of transactions and significant accounts Risk categorization is included. Repeal the GEE-F-045 format. The chapter related to risk assessment is updated. Note: It is published with this date as this is the date of disclosure of the document, which was used for the purposes of executing the current risk management cycle.	

For more information contact:

Author(s): Edna Carolina Vargas
Telephone: 50559 mailbox: geraseconint@ecopetrol.com.co
Division: Internal Control Assurance Corporate Management

Electronically reviewed by:	Electronically approved by:
ANGELICA MARIA ALAIX M. **Professional** **ID. No. 52.516.825** **Internal Control Assurance** **Corporate Management** **MÓNICA JIMENES G.** **General Secretary** **ID. No. 52.411.766** **General Secretary & Presidential Support**	**HELBER ALONSO MELO HERNÁNDEZ** **Internal Control** **Assurance Corporate Management** **ID. No. 79.862.626** **Internal Control Assurance** **Corporate Management**

Document signed electronically, in accordance with the provisions of Decree 2364 of 2012, whereby article 7 of Law 527 of 1999 is regulated, on the electronic signature and other provisions are dictated.
To verify compliance with this mechanism, the system generates an electronic report that shows the traceability of the review and approval actions by those responsible. If you need to verify this information, request said report from the Service Desk.

5. ANNEX 1

Example of a KRI

Objective	Risk	Cause	KRI
Ensure the start, execution, closure and settlement of contracts	Breach of the obligations agreed in the contract	Failure to take timely action as per contract monitoring alerts, requests, payments, claims filed by the contractor.	Percentage of contracts with claims for alleged breaches by Ecopetrol

Description:
Percentage of contracts with claims for alleged breaches of Ecopetrol. This KRI monitors the cause:
Failure to take timely action as per contract monitoring alerts, requests, payments, claims filed by the contractor.

Formula: Number of contracts with claims for alleged breaches by Ecopetrol in the month / Number of contracts in execution and at closing and settlement.

Measurement frequency: Monthly

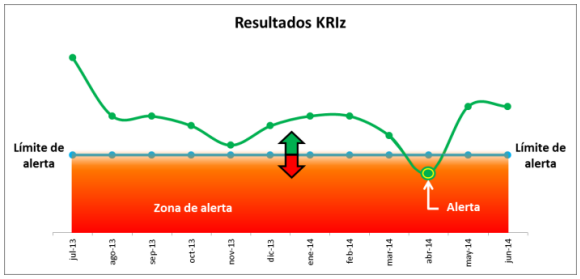
Measurement Unit: Percentage

Source:
- Consolidated national report claims tab for the month.
- Official SAP hiring report ALL COMPANIES

Alert limit: 0.15% (maximum value)

Trend: Negative (values below the control limit indicate better behavior)
Evidence Location: UAE measurement file located in the SharePoint Supply Management.

6. ANNEX 2 KRIS trend example



Example KRI results with maximum alert limit (negative trend).

Example KRI results with minimum alert limit (positive trend).

7. ANNEX 3

To carry out the explicit incorporation of the compliance risk event that covers fraud, corruption, bribery, money laundering and terrorist financing, and violations of the FCPA law issues in the risk matrices and process controls, the following generic event is provided, which must be incorporated in each process with the respective causes and consequences, according to its context and particular details, according to the level of deployment of the risk and control matrix.

GENERIC COMPLIANCE RISK EVENT: Fraud, corruption, bribery, money laundering, terrorist financing, and FCPA violations in the process "Name of process / subprocess"

The identification of these events must be carried out during phase 3 of Risk and Control Identification and Updating of the process risk management cycle, while for identified events, the rest of the phases of the cycle must be supplied to secure ensure the particular design of each of these risks, according to the nature of the processes.

As an example, a risk is illustrated below:

Process Level 1	Description of Process objective:	Risk Name	Description of Risk
Compliance Contracts	Ensure the start, execution, closure and balance of contracts, making adequate eventuality management and evaluating the contractor's performance.	Fraud, corruption, bribery, money laundering, terrorist financing and FCPA violations in the Contract Management process.	Fraud, corruption, bribery, money laundering, terrorist financing, and FCPA violations in the Contract Management process Related to: - Receiving or Authorizing payments, of goods and/or services that do not comply with the agreed conditions, or that have not been received. - Modification of contract information in the systems by unauthorized spokespersons. - Misuse of resources in contractual performance. - Double payments. - Leakage of process critical information. The foregoing may cause involvement in legal processes and economic losses.