BUSINESS RISK MANAGEMENT PROCEDURE

Version	Description of Changes	Approval	Effective Date
1.0	Initial version	Andrés Wainer	May 2016
2.0	See Section 6. Track Changes	Andrés Wainer	June 2021
3.0	Updates regarding risk appetite, impact and probability scales, the effectiveness of mitigation measures, and residual risk calculation. Category change: from “Appendix to the Risk Management Policy” to “Procedure”	Andrés Wainer	October 2025

RISK MANAGEMENT PROCEDURE

Effective Date: October 2025

Version 3.0

TABLE OF CONTENTS

1. Introduction

Every business encounters risks, and the challenge lies in assessing the acceptable level of uncertainty. Corporate risk management enables management to effectively address this uncertainty, thereby improving the company's ability to maintain and continue generating value.

Management must establish a strategy and objectives for growth and profitability while striking an optimal balance with the associated business risks so as to maintain and increase the company's value over time.

In this context, it is the responsibility of each Operation and the Corporate Office to ensure that relevant business risks are identified and mitigated to such an extent that, should they materialize, their impact would be manageable, thereby ensuring business continuity.

It is worth highlighting the benefits of risk management:

- ✓ **It contributes to the achievement of organizational objectives** by improving decision-making and anticipating events that could affect the attainment of goals.
- ✓ **It promotes a culture of shared responsibility** by strengthening the organization's commitment and reinforcing governance, internal control, and regulatory compliance.
- ✓ **It reduces uncertainty and improves organizational resilience** by lowering the likelihood of crises, operational disruptions, and unanticipated financial losses.
- ✓ **It protects equity and business continuity** by identifying threats that could compromise physical, financial, technological, and human assets.
- ✓ **It strengthens the organization's reputation and stakeholder trust** by increasing transparency regarding risks and decisions, as well as by protecting the brand.
- ✓ **It optimizes resource allocation and prioritization** by focusing efforts and resources on the issues most critical to business success.

The methodology presented below enables structured risk management, with uniform evaluation criteria and standardized reporting to the Board of Directors. This methodology is based on international standards, such as ISO 31000, and takes into account international best practices in this area.

2. Objective

This methodology provides the necessary guidelines for effectively managing business risks that could adversely affect the achievement of the Company's objectives.

3. Considerations

a. **Business risk**: "the possibility that an internal or external event or action will adversely affect an organization's ability to successfully execute its strategies and achieve its objectives" (definition taken from

the book *Comprehensive Business Risk Management* published by Deloitte). At Coca-Cola Andina, business risks are referred to as “Risk Pillars.”

b. **Specific risk**: An incident or event, arising from internal or external sources, that triggers the materialization of a business risk. For example, for the “business continuity” risk, the following specific risks were identified: strikes, disruption in the supply of raw materials, power outages, and the availability of returnable containers, among others.

c. **Assessment techniques:** The risk assessment methodology consists of a combination of qualitative and quantitative techniques. In general, qualitative techniques should be applied when risks are not quantifiable, when sufficient and credible data for a quantitative assessment are unavailable, or when obtaining and analyzing such data is not cost-effective. Quantitative techniques typically provide greater precision and are used in more complex and sophisticated activities to complement qualitative techniques; they require a greater degree of effort and rigor, sometimes employing mathematical models. In general, and given the characteristics of the risks in question, it is most likely that qualitative techniques will need to be applied.

4. Risk Management Process

The Risk Management process is a continuous process in which the following phases can be distinguished:

As well as the following roles and responsibilities:

a. Front-line operational risk management:
   - ✓ **Risk owner:** Responsible for ensuring the mitigation and control of the risks under their purview.
   - ✓ **Control Owner:** Responsible for ensuring compliance with the control design and overseeing its timely execution.
   - ✓ **Control Implementer:** Responsible for performing the control and generating evidence in accordance with the established design.

b. Second line of defense for risk management:
   - ✓ **Local Risk Manager:** Responsible for providing methodological support to the various risk owners to ensure proper detection, assessment of risks/controls, as well as monitoring of action plans when required.

c. Third line of risk management:
   - ✓ **Internal Audit**: Provides independent and objective assurance regarding the effectiveness of the risk management system, internal controls, and governance processes.

4.1. PHASE 1: INTERNAL/EXTERNAL CONTEXT ANALYSIS.

Context analysis is the fundamental starting point for risk management. It involves understanding the environment in which Coca-Cola Andina operates across its various operations, both externally (political, economic, social, technological, legal, and environmental factors) and internally (structure, culture, capabilities, processes, and strategic objectives).

This understanding ensures that the identification, analysis, and treatment of risks are carried out in a manner that is relevant and aligned with the organization's reality.

It is recommended to use tools such as PESTEL or SWOT periodically or when updating the risk matrix.

4.2. PHASE 2: RISK IDENTIFICATION

According to the methodology, the next step is to identify business risks and their specific associated risks.

Among the sources for identifying risks, we can distinguish the following:

- ✓ **Definitions by the Board of Directors or the Corporate Sustainability and Risk Committee**: Both the *Board of Directors* of Coca-Cola Andina and the *Corporate Sustainability and Risk Committee* have, within their responsibilities, the authority to establish the business risks (risk pillars) that will be

incorporated into the risk management process, regardless of whether the respective departments have been managing them as part of their normal operations.

- ✓ **Emergencies or crises**: As indicated in the *Corporate Emergency Management Policy* under the section "Operational Responsibilities," following an emergency, the local risk team, in conjunction with members of the Emergency Management Team (EMT), must conduct an analysis of the situation and review the adequacy of the business risk matrices in light of the event that occurred. Examples of this include the 2019 social unrest in Chile and the COVID-19 pandemic.
- ✓ **Strategic Plan Analysis**: To achieve its mission, the Company has developed a strategy based on the integration of pillars of business growth and sustainability, aligned with its vision and organizational values. Each of these pillars (or "strategic pillars") is subject to a series of factors and events that could affect their development and fulfillment and, therefore, must be identified and managed.
- ✓ **Analysis of Critical Business Processes**: Critical processes are those essential to the business, such that a disruption to them would result in a significant impact and/or a crisis within the company. Given this, the factors that could trigger a disruption to these processes must be identified and managed.
- ✓ **Current legislation and regulations in the jurisdictions of the countries in which the Company operates**, for the purpose of identifying potential legal, regulatory, and compliance risks that may expose the Company to administrative, civil, or criminal penalties.
- ✓ **Benchmarking of risks reported in international reports** or by peer companies of interest to Coca-Cola Andina.
- ✓ **Others:** Observations and findings detected during internal and external audit processes, incident and complaint analyses, workshops or interviews with key experts, consultations, or surveys.

When identifying new risks, one must consider the following factors to facilitate the management of the risk matrix and ensure the comparability of information:

a. You should always verify whether it is truly a new risk and not a redefinition or cause of a risk already included in the matrix.

b. Consistency in risk definitions:

   - ✓ A risk must be described in a consistent manner across all operations; therefore, any new risk or modification to an existing one must be analyzed and approved by the *Risk Administrators Committee*, which convenes on a biweekly basis (for more details, see Phase 6: Monitoring and Review). ***A risk can be described as the following: Due to <CAUSE>… <RISK> may arise… resulting in <EFFECTS>***
   - ✓ If a risk is not applicable to an operation (i.e., the factors that could cause the risk to materialize are not present and therefore its probability of occurrence is 0), it must be recorded in the matrix as **"not applicable"** and the reasons for this must be explained.

When a new risk is identified, it must be recorded in the matrix, providing the following information:

- ✓ **Name and description of the risk**: The name should be "self-explanatory" (e.g., "Downtime of a critical contractor"), avoiding codes and sequential numbers. The description should be brief but as clear as possible.
- ✓ **Person Responsible**: The name, email address, and job title must be provided. In certain special cases, more than one person may be designated as responsible for the risk. The risk owner must be a first-line manager (reporting to the general manager of each operation), except in specific cases.
- ✓ **Macroprocesses, Processes, Subprocesses,** and, if possible, **Procedures**
- ✓ **Factor**: Risk factors are classified as: Business Risks, Crime Prevention Model, and IT Risks
- ✓ **Category:**
    - Category I): corresponds to the defined business risk pillar and also to the Criminal Liability of the Legal Entity.
    - Category II): Another grouping of *business risks* includes strategic, financial, operational, and compliance risks; and, in the case of the *Criminal Liability of the Legal Entity*, the categories of crimes will be classified.

- **Strategic** risk is defined as the current and future impact on revenue and capital that could arise from adverse business decisions, the improper implementation of decisions, or a lack of responsiveness to industry changes. This category includes risks related to strategy, political, economic, regulatory, and global market conditions; it may also include reputational risk, leadership risk, brand risk, and changing customer needs.
- **Financial** risk is the probability that an event will occur with negative financial consequences for the organization. It includes risks related to volatility in currencies, interest rates, and commodities; it may also include credit risk, liquidity risk, and market risk.
- **Operational** risk is a type of risk that can cause losses to a company due to human error, inadequate or flawed internal processes, system failures, and other factors. It includes risks related to the organization's human resources, business processes, technology, business continuity, channel effectiveness, client satisfaction, health and safety, the environment, product/service failure, efficiency, capacity, and change integration.
- Regulatory **compliance** risk is defined as non-compliance with legal provisions, regulations, standards adopted by the organization, and codes of conduct applicable to its activities, which may result in penalties and/or reputational damage, thereby causing an adverse impact on the institution's results, and/or capital, and/or business development expectations.

- ✓ **Causes and effects of risk**: Identifying the causes and effects will facilitate risk assessment and the identification of mitigation measures.

- **Causes of risk**: Causes are specific events in the environment that give rise to risks. For example, the need to expand into new markets, the use of new, untested technology, a lack of specialized personnel, etc.
- **Effects of risk:** Effects are unforeseen variations in objectives (positive or negative) that arise as a result of risks materializing. For example, achieving a goal earlier than planned, exceeding an authorized budget, failing to meet contractually agreed-upon performance targets, etc.

4.3. PHASE 3: RISK ANALYSIS:

PHASE 3: 1. Determining the inherent risk level.

Business risks can materialize through various **specific risks**, which must be evaluated accordingly.

Specific risks are assessed from two perspectives: **impact and probability.** The first reflects the consequences that the materialization of the specific risk may cause in various dimensions and in relation to business objectives. The second represents the likelihood that the identified specific risk will occur based on various defined factors.

It is important to note that the assessment conducted at this stage must consider the **inherent** impact and probability—that is, those inherent to the nature of the risk—in the absence of any action that could be taken to alter them.

In general terms, it can be concluded that a risk with a low probability of occurrence and a minor impact does not warrant further consideration; conversely, **risks with a high probability of occurrence and a significant impact** require **considerable attention**; therefore, it is important that the analyses be thorough.

a. Impact Assessment

Impact can be defined as the greatest harm that would result for the operation if the risk were to materialize. Each operation must assess the impact of the risk based on its effect on each of the following areas:

- **Economic**: Financial impact calculated as a percentage of EBITDA.
- **Business Interruption:** Impact on the continuity of production and sales processes.
- **Occupational Health and Safety**: Impact on the health or safety of employees or third parties.
- **Environment**: Actual or potential impact on the environment (air, atmosphere, water, soil, flora, and fauna).
- **Community Relations:** Actual or potential impact on the quality of life of citizens and stakeholders caused by our products or activities.
- **Reputation:** Impact on public perception of the company's actions.
- **Legal and Regulatory Non-compliance:** Impact resulting from failure to comply with contractual terms or guidelines issued by a regulatory body.

- **Criminal Liability of the Company:** Practices, actions, or situations that may result in an impact due to non-compliance with the law establishing the criminal liability of the legal entity

  Each area is rated on a scale of 1–5 with specific descriptors.

b. Probability Assessment

Each operation must assess the probability of risk occurrence using best judgment, based on the following: Probability of Occurrence, Frequency of the Process, Benefit or Gain

c. Calculation of the inherent risk level.

The risk level is calculated as: Impact * Probability

PROBABILITY	1 VERY LOW	2 LOW	3 MODERATE	4 HIGH	5 VERY HIGH
5 ALMOST CERTAIN	MODERATE 5	HIGH 10	EXTREME 15	EXTREME 20	EXTREME 25
4 LIKELY	LOW 4	MODERATE 8	HIGH 12	EXTREME 16	EXTREME 20
3 POSSIBLE	LOW 3	MODERATE 6	MODERATE 9	HIGH 12	EXTREME 15
2 UNLIKELY	LOW 2	LOW 4	MODERATE 6	MODERATE 8	HIGH 10
1 REMOTE	LOW 1	LOW 2	LOW 3	MODERATE 4	MODERATE 5

IMPACT

Given the determined risk level, the **primary focus** will undoubtedly be on those risks for which an **extreme risk** level was determined, followed by those with a **high risk** level.

Since the assessment technique to be used is primarily **qualitative**, it is recommended to carefully review the results to **ensure that the calculated risk level (impact * probability) is correct**.

PHASE 3: 2. Determining the Effectiveness of Mitigation Actions (controls)

Mitigation measures (or "controls") vary in nature; their **objective is to help reduce the probability of occurrence and/or the impact of risks** and, in this way, maintain and continue to generate value for the organization. For example, accounting control processes (inventories, cash counts, bank reconciliations, etc.) reduce the probability or likelihood of potential errors (risks) occurring in financial statements; whereas insurance policies for fire, earthquakes, etc., are mitigation measures primarily aimed at reducing the financial impact.

As noted, **mitigating actions are directly related to the nature of the risk they mitigate**; therefore, those related to mitigating errors in financial statements are of a completely different nature than those related to operational continuity risk. For this reason, it is necessary **to determine how these actions contribute to mitigating the specific risk**.

When identifying a new mitigating action or control, it must be recorded in the matrix, providing the following **information** (at a minimum):

- ✓ **Name and description of the control**: The **name should be "self-explanatory"** (e.g., "bank reconciliation"), avoiding codes and sequential numbers. The **description should be brief** but as clear as possible, **preferably using the 5W methodology**, which is based on answering five key questions in English that begin with "W." These questions are used to design, evaluate, or improve controls in risk management, audit, or compliance processes. This approach helps ensure that a control is **clear, applicable, and effective**. The questions are:
  - **What:** What is being controlled? Describe the **risk, process, or activity** that is under control.
  - **Why:** Why is it being controlled? Explain the **objective of the control**—that is, the risk it is intended to mitigate.
  - **Where:** Where is the control applied? Specify the **location, system, area, or unit** where it is implemented, citing supporting evidence.
  - **When:** When is the control performed? Define the **frequency or timing** of its execution (daily, monthly, on an as-needed basis, etc.).
  - **Who:** Who performs it? Identify the **person responsible** for applying the control (position, role, or area).
- ✓ **Intrinsic attributes or characteristics of the control:** frequency, documentation, purpose, and type of control.
  - **Documentation:** The degree of formality and support for the functional description of the control. It may be contained in a ***policy, standard, procedure, or training program***.

- **Purpose:** Indicates the objective or nature of the control, which determines whether it reduces probability or impact. It can be: ***preventive, detective, corrective, or directive.***
- **Type of Control:** Indicates the manner in which the control activity is performed. It can be: **manual, automatic, or semi-automatic**.

✓ **Person Responsible**: The name, email address, and job title must be provided.

✓ **Evidence of control**: You must detail what supporting documentation exists and its location (ideally, the file name and where it is stored).

The contribution of each mitigating action will be calculated based on its attributes: Purpose of the Control, Type of Control, and Control Documentation; these values each have an individual contribution percentage.

The total **mitigation contribution** is calculated as the **weighted sum** of the various attributes.

The **frequency of** control **execution** is not used in the calculation, as its mitigating effectiveness depends largely on the risk with which it is associated.

PHASE 3: 3. Determining Residual Risk

Risk exposure, or **residual risk,** is the risk that remains after operations have implemented their mitigation actions. **It is determined by taking into account the risk level and the level of contribution (effectiveness) of the mitigation actions**, as follows:

Residual Risk = Residual Impact * Residual Probability

*Residual Impact = Inherent Impact * % Contribution of the Control*

*Residual Probability = Inherent Probability * % Contribution of the Control*

To establish the level of residual risk, we must follow these steps:

- 1. Calculate the **% contribution** resulting from the control attributes (purpose, type of control, and documentation).
- 2. Determine whether it applies to **probability or impact**, considering:
  a. If the control is **preventive, detective, or directive**: it will be applied to **probability.**
  b. If the control is **corrective**: it applies to the **impact**.
- 3. Calculate the residual risk, considering the following cases:
  - **Risk with only one control**:
    - **If the controls mitigate the probability:**

      Residual Risk = Inherent Impact * Residual Probability

      *Residual Probability = Inherent Probability * (100% * % Contribution of the Control)*
    - **If controls mitigate the impact:**

- Residual Risk = Residual Impact * Inherent Probability
  *Residual Impact = Inherent Impact * (100% * % Contribution of the Control)*

- **Risk with 2 or more controls, all of which address either probability or impact:** Take 70% of the highest % contribution and 30% of the average of the remaining % contributions of the controls, applying this to the inherent probability or impact, as appropriate. In summary:
  - **If the controls mitigate the probability:**
    - Residual Risk = Inherent Impact * Residual Probability
      *Residual Probability = Inherent Probability * (70% * highest contribution percentage) * (30% * average of the contribution percentages of the remaining controls).*
  - **If the controls mitigate the impact:**
    - Residual Risk = Residual Impact * Inherent Probability
      *Residual Impact = Inherent Impact * (70% * highest contribution percentage) * (30% * average contribution percentage of the remaining controls).*
- **Risk with 2 or more controls, one targeting probability and the other targeting impact:** the following should be applied:
  - **2 controls**, one mitigating probability and the other mitigating impact:
    Residual Risk = Residual Impact * Residual Probability
    *Residual Probability = Inherent Probability * (100% * control contribution percentage)*
    *Residual Impact = Inherent Impact * (100% * control contribution percentage)*
  - **4** or more controls
    Residual Risk = Residual Impact * Residual Probability
    *Residual Probability = Inherent Probability * (70% * highest contribution percentage) * (30% * average contribution percentage of the remaining controls).*
    *Residual Impact = Inherent Impact * (70% * highest contribution percentage) * (30% * average contribution percentage of the remaining controls).*

4.4. PHASE 4: RISK ASSESSMENT:

This step involves comparing the results obtained from the risk analysis with the previously defined criteria to determine whether additional measures are necessary and how urgent they are. To do this, the following must be considered:

EXTREME	Action is required in the short term (12 months)
HIGH	Action is required in the medium term (between 1 and 2 years)
MODERATE	Action is required in the medium term (between 1 and 2 years)
LOW	No additional actions are required. Monitor the effectiveness and efficiency of existing measures

Consequently, Operations must implement mitigation measures in the short or medium term, as indicated in the table above.

Based on this comparison, different courses of action may be chosen, such as:

- Take no action and accept the risk;
- Evaluate possible risk management strategies;
- Conducting a more in-depth analysis to gain a better understanding of the risk;
- Maintaining existing controls if they are deemed adequate; or
- Reviewing established objectives in light of the identified risk.

When making these decisions, both the organizational environment and the perceived and actual implications for internal and external stakeholders must be considered.

Finally, the results of this assessment must be documented, properly communicated, and validated with the appropriate levels within the organization.

4.5. PHASE 5: RISK TREATMENT.

In cases where a need is identified to implement mitigation actions that did not previously exist (or to improve existing ones), action plans must be implemented to address the existing gap or weakness. These action plans must be properly documented so that they can easily identify their purpose, implementation date, required resources (if applicable), monitoring of the plan's implementation, and monitoring of its effectiveness in relation to the purpose for which it was created. Additionally, they must meet the following requirements:

- Be formal and provide an appropriate level of detail, written in language that ensures they are understood by everyone
- Clearly identify the responsible parties and deadlines for each specific task
- Be known to the relevant individuals
- If applicable, ensure that staff is trained—that is, both staff and management know exactly what to do and have participated in specially designed tests
- Where applicable, they must be tested, and adjustments must be made based on the results of those tests
- Be reviewed periodically
- Progress reports shall be submitted to the Corporate Sustainability and Risk Committee if requested by the Committee. This presentation may be made by the Manager of Management Control, Sustainability, and Risk; the Operations Administration and Finance Manager; or the Local Risk Manager, as determined at the time.

If the actual risk exposure or residual risk falls within the acceptable level, Operations must ensure that the mitigating actions—which allow that level of exposure to be maintained—are sustained over time. This implies having adequate personnel, a formal assignment of roles and responsibilities, properly designed and documented processes, training, appropriate controls, and ongoing monitoring, among other measures.

By way of illustration, and in accordance with the relevant literature, the treatment of residual risk generally focuses on any of the following options:

a. ***Avoid the risk***: Cease activities that generate risks, when feasible and provided it does not affect legal requirements or operational efficiency. Example: discontinuing a product or process through an administrative decision.

b. ***Modifying the probability or consequences of the risk***: This is achieved by optimizing procedures and implementing controls or mitigating actions aimed at reducing the frequency of occurrence (e.g., training, supervision, succession planning, etc.) and/or minimizing the impact (e.g., purchasing partial insurance).

c. ***Sharing the risk***: Activities and measures aimed at sharing with a third party the responsibility for managing the risk and/or the obligation for the financial consequences of the risk, should it occur. Example: insurance policies.

d. ***Accepting the risk***: Accepting the risk because the potential returns are attractive relative to the risks involved. Example: Developing contingency plans to manage the risk, having sufficient capital available to address the risk if it materializes, etc.

e. ***Eliminate the source of risk***: Directly remove the cause of the risk. Example: Removing a defective machine that could cause injuries.

When selecting a strategy to address risks, it is necessary to evaluate its potential costs and benefits. After selecting the strategies, the responsible parties, deadlines, performance indicators, measurement period, etc., must be defined.

4.6. PHASE 6: MONITORING AND REVIEW

The actions undertaken in risk management must be incorporated into processes, factored into strategies, budgets, and projects, and monitored on an ongoing basis to ensure their continuity, effectiveness, and continuous improvement.

Ongoing and timely monitoring promotes proper risk management and ensures the continuity and quality of mitigation actions; otherwise, these actions may gradually lose their effectiveness.

To carry out this work, each Operation has a Local Risk Manager, whose primary function is to coordinate the process (see a detailed description of their tasks in the Corporate Risk Management Policy, section “Structure and Responsibilities in Risk Management”).

In addition, there are coordination bodies at the Coca-Cola Andina Group level, such as the Risk Administrators Committee, which meets periodically. This body conducts *Benchmarking* and identifies synergies, which includes standardizing risk identification criteria and mitigation plans by transferring best practices from one operation to another; implementing improvements in severity assessment methodologies; sharing lessons learned from risk materialization and using them to redefine mitigation plans; and, finally, identifying new aspects of the process to be developed, conducting refresher training, etc.

To facilitate data collection, continuous monitoring, and reporting to the Corporate Office and the Board of Directors, the company utilizes a technological tool that enables better management of information and facilitates access for risk managers, providing visibility and accurate reporting, that is, providing a set of reports tailored to the needs of different users (Board of Directors, Local Risk Managers, Risk Officers, etc.).

At the corporate governance level, the Corporate Sustainability and Risk Committee, Corporate Internal Audit, Corporate Compliance and Ethics Management/Governance, Compliance, and Integrity Committee, and the Board of Directors participate in monitoring the process.

4.7. CROSS-FUNCTIONAL COMMUNICATION AND CONSULTATION

Communication and consultation are cross-functional processes across all the phases outlined above that seek to ensure that internal and external stakeholders are engaged, informed, and have an adequate understanding of the risks facing the organization.

The objectives of this stage are:

- Promote a common understanding of risk and its implications.
- Facilitate the accurate identification of risks through shared knowledge.
- Support decision-making based on clear and relevant information.
- Foster trust and collaboration among departments, teams, authorities, and other stakeholders.

It must be carried out continuously throughout all stages of the risk management process and adapted to the context and level of participation of each stakeholder.

4.8. RECORD-KEEPING AND DOCUMENTATION

This record-keeping process aims to document the entire risk management process in a structured and consistent manner, ensuring that key information is available for decision-making, audits, continuous improvement, and accountability.

This process must be adapted to the organizational context and ensure that the recorded information is relevant, accurate, up-to-date, and accessible.

5. Conclusion

Operations must reasonably ensure that the business risks identified within them are mitigated. To this end, they must establish sufficient and effective processes, procedures, and monitoring controls that allow for testing the effectiveness of mitigation actions.

6. Track changes

Version	Description of the main changes (For further information, please contact politicascorporativas@koandina.com)	Approval	Effective Date
1.0	Initial version	Andrés Wainer	May 2016
2.0	Major changes in this version: Section 1. Introduction: The introduction has been updated to highlight the benefits of risk management. Section 3. Considerations: The concept of “risk pillars” is introduced. Section 4.1. Phase 1: Risk Identification: The sources of risk identification and the considerations to be made when identifying and recording new risks are established. Section 4.2. Phase 2: Risk Severity Assessment: Clarification is provided regarding inherent probability and impact, as well as risks not applicable to an Operation. Section 4.3. Phase 3: Analysis of the Effectiveness of Mitigation Actions: Describes the information to be recorded when identifying a new mitigation action or control. Section 4.4. Phase 4: Determination of Risk Exposure (Residual Risk): The formula for calculating residual risk is modified. Section 4.5. Phase 5: Analysis of Effective Exposure and Actions to Be Taken: Guidelines are established for defining and documenting action plans.	Andrés Wainer	June 2021

Version	Description of the main changes (For further information, please contact politicascorporativas@koandina.com)	Approval	Effective Date
	Section 4.6. Phase 6: Monitoring and Continuous Improvement: Describes the structure, coordination bodies, and tools implemented to ensure the monitoring and continuous improvement of the risk management process. Examples related to IT Continuity have been removed.		
3.0	Updates regarding risk appetite, impact and probability scales, the effectiveness of mitigation measures, and the calculation of residual risk. Category change: from “Appendix to the Risk Management Policy” to “Procedure” Additionally, methodological changes have been made to the criteria for assessing inherent risk and residual risk.	Andrés Wainer	October 2025