RISK MANAGEMENT CORPORATE POLICY

ANNEX – Risk Management Methodology

Version	Description of Changes	Approval	Effective Date
1.0	Initial Version	Andrés Wainer	May 2016
2.0	See section 6. Tracking Changes	Andrés Wainer	June 2021

This document contains proprietary information of the Coca-Cola Andina Group, which has been strictly prepared for the purpose of being used in the Company's operations and may not be partially or wholly provided, rephrased, or disclosed to third parties without the express authorization of the Corporate Management Area responsible for this document.

TABLE OF CONTENTS

1. Introduction

Every business face risk: the issue is to determine how much uncertainty can be handled. Corporate risk management enables management to deal with uncertainty effectively, improving the ability to maintain and generate value.

To maintain and increase the value of the company over time, management must establish strategies and objectives for growth and profitability while maintaining an optimal balance with the associated business risks.

In this context, it is the responsibility of each Operation and Corporate to ensure that the relevant business risks are identified and mitigated to the point where, if they materialize, their impact is manageable, ensuring the business's continuity.

The benefits of risk management are as follows:

- ✓ Enhances the likelihood of achieving the company's goals.
- ✓ Identifies and shares accountability.
- ✓ Focus is generated and strengthened on critical issues.
- ✓ Contributes to reduction of surprises and crises in the organization.
- ✓ Generates information and transparency of identified risks and decisions made.
- ✓ Enhances internal control.

The methodology outlined below facilitates a more structured risk management, with uniform evaluation criteria and standard reporting to the Board of Directors.

2. Objective

This methodology provides the necessary guidelines for an effective management of business risks that may jeopardize the achievement of the Company's goals.

3. Considerations

a. Business risk is defined as "the possibility that an event or action, whether internal or external, will have a negative impact on an organization's ability to successfully execute its strategies and achieve its objectives" (definition obtained from the book "Integral Business Risk Management" published by Deloitte). Business risks are referred to as "Risk Pillars" at Coca-Cola Andina.

b. Specific risk: An incident or event generated by internal or external sources that causes the business risk to materialize. For example, the following specific risks were identified for the business risk "industrial continuity": strikes, interruption in raw material supply, power outage, and availability of returnable containers, among others.

c. Techniques for risk evaluation: The risk evaluation methodology combines qualitative and quantitative techniques. In general, qualitative techniques should be used when risks cannot be quantified, there is insufficient and credible data for quantitative assessment, or obtaining and analyzing them is not cost-effective. Quantitative techniques typically provide greater precision and are used to supplement qualitative

techniques in more complex and sophisticated activities that require a greater degree of effort and rigor, sometimes using mathematical models. In general, and given the nature of the risks involved, qualitative techniques should almost certainly be used.

4. Risk Management Process

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

Phase 1: Identification and classification of risks.

Phase 2: Determination of the severity of the risk.

Phase 3: Analysis of the effectiveness of mitigating actions.

Phase 4: Determination of risk exposure.

Phase 5: Analysis of effective exposure and actions to be taken.

Phase 6: Monitoring and continuous improvement.

4.1. Phase 1: Identification and classification of risks

According to the methodology, the first step is to identify business risks, followed by the identification of their specific risks, as indicated in points 2.a and 2.b of this document.

Within the sources of risk identification, we can identify the following:

- ✓ Definitions of the Board of Directors or the Corporate Sustainability and Risk Committee: Both the Coca-Cola Andina Board of Directors and the Corporate Sustainability and Risk Committee have the responsibility to identify the business risks (risk pillars) that will be incorporated into the Risk Management process, regardless of whether the respective areas have previously managed them in the development of their normal processes.
- ✓ Emergencies or crisis situations: As stated in the section "Operational Responsibilities" of the Corporate Policy for Emergency Management, following an emergency, the local risk team, in collaboration with members of the EME, must conduct an analysis of the situation and review the adequacy of the business risk matrices considering the event that occurred. Examples include the 2019 Chilean social outbreak and the COVID-19 pandemic.
- ✓ Analysis of the Strategic Plan: To achieve its mission, the Company has developed a strategy based on the integration of business growth and sustainability pillars that are aligned with its vision and organizational values. Each of these pillars (or "strategic pillars") is susceptible to a variety of factors and events that may have an impact on its development and fulfillment and must therefore be identified and managed.
- ✓ Analysis of the critical processes of the business: Critical processes are those that are essential for the business, so that a suspension of them generates a high impact and/or a crisis within the company. Given the above, the factors that may trigger a suspension of these processes must be identified and managed.

To facilitate the administration of the risk matrix and the comparability of information, the following considerations should be taken into account when identifying new risks:

a. It should always be confirmed that it is a new risk and not a redefinition or cause of an existing risk in the matrix.
b. Uniformity in the definition of risks:
   - ✓ A risk must be described in the same way in all operations, so any new risk or modification of an existing one must be analyzed and agreed upon by the Risk Management Committee, which meets every two weeks (for more details, see Phase 6: monitoring and continuous improvement).
   - ✓ In the event that a risk is not applicable to a transaction (i.e., the factors that may materialize the risk are not present and therefore it has a probability of occurrence equal to 0), it should be recorded in the matrix indicating that it is "not applicable" and explaining the reasons for this.

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

- ✓ Name and description of the risk: the name should be "self-explanatory" (e.g., "Shutdown of a critical contractor") avoiding correlative codes and numbers. The description should be brief, but as clear as possible,
- ✓ Person in charge: the name, e-mail and position must be indicated. In certain special cases, more than one person responsible for the risk may be indicated.
- ✓ Process and associated sub-process: according to Coca Cola Andina's standard definition of processes.
- ✓ Category: Business risks are classified as strategic, financial, operational, and compliance:
  - Strategic risk is defined as the current and future impact on earnings and capital that could result from poor business decisions, poor decision implementation, or a failure to respond to industry changes. This category includes risks associated with strategy, politics, economics, regulation, and global market conditions; it may also include reputational risk, leadership risk, brand risk, and changing customer needs.
  - Financial risk is the likelihood of an event occurring with negative financial consequences for the organization. It includes currency, interest rate, and commodity volatility risks, as well as credit, liquidity, and market risk.
  - Operational risk is a type of risk that can cause a company to lose money due to human error, insufficient or faulty internal processes, system failure, and other factors. It includes risks related to human resources, business processes, technology, business continuity, channel effectiveness, customer satisfaction, health and safety, the environment, product/service failure, efficiency, capacity, and change integration for the organization.
  - 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 sanctions and/or reputational damage, causing an adverse impact on the results, capital, and/or expectations for the development of the institution's business.

- ✓ Subcategory: the subcategory pertains to the pillar of risk.
- ✓ Causes and effects of risk: the identification of causes and effects will facilitate risk assessment and the identification of mitigation actions.
  - Causes of risk: Causes are specific events in the environment that give rise to risks. For example, the need to grow in new markets, use new unproven technology, lack of specialized personnel, etc.
  - Risk effects are unanticipated changes in objectives (positive or negative) that occur because of risk materialization. For example, exceeding an authorized budget, failing to meet contractually agreed-upon performance targets, and so on.

4.2. Phase 2: Determination of the severity of the risk

Business risks can materialize through different specific risks, which must be assessed accordingly.

Specific risks are assessed from two perspectives: impact and probability (frequency). The former reflects the consequences of the specific risk's materialization in relation to the business objectives. The second represents the possibility of occurrence of the specific risk identified.

It should be noted that the assessment at this stage should 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 change them.

In general, it can be concluded that a risk with a low probability of occurrence and little impact does not merit further consideration, whereas risks with a high probability of occurrence and significant impact require careful consideration; thus, careful analyses are required.

a. Impact Assessment

The impact is defined as the damage that would be done to the operation if the risk occurred. A catastrophic category impact could include the complete cessation of the Operation's activity, sanctions for closing the company, and damage to the Operation's and its executives' reputations, among other things.

The corresponding impact assessment must be completed in accordance with the table below:

Impact Guidelines		
Category	Value	Impacts of Risk Materialization
Catastrophic	**5**	Operation-wide impact
High	**4**	Significant impact for the entity, but it is feasible to manage and thus continue to operate
Moderate	**3**	No significant or long-term impact for the entity
Low	**1**	Unimportant

Note: value 2 is omitted to facilitate further analysis.

As a result, each Operation must assess the impact of a specific risk based on its impact on the business risk with which it is associated. To do so, it must define the criteria (considering the nature of the risks) in accordance with the guidelines outlined in the table above.

For example, in the case of the business risks "people safety," "environment," and "business continuity," applying the guidelines in the table above yields the following reference framework when assessing the specific risks:

Impact Guidelines			Suggested criteria for the indicated business risks		
Category	Value	Impact of the materialization of the specific risk	Personal Safety	Environment	Industrial Continuity
Catastrophic	**5**	Operation-wide impact	Sanctions with suspension of principal operations, fines, or lawsuits.	Long-term environmental impact, suspension of operations due to noncompliance with standards and/or regulations.	The inability to continue normal operations at the Operation level
High	**4**	Significant impact for the entity, but it is feasible to manage and thus continue to operate	Sanctions with suspension of NON-major operations, high fines or lawsuits.	Serious environmental impact in the medium term, major regulatory violations	Significant interruptions in operations within one or more business units.
Moderate	**3**	No significant or lasting effect on the entity	Fines or Claims	Moderate impact on the environment, fines for violation of rules and/or regulations	Moderate disruptions within one or more business units
Low	**1**	Unimportant	Fines or Claims	Minor environmental impact, reporting for regulatory bodies	Outages reduced to one business unit

Example:

In the case of the business risk "business continuity," the Guidelines identify strike as a specific risk; therefore, the impact of this specific risk should be classified using the criteria provided. In this case, a general strike lasting several weeks, for example, should be classified as level 5 (catastrophic), because, according to the table above, a general strike makes it impossible to continue normal operations.

b. Probability Assessment

Each specific risk identified must have an associated probability, for which the following criterion is established:

Probability Matrix		
Category	Value	Description
High	**5**	Based on historical precedent and analysis of recent and upcoming events, there is a high degree of certainty that it will occur within the next three years.
Moderate	**4**	Based on historical background, analysis of recent and future events, there is a sufficient degree of certainty that it will occur in the next 3 years.
Low	**3**	The possibility of occurrence is low
Very Low	**2**	The possibility of occurrence is less than low

It should be noted that, as indicated in point 2.c, the qualification of the impact and probability of a specific risk will be based primarily on experience and professional judgment, i.e., qualitative assessment techniques. For example, it is common sense that, given the planet's global warming, the likelihood of a water cut is increasing; however, each Operation must evaluate its occurrence considering the internal and external factors that influence it. Thus, given the current level of drought in Santiago, the probability of water cut may be in category 5 (high), whereas in another Operation it may be in category 2 (very low).

If a risk is not applicable to a transaction (i.e., the factors that may materialize the risk are not present, and thus it has a probability of occurrence equal to 0), it should be recorded in the matrix as "not applicable" and explained why.

The preceding exercise should be performed for each specific risk.

c. Severity Calculation

The severity of the risk corresponds to the inherent risk. Inherent risk is the risk that an operation faces in the absence of mitigating actions to reduce its probability of the occurrence.

Severity is the result of: Impact * Probability

The levels of severity are the following:

Severity Matrix					
Impact		Probability		Level of Severity	
Category	Value	Category	Value	Value	Category
Catastrophic	5	High	5	25.0	**High**
Catastrophic	5	Moderate	4	20.0	**High**
High	4	High	5	20.0	**High**
High	4	Moderate	4	16.0	**High**
Catastrophic	5	Low	3	15.0	**Moderate**
Moderate	3	High	5	15.0	**Moderate**
High	4	Low	3	12.0	**Moderate**
Moderate	3	Moderate	4	12.0	**Moderate**
Catastrophic	5	Very Low	2	10.0	**Moderate**
Moderate	3	Low	3	9.0	**Moderate**
High	4	Very Low	2	8.0	**Moderate**
Moderate	3	Very Low	2	6.0	**Low**
Low	1	High	5	5.0	**Low**
Low	1	Moderate	4	4.0	**Low**
Low	1	Low	3	3.0	**Low**
Low	1	Very Low	2	2.0	**Low**

Given the severity of the risks identified, the primary focus will undoubtedly be on those with a high severity, followed by those with a moderate severity.

Because the assessment technique is essentially qualitative (see point 2.c), it is recommended that the results be carefully reviewed to ensure that the calculated severity (impact*probability) is correct. For example, the probability of occurrence of the "business continuity" risk and its specific risk of power outages could be considered very low, but this is more than prudent to arbitrarily define it as high. The risk of a power outage can occur at any time.

4.3. Phase 3: Analysis of the effectiveness of mitigating actions

The purpose of mitigating actions (or "controls") is to contribute to reducing the probability of occurrence and/or impact of risks and, as a result, to maintain and continue generating value for the company. For example, accounting control processes (inventories, audits, bank reconciliation, etc.) reduce the probability or likelihood of occurrence of potential errors (risks) in the financial statements, whereas insurance against fire, earthquakes, etc., are mitigating actions aimed primarily at reducing the financial impact.

As indicated, mitigating actions are directly related to the nature of the risk they mitigate; therefore, those related to mitigating errors in the financial statements are of a totally different nature from those related to IT continuity risk. Determining how the actions assist to minimizing the specific risk is therefore required. Again, judgment and experience are required for this assessment.

When a new mitigating action or control is identified, it should be recorded in the matrix detailing the following information (at a minimum):

Name and description of the control: the name should be "self-explanatory" (example: "bank reconciliation"), avoiding correlative codes and numbers. The description should be brief, but as clear as possible.

Responsible party: name, e-mail address, and position must be given.

Evidence of the control: detail what supporting documentation exists, location and the policies/standards/procedures where the controls are formalized, if any.

The contribution of the set of mitigating actions for a specific risk should be classified according to the table below:

Mitigation action contribution percentage		
Category	Percentage	General description
Optimal	**95%**	The action reasonably mitigates the risk, however, it presents weaknesses in a way that could affect its continuity and quality, for example, in case of a change in the organizational structure.
Good	**85%**	The action reasonably mitigates the risk, however, it presents weaknesses in a way that could affect its continuity and quality, for example, in case of a change in the organizational structure.
Moderate	**50%**	The action does NOT reasonably mitigate the risk; however, it presents certain positive elements regarding its design and operation.
Deficient	**0%**	To mitigate the risk in a reasonable manner, there is either no mitigating action or the present one must be redesigned from its inception.

4.4. Phase 4: Determining risk exposure (residual risk)

The risk exposure or residual risk is that which remains after the Operations have implemented their mitigating actions. It is determined by taking into account the severity and the level of contribution (effectiveness) of the mitigating actions, i.e.:

*Effective exposure level = Severity *(1- contribution % of mitigating actions).*

In this formula, the highest contribution % of the set of actions that mitigate the risk must be considered.

From the above, the following graph is obtained:

Exposición efectiva al riesgo					
	Contribución:	*Óptima 95%*	*Buena 85%*	*Media 50%*	*Deficiente 0%*
	Exposición:	Exposición (1-95%)	Exposición (1-85%)	Exposición (1-50%)	Exposición 100%
Severidad Alto	*25*	1,25	3,75	12,50	25,00
	20	1,00	3,00	10,00	20,00
25*(1-95%)	*16*	0,80	2,40	8,00	16,00
Severidad Medio	*15*	0,75	2,25	7,50	15,00
	12	0,60	1,80	6,00	12,00
	10	0,50	1,50	5,00	10,00
	9	0,45	1,35	4,50	9,00
	8	0,40	1,20	4,00	8,00
Severidad Bajo	*6*	0,30	0,90	3,00	6,00
	5	0,25	0,75	2,50	5,00
	4	0,20	0,60	2,00	4,00
	3	0,15	0,45	1,50	3,00
	2	0,10	0,30	1,00	2,00
	1	0,05	0,15	0,50	1,00

For example, for a risk whose severity is 25 and which has mitigating actions whose contribution is optimal (equal to 95%), its effective exposure will be 1.25 points, i.e., 25*(1-95%) which is the same as 25*5%. Similarly, for the same risk, but with mitigating actions whose contribution is moderate (equal to 50%), its effective exposure will be 12.5 points.

4.5 Phase 5: Analysis of actual exposure and actions to be taken

Once the previous phases have been completed, it is necessary to determine the actions to be taken and their degree of urgency, depending on the severity of each risk and its exposure. To this end, the following should be considered:

Risk tolerance level		
Severity	Effective exposure	Mitigating actions required
HIGH	0 - 3.75	**Acceptable**: No additional actions are required; however, **the effectiveness and efficiency of existing actions should be monitored to ensure that they are maintained.**
	Greater than 3.75	**Not acceptable:** Actions are required in the short term.
MODERATE	0 - 2.25	**Acceptable:** no additional actions are required; however, **the effectiveness and efficiency of existing actions should be monitored to ensure that they are maintained.**
	4 - 7.5	**Acceptable, with reservations:** Medium-term actions are required.
	8 – 15	**Not acceptable:** Short-term actions are required.
LOW	Given that the impact of this risk is mainly low, no actions are required in the short or medium term, leaving the decision to incorporate improvements to Operations. However, it is necessary to monitor that the severity of the risk remains low.	

Consequently, Operations should generate mitigating actions in the short or medium term as shown in the table above.

In cases where the need to implement mitigating actions that did not exist (or improve existing ones) is identified, action plans must be implemented to remedy the existing gap or weakness. These action plans must be adequately recorded, so that at least their purpose, date of implementation, resources required (if applicable), monitoring of the implementation of the plan and monitoring of its effectiveness with respect to its original purpose can be identified. In addition, they must comply with the following:

- Be formal and with an adequate level of detail, written in a language that gives assurance of being understood by all.
- Clearly identify those responsible and deadlines for each specific task.
- Be known to the relevant persons
- Where applicable, that staff are trained, i.e., both staff and management know precisely what to do and have participated in specially designed tests
- Where applicable, be tested and adjustments made according to the tests performed
- Be reviewed periodically
- Progress reports are provided to the Corporate Sustainability and Risk Committee, if required. This presentation may be made by the Management Control, Sustainability and Risk Manager, by the Operation's Administration and Finance Manager or by the Local Risk Manager, as defined at the time.

In the event that the effective exposure to the risk or residual risk is within the acceptable level, the Operations must ensure that the mitigating actions, which allow maintaining that level of exposure, are maintained over time, this implies the existence of adequate personnel, formal assignment of roles and responsibilities, properly designed and documented processes, training, timely controls and permanent monitoring, among others.

By way of illustration, and according to the literature on the subject, the treatment of residual risk is generally oriented, in general, to any of the following options:

a. **Avoid / Eliminate the risk**: Exit the activities that generate the risks when this is feasible and does not affect legal requirements or operational efficiency. Example: suspend a product or process by an administrative decision.
b. **Mitigate the risk**: This is achieved by optimizing procedures and implementing controls or mitigating actions to reduce the frequency of occurrence (e.g., training, supervision, succession, etc.) and/or minimize the severity of its impact (e.g., taking out partial insurance).
c. **Disperse or atomize the risk**: This is achieved by distributing or localizing the risk in different places, processes or people. Example: Information of great importance can be duplicated and stored in a distant and secure location, instead of leaving it concentrated in a single place.
d. **Risk transfer**: Activities and measures aimed at transferring to a third party the responsibility for risk management and/or the liability for the financial consequences of the risk, should it occur. This technique does not reduce the frequency or impact but involves another party in the responsibility. Example: insurance policies.
e. **Accept the risk:** Acceptance of the risk because the potential returns are attractive in relation to the risks involved. Example: Drawing up contingency plans for its management, having sufficient capital to face the materialization of the risk, etc.

In the selection of the strategy to deal with the risks, it is necessary to evaluate the potential costs and benefits. After selecting the strategies, the responsible parties, deadlines, achievement indicators, measurement period, etc. must be defined.

4.6 Phase 6: Monitoring and continuous improvement

The actions undertaken in risk management must be incorporated into the processes, considered in the strategies, budgets and projects, and permanently monitored to ensure their continuity, effectiveness and constant improvement.

Permanent and timely monitoring favors the adequate management of risks and the continuity and quality of mitigating actions, otherwise they may lose their effectiveness.

To carry out this task, each Operation has a Local Risk Manager, whose main function is to coordinate the process (see details of his/her tasks in the Corporate Risk Management Policy, section "Risk Management Structure and Responsibilities").

Additionally, there are coordination instances at the Coca-Cola Andina Group level, such as the Risk Managers Board, which meets periodically. In this instance, Benchmarking and identification of synergies are carried out, which includes standardizing risk identification criteria and mitigation plans, taking the best practices from one operation to another; implementing improvements in severity assessment methodologies, sharing lessons learned from risk materialization and redefining mitigation plans based on this and, finally, identifying new aspects to be developed in the process, conducting update training, etc.

To facilitate the survey, continuous monitoring and reporting to Corporate and Board of Directors, we have the support of a technological tool that allows us to better manage the information and facilitate access to risk managers, providing visibility and assertive reporting, i.e., having a set of reports tailored to the needs of different users (Board of Directors, Local Risk Managers, Risk Managers, etc.).

At the Corporate Governance level, the Corporate Sustainability and Risk Committee, Corporate Internal Audit and the Board of Directors participate in monitoring the process.

5. Conclusion

Operations must reasonably ensure that the business risks identified in them are mitigated. To this end, they shall establish sufficient and competent monitoring processes, procedures and controls to test the effectiveness of the mitigating actions.

6. Tracking Changes

Version	Description of Main Changes (for more information, please write to politicascorporativas@koandina.com	Approval	Effective Date
1.0	Initial version	Andrés Wainer	May 2016
2.0	Main changes in this version: Section 1. Introduction: the introduction is updated, and the benefits of risk management are highlighted. Section 3. Considerations: the concept of "risk pillars" is introduced. Section 4.1. Phase 1 Risk identification: establishes the sources of risk identification and the considerations to be made when identifying and registering new risks. Section 4.2. Phase 2 Determination of risk severity: a clarification is made about the probability and impact inherent and the risks not applicable to an Operation. Section 4.3. Phase 3 Analysis of the effectiveness of mitigating actions: details the information to be recorded when identifying a new mitigating 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 the definition and recording of action plans. Section 4.6. Phase 6 Monitoring and continuous improvement: The structure, coordination instances and tools implemented to ensure the monitoring and continuous improvement of the Risk Management process are detailed. The examples related to IT Continuity are eliminated.	Andrés Wainer	June 2021