

Policy of Administration and Management of Risks





PURPOSE

This policy defines the framework for risk administration and management at Team Foods Colombia S.A. and all companies within the business group led and controlled by the parent company (hereinafter “Alianza Team®” or the “Organization”). It outlines the principles, guidelines, roles, responsibilities, structure, communication, training, objectives, strategies, and procedures that make up the Integrated Risk Management System, as defined in Section Four of this Policy. The objective is to guide actions that strengthen prevention, mitigation, and risk assurance, while also enabling the capture of opportunities, to effectively and efficiently achieve the Organization’s strategic objectives and ensure its growth in the short, medium, and long term.





SCOPE

This policy applies to all companies within Alianza Team®, including managers, employees, contractors, suppliers, and other stakeholders. Alianza Team® may also extend this policy to other activities across its value chain where risk management practices are required.



ASSOCIATED RISKS

Inadequate risk administration and management can disrupt organizational processes, leading to short-, medium-, and long-term impacts and deviations from established objectives. To mitigate this, the following categories of risks are addressed:



Strategics



Emerging



Operational



Financial



Compliance



DEFINITIONS

The following are the key terms used within the Organization's Risk Management framework:

Risk Appetite: The level of risk the Organization is willing to tolerate.


Cause: Factors or circumstances that give rise to risks.

Consequence: The outcome of an event that impacts objectives.

Control / Control Activity: Measures implemented to manage or modify a risk.

Event: The occurrence or change of specific circumstances.

Risk Factor: Internal or external sources that may create risk and potentially lead to losses.



Impact: The effect that occurs if a risk materializes.

Risk Management Leaders: Individuals appointed by the Executive Committee to analyze, evaluate, and execute actions for managing risks, as well as any additional risk-related activities.

Risk Maps: Tools used to systematically identify and classify risks by defined levels.

Risk Materialization / Loss Event: Incidents arising from one or more risks that may or may not cause loss.

Risk Treatment Measures: Avoid, reduce, transfer, retain, or accept risk.

Risk Level: The rating assigned to a risk according to a defined scale (Extreme, High, Moderate, Low).

Opportunity: Benefits or possibilities that arise from the occurrence of a specific event.

Action Plan: A defined measure to mitigate one or more risks by reducing impact, lowering the probability of occurrence, or strengthening controls.

Crisis Management Plan: A detailed set of activities designed to resolve unexpected events that may affect the Organization's image or reputation.

Business Continuity Plan: Procedures, resources, systems, and roles designed to resume and sustain operations in the event of disruption.

Probability: The likelihood of an event occurring.

Risk: The possibility of an event materializing and negatively affecting the Organization.

Inherent Risk: The level of risk assessed without considering existing controls.

Residual Risk: The level of risk assessed after controls are applied.

Priority Risks: Risks with a residual level rated as Extreme or High, requiring urgent action plans for mitigation.

Comprehensive Risk Management System: A dynamic, multi-stage process that provides a holistic view of risks and their impact, supporting decision-making and enhancing organizational value in the short, medium, and long term.

GUIDELINES



GENERAL CONDITIONS

This document has been developed in alignment with leading international standards in risk management: ISO 31000:2018, COSO ERM:2017, and the Australian Standard AS/NZ 4360:2004. These frameworks provide key guidelines for effective risk administration and management.

By applying the Integrated Risk Management System, Alianza Team® will be able to:

- Manage risks that could impact business continuity,
- Increase the likelihood of achieving objectives,
- Support the effective execution of plans, programs, and projects aligned with strategic goals,
- Provide a reliable foundation for decision-making and planning,
- Minimize potential losses,
- Strengthen internal controls,
- Build trust and transparency among stakeholders,
- Enhance operational effectiveness and efficiency,
- Optimize the allocation of resources for risk management,
- Safeguard the Organization's assets,
- Equip the Organization with tools to respond to unexpected events, and
- Improve decision-making to maximize opportunities.



1. Policy Statement

In line with internal control standards and best practices in risk management, Alianza Team® is committed to maintaining efficiency, effectiveness, and operational capacity, while safeguarding the resources under its administration. To achieve this, the Organization must implement a Integrated Risk Management System designed to minimize costs and potential damages, establish methods for risk treatment and monitoring, and prevent or avoid the occurrence of events that could disrupt processes or hinder the achievement of objectives. Where prevention is not reasonably possible, the system must ensure appropriate measures to mitigate the impact.

2. Risk Governance

The Integrated Risk Management System assigns specific responsibilities to the following areas:

Board of Directors / Audit Committee

Oversees key risk issues relevant to the Organization to support informed decision-making and monitors the ongoing management of significant business risks.



President/CEO

Approves policies and guidelines related to the Integrated Risk Management System and monitors the ongoing management of major business risks.

Vice President of Corporate Affairs

Approves procedures related to the Risk Management System and tracks the periodic evolution of relevant business risks.

Corporate Risk Management Office

Acting as the second line of defense, it coordinates activities for risk identification, measurement, control, monitoring, consolidation, and reporting, while supporting Administration (the first line of defense). It is responsible for designing and updating policies and procedures, and for promoting effective compliance and system performance.

Risk Management Leaders

Accountable for monitoring the effectiveness of the Risk Management System, managing risks specific to their processes or areas (risk maps), and addressing new risks that emerge due to the dynamic nature of the business.

Risk Management Committee

Composed of Risk Management Leaders and the Corporate Risk Management Office, this body monitors risk levels, mitigation plans, treatment of materialized risks, and other activities that support the Risk Management System.

3. General Policy Guidelines

Alianza Team® has defined the following guidelines to strengthen its Risk Management framework:

- Compliance with this policy is mandatory and fundamental to its effectiveness.
- Senior management is fully committed to the Integrated Risk Management System, driving its objectives across the organization and ensuring compliance through monitoring and oversight.
- The function responsible for leading the Risk Management System operates independently from business units, ensuring impartiality.
- Adequate resources must be allocated to support the execution of the Risk Management System.
- The Risk Management System must align with the Organization's strategic objectives.

- The system must be unified and focused on risk coverage, control, and quantification.
- All employees are responsible for executing the processes of the Risk Management System.
- Action plans will be defined and implemented for priority risks.
- Both priority and non-priority risks will be subject to continuous monitoring.
- The Organization will cooperate with governmental bodies and agencies, establishing effective communication channels to strengthen resilience.
- Risks associated with potential disruptions to operations must be identified, with corresponding treatment plans developed and implemented.
- Compliance with the policies and commitments established in Alianza Team®'s Policy Guidelines is mandatory.
- The Organization will ensure early detection and prevention of threats to human rights and the environment through due diligence in operations and across the value chain.
- Climate- and nature-related risks are recognized as emerging risks and will be managed under the same procedures, complemented with additional analysis as required.
- A culture of risk management will be promoted and developed at all organizational levels, fostering continuous improvement through testing and auditing of the plans and procedures that form part of the risk management process.

4. Risk Management Methodology

The Integrated Risk Management System is a dynamic process structured in defined stages. When applied sequentially, these stages support effective decision-making by providing a holistic view of risks and their potential impact.

The risk management methodology includes the following stages:

Each of these elements represents a key stage in the methodology and together produce the risk matrix for processes, areas, programs, projects, sites, plants, countries, and/or at the corporate level. This matrix supplies the Organization with the necessary information to make informed decisions about managing risks that could create deviations from its objectives.

4.1. Scope, Context, and Criteria

The Integrated Risk Management System can be applied across multiple levels of the Organization (strategic, operational, financial, project, process, program, or other activities). Defining the scope requires clarifying the objectives of each level and ensuring alignment with the Organization's overall goals.

The context for risk management must be established by understanding both the external and internal environments in which the Organization operates and should reflect the specific circumstances of the activities where the risk process will be applied.



Responsibility for managing internal factors lies with all employees of the Organization.

Responsibility for managing external factors lies with the Board of Directors, the President/CEO, Vice Presidents, General Managers, Directors, and Managers.

The Organization must determine the level and types of risks it is willing or unwilling to assume in relation to its objectives. It must also define criteria to evaluate the significance of risks and to support decision-making. These criteria must be consistent with the risk management framework, tailored to the purpose and scope of the activity, and reflect the Organization's values, objectives, and resources. They must also align with the Organization's policies and declarations on risk administration and management, while incorporating legal obligations and stakeholder perspectives.

4.2 Risk Assessment

The Corporate Risk Management Office will update the Organization's risk maps annually. If this cannot be performed, risks will be updated based on the criteria defined in the Comprehensive Risk Management System procedures.

Risks are assessed in two stages:

Inherent Risk: The level of risk assessed without considering existing control measures.

Residual Risk: The level of risk assessed after the implementation and evaluation of controls.


Once risks are identified, they are rated and quantified using three variables: Probability, Impact, and Control.

Risk assessment may be qualitative, semi-qualitative, or quantitative, depending on the availability of data and information.

The purpose of risk analysis is to understand the nature and characteristics of risks, including—when appropriate—their level. This analysis involves a detailed review of uncertainties, sources of risk, potential consequences, probabilities, events, scenarios, controls, and the effectiveness of those controls. A single event may have multiple causes and consequences, potentially affecting several objectives.

Inherent Risk refers to the intrinsic exposure of each activity before applying any internal controls. It reflects both the Organization's vulnerability to a particular activity and the probability that an adverse event may compromise its objectives.

Once Controls or Control Activities are identified, they are evaluated considering design, implementation, execution, effectiveness, and the occurrence of related events.



Once Controls or Control Activities are identified, they are evaluated considering design, implementation, execution, effectiveness, and the occurrence of related events.

Residual Risk is the level of risk that remains after controls are applied. It is important to note that risk exposure can never be entirely eliminated. Therefore, the Organization must strike a balance between allocating resources and mechanisms to minimize or mitigate risks and maintaining a level of confidence aligned with its Risk Appetite.

4.3 Risk Treatment

The Organization must implement measures to manage its Residual Risk exposure and mitigate risks that could significantly impact its objectives. To achieve this, action plans must be developed to reduce or control identified risk levels.

The monitoring process for these action plans must ensure they meet their intended objectives in terms of reducing probability, impact, and/or strengthening controls. It must also verify that plans are executed within the agreed timelines and deliverables.

4.4 Monitoring and Supervision

Monitoring and supervision are critical to ensuring that risk-related actions are effectively implemented. They also provide the basis for evaluating implementation efficiency and for conducting ongoing reviews to identify factors or circumstances that may affect the execution of corrective or preventive measures.

4.5. Communication and Consultation

Communication efforts must ensure that all members of the Organization recognize risk management and prevention as integral to the corporate culture. Risk considerations should be seen as essential inputs for both decision-making and the achievement of organizational objectives.

Information should be disclosed annually across all organizational levels, while upholding the principles of confidentiality, integrity, and availability.

4.6 Recording and Reporting

The Integrated Risk Management System and its outcomes must be formally documented and reported through the risk map to ensure full traceability of risks, their analysis, and treatment.

