

NATURA &CO HOLDING S.A.

ENTERPRISE RISK MANAGEMENT POLICY

1. Purpose

The purpose of this Enterprise Risk Management Policy (“Policy”) is to set standard guidelines and define the principles, roles and responsibilities regarding Enterprise Risk Management (ERM) practices for Natura &Co, supporting decision making-processes and providing relevant insights considering the balance of risk and performance.

2. Scope and Application

This Policy applies to all entities of Natura &Co Group, including, for the avoidance of doubt, all the subsidiaries of irrespective of the country of incorporation, registration or office location.

3. Definitions

Action Plan: An action, or a set of actions, developed to reduce a Risk Exposure.

Company or Group: Natura &Co Holding S.A. and its controlled companies, known as Business Units (BUs), namely Natura Cosméticos and Avon Products, Inc (“Avon”).

Committee of Sponsoring Organizations of the Treadway Commission (COSO): Joint initiative composed by specialized and recognized organizations of the private sector, dedicated to providing thought leadership through the development of frameworks and guidance on Enterprise Risk Management, Internal Control and Fraud deterrence.

Emerging Risks: Risks that may have its exposure increased, despite of its current levels as stated in the current Risk Map, due to an abrupt change of internal and/or external factors that affect its scenario.

Executive Leadership: Represented by the Executive Management of Group and Business Units as well as by the members of the Group’s Committees, such as ExCom, ELT, Comex, Summit. They are responsible for managing the Company and conducting the business and its operational and financial processes.

IIA (The Institute of Internal Auditors): International professional association and authority for Internal Audit, Enterprise Risk Management, Corporate Governance, Internal Control, and Information Technology Audit matters.

Impact: The extent to which a Risk might affect the Company. A potential consequence of a Risk materialization measured in financial and/or non-financial terms.

ISO (International Organization for Standardization): Worldwide federation that prepares consensus-based and market relevant International Standards through technical committees.

ISO 31000: International Standard issued by ISO with guidelines for Risk Management.

Likelihood: Probability of an event occurring. In Risk Management terminology, it is used to refer to the chance that something will happen, regardless of being defined, measured, or determined in an objective or subjective, qualitative or quantitative way, or being described with the use of general or mathematical terms, such as probability or frequency during a certain period.

Risk: The possibility that events will occur and affect the achievement of strategy and business objectives, hindering creation or even destroying existing value, or potentially contributing to the decision-making process for a strategic or business opportunity.

Risk Appetite: Aggregate level of exposure and types of Risk the company is willing to assume in order to achieve its strategic objectives.

Risk Exposure: Combination of Impact and Likelihood that represents adverse effects from Risks.

Risk Map: Graphic representation of Risk Exposure levels in two axes of analysis (Impact and Likelihood), comprising a 4x4 matrix.

Risk Management: Set of activities and procedures defined to manage Risks and opportunities. In the context of this Policy, refers specifically to the Group's Enterprise Risk Management (ERM) approach.

Risk Owners: Managers or executives who have the accountability and authority to manage Risks and opportunities in different business and operational areas within the Company. They are designated by the Executive Leadership as responsible for the identification and effective application of Risk Management procedures in line with the agreed Risk Appetite.

Risk Response: Position taken when a Risk is identified, upon the decision of mitigating, rejecting or retaining it. The Group's overall ERM strategy indicates mitigate as the preferred Risk Response, which will outcome the need of defining an Action Plan to mitigate that Risk.

4. Principles and Guidelines

The Group is committed to keep a robust and integrated governance model to ensure, in the benefit of its stakeholders, the achievement of corporate goals and performance of its responsibilities with accountability, compliance, disclosure and fairness.

Risk Management practices, which includes the identification of opportunities and threats, is seen by the Group as a core component of the commitment stated herein. It is a constant and transparent process incumbent upon all professionals who work for the Group in every hierarchical level. Each one is responsible for becoming aware of Risks involved in their area, considering short, medium and long term aspects, along with managing and reporting them in accordance with concepts, guidelines and instructions shortly described in this Policy and detailed in its supplementary documents.

Natura &Co ERM methodological approach is based on the integrated framework suggested by COSO and guidelines defined on ISO 31000 for Risk Management, also observing the concepts established on the Three Lines Model, developed by the IIA, which is illustrated below in figure 1.

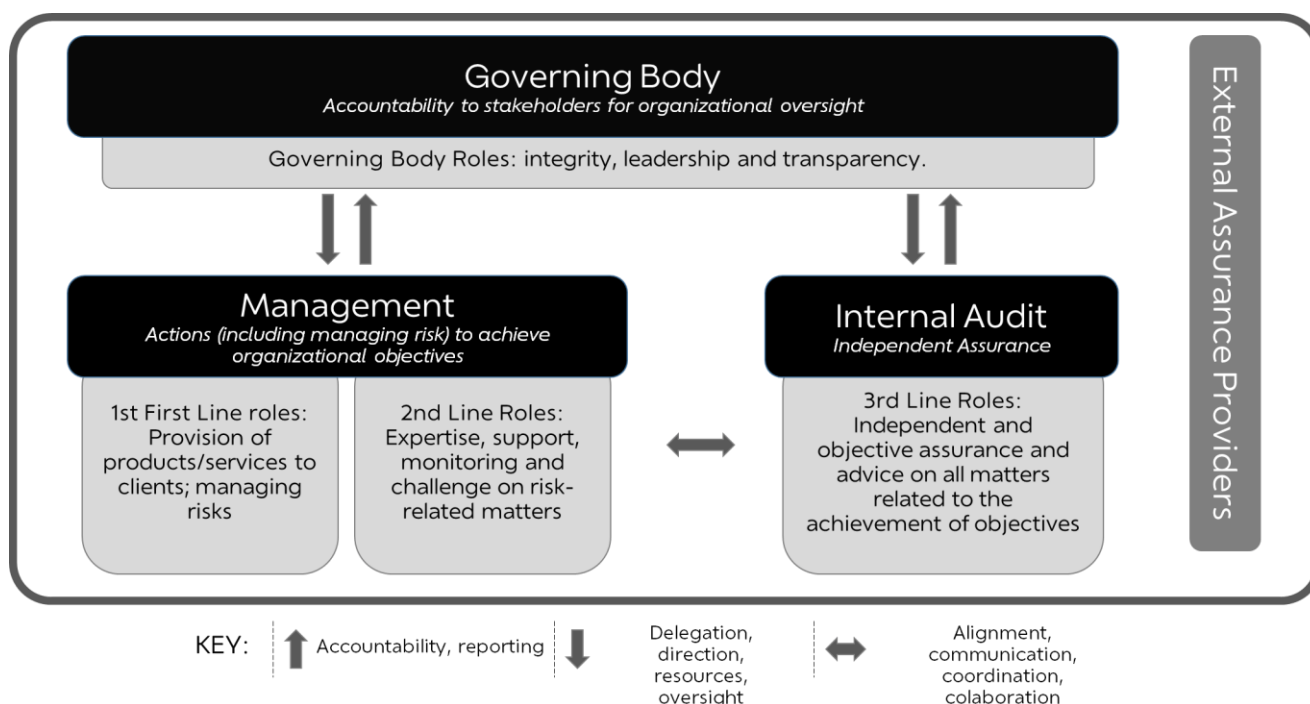


Figure 1 – Adapted from the IIA's Three Lines Model

The IIA's Three Lines Model ensures there is segregation between direct accountability for: Risk decisions (First Line); independent oversight on Risk decisions along with definitions for the Risk Management framework (Second Line); and independent assurance on the effectiveness of Risk Management, control and governance processes (Third Line).

The First Line is most directly aligned with decision-making for business strategy, and therefore in charge of daily execution of Risk ownership, and it is formed by the business areas, including affiliates and controlled companies. The Second Line works through independent structures supporting the business and is formed by areas such as Risk Management and Internal Control, Compliance, Regulatory, and Information Security, who provide instruments for the First Line managers to effectively manage Risks with a preventive approach. The Third Line is formed by Internal Audit, working with an independent look to verify the effectiveness of the model with a detective focus. More comprehensive roles and responsibilities of each line can be found in item 5 (Roles and Responsibilities) of this Policy.

4.1 Natura &Co ERM Framework

The Group's ERM methodology is summarized in the framework showed in figure 2. It is a continuous process that encompasses four main steps: i) Identification and Analysis; ii) Assessment; iii) Response; iv) and Oversight. The framework contemplates ISO 31000 guidelines segregated in different great group of activities.

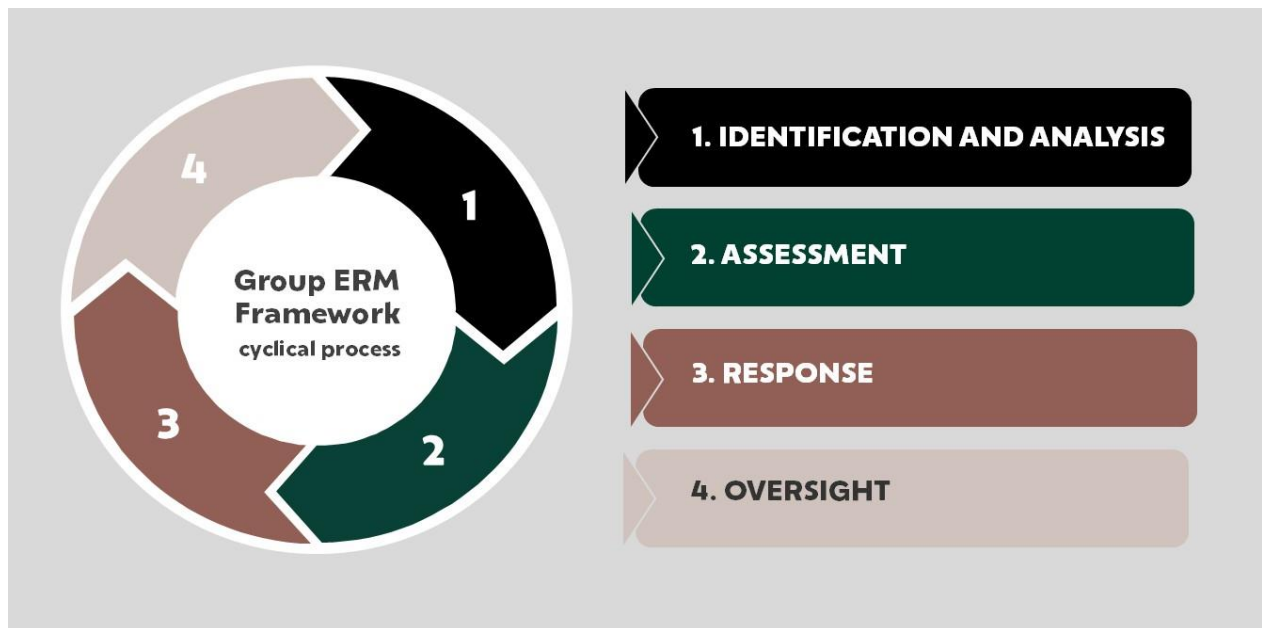


Figure 2 – Graphic representation of Natura &Co Risk Management Framework

Where:

Identification and Analysis

Identification and Analysis is an iterative process, that contemplates the verification of internal and external factors that contribute on the debate of events that may affect the scope of business goals, in short, medium and long term aspects from a preventive perspective during decision-making processes, as well as assessing their implications.

To establish the context for identification, it is important to consider both internal and external environments, captured and reflected in the Group's strategy. Internal factors to be observed include the Company's vision and mission, strategic objectives, initiatives to support the achievement of goals, corporate governance (standards, procedures and guidelines), relationship with internal stakeholders and contractual matters, organizational culture and structures, data and processes. External factors comprehend the circumstances that surrounds the Company in the international, national, regional and local contexts, such as social, cultural, political, legal, regulatory, financial, technological, economic, environmental factors and relationship with external stakeholders.

Risk Owners, jointly with other corporate areas, and taking into account their capacity to contribute with relevant information, shall proceed with the analysis of Risks to identify root causes, processes and areas that might be affected in case of materialization, aligned with potential causes and consequences for the Company.

Assessment

Risk assessments will look at potential Impact and Likelihood of a materialization, which will define the level of Risk Exposure. The graphic representation of the Company's Risks Exposure levels will comprise a 4x4 matrix (Risk Map) to support the decision-making process and prioritization of themes.

Risks must be properly identified, assessed and prioritized in order to ensure that the most relevant themes will be periodically monitored in the adequate governance forums, the response initiatives will be timely addressed, and the exposures will be managed within acceptable levels.

Response

Response refers to the response strategy for Risks, or how the Company will choose to handle Risks. It shall be aligned to the Company's Risk Appetite, oriented by Risk Exposure levels, as their positioning on the Risk Map. The definition of actions and initiatives for Risk Response and mitigation design will aim at a mindful decision-making for best response alternatives, considering short, medium and long term outcomes. The timeframe for mitigation must be compatible with the severity and speed of onset of each risk, in order to allow for an adequate reduction of exposure.

The responses must be the optimal alternative of reaction in light of the possibilities, considering Company's Risk Appetite, which will best balance the reduction of exposure and related costs. Upon the implementation of a Risk Response, it is important to consider forward mitigation initiatives (Action Plans) proposed and performed by the Risk Owners.

The Action Plans will be implemented, executed and managed by the First Line, will be monitored and supported by the Second Line, and will be discussed in governance forums when applicable.

Oversight

Oversight involves monitoring and performing a critical analysis means the verification, supervision, critical observation and improvement implementation processes based on the identification of changes in the required or expected level of performance. Forums where Risks are overseen are initially defined by considering the origin of each risk and functional knowledge

It is important that all aspects of the Risk management process are monitored in order to (i) ensure that the controls and management practices are effective and efficient in the design and operation; (ii) gather information that may improve the Risk assessment process; (iii) improve the process through the analysis of events, changes, trends, successes and failures; (iv) identify changes in the external and internal contexts, which may even have an influence on past response choices and priorities; (v) identify emerging Risks.

5 Roles and Responsibilities

5.1 Board of Directors

- To define the Risk management philosophy of the organization in line with the mission, values, and principles set;
- To set the Group's levels of Risk Appetite based on the short-, mid- and longterm business goals;
- To review and approve the general definitions of Risk management strategies, including this Policy;
- To monitor critical alignments: strategy, Risks, controls, compliance, incentives, and people;
- To periodically acknowledge and assess whether the corporate Risk management processes, including scenarios that have been prioritized, allow the Board of Directors to achieve its Risk supervision goals, and recommend alterations if required.

5.2 Audit, Risk Management and Finance Committee

- To supervise the suitability of processes related to risk management and to the internal controls system, in line with the guidelines set by the Board of Directors;
-

- to support managers in the formulation of concepts and methodologies used in the management of Corporate Risk, as well as the Risk Map , which classifies them in accordance with the severity of their potential impacts;
- To assess and monitor the Company's risk exposures;
- To track the evolution of the management of identified risks, as well as the compliance with the applicable legislation, policies, rules and procedures of the Group, and the effectiveness of controls and addressed response actions;
- To assess the suitability of the human and financial resources allocated to the Corporate Risk management process of the Group.
- To keep the Board of Directors properly informed of the effectiveness of the Risk management processes, including prioritized scenarios, as well as, whenever necessary, to recommend changes to the concepts and risk appetite levels.

5.3 Executive leadership (Group and Business Units)

- To submit the general guidelines on the management of risks and limits of exposure for approval of the Audit, Risk Management and Finances Committee and the Board of Directors;
- To assess the performance of the Risk management process;
- To ensure the resources required for the implementation of the general guidelines on Risk management;
- To validate the periodic reviews of the Risk map with an Impact on the Group's strategies;
- To monitor the behavior of exposures of priority Risks.

5.4 Chief Executive Officers (Group and Business Units)

- To promote the integration between ERM and the cycles of review and construction of the Group's and Business Unit's strategic plan

5.5 Enterprise Risk Management and Internal Controls Area (Group and Business Units)

The Risk and Internal Controls Area assumes several responsibilities regarding its Enterprise Risk Management, Internal Controls and Insurance structure. Its main responsibilities are:

- Developing and implementing the Enterprise Risk Management strategy and methodology in compliance with the applicable laws, regulations, policies, rules, internal procedures and best management practices.
 - Jointly with 2nd and 3rd lines, to reconcile the risk measures, impact and probability so the same Risk classification concepts are used for all activities;
 - Keeping this Policy, the Enterprise Risk Management Procedure and other supplementary Risk documents updated (Risk Map, etc.).
 - Promoting an Enterprise Risk management culture in the organization;
 - Providing tools for Risk owners to properly and timely identify, analyze, assess Risk and give the best set of responses;
 - Periodically monitoring the levels of exposure to Risks;
 - Reporting to the Executive Leadership and the Audit, Risk Management and Finances Committee the levels of potential exposure of the main Risks;
-

- Monitoring the implementation of the Risk owners' action plans, whenever applicable, in order to verify their mitigation or reduction, reporting it to the Executive Leadership and the Audit, Risk Management and Finances Committee.

5.6 Internal Audit

- Assessing the reliability of information, reviewing the effectiveness and efficiency of transactions and information produced by these, and protecting the Company's assets ensuring compliance with laws, regulations and contracts;
- Examining the internal controls system, providing an assessment of its effectiveness to the senior management;
- Providing advice to the Group Chief Executive Officer and to the Board of Directors, through the Audit, Risk Management and Finances Committee, monitoring, examining, assessing, informing, and recommending improvements for the internal environment and effectiveness of the Enterprise Risk Management process;
- Identifying and indicating the Risks that may not have been mapped by the organization, by means of an independent assessment of the internal controls' environment;
- Assessing the quality and effectiveness of the enterprise risk management processes of the Company, periodically monitoring the risk mitigating actions and the frailties recorded in the audit reports and feed the enterprise risk management model with information.

5.7 Risk Owners

- Identifying, assessing, mitigating and monitoring the Risks of the processes and business under their responsibility, based on the criteria set by the Group;
- Defining and implementing mitigating actions and management practices for the exposure to Risks;
- Creating and updating the key indicators used to monitor Risks;
- Ensuring the performance and effectiveness of existing Internal Controls used to mitigate Risks;
- Formalizing occasional exposures to Risks identified due to the monitoring of transactions that are unknown to Management.

6 Risk Reporting

The forums to share and monitor exposures are initially defined considering each risk's classification, as described below:

Level of Exposure of the Risk	Sharing and Monitoring Forum
4. Severe	Board of Directors, Audit, Risk Management and Finances Committee and Executive Leadership
3. High	Audit, Risk Management and Finances Committee, Executive Leadership and Vice-presidencies responsible for the business unit(s)
2. Moderate	Officers responsible for the business units
1. Low	Officers responsible for the business units

The forums created may, at any time, request that risk subjects are registered for monitoring and acknowledgement, regardless of the indicated levels of exposure, and the owners of the subjects (risks)

shall prepare documentation that will allow the timely understanding of the current exposures, the stage of implementation of the actions and the deadline for completion of those actions, as well as restrictions or extraordinary events responsible for occasional extensions.

7 Final Considerations

Due to the size of the Group, its business particularities, complexity of structures, diverse operational contexts and geographical locations, along with different jurisdictions and regulatory environments where the Business Units operates, this Policy may be complemented by specific procedures (ERM procedure, and other supplementary documents) applicable and/or required.

The revised Policy was approved on May , 2024 by the Board of Directors of Natura &Co Group, replacing its prior version, becoming effective immediately, on the date of its publishing and disclosure, and shall remain in force for an indefinite term, until it is resolved otherwise.