Enterprise **Risk Management**

At Natura &Co, we know the importance of implementing an effective Enterprise Risk Management system. This means identifying risks that could significantly impact our company's value or reputation, while also recognizing opportunities for growth.

Our adaptation process ensures synchronicity between our strategies, societal progress, and organizational ethos.

One of our main challenges has been aligning risk management practices with our commitment to generating positive economic, social, and environmental results.

Risk management guidelines and methodology

We align with respected institutions for risk management guidance, integrating their insights while staying true to our values. Our adaptation process ensures synchronicity between our strategies, societal progress, and organizational ethos. Natura & Co's Enterprise Risk Management applies the guidelines of COSO (Committee of Sponsoring Organizations of the Treadway Commission), the Brazilian Institute of Corporate Governance (IBGC), and ISO 31000.

Internally, we have a Global Risk Management Policy (see Risk Management Policy for further details) and a Business Risk Management Procedure for each business unit. These methodologies do not represent a static or immutable document, so we continually update and adapt them.

In 2023, we moved forward with a comprehensive global manual called Risk Fundamentals. This manual provides a detailed overview of the methodology and ensures transparency and alignment at all levels of the organization's governance.

In Latin America, we updated our Enterprise Risk Management Procedure, emphasizing adjustments to increase the traceability of risks originating in the operating units, which can have material impacts on the organization, and to generate greater robustness in our risk management.

Our risk management structure follows the Three Line Model proposed by The Institute of Internal Auditors (IIA), which organizations widely recognize. In the First Line, the business areas, including subsidiaries and controlled companies, are directly involved in risk decisions, the day-to-day execution of risk management, and the implementation of business strategies. The Second Line acts in a guiding role, offering support to the business areas through functions such as Risk Management and Internal Control, Compliance, Regulatory, and Information Security. Its role is to provide tools and guidelines so First Line managers can effectively manage risks preventively. Finally, the Third Line, formed by Internal Audit, independently verifies the effectiveness of the organization's risk management, control, and governance model. It takes a more investigative approach, identifying possible flaws or areas for improvement in the risk management system.

To simplify and ensure seamless integration, Enterprise Risk Management focuses on identifying threats to organizational performance and preventing value-destructive events from slipping through the cracks. This involves vigilant monitoring and implementation of necessary mitigating measures and controls.

Enterprise Risk Management focuses on identifying threats to organizational performance and preventing value-destructive events from slipping through the cracks.

These activities are overseen at the operational executive level by the Chief of Internal Controls, Risk Management, and Internal Audit, who reports directly to the Audit, Risk Management, and Finance Committee.

Responsibilities encompass more than just overseeing the sufficiency of risk management processes and internal controls. They extend to assessing and monitoring our risk exposure, tracking management's efforts, and ensuring senior management remains well-informed about the efficacy of risk management processes.

In addition, the Audit, Risk Management, and Finance Committee, a representative body of the Board of Directors, guides business risk assessment, monitoring, and management. This Board defines the organization's risk management philosophy and provides incentives and organizational structures for appropriate risk management. It comprises seven non-executive members with experience in enterprise risk management (more information in the Corporate Governance section).

Our risk assessment methodology evaluates two vectors relating to potential adverse events that could impact our organization: the magnitude of their impact (on the financial and reputational outlook) and the probability of their occurrence. Risk management and prioritization are linked to the residual exposure of these adverse events, i.e., after considering the controls or actions implemented.

Reporting of risks is contingent upon the level of exposure of the business, as outlined below:

Level of Exposure to the Risk	Sharing and Monitoring Forum
4 - Severe	Board of Directors, Audit, Risk Management and Finance Committee, and Executive Leadership
3 - High	Audit, Risk Management and Finance Committee, Executive Leadership, and Vice-presidencies responsible for the Business Units
2 - Moderate	Officers responsible for the Business Units
1 - Low	Officers responsible for the Business Units

We adopt circularity and regeneration practices to address the climate crisis and protect the Amazon…

Risks and Risk Factors

Natura &Co assesses risks and their associated factors based on four principles. We do not accept risks that could compromise these principles:

- **Sustainability:** A perpetual commitment to sustainability. We adopt circularity and regeneration practices to address the climate crisis and protect the Amazon, aiming to reduce greenhouse gas emissions, water consumption, pollution, solid waste, deforestation, overconsumption, and our environmental footprint.
- **Human Rights:** We are committed to continuously defending human rights and promoting gender equality, including ensuring fair and equitable remuneration, especially for our essential network of relationships crucial to the success of our business.
- **Growth:** Maintaining, modernizing, revitalizing, and improving our brands is essential to expanding our consumer, suppliers, and consultants' work.
- **Compliance:** Compliance with the Code of Conduct and regional and local laws and regulations in jurisdictions where the group operates and conducts business.

As a publicly traded company listed on the Brazilian Stock Exchange (B3) since 2004, we are subject to the Brazilian Securities and Exchange Commission (CVM) regulations. Until 2023, we were subject to the rules of the Securities and Exchange Commission (SEC) (as announced in the Material Fact of January 18, 2024), which requires the annual submission of the Reference Form (FR).

Both forms include a crucial section, Risk Factors, designed to compile information that provides a comprehensive and descriptive understanding of the elements that may impact our company. This practice not only promotes transparency but also safeguards the interests of stakeholders by enabling a more informed and accurate assessment of the organization's situation. This report also includes a section on internal controls, which presents the results of our control environment, which is audited by independent external auditors.

Below, we highlight some of our organization's leading risk factors based on residual risk exposure. For a comprehensive summary of our risk factors, please explore our Reference Form.

Climate change also poses a significant threat, giving rise to transition and physical risks that could adversely affect our operations. This prompts diligent monitoring in alignment with the Task Force on Climate-Related Financial Disclosures.

Each Business Unit maintains a dedicated Cyber Board overseen by a senior Business Information Security Officer.

1. Cyber Threats

Companies that use technology and virtual environments intensively face various cybersecurity risks, such as attacks via third parties, malware infection, and unauthorized access to confidential data. These threats can result in business losses, information theft, and reputation damage, demanding ongoing evolution of techniques to prevent, detect, and respond quickly to attacks.

Natura &Co adopts a series of mitigation measures overseen by The Chief Information Security Officer (CISO) as leader of the Cyber Hub. During 2023, the team continued to provide strategic direction, assurance, operational services, and improvements to all our business units. Our governance continued to progress, with the CISO frequently reporting to the Board of Directors directly or through the Cybersecurity Subcommittee, which reports to the Audit, Risk Management, and Finance Committee.

The meetings are chaired by Andrew McMaster, an independent director and member of the Audit, Risk Management, and Finance Committee, who has extensive experience in leading technology and organization improvement programs.

In addition, each Business Unit maintains a dedicated Cyber Board overseen by a senior Business Information Security Officer. These Boards are supported by a mature risk

We maintain vigilant oversight of the political and economic landscape across all our countries…

management structure linked to the Enterprise Risk Management Framework.

We have adopted a Global Cybersecurity Program, and over the past two years, since implementing this global framework, several initiatives have been undertaken, including the adoption of market-leading solutions, review and creation of new processes, and structuring of teams with defined responsibilities and clear operational models. These actions have enhanced our security level in the control environment based on NIST CSF. In 2023, we updated our Information Security Policy and published new technical security standards.

We also completed updated mandatory training for all staff, including regular phishing testing. Our improvements in cybersecurity maturity have been independently assessed using the National Institute of Standards & Technology (NIST) Cyber Security Framework.

In 2023, our advances in cyber maturity were once more propelled by strategic investments in new technologies and processes. We highlight the Cyber Incident Exercise up to the Board of Directors level to strengthen our capacity to respond to the most critical incidents and test our Business Continuity Plans. In addition, new automation and integrations to the new identity and access management platform guaranteed further efficiency in this process. The expanding the Security Operations Center and Vulnerability Management Service has reduced the number of known vulnerabilities and the company's overall security stance. We have also enhanced protection in various other technologies, allowing a safer and more trusted environment for all the company's operations.

2. Tax Burden

Our main economic activities currently originate from Brazil, where a complex tax system is undergoing changes; recently, the Brazilian tax reform was approved. The full impact of this reform on our organization remains to be determined and depends on the regulations being finalized. We diligently follow this process to measure eventual increases in our business' tax burden, always envisioning fair taxation. The transition to the new Brazilian tax system will be gradual, with implementation expected between 2026 and 2030.

We conduct thorough evaluations of the potential financial impacts and devise strategic business measures to position the business accordingly, following the regulatory and legal contexts. To ensure compliance with all tax obligations, we maintain a dedicated team of specialists who closely monitor and interpret new regulations and guarantee their implementation and compliance.

3. Macroeconomic and Geopolitical Conditions

Uncertainties in macroeconomic and geopolitical conditions, along with prolonged and accentuated inflationary pressures, an increase in unemployment, and a decrease in purchasing power, can affect consumers' demand for our products and impact our sales and/or operational profitability.

We believe that dealing for many years with market conditions involving economic and political instabilities has enabled us to operate and develop our business successfully.

We maintain vigilant oversight of the political and economic landscape across all our countries, weighing the risks and rewards associated with each location. This assessment remains connected to our commercial strategy, tailored to accommodate each market's unique characteristics. To bolster resilience, we implement various measures to diversify our investments and operations, minimizing vulnerability to adverse events in any particular market. We implement solid enterprise risk management practices, continually monitoring external events linked to the subject.

4. Litigation

We are currently engaged in various legal proceedings in the geographies where we operate and may encounter additional ones in the future. Companies operating in our market segment face litigation risks involving civil, administrative, environmental, labor and employment, taxation, commercial sanctions, and sanitary compliance. The high litigiousness, uncertainty, and volatility in the regulatory landscape in the countries where we operate can affect favorable outcomes and our financial standing due to possible adjustments in the provisions. We diligently and continuously review and update these provisions to reflect judicial decisions, counting on the support and analyses of top-notch law firms to safeguard the company's rights.

We have legal expertise areas organized by subjects that, among other responsibilities, promote orientations about the detailed standards in regulations and specific and relevant laws to fulfill their purpose. In addition, our legal and regulatory teams monitor and revise our practices to ensure, preventively, that we are aligned with the laws applicable to our organization.

Furthermore, we proactively conduct thorough root-cause analyses of significant legal disputes and implement action plans to mitigate risks and minimize liabilities. We use a casuistic approach to cases, agreements policies, and mediation to avoid and diminish our litigiousness index.

5. Data Privacy

The company's operations are increasingly dependent on IT and data management systems, particularly with the advances of digitalization, the growing adoption of artificial intelligence (AI), and the large-scale collection and processing of personal data. These characteristics are common in business models such as ours and can expose the organization to various risks, such as breaches of personal data and sensitive information, as well as potential misuse by malicious third parties.

Privacy and security function together at Natura &Co to demonstrate our commitment to the responsible collecting, using, caring for, and protecting personal data under applicable laws and our ethical values. Privacy and data protection are embedded as fundamental enablers to the future growth of our business.

We embarked on a unified Global Privacy and Data Protection Program in 2022, per the GDPR (General Data Protection Regulation) in the European Union. This program not only meets regulatory requirements but also incorporates measurement tools to demonstrate compliance effectively across the company's entire operations, including suppliers.

The company's Data Privacy function is led by our Chief Privacy Officer and Group Data Protection Officer, who is responsible for defining and managing our strategic approach to privacy, which incorporates the principles of lawfulness, fairness and transparency, purpose limitation, data minimization and accuracy, integrity, confidentiality and storage limitation, and accountability to be embraced by the whole company.

Additionally, Natura &Co's Privacy Program, Policy, and Standard benchmarked the highest score possible within its sub-category in the Household and Personal Products sector in the S&P Global Corporate Sustainability Assessment for 2023. A series of initiatives are underway to support our strategic vision alongside continuous monitoring of the regulatory environment, particularly concerning legal frameworks and enforcement trends related to privacy and artificial intelligence. Audit and monitoring programs are in place to ensure we meet applicable regulatory requirements, such as automated and manual tools, third parties, and internal control functions, including internal audit.