nexa

Enterprise Risk Management

Policy

NEXA
LISTED
NYSE

Summary

1. OBJECTIVE

The objective of this policy is to establish guidelines for the Enterprise Risk Management (ERM) process at Nexa Resources S.A. (“Nexa” or the “Company”). It defines the responsibilities of all participants in the ERM process, including risk identification, evaluation, treatment, monitoring, and reporting. This policy aims to integrate risk considerations into the Company’s strategic decision-making.

2. SCOPE

This policy applies to Nexa, its directly supervised contractors and all subsidiaries and assets that are owned, controlled, or operated by Nexa, either directly or indirectly, worldwide.

3. REFERENCES

- COSO ERM Framework
- ISO 31000: 2018 Risk Management Guidelines
- Risk Committee Charter
- Nexa’s ERM Manual
- Internal Rules of the Board of Directors
- Charters of the Audit Committee, Finance Committee, Compensation, Nominating and Governance Committee and Sustainability and Capital Projects Committee
- Management Committee (ManCo) Internal Rules
- Nexa’s Financial Risks Policy

4. DEFINITIONS

Accepted Risks: Risks that the Company chooses not to actively address with new measures because existing Controls are deemed sufficient and, based on the evaluation, it is neither possible nor reasonable to implement additional actions. These Risks will be accepted at their current level of exposure, with ongoing monitoring to ensure they do not escalate into Risks requiring further mitigation or intervention.

Action Plan: It is a temporary, specific action with a defined time frame for its implementation. Designed to address a deficiency in Risk management or implement new Controls. Its purpose is to close gaps, improve or reinforce existing control. The Action Plan must have a responsible person and a conclusion date.

Controls: Activities that are part of the organization's regular operations, performed to mitigate a Risk’s Impact or Likelihood.

Emerging Risks: Risks that have not yet fully manifested but could have a significant Impact on the achievement of the organization's strategic objectives and potentially alter its Risk profile in the future. These Risks may arise from technological, social, regulatory and other changes in the business context.

Enterprise Risk Management (“ERM”): Process that has the objective of identifying potential events that may affect the Company’s ability to meet its strategic objectives and to define and implement actions to manage them. ERM includes the culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage Risk in creating, preserving, and realizing value.

Executive Officers: Jointly the chief Executive Officers and all vice-presidents and officers.

Impact: The result or effect of a Risk. There may be a range of possible Impacts associated with a Risk. The Risk’s Impact may be positive or negative relative to the entity’s strategy or business objectives.

Inherent Risk: Intrinsic level of Risk to the business or activity, without considering the implementation of mitigating Controls or Action Plans.

Likelihood: The possibility that a Risk will occur.

Prioritized Risks: Strategy-related Risks that are relevant to the Company, whether to achieve specific objectives, that are out of the defined Risk Appetite, classified as “High” or “Critical”.

Residual Risk: Remaining level of Risk after considering all Controls and Action Plans implemented to mitigate Inherent Risks.

Risk: Any potential event that may affect the Company's ability to achieve its objectives and its strategic business plans.

Risk Appetite: The types and level of Risk the Company is willing to take in pursuit of value.

Risk Area: Area of Nexa responsible for coordinating Nexa's ERM process and ensuring the correct flow of Risk information and reporting within the Company.

Risk Categories: Risk Taxonomy used to improve integrated Risk management, as well as to assist the Company in determining its Appetite.

Risk Factors: Factors that contribute to the Risk to eventually materialize. The same Risk can contain one or more related factors.

Risk Matrix: Diagram prepared based on the Risks general analysis and management’s own assessment, considering the Risks’ Impact and Likelihood.

Risk Owners: Individuals responsible for managing specific Risks in their units / areas.

Risk Register: Record of information of identified Risks.

Risks Governance Model: processes and activities that Nexa follows to manage the Risks.

5. RESPONSIBILITIES

5.1 Board of Directors

The main oversight responsibilities in relation to Nexa’s ERM are to:

- Approve the general guidance of the Company's business, its mission, its strategic goals and its guidelines and ensure that the Executive Officers comply with such mission, strategic goals and guidelines taking into account the Company’s Risks and Appetite and according to the Board of Directors’ Committees’ recommendation.
- Review and approve the Company’s Risk Appetite statement and changes to it when applicable.
- Approve the budget and strategic plan which takes into account the Company’s Risks and Appetite.
- Approve Nexa’s ERM policy and monitor the compliance of this policy.
- Oversee the Company’s Prioritized Risks and Risk exposure

5.2 Board Committees

The main oversight responsibilities of the Audit; Finance; Compensation, Nominating and Governance; and the Sustainability and Capital Projects Committees in relation to Nexa’s ERM are to:

- Support the Board in its monitoring of Nexa’s ERM in matters related to the responsibilities of each Committee, according to each Committee’s charters.

- Discuss the Risks that will be classified as Accepted Risks and submit them for approval by the Board.
- Discuss the Prioritized Risks and how they are treated and monitored, keeping up with their Action Plans.
- Monitor Company's processes or Controls, including Mitigating Actions being taken.
- Report to the Board of Directors regularly its oversight of the ERM process.

Besides the responsibilities listed above the **Audit Committee also undertakes the following attributions**:

- Monitor the Company's Risk management Controls and processes, according to the ERM Policy.
- Understand the Company's framework for Risk assessment, including appropriate guidelines and policies to govern the process.
- Evaluate the organizational structure and activities of the Company's Risk management process.
- Evaluate management's implementation and maintenance of the Risk management structures and policies.

5.3 Management Committee

The main attributions in relation to Nexa's ERM are to:

- Adopt a strategic planning process and annually propose to the Board the Company's budget and strategic plan which considers the business Risks.
- Promote and enforce compliance with the Company's policies, as well as the Company's ERM policy.
- Propose Risk Appetite and present to the Board for review and approval, upon the committees' recommendation, when applicable.
- Recommend the Risks that will be classified as Accepted Risks and submit them for approval by the Board's Committees.
- Recommend the Risks that will be classified as Prioritized Risks and submit them for approval by the Board's Committees.
- Execute and coordinate the Risk management process, ensuring the application of the defined methodology, assisting in the supervision of Risks, monitoring of the Action Plan and Prioritized Risks.
- Individually, each Executive Officer should periodically hold meetings with their respective teams to monitor identified Risks and, Action Plans to respond to these Risks and associated Controls.

5.4 Risk Committee

Risk Committee ("RiskCo") is a standing committee of the Management Committee for the primary purpose of assisting them in fulfilling their implementation and execution responsibilities with respect to:

- Monitoring and managing the Company's Risks that may affect the achievement of the Company's objectives.
- Providing oversight across all categories of Risk and enhancing the Risk culture.
- Approving and overseeing the processes used to identify, evaluate and manage Risks.
- Issuing recommendations to the Management Committee related to a) performance of Risk Controls, b) compliance with Action Plans and c) Risk response strategies, among others.

5.5 Internal Audit, Internal Controls, Compliance and Ethical Line area

The main attributions in relation to Nexa's ERM are to:

- Internal Audit: The Internal Audit team incorporates the ERM Risk Matrix as input for their annual audit planning to ensure a Risk-based approach. They identify Risks during audit processes and communicate significant observations to the ERM area. Additionally, they assess the effectiveness of the Risk management processes, ensuring compliance with established policies, and provide recommendations for improving Risk mitigation.

- Internal Controls: The Internal Controls team enhances the control environment to ensure Controls effectively mitigate identified Risks and collaborate with ERM area to share the status of effectiveness of implemented Controls.

- Compliance: The Compliance team integrates the ERM Risk Matrix into their annual planning to address key Risks, ensuring adherence to all relevant compliance requirements. They also investigate potential compliance breaches and communicate any identified Risks to the ERM Area.

- Ethical Line: The Ethics Line team provides a confidential and secure mechanism for employees to report ethical concerns, misconduct, or potential Risks. They monitor and investigate reports received through the ethics line, communicate any identified Risks or ethical issues to the ERM Area for inclusion in the Risk assessment process, and promote awareness of ethical standards and the importance of reporting within the organization.

5.6 Risk Owners

The main attributions in relation to Nexa's ERM are to:

- Lead Risk management efforts, ensuring continuous monitoring and updates.
- Promote effective participation and a multidisciplinary approach in Risk assessments.
- Ensure the definition and implementation of response measures in coordination with Control Owners and Action Plan Owners.
- Monitor the evolution of Risk and the status of response measures, reporting progress to the Risk Team and other key stakeholders.
- Ensure the implemented actions are effective and aligned with Nexa's strategic objectives.
- Communicate the Emerging Risks to the Risks Area to include them in the Risk Matrix.

5.7 Focal Points

The main attributions in relation to Nexa's ERM are to:

- Assist the ERM Area in the Risk Assessment Process at their unit or corporate area.
- Help ERM Area to contact Risk Owners and experts.
- Support the monitoring of compliance with Controls and Action Plans.
- Participate in follow-up and monitoring meetings.
- Promote communication with the ERM team.
- Encourage participation in ERM training sessions.

5.8 Risks Area

The main attributions in relation to Nexa's ERM are to:

- Develop the strategy, apply the methodology and promote the ERM culture, in accordance with current regulations and best market practices.
- Monitor the Risks reported by the units and corporate areas.
- Monitor the implementation of the Action Plans developed to mitigate the Impacts of identified Risks.
- Report the level of exposure of Nexa to the identified Risks to the Executive Officers, to the respective Committee, the Audit Committee and the Board of Directors, when applicable.

- Monitor market trends and their connection to the business and possible Impacts to Nexa.
- Provide training to disseminate the ERM culture and methodology.
- Discuss the Risk Matrix with the Internal Audit, Internal Controls, Compliance and Ethical Line areas.

6. RISK GOVERNANCE STRUCTURE

Nexa's structured Risks Governance Model comprises of three levels: (i) an **executive level**, which includes a clear executive view in consolidating Risk information for monitoring by the Board of Directors; (ii) a **tactical level**, where leaders have formal forums for discussion; and (iii) a **transactional level**, where there is a methodological integration, so the information is aligned. Through this model, there are structured discussions on Risks and their prioritization, together with periodic reports made available by Risk Owners with the support of the ERM area. These three levels are detailed below:

- ***Executive Level***, The executive level addresses strategic and Prioritized Risks that could significantly Impact the long-term objectives and viability of the company. The main objectives at this level are to provide senior management with a consolidated view of the most significant Risks and to establish alignment between Risk management and the organization's strategic objectives.
  This level encompasses the Board of Directors, the Management Committee, the Risk Committee, and Corporate VPs and Officers (when applicable) who are responsible for overseeing the Enterprise Risk Management (ERM) policy, defining the Risk Appetite, and ensuring the effectiveness of the Risk management processes.

- ***Tactical Level,*** The tactical level addresses Risks identified by the business areas and operational units having structured discussions about Prioritized Risks and which ones should be escalated to the Executive level. The main objectives at this level are to translate the strategic policies into concrete actions and to ensure that the strategies defined by senior management are executed correctly.

  This level includes Corporate VPs, General Managers of Operational Units, and General Managers of Corporate Areas who oversee the implementation of mitigation strategies, monitor action plans, and make informed decisions about which risks to escalate.

- ***Transactional Level,*** The transactional level addresses Risks that emerge in daily operational processes, including the health and safety of personnel. The main objective at this level is to manage the Risks that arise from daily activities and operational processes, preventing them from escalating to higher levels of the organization. Which is focused on addressing events that can compromise production processes, as well as the health and safety of those involved. This level is composed of all the employees related to the first phase of the ERM process and is a recurrent activity.

  This level involves Operational Unit General Managers, Area Managers within Units, and Process Leaders who participate in the initial phase of the ERM process, focusing on the identification and reporting of operational and safety Risks on a recurring basis.

7. RISK MANAGEMENT PROCESS

Our overall process for assessing and managing Risks is consistent with the COSO ERM and ISO 31000 frameworks. It includes systematic and common practices within Nexa and subsidiaries to establish the Risk context and to communicate, discuss, identify, assess, treat, monitor, record and report on Risks.

The ERM process in Nexa includes Risks of different nature: Strategic, Financial, Operational and Compliance.

ERM must also relate to other management processes. ERM becomes more effective by integrating ERM practices with business activities and understanding how Risk potentially affects the entity as a whole. In this way, as part of the ERM process, together with all the areas and business units, more operational and projects-related Risks are identified to help the Company have its Risks within its Risk Appetite.

All the identified Risks are, at least, annually reviewed and updated if necessary. Additionally, Nexa's Business areas and units are empowered to include Emerging Risks at any moment, outside of the annual identifying phase of the ERM process, as new situations may arise, or changes may occur.

The main stages of the risk management process are as follows:

7.1 Risk Identification:

The Risk identification stage involves systematically recognizing and documenting Risks that could potentially affect the achievement of the organization's objectives. This includes identifying Risks, Risk Factors, and their potential Impacts. Risks are classified according to the defined Risk taxonomy, which helps in categorizing and organizing them for further analysis.

7.2 Risk Analysis

During the Risk analysis phase, existing Controls are mapped, and Risk Owners are designated. This step is crucial for understanding the current Risk environment and identifying where additional Controls or interventions may be needed.

7.3 Risk Evaluation

Evaluate Risks based on their Impact and Likelihood.

- *Impact:* considers the consequences of its materialization are assessed in seven (7) dimensions: financial, environmental, health and safety, social and human rights, legal and compliance, reputational and cyber and information security. Impact is ranked in five (5) levels: minimal, minor, moderate, major and extreme.

- *Likelihood*: is the possibility of its occurrence is determined and evaluated in five (5) levels: remote, unlikely, occasional, likely and very likely.

As result of the evaluation, Risks are classified among five (5) levels: Very Low, Low, Medium, High or Critical.

7.4 Risk Appetite

Risk Appetite is the degree of Risk the Company is willing to take in pursuit of value or to achieve a desired level of return or growth – outcome. It seeks a balance between Risk and reward and can vary over time and from work-to-work area. It can vary over time and from work-to-work area. The Risk Appetite should be proposed by the Management Committee and approved by the Board of Directors and communicated across the organization.

Nexa's Risk Appetite is part of its overall Risk process, and its main objectives are described as follow:

- To create transparency and consistency for the type and level of Risks that the Company is willing to take to achieve strategic and operational objectives.
- To drive Risk behavior and set the tone for Risk culture in the Company.
- To provide a reference point to benchmarking Risk taking and required Risk response strategies.
- To eliminate excessive Risk aversion by articulating preference for Risk taking.
- To define thresholds for Risk taking that optimize Risk and reward.
- To help integrate Risk taking and performance management.
- To assist with the definition of Risk metrics that support day-to-day business operations.

7.5 Risk Prioritization

Based on the evaluation and appetite, Risks are prioritized to define the appropriate treatment options.

7.6 Risk Treatment

Risks classified as "High”, or "Critical" and Risks "Outside Appetite" must be prioritized to mitigate their Impact and/or Likelihood. The development of Action Plans to reduce Risk levels is mandatory.

The purpose of Risk treatment is to select and implement options for addressing Risks, involving the selection, formalization, and implementation of Action Plans. These options may include removing the Risk source, altering its Likelihood, leveraging opportunities, modifying its consequences, sharing the Risk, or retaining the Risk. The most appropriate treatment involves balancing potential benefits against the costs, efforts, or disadvantages of implementation.

Risk Owners play a key role in developing Action Plans, specifying necessary resources, responsible individuals, and schedules. The Risk Area provides guidance and methodological support to Risk Owners. Risks that cannot be mitigated to reduce Nexa’s exposure should be discussed at the appropriate level for approval as Accepted Risks, considering Nexa’s Risk Appetite.

7.7 Risk Monitoring

Monitoring the Action Plans, evaluation of changes in the level of Impact or probability of the Risk, due to internal or external factors, should be performed regularly.

7.8 Reporting

Risks Area is responsible for structuring the necessary actions and materials relevant to what must be presented at each governance level, considering the hierarchy of information. These materials must be updated according to the frequency of the applicable forums.