Summary

1.OBJECTIVE

This Risk Management Policy (the "Policy") aims to establish principles, guidelines, and responsibilities for Risk Management at Companhia Brasileira de Alumínio (CBA our "the Company"), integrating risk considerations into strategic decision-making processes.

2.SCOPE

This Policy applies to CBA, its subsidiaries, and controlled entities, and is applicable to all areas within the Company and its units.

3.REFERENCES

- ABNT NBR ISO 31000:2018 - Risk Management – Guidelines
- Institute of Internal Auditors - The Three Lines Model 2020 - An Update to the Three Lines of Defense
- COSO - Enterprise Risk Management, Integrated with Strategy and Performance 2017
- Corporate Governance Guidelines from the Company's Bylaws
- Internal Regulations of the Board of Directors and the Statutory Audit Committee
- Novo Mercado Listing Rules of B3 S.A. – Brazil, Stock Exchange, Over the Counter
- Applicable Regulations issued by the Securities and Exchange Commission (CVM)
- Guidelines and principles outlined in the Company's Code of Conduct

4.DEFINITIONS

Risk Appetite: A broad expression of the amount of risk an organization is willing to take to implement its strategy, achieve its objectives, and create value for stakeholders in alignment with its strategic goals.

Risk-Oriented Areas: Refers to the areas considered the "Second Line of Defense" in risk management. These areas provide support in managing specific types of risks, such as Risk Management, Internal Controls, Compliance, Market Risk, Information Security, Sustainability, Environmental Management, Health, and Safety.

Control Activities: Actions established through preventive or detective policies and procedures that help ensure compliance with directives set by management, aimed at mitigating risks to achieving the Company's objectives or strategies.

Executive Management: The team consisting of Directors and General Managers who report directly to the Chief Executive Officer (CEO).

Risk Owner: Leadership reporting directly to the CEO, possessing the highest domain and technical knowledge regarding the corresponding risk, and holding the responsibility and authority to manage that risk, even if not all control activities fall within their area of responsibility.

Event: An incident or occurrence from internal or external sources that may impact the implementation of strategy and achievement of objectives either negatively, positively, or both.

Facilitator: An employee designated by the Risk Owner to assist in the activities of identifying, analyzing, assessing, treating, monitoring, recording, and reporting risks.

Risk Source: An element that, individually or in combination, has the potential to give rise to a risk.

Risk Management: The process of identifying, evaluating, and controlling risks that may negatively impact the Company's capital or results.

Impact: The consequence of the occurrence of a risk event on objectives.

Risk Level: The magnitude of a risk or combination of risks, expressed in terms of the combination of impacts and their probabilities.

Opportunity: The possibility of an event occurring that positively affects the achievement of objectives.

Stakeholder: An individual or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity of the organization.

Probability: A measure of the likelihood of a risk event occurring.

Risk: The possibility of an event occurring and adversely affecting the achievement of objectives.

Compliance Risk: The risk of losses resulting from legal penalties and reputational damage if the organization fails to meet or adhere to laws, regulations, standards, and internal policies.

Governance Risk: The risk of losses resulting from inadequate corporate governance practices.

Strategic Risk: Long-term risk or opportunity risk related to strategic objectives and the strategies adopted to achieve them.

Financial Risk: The risk of losses resulting from financial operations related to credit, liquidity, and market.

Inherent Risk: The risk intrinsic to the nature of the business, process, or activity, regardless of the controls in place.

Operational Risk: The risk of losses resulting directly or indirectly from failures or inadequacies in internal processes, people, systems, or external events.

Residual Risk: The risk retained consciously by management that remains even after risk treatment measures have been implemented.

Socio-Environmental Risk: The risk of harm to the community or society and/or the environment, as well as to third parties affected by such damage.

Risk Tolerance: The acceptable level of variation in performance relative to the target for achieving a specific objective, at the tactical or operational level.

5.RISK MANAGEMENT PRINCIPLES

The purpose of Risk Management is to create and protect value. It enables continuous improvement of activities and performance, encourages innovation, and supports the achievement of strategic objectives.

The principles of Risk Management represent the conditions that must be integrated into the Risk Management framework and process to ensure its effectiveness and embed it within the culture of CBA. These principles reflect a shared set of values, behaviors, and practices that define how CBA addresses Strategic, Financial, Operational, Socio-Environmental, Governance, and Compliance Risks.

The Risk Management principles at CBA are as follows:

- Systematic, Structured, and Comprehensive Implementation.
- Integration with Strategy, Work Processes, Projects, and Organizational Programs.
- Dynamic, Incremental, Customized, and Responsive to Change.
- Based on the Best Available Information and Integrated into Decision-Making.
- Openness to Opportunities and Innovation for Continuous Improvement.
- Respect for Human and Cultural Factors within the Organization.
- Transparency and Inclusion of Stakeholders.

6.RISK MANAGEMENT PROCESS GUIDELINES

The Risk Management process comprises activities designed to identify, analyze, assess, treat, monitor, communicate, and record potential events or situations that may impact the achievement of CBA's objectives. The stages of the Risk Management process are outlined below:

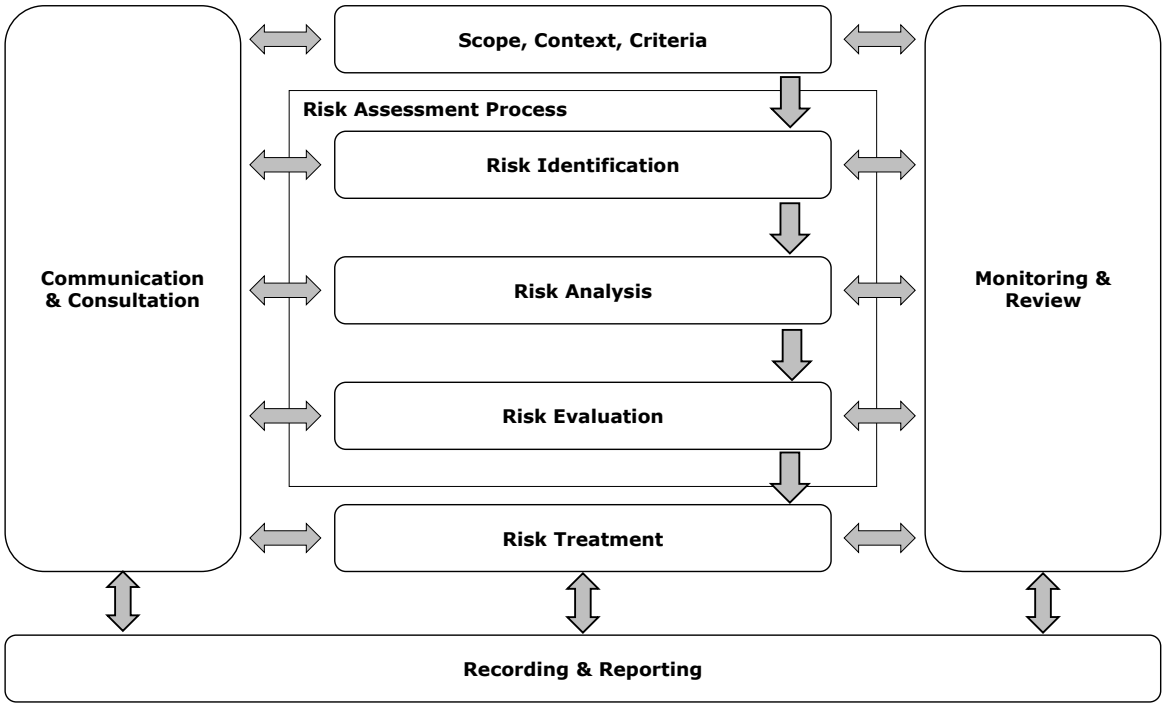


Figure 1 - Risk Management Process according to ABNT NBR ISO 31000:2018

6.1 Communication & Consultation

Throughout all stages of the Risk Management process, effective informational and consultative communication must be maintained between CBA and both internal and external stakeholders, to:

a) Properly Establish Context: Ensure that stakeholder views and perceptions, including needs, assumptions, concepts, and concerns, are identified, documented, and considered.

b) Ensure Adequate Identification and Analysis of Risks: Gather diverse areas of expertise to identify and analyze risks comprehensively.

c) Ensure Awareness and Support: Make sure all parties involved are aware of their roles and responsibilities and validate and support the risk treatment measures.

6.2 Scope, Context, Criteria

This stage involves defining the scope of the Risk Management process. In addition to establishing context, it includes understanding the internal and external environment in which the risk assessment process operates, the organizational governance structure, the objectives and outcomes to be achieved, and the key factors (such as business processes, people, stakeholders, systems, legislation, budget, among others) that may impact the intended or established results by the Company.

Defining risk criteria involves establishing the methodology and criteria to be used in subsequent stages, such as probability scales, impact scales, how to determine if the Risk Level is tolerable or acceptable, and whether additional treatment actions are needed. This includes guidelines for prioritizing and addressing risks.

6.3 Risk Identification

Risk identification is the process of searching for, recognizing, and describing risks, based on the established context, and supported by communication and consultation with internal and external stakeholders. The goal is to produce a comprehensive list of risks, including their causes, sources, and events, which may impact the achievement of objectives identified in the context establishment stage. Risk identification should occur at least annually.

In the risk identification process, the Company classifies its risks into major macro categories (Strategic, Financial, Operational, Socio-Environmental, and Governance and Compliance).

6.4 Risk Analysis

Risk analysis is the stage of understanding the nature of the risk and determining the Risk Level, providing the basis for risk assessment and treatment decisions. The outcome of risk analysis will be to assign a classification for each identified risk, both for the probability and impact of the event, with their combination determining the Risk Level. Risk analyses should occur at least annually.

6.5 Risk Evaluation

The purpose of the risk evaluation stage is to support decision-making based on the results of the risk analysis, determining which risks require treatment and prioritizing their treatment implementation. This involves comparing the Risk Level with the established risk criteria from the context establishment stage to determine whether the risk and its magnitude are acceptable or tolerable, or if any treatment is required. Risk evaluations should occur at least annually.

Below are the criteria for prioritizing and treating risks:

Risk Level	Criteria for Prioritization and Risk Treatment
Critical	All risks at this level must be communicated to the Board of Directors, Statutory Audit Committee, and Executive Management, and require an immediate response. Postponement of measures is only permitted with authorization in accordance with established thresholds.
High	All risks at this level must be communicated to Executive Management and the Statutory Audit Committee, with actions taken within a specified time. Postponement of measures will only be accepted with authorization according to established thresholds.
Medium	Typically, no purposeful measures are required, but specific monitoring activities are necessary. Risk Owners must pay attention to maintaining responses and controls to keep the risk at this level or reduce it.
Low	Typically, no purposeful measures are required, but minimal controls are necessary to maintain or reduce the risk to this level.
Very Low	No additional measures are necessary. Controls should be maintained or reduced to keep the risk at this level.

6.6 Risk Treatment

The risk treatment stage aims to select and implement options for addressing risks, including the development of treatment plans that, once implemented, will involve the introduction of new controls or modifications to existing ones.

Risk treatment involves choosing one of the following options:

- **Risk acceptance:** No action will be taken to affect the probability or impact. The risk will be monitored only. Choosing this option must be justified and approved.
- **Risk avoidance:** Take action to prevent the initiation or continuation of the activity, process, or project to avoid the risk.

- **Risk mitigation:** Implement actions to reduce the impact and/or probability of the risk occurring or address both impact and probability.

- **Risk transfer:** Transfer or share a portion of the risk, such as through outsourcing activities or purchasing insurance.

Treatment should be cyclical and include: (i) evaluating the treatment already implemented; (ii) assessing residual risk levels against the defined Risk Appetite and Risk Tolerances; (iii) defining and implementing additional treatment where residual risk exceeds the Appetite and Tolerances; and (iv) evaluating the effectiveness of the treatment.

6.6.1 Approval Authority for Risk Acceptance

In cases where the risk is accepted (i.e., no action will be taken to reduce the impact or probability of the risk occurring), the following approval authorities must be followed, formally documented, and communicated to higher levels:

Risk Level	Approval Authority for Risk Acceptance
Critical	Board of Directors
High	Executive Management
Medium	Director / General Manager
Low	Manager
Very Low	Coordinator / Supervisor

6.7 Monitoring & Review

Monitoring and review activities are conducted with the purpose of (i) detecting changes in the external and internal context that may require a review of current treatments and their priorities, as well as identifying emerging risks (ii) obtaining additional information to enhance the risk management policy, structure, and process; analyzing events (including "near-misses"), changes, trends, successes, and failures, and deriving lessons from them (iii) Ensuring that controls are effective and efficient in their design and operation.

During monitoring, it is important to verify whether the actions outlined in the risk treatment plans are being implemented and to allow sufficient time for these actions to achieve their intended objectives.

6.7.1 Approval Authority for Changes or Postponements of Treatment Plans

In cases of changes or postponements to treatment plans, the following approval authorities must be adhered to, formally documented, and communicated to higher levels:

Risk Level	Approval Authority for Changes or Postponements of Treatment Plans
Critical	Board of Directors
High	Executive Management
Medium	Director / General Manager
Low	Manager
Very Low	Coordinator / Supervisor

6.8 Recording & Reporting

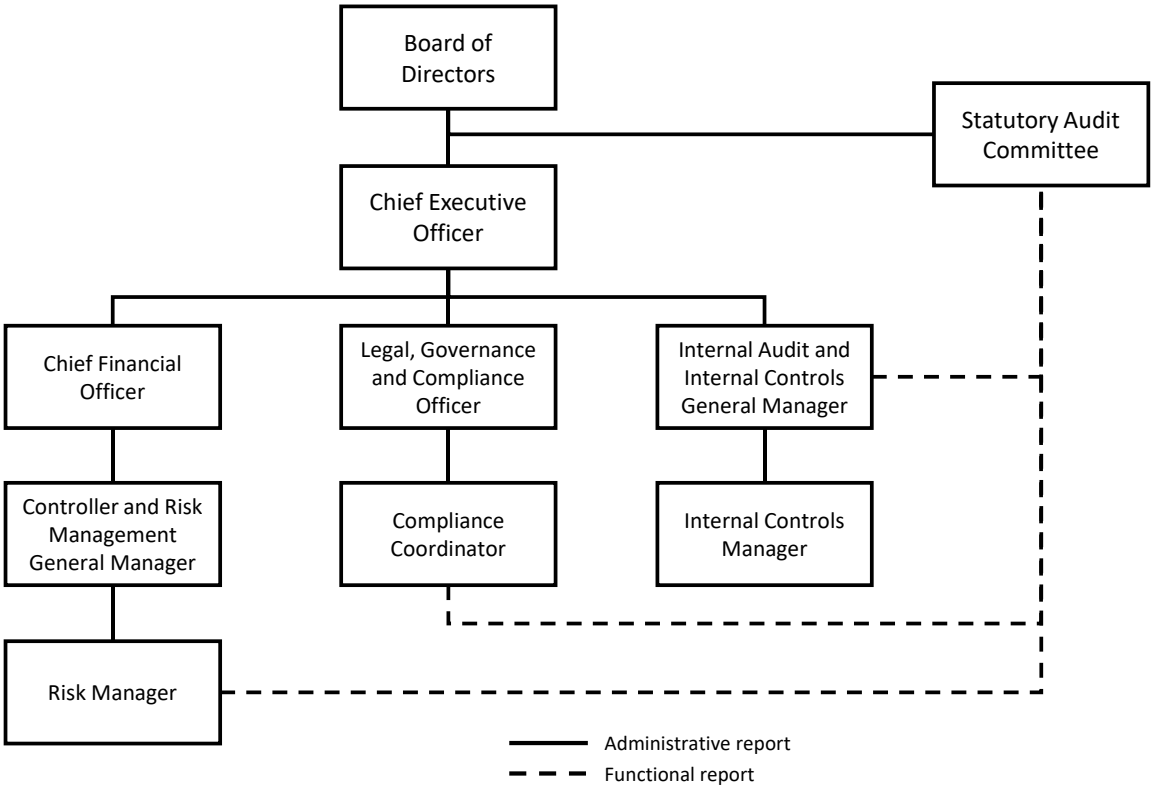
The recording and reporting stage of risk management involves activities conducted throughout the entire Risk Management process and consists of the continuous documentation and sharing of information related to identified risks and their treatments with the various stakeholders.

Reporting should be clear, concise, relevant, consistent, and timely to ensure that all individuals involved in the Risk Management process are aware of the risks and their treatments.

Information must be accessible to stakeholders so that all involved parties understand their roles and responsibilities and have a solid foundation to act effectively and efficiently within the process.

7. RISK MANAGEMENT RESPONSIBILITIES

The roles and responsibilities for risk management at CBA are based on The Institute of Internal Auditors' Three Lines Model, as outlined in the organizational chart and table below:



RESPONSIBLE	ACTIVITY
A. Board of Directors	**1.** Approve this Policy. **2.** Determine and approve the Risk Appetite for CBA, as well as the Tolerance ranges for deviations from the Risk Levels deemed acceptable. **3.** Systematically oversee risk management and the achievement of objectives. **4.** Periodically reassess the adequacy of the risk management strategy adopted by CBA. **5.** Review the portfolio of critical risks and, if necessary, high risks identified by CBA management. **6.** Verify whether Risk Owners are addressing risks and what mitigation actions are being taken. **7.** Receive reports from the Statutory Audit Committee on the activities of the Risk Management Department, and evaluate, at least annually, whether the structure and budget of this department are sufficient for the performance of its functions.

B. Statutory Audit Committee, Advisory Body to the Board of Directors	**1.** Support and promote the dissemination of a risk management culture. **2.** Decide on the standards for the risk management process (methodology, systems, reporting mechanisms, etc.) and, if necessary, request adjustments. **3.** Evaluate this Policy, the methodology, and the procedures for risk management, requesting adjustments if needed, monitoring compliance, and assessing performance against the approved risk limits. **4.** Validate the annual planning of the Risk Management Department and, if necessary, request adjustments and monitor the execution of its tasks. **5.** Systematically oversee risk management and the achievement of objectives. **6.** Supervise the initiatives of the CBA Risk Management Department. **7.** Assess the effectiveness and adequacy of the risk management system. **8.** Recommend Risk Appetite to the Board of Directors, as well as the Tolerance ranges for deviations from the Risk Levels. **9.** Evaluate and monitor the Company's risk exposures.
C. Executive Management	**1.** Promote a risk management culture within CBA. **2.** Ensure the implementation of an effective risk management model aligned with CBA's strategy. **3.** Provide the necessary resources for effective risk management operations. **4.** Promote the integration of risk management with CBA's management and governance processes. **5.** Propose Risk Appetite to the Statutory Audit Committee and the Board of Directors, as well as the Tolerance ranges for deviations from Risk Levels. **6.** Review risks assessed by Risk Owners. **7.** Supervise whether Risk Owners are addressing risks and the treatments being implemented. **8.** Discuss with Risk Owners the exposure to major risks and monitor actions taken to control such exposures. **9.** Manage and monitor Risk Appetite and Tolerances.
D. Risk Management Department, whose members do not perform operational functions	**1.** Promote the risk management culture at CBA. **2.** Coordinate the risk management process at CBA and ensure proper information flow and reporting within the Company. **3.** Develop and apply the risk management strategy and methodology, in compliance with current regulations and best market practices. **4.** Propose the Risk Appetite to the Executive Management and the Statutory Audit Committee, as well as the tolerance ranges for deviations from acceptable Risk Levels. **5.** Review the Risk Appetite at least once a year. **6.** Provide the tools for risk management at CBA and ensure their functionality. **7.** Review and monitor the risks reported by Risk Owners. **8.** Monitor the status and implementation of action plans developed in

	response to risk treatments. **9.** Present and report the level of risk exposure at CBA to the Executive Management, Statutory Audit Committee, and Board of Directors. **10.** Track market trends and connect them with business impacts and potential effects for CBA. **11.** Train employees and promote adherence to the methodology adopted by CBA. **12.** Ensure the maintenance of the Risk Management Policy and verify compliance with established limits. **13.** Advise risk-focused areas/business units on identifying and assessing diverse types of risks.
E. Risk Owner	**1.** Ensure that risk management, at various levels, aligns with CBA's strategy. **2.** Act as the direct responsible party for risk management in the Risk Specialist Areas and be accountable for the status of identified risks in their area. **3.** Identify, analyze, and evaluate, at least annually, the risks that may affect the strategic objectives of the areas/business units under their responsibility. **4.** Define the response to each risk under their responsibility. **5.** Promote risk treatment, considering the implementation, deadlines, effectiveness of mitigating actions, and monitoring residual risks. **6.** Validate and provide, whenever requested, information to the Risk Management area. **7.** Report, whenever requested, to governance forums on the risks under their responsibility.
F. Facilitator	**1.** Assist the Risk Owner in the identification, analysis, evaluation, treatment, monitoring, recording, and reporting of risks. **2.** Coordinate stakeholders in the identification, analysis, evaluation, treatment, and monitoring of risks. **3.** Periodically review risk information. **4.** Monitor the status of action plans with those responsible for their implementation. **5.** Report, whenever requested, to the Risk Management Department on the status of the respective action plans.
G. Specific Risk-Oriented Areas (Internal Controls, Compliance, Market Risks, Information Security, Sustainability, Environment, Health, and Safety)	**1.** Operate within the risk management guidelines established by the Risk Management Department. **2.** Define methodologies, minimum technical, technological, and management standards, as well as Risk Indicators to be adopted by other areas. **3.** Equip and train other areas, supporting their development in managing specific risks. **4.** Define the prioritization of critical control elements and assess their integrity. **5.** Support the identification, analysis, and evaluation of risks, as well as provide recommendations and support for the implementation of controls. **6.** Evaluate the effectiveness of controls related to significant potential

	risks, performed by areas that provide products and services to clients.
H. Internal Audit	**1.** Evaluate the risks managed by the Risk Owners and, when necessary, recommend improvements in risk management. **2.** Audit the Risk Management process at least every three years, assessing its quality, and provide an independent opinion on the effectiveness of risk management, internal controls, and compliance.

8. GENERAL INFORMATION

It is the responsibility of the areas involved in the Risk Management process to communicate any changes in the Risk Management process to the Risk Management Department. Exceptions to what is established in this Policy must be approved by the Board of Directors of ABC.

The specific procedures and details of the Risk Management process, as well as the methodologies used by ABC, are described in the ABC Risk Management Managerial Standard.

This Policy should be reviewed every three years or as needed.

This Policy becomes effective on the date of its approval and may only be amended by resolution of the Company's Board of Directors. It can be consulted at https://ri.cba.com.br/en/esg/bylaws-and-policies/