Transformamos el presente.
Fortalecemos el mañana.

Risk Management and Internal Control Policy

Approved by the Board of Directors of CELSA STEEL on October 30, 2025.

Table of Contents

1. Purpose and scope

Purpose: To establish an efficient and effective framework for identifying, assessing, controlling, and mitigating the risks faced by the organization that could prevent or hinder the achievement of the strategic objectives of the CELSA group (hereinafter "CELSA" or "Group"). This document lays the foundations for consistent, proactive, and systematic risk management within the risk tolerance and appetite thresholds established by the Board of Directors.

Due to the nature of its operations, CELSA is subject to various risks inherent in the countries, sectors, and markets in which it operates, which may prevent it from successfully achieving its strategic objectives. Therefore, this policy defines the basis of the risk management system, based on the methodological framework established in COSO (Committee of Sponsoring Organizations of the Treadway Commission) III - Enterprise Risk Management Framework[1], as a reference standard, adapted to the specific needs of CELSA.

Scope: applicable to all entities, employees, and organizational levels of the Group, covering all its activities, locations, and operations. In those investee companies where this document may not be applicable, the *Internal Audit & Risk Control* area will promote principles consistent with those established in this document, always maintaining the necessary mechanisms to ensure adequate control.

2. Definitions

For clear and uniform application of the policy, the following definitions are established:

- **Risk:** An event or set of circumstances that could negatively impact the organization, affecting the fulfillment of its strategic objectives. Risks can be accepted, avoided, transferred, or mitigated. Each risk has one or more distinct characteristics and requires specific management. At CELSA, we group them according to their nature into four main categories:

[1] https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf

- **Strategic Risks**: arising from CELSA's strategic position in the environment in which it operates, its relationships with third parties, the planning and organization of its personnel, and events that could negatively affect the fulfillment of the objectives defined in the strategic plan.
- **Operational Risks**: referring to direct or indirect economic losses caused by inadequate internal processes, technological failures, human error, or because of external events, including natural disasters, disruption to the supply chain, and information technology.
- **Financial Risks**: associated with changes in the financial and/or goods and services markets that affect the costs and revenues of the activity, including exchange rate management, liquidity risk, interest rate risk, or credit risk related to the possibility of a counterparty defaulting on its payment obligations.
- **Compliance Risks**: associated with non-compliance with legal or contractual provisions or standards and codes of conduct applicable to the activity, which may lead to penalties and/or damage to reputation, thereby causing an adverse impact on the Group's results.

- **Risk Appetite:** Level of risk that an organization is willing to assume to achieve its strategic objectives.
- **Risk Tolerance:** Acceptable margin of variation with respect to the level of risk that the organization is willing to bear in achieving its objectives. It represents the limit where risk can fluctuate without triggering an immediate corrective response and is defined in terms of risk appetite.
- **Controls:** Measure, action, or mechanism implemented to mitigate (preventive or detective) a risk event, reducing its probability of occurrence or impact on the organization.
- **KPI (Key Performance Indicator):** Quantitative metric used to evaluate the performance of an activity, process, or area in relation to an objective or the performance of an area.
- **KRI (Key Risk Indicator):** Quantitative metric that allows the probability of occurrence or potential impact of a risk to be anticipated. It is used as an early warning signal to detect deviations that could indicate the potential materialization of a risk, allowing for anticipatory decision-making.

3. General principles

1. **Risk management is part of the strategy for achieving objectives,** including the process of identification, assessment, and mitigation, based on the risk appetite defined by the Board of Directors. Each area must follow the

guidelines established in CELSA's risk model to ensure the consistency and integrity of the Group's risk management.

2. **Protecting the value chain, people, assets, the environment, and reputation** through the development of mechanisms and processes that enable risks to be mitigated efficiently, within defined tolerance margins. This includes the proactive assessment and mitigation of risks, as well as the definition of contingency, resilience, and crisis management plans that enable CELSA to reduce the effect of a materialized risk, both in terms of probability and impact.
3. **Preserving the continuity, reliability, and integrity of information** provided to shareholders and any other interested parties. The implementation of internal controls that ensure the reliability, integrity, and traceability of information (financial and non-financial) is essential to meet the expectations of regulators and/or stakeholders in the Group. Each area will lead the deployment of the applicable mitigating controls under its responsibility, as well as coordination with the other areas to which they apply.
4. **Establish a single assurance model and a common language** throughout the organization to manage risks, ensuring the integration and coexistence of the corporate risk map, together with specific detailed/area-specific risk maps. Each organizational area is responsible for managing its risks and may rely on the corporate risk management team to ensure consistency in reporting to both the management team and the Board of Directors.
5. **Promote proactive and integrated management in decision-making**, assessing both risks and opportunities, both when defining strategic objectives and when making decisions to achieve them, in line with the guidelines of environmental, social, and governance (ESG) risk management models.
6. **Promote training, awareness, and monitoring in risk management as part of continuous improvement**, improving the effectiveness and efficiency of controls through the assurance (audit) function, mitigating or transferring risks, and proactively and preventively assessing CELSA's ability to respond to disruptive impacts on its value chain. This includes defining score and dashboards with key performance indicators (KPIs) and key risk indicators (KRIs) to monitor the evolution of risks and make decisions in accordance with risk appetite.

4. Roles and responsibilities

To ensure its proper functioning, CELSA's risk management has an integrated governance framework based on the three lines model, considered best practice in commonly accepted models worldwide, which provides segregation between the functions of risk design, execution, and supervision.

All CELSA members are responsible for understanding and implementing this policy within their area of responsibility. In addition, the following responsibilities are defined in the model:

Board of Directors:

- Approve and supervise the implementation of the Risk Management and Control Policy, which defines the risk management strategy, as well as approve and monitor the evolution of risk appetite.

Audit and Control Committee:

- To supervise the proper functioning of the risk management and internal control system.
- Regularly report to the Board of Directors on the most relevant aspects related to the supervision of CELSA's risk management model.

Management Committee and CEO

- Lead the design, implementation, and monitoring of the risk management system, as well as lead the risk management strategy, in accordance with the risk appetite defined by the Board of Directors.
- Validate the policies that develop risk management and control in each of its areas of responsibility.
- Provide sufficient resources to implement risk mitigation plans, in line with CELSA's risk appetite.

Area managers and management team

- Understand, assess, and monitor the risks that form part of their area of responsibility, ensuring that CELSA's risk maps are kept up to date, in accordance with the methodology established by the risk and control area.
- Ensure that risk mitigation controls are adequately designed and, if not, lead the implementation of the necessary remediation plans.

Risk and control team

- Supervise, integrate, and coordinate all CELSA risk maps, ensuring consistency and coherence between them and guaranteeing a unified reporting source.
- Support the Management Committee in the analysis of risks, controls, and action plans, as well as in monitoring and reporting on the evolution of the model to the Board of Directors and the Audit and Control Committee.
- Support all teams that manage risks within the Group, ensuring consistent assessment and treatment through training or assistance in the design of their models.

Internal Audit

- Independently and objectively evaluate the operational effectiveness of CELSA's risk management and control system, and periodically report to the Audit and Control Committee and the Management Committee on any weaknesses detected and proposed corrective measures.

5. Approval, communication, and updating

This policy will be reviewed periodically to ensure its relevance and effectiveness, at least every 12 months, or more frequently if circumstances require.

To ensure its proper implementation and compliance, this policy will be disseminated internally and externally through the Group's website. In addition, appropriate measures will be taken to promote awareness and ensure compliance by all areas involved.

6. References and annexes

This Risk and Control Policy constitute the general framework for risk management and internal control and articulates the various specific procedures detailed below:

- *Risk identification, assessment, and analysis procedure*
- *Counterparty risk management procedure*
- *Internal Control System Procedure for Financial and Non-Financial Information (SCIIF and SCIINF)*
- *Resilience and Business Continuity Procedure*
- *General crisis management plan procedure*