

PREPARED BY:
Strategic Management Control Manager

REVIEWED BY:
Audit and Risk Committee
Chief Executive's Office
General Management

APPROVED BY:
Board of Directors

Code: GE-P001
Version: 01
Approved: June 23, 2023

CORPORATE POLICY OF INTERNAL CONTROL AND INTEGRAL RISK MANAGEMENT

1. OBJECTIVE

Define our Corporate Policy for Internal Control and Comprehensive Risk Management in the company, considering the criteria and framework for action to develop, strengthen and maintain an internal control and comprehensive risk management system that helps the company meet its organizational objectives.

2. SCOPE

The application of this policy is applicable to all members of Corporación Aceros Arequipa and Subsidiaries (hereinafter CAASA).

3. REASON

Model of the Three Lines

Internal control and risk management are carried out by all members of the company; Board of Directors, Senior Management, Managers, Assistant Managers, Heads, Collaborators and the Internal Audit area. We understand that, according to the COSO framework, internal control is performed through three lines of defense¹:

- **First line of defense:** Process Owners and Collaborators, responsible for maintaining an effective and efficient internal control system.
- **Second line of defense:** The support areas, such as Quality Management, Environment, Occupational Health and Safety, Legal Services, Property Security, Quality Control, Budget Control, Inventory Control, among others, supervise compliance with the control guidelines that we have established.
- **Third line of defense:** The Internal Audit area is responsible for evaluating the organization's internal control system and recommending corrective measures or improvements, which may be taken into consideration by the Process Owners. His position is independent of the business areas that will be the subject of his analysis.

¹COSO "Internal Control – Integrated Framework 2013" / page 147

Each of the people that make up our organization fulfills a function within the internal control and comprehensive risk management system, the main responsibilities being the following:

3.1 Board of Directors

It is responsible for approving the internal control and comprehensive risk management policy and defining the corresponding roles, responsibilities and reporting lines. As well as supervising its effectiveness and suitability², for this purpose, assigns direct responsibility for risk management and the implementation, maintenance and permanent updating of internal control systems to the Executive Presidency and General Management.

Likewise, it delegates to the Audit and Risk Committee (CAR) the evaluation of the effectiveness of the internal control system³ and risk management

3.2 Audit and Risk Committee (CAR)

It is responsible for ensuring that CAASA has an effective internal control system and that policies and procedures are implemented to ensure adequate risk management, ensure compliance with corporate codes and policies approved by the Board of Directors, periodically monitor management of risks and report it to the Board of Directors, and consider the effectiveness of CAASA's internal control over annual and interim financial information, including information technology security and control⁴.

3.3 Executive Presidency

In coordination with the General Manager, defines the Corporate Strategic Plan, determines the short, medium and long term objectives⁵, identifies risks at the entity level and assists in the implementation of strategies to mitigate them. He is responsible for promoting a risk management culture within our company.

²Code of Good Corporate Governance for Peruvian Companies. 2013 – “Principle 25” / page 14

³CAASA's Internal Audit Activity Statute. Sep 2020 – “Scope” / Page 1

⁴Statute of the Audit and Risk Committee / page 4

⁵Aceros Arequipa SA Corporation Statute – “Article 63” / Page 16

Annually, in conjunction with the General Management, presents to the Board of Directors our strategic plan and the main risks to which the business is exposed (strategic risks at the entity level).

3.4 General management

It is responsible for designing, implementing, maintaining and supervising the internal control system and managing the risks to which we are exposed. The responsibilities of the General Manager, in relation to internal control and comprehensive risk management include⁶:

- Define the objectives and goals, the structure of the organization, the delegation of powers, the internal regulations (business policies, codes, guidelines, among others) and the supervision of the results of the officials and collaborators.
- Supervise internal control activities and comprehensive risk management at the Corporate level, assigning the Macroprocess Owners the responsibility for identifying risks and the design, implementation and evaluation of the effectiveness of the controls established in each of their processes.
- Periodically validate with the Board of Directors the risks at the entity level, the associated control activities and the required action plans.

3.5 Macroprocess Owners

Assigned to Managers who have adequate experience and professional judgment for the management of the operational and support processes for which they are responsible, their responsibilities include:

- Supervise the implementation of internal regulations (corporate policies, codes and regulations), as well as define the procedures, instructions and guidelines for the fulfillment of the objectives of its operational or functional units.
- Guarantee that processes are designed to achieve business objectives, minimizing losses and optimizing the use of resources.

⁶COSO "Internal Control – Integrated Framework. 2013" / page 149

- Ensure the implementation and maintenance of comprehensive risk management in the processes under their responsibility, under the GIRO methodology.
- Supervise the control system defined in its processes.

3.6 Process / Sub-Process Owners

Responsibility for our Processes and Sub-Processes is assigned, depending on the degree of complexity and impact on business objectives, to: Managers, Assistant Managers, Supervisors and Supervisors who have experience and adequate professional judgment, their responsibilities include:

- Strengthen the execution of the processes under their responsibility, seeking efficiency and effectiveness in their operations and the fulfillment of business objectives.
- Measure the performance of the process and be accountable for the results achieved.
- Identify and evaluate the risks inherent to the activities of the processes under their responsibility, and define sufficient controls for their administration, in accordance with the GIRO methodology.
- Execute monitoring activities to ensure the correct design and operation of the implemented controls.
- Keep the documentation of your process updated: i) Flowchart, ii) Matrix of risks and controls, and iii) Matrix of segregation of functions (if applicable).

3.7 All Collaborators

- Comply with internal policies, procedures and standards within the scope of our roles and responsibilities.
- Report the identification of new risks or materialization of any risk to the corresponding Process Owner or Sub-Process.
- Report to your direct boss or manager any breach of internal rules, regulations or laws within the framework of CAASA operations.
- Report through the ethics line any breach or suspected breach of the guidelines of our code of ethics and code against acts of fraud and corruption.

3.8 Management Strategic Control Management

- Define and update the risk management methodology considering the reference frameworks, good practices and standards of the external framework, ensuring its continuous improvement.
- Assist Senior Management, Process Owners and collaborators in the deployment of the risk management methodology to identify, analyze, control and monitor risks at the entity and process level.
- Report to the Audit and Risk Committee (CAR) the progress in the implementation and strengthening of the CAASA risk management system.

3.9 Internal audit

Performs audit work exclusively, has autonomy, experience and specialization in the issues under its evaluation, and independence for monitoring and evaluating the effectiveness of the internal control system.

The Internal Audit Manager reports directly to the Audit and Risk Committee (CAR) on its plans, budget, activities, progress, results obtained and actions taken. The Internal Audit Manager reports organizationally to the Board of Directors, so his appointment and dismissal correspond to the Board of Directors at the proposal of the Audit and Risk Committee (CAR)⁷.

4. REGULATORY OR REFERENCE FRAMEWORK

4.1 Corporate Framework

The Internal Control and Comprehensive Risk Management Policy is framed within:

- The Vision, to the extent that we propose to be recognized as the leading Steel Group in the national steel market, located among the most profitable in the region and with an active presence in the foreign market.

⁷CAASA's Internal Audit Activity Statute. Set 14 – “Authority and Independence” / Pages 1 and 2

- The Mission, by offering steel solutions to our clients, through innovation, continuous improvement and human development, contributing to the growth of the countries in which we participate and increasing value for our shareholders and interest groups.
- Corporate Values, teamwork, passion for work and focus on what is relevant.
- The Code of Ethics, where the philosophy and principles that govern us are detailed, which serve as a guiding element in the relationship with the various interest groups.
- The Code against acts of fraud and corruption, which communicates the guidelines and responsibilities assigned to prevent, detect, investigate and respond to any act of fraud and corruption, maintaining a culture of zero tolerance for any illegal act.
- The corporate policies mentioned in annex 1 that allow us to comply with the sustainable management of the business and the generation of shared value.
- The Good Corporate Governance Practices, that promotes a climate of respect for the rights of shareholders and investors in general; It contributes to generating value, solidity and efficiency in the company

4.2 Methodological and Conceptual Framework

We adopt the following conceptual frameworks:

- The Internal Control reference framework (2013) and the integrated Risk Management framework - ERM (2017) of COSO (Committee of Sponsoring Organizations of the Treadway Commission). COSO is recognized globally as the leading framework for designing, implementing and developing internal control and evaluating its effectiveness.
- The position statement of the Institute of Internal Auditors - IIA (for its acronym in English): The three lines of defense for effective risk management and control.

Additionally, for specialized functions, we complement the adoption with other reference frameworks such as ISO 31000, COBIT 5 for the management of Information Technology, the Code of Good Corporate Governance issued by the Superintendency of Stock Market (SMV), etc.

4.3 Corporate Policies

The Internal Control and Comprehensive Risk Management Policy is developed and complemented by our Corporate Policies and Codes. These are approved by the Board of Directors in order to strengthen the internal control environment of the Corporation (See Annex I: List of Corporate Policies and Codes).

4.4 TFCF (Task Force on Climate-related Financial Disclosures)

It is an international initiative that establishes recommendations for companies to disclose climate-related financial information, allowing them to evaluate and manage the risks and opportunities associated with climate change in their operations and strategies.

Our methodology focuses on classifying the risks and opportunities in the face of climate change taking into account what is proposed by the TCFD, which are classified as:

- Physical risks: They refer to natural disasters or environmental events caused by climate change.
- Transition risks: They refer to changes in policies, legislation, technology and the market for the mitigation of climate change.

5. DEFINITIONS

5.1. Risk

Uncertainty that a fact or event may adversely impact the achievement of our objectives.

5.2. Control

Measure or activity adopted to mitigate the impact and/or reduce the probability of occurrence of risks. The design of the control must contemplate an evaluation of the cost and benefit of its implementation, in addition each control must leave a minimum record or evidence that it is operating as it was designed.

5.3. Internal control

It is a process carried out by the Board of Directors, Senior Management, Process Owners and Collaborators, designed with the objective of providing reasonable, not absolute, security regarding the achievement of business objectives.

5.4. Risk appetite

Degree of tolerance or level of exposure (criticality) to the risk that the organization is willing to accept in the search for value. To do this, define risk response strategies.

5.5. Chance

Action or potential action that creates or alters the objectives and/or approaches for create, preserve and materialize value.

6. INTERNAL CONTROL GUIDELINES

6.1 By adopting this policy, we seek the following results:

- Self control: Capacity of each collaborator to control their work, detect deviations and carry out corrective actions.
- Effectiveness: Degree of completion of planned activities and obtaining of results.
- Efficiency: Rational and optimal use of resources.

6.2 professional judgment

The internal control system requires the application of professional judgment when designing, implementing and executing the control activities under its responsibility. That is why we must have collaborators who meet the appropriate profile for positions of greater risk and responsibility.

6.3 Internal Control System Documentation

We have a process documentation methodology that describes the information requirements of each process. These information requirements include documentation of a risk and control matrix and evidence of compliance therewith.

7. INTEGRAL RISK MANAGEMENT GUIDELINES

7.1 Risk Classification

Risks can be classified in three ways: (a) By the objectives they affect, (b) By their origin and (c) By the level in the organization.

a. For the objectives⁸ that affect:

- Strategic risks: They impact the achievement of our vision, mission and strategic objectives. They are related to (a) price volatility and market variables, (b) environmental uncertainty, (c) regulatory changes, (d) responsiveness to industry changes, (e) misapplication of decisions strategies, among others. Our main tool to mitigate these risks is the Strategic Control Cycle and the Corporate Strategic Plan.
- Operational risks: They impact the effective use of company resources, and that these are properly guarded, due to (a) inadequate processes, (b) personnel or information technology failures, or (c) external events.
- Information risks: They impact the integrity of the financial and non-financial information, both internal and external, used or issued to the various stakeholders.
- Compliance risks: They impact compliance with applicable external (legal and sectorial standards) and internal (eg Codes, corporate policies, RIT, among others) regulations.

b. By its origin:

- external: risks that come from the environment.
- internal: risks that are generated in our processes.

c. By level in the organization:

- Entity Level: risks that affect the achievement of our Strategic Objectives.
- Process Level: risks that affect the achievement of the objectives of a specific process.

7.2 Risk assessment

The evaluation criteria allow us to measure and prioritize risks throughout our Corporation and are of at least two types: (a) Impact and (b) Probability (See Annex II: Risk evaluation criteria).

⁸Enterprise Risk Management (2017) – Integrated Framework – / page 11

- a. Impact:** It refers to the extent to which a risk event could affect us. Impact assessment criteria include: (i) Economic loss, (ii) Impact on operations and information systems, (iii) Impact on reputation and image, (iv) Regulatory and legal impact (includes ethical and corruption impact), (v) Environmental impact and (vi) Impact on Occupational Health and Safety.
- b. Probability:** It refers to the number of times that the risk could materialize in a period. The probability evaluation criteria are (i) Frequency, (ii) Exposure and (iii) Estimation of occurrence (experience and professional judgment).

In some areas or sub-processes, additional criteria could be considered to complement the analysis and evaluation of the impact or the probability of occurrence of risks, especially in the case of natural disasters or when it is necessary to comply with external norms and regulations, such as: the exposure to risk, reversibility, speed of occurrence (latency), vulnerability, among others.

8. INTERNAL CONTROL COMPONENTS AND COMPREHENSIVE RISK MANAGEMENT

By adhering to the COSO model, we declare compliance with the internal control principles for each component:

8.1 Control Environment

It is the set of rules, processes and structures that constitute the basis of internal control of the company.

The principles of this component are⁹:

- a. We demonstrate commitment to integrity and ethical values.
- b. The Board demonstrates independence from Senior Management and exercises supervision of the performance of the internal control system, through the Audit and Risk Committee.
- c. The Senior Management establishes, with the supervision of the Board of Directors, the structures, reporting lines and levels of authority and responsibility appropriate to achieve the objectives of the company.

⁹COSO "Internal Control – Integrated Framework. 2013" / page 31

d. We demonstrate commitment to attract, develop and retain competent professionals in line with the company's objectives, in accordance with the Human Management policy.

e. We define the responsibilities of people and the level of internal control to achieve the company's objectives.

8.2 Definition of objectives

The definition of strategic objectives is a precondition for event identification, risk assessment and risk response. First, the strategic objectives must be defined, before identifying the risks that the organization faces and defining the actions necessary to manage them¹⁰.

This is how we define and update our corporate objectives through the annual Corporate Strategic Planning meetings.

8.3 Event Identification

The Board of Directors and Senior Management recognize that uncertainty exists, therefore, there is no certainty of when an event with negative or positive effects may occur during the course of operations. During his tenure, Senior Management considers a series of potential events, affected by both internal and external factors. If the event may have a negative impact, it represents a risk, whereas events with a potential positive impact may represent opportunities for us. Management must manage both risks and opportunities and define actions and provide resources to mitigate risks and take advantage of opportunities¹¹.

8.4 Risk assessment

Risk assessment allows us to take into account the degree to which potential events could have an impact on the achievement of our strategic objectives. This evaluation is carried out from two perspectives: probability and impact¹²; using a qualitative and quantitative combination of methods.

a. We define and identify our objectives with sufficient clarity to allow the identification and evaluation of risks.

¹⁰Enterprise Risk Management – Integrated Framework – page 21

¹¹Enterprise Risk Management – Integrated Framework – / page 37

¹²COSO “Internal Control – Integrated Framework. 2013” / page 59

- b. We identify the risks to achieve our strategic objectives and analyze them to determine how they should be managed.
- c. We consider the probability of fraud, corruption and any other event that violates ethics and integrity when evaluating the risks for the achievement of objectives.
- d. We identify and evaluate changes that could significantly affect the internal control system.

8.5 Risk Response

After evaluating the relevant risks and based on the company's risk appetite, Senior Management and Officials determine the response strategy. These strategies can be those of accepting, mitigating, sharing or avoiding. When considering the strategy, its effect on the probability and impact of risk is evaluated, as well as the costs and benefits, and the one that places the residual risk within the tolerance level established according to the risk appetite of the company is selected¹³.

8.6 Control Activities

Depending on their nature, controls can be preventive or detective and can include manual, semi-automatic and automatic activities. The principles of this component are¹⁴:

- i. We define and develop control activities in business processes that contribute to mitigating risks to acceptable levels.
- ii. We define and develop control activities in information systems that contribute to IT risk management.
- iii. We deploy control activities through policies and codes that establish the general lines of internal control and procedures or instructions that put said policies and codes into practice.

Segregation of duties is integrated into the design and development of control activities. In those areas where it is not practical to carry out a segregation of duties, the Process Owner selects and develops alternative control activities with which compliance is mandatory.

¹³Enterprise Risk Management – Integrated Framework – / page 81

¹⁴COSO “Internal Control – Integrated Framework. 2013” / page 87

8.7 Information and communication

We have various internal and external communication channels with interested parties to ensure compliance with business objectives and reinforce internal control systems. According to the COSO framework¹⁵:

- a. We obtain, generate and use relevant and quality information to support the operation of the internal control system.
- b. We communicate information internally, including the objectives and responsibilities that are necessary to support the functioning of the internal control system.
- c. We communicate with external stakeholders about key issues affecting the operation of internal control and our codes of conduct.

8.8 Supervisory Activities

For us, continuous evaluations (ISO audits, Legal Requirements Compliance Audits, product quality controls, budget control, occupational health and safety supervision, environmental inspections, etc.), independent evaluations (internal and external audits) or a combination of both, are used to determine whether each of the components of internal control and the controls to comply with the principles of each component are present and functioning properly. The principles of this component are¹⁶:

- a. We select, develop and carry out continuous and/or independent evaluations to determine if the components of the internal control system are present and functioning.
- b. The results of the evaluations are communicated to us in a timely manner to apply corrective measures.

¹⁵COSO "Internal Control – Integrated Framework. 2013" / page 105

¹⁶COSO "Internal Control – Integrated Framework. 2013" / page 123

9. INTERNAL CONTROL LIMITATIONS

Internal control, regardless of how well designed, implemented and developed it may be, can only provide reasonable and not absolute assurance to the Board of Directors and Senior Management regarding the achievement of our objectives. The likelihood that the objectives will be achieved will be affected by the limitations inherent in all internal control systems. These limitations include the fact that professional judgement/judgment may be deficient when making decisions, the impact of external events beyond the control of the company and human errors¹⁷.

10. VALIDITY AND REPEALS

This Policy was initially approved at the Board of Directors meeting held on January 26, 2017 and modified on June 23, 2023. This Policy is effective from the date of its approval.



¹⁷COSO "Internal Control – Integrated Framework. 2013" / page 13705

ANNEX I: List of Codes and Corporate Policies

Code of ethics
Code against Acts of Fraud and Corruption
Corporate Investment Policy
Corporate Inventory Policy
Corporate Policy for the Purchase of Goods and Services
Corporate Policy for Internal Control and Comprehensive Risk Management
Corporate Fixed Asset Policy
Corporate Credit and Collection Policy
Corporate Information Policy
Corporate Human Management Policy
Corporate Human Rights and Diversity Policy
Corporate Tax Management Policy
Corporate Tax Strategy Policy
Corporate Occupational Health and Safety Policy
Corporate Environmental Policy
Corporate Social Responsibility Policy

Note: This information is referential. Up-to-date corporate codes and policies can be found on our intranet or the Goldenbelt tool.

ANNEX II: Risk assessment criteria

Impact	Low	Moderate	Considerable	High
Economic (Operating Ut. > 50 MM) <i>Applicable if Average Operating Income of the last 3 years is greater than 50 million soles</i>	<ul style="list-style-type: none"> Less than 0.25% of the average Operating Profit of the last 3 years. 	<ul style="list-style-type: none"> Between 0.25% and 0.5% of the average Operating Profit of the last 3 years. 	<ul style="list-style-type: none"> Between 0.5% and 1% of the average Operating Profit of the last 3 years. 	<ul style="list-style-type: none"> Greater than 1% of the average Operating Profit of the last 3 years.
Economic (Oper. Ut. < 50 MM) <i>Applicable if Average Operating Income of the last 3 years is less than 50 million soles</i>	<ul style="list-style-type: none"> Less than 250 thousand soles. 	<ul style="list-style-type: none"> Between 250 thousand and 500 thousand soles. 	<ul style="list-style-type: none"> Between 500 thousand and 1 million soles. 	<ul style="list-style-type: none"> Greater than 1 million soles.
Impact on operations and information systems (qualitative)	<ul style="list-style-type: none"> Interruption of operations less than 1 hour. The integrity and/or timeliness of the information is not affected. 	<ul style="list-style-type: none"> Interruption of operations between 1 and 8 hours. The integrity and/or timeliness of critical information is affected 	<ul style="list-style-type: none"> Interruption of operations between 8 and 24 hours. Loss of non-critical CAASA or third party information that cannot be recovered 	<ul style="list-style-type: none"> Interruption of operations greater than 24 hours. Loss of critical CAASA or third party information that cannot be recovered
Impact on reputation and image (qualitative)	<ul style="list-style-type: none"> Minimum public knowledge and low or null responsibility of the company. 	<ul style="list-style-type: none"> Moderate public knowledge. There may be liability. 	<ul style="list-style-type: none"> Wide media coverage. Perception of company responsibility. 	<ul style="list-style-type: none"> massive public knowledge and wide frequency or permanence in the media. Receive political interest. Perception of company responsibility.
Regulatory and legal impact (qualitative)	<ul style="list-style-type: none"> could generate non-compliance with internal or legal, sectoral, labor or tax regulations. 	<ul style="list-style-type: none"> originates non-compliance with internal or legal, sectoral, labor or tax regulations, but does not generate payment of penalties. 	<ul style="list-style-type: none"> Failure to comply with legal, sectoral, labor or tax regulations, determines the payment of penalties. Ethical offenses that do not comply with internal regulations, do not incur a crime. 	<ul style="list-style-type: none"> Severe non-compliance with legal, sectoral, labor or tax regulations, determines the payment of penalties, could generate criminal sanctions for the entity or representative, and/or the intervention of the regulator. Ethical misconduct in a systematic way that fails to comply with internal regulations and/or commits a crime.
Environmental Impact (Nature of the event/affect)	<ul style="list-style-type: none"> The scope of the impact is at the activity level. Affectation of environments and infrastructure of the company that is on pavement. 	<ul style="list-style-type: none"> The scope of the impact involves the entire process. Affectation of 1 environmental factor (Air, Soil, Water, Flora and Fauna) 	<ul style="list-style-type: none"> The scope of the impact involves other processes. Affectation of 2 or more environmental factors (Air, Soil, Water, Flora and Fauna) 	<ul style="list-style-type: none"> The scope of the impact extends beyond the limits of the company. Affectation of the sensitive natural environment or population (nature reserves)
Occupational Health and Safety (Nature of the incident and damage)	<ul style="list-style-type: none"> Very minor injuries, may cause discomfort or discomfort 	<ul style="list-style-type: none"> Minor injuries, without sick leave, without disability, may require first aid. 	<ul style="list-style-type: none"> Temporary disability. Reversible damage to health. 	<ul style="list-style-type: none"> Permanent total or partial disability Irreversible/fatal damage

Probability	Low	Moderate	Considerable	High
Frequency	It has never happened. Less than 0.5% of cases / transactions.	During the last year the event has not occurred, but it has occurred before. Between 0.5% and 1% of cases / transactions.	During the last year the event has occurred once. Between 1% and 5% of cases / transactions.	During the last year the event has occurred more than once. Greater than 5% of cases / transactions.
Exposure	Continuous exposure, below 50% of the acceptable limit.	Continuous exposure, between 50% and 75% of the acceptable limit.	Continuous exposure, between 75% and 100% of the acceptable limit.	Continuous exposure, above the acceptable limit.
Estimation of occurrence (experience and professional judgment)	Low occurrence estimate.	Estimate of moderate occurrence.	Considerable occurrence estimate.	High occurrence estimate.

