| GERDAU Shape the future | RISK MANAGEMENT POLICY |
|---|---|

## 1. OBJECTIVE

Establish corporate guidelines for risk management, scope, definitions, information flow and organizational structure to manage and report critical risks. Designate responsibility to identify and treat risks, to prevent and minimize impacts to Gerdau.

## 2. SCOPE

This Policy applies to all Gerdau Entities, Business Divisions and Corporate processes.
Includes all known risk factors monitored by the company's management team, including those described in section 4 from *Reference Form (document published on the Gerdau website and filed in Brazilian Securities and Exchange Commission - CVM).*

## 3. DEFINITIONS

a) Ethic Channel: A system available on the internet and intranet, to report complaints and ethical concerns and clarify questions related to Ethics.
b) Risk Committee: Support and advisory committee for Gerdau S.A Board of Directors. The committee is formed by CEO, Directors and Managers of the main areas that work in risk analysis (i.e. Internal Audit, Compliance, Finance, Tax, Accounting, Legal and Operations) and other invited areas, as necessary. As provided on internal regulations, the Risk Committee is responsible for, among others, advising the Statutory Board in the identification, management, and treatment for all risks categories, such as credit, market, liquidity, financial, operational, regulatory, technological, social and environmental, especially on climate change, image (reputational) and strategic.
c) Fiscal Council: An independent committee that supervises the Board of Directors and Operational Directors. The independent members are elected at the General Shareholders' Meeting and perform certain functions in alignment with the company's Audit Committee.
d) Business Division (BD): Division of the Gerdau organizational structure, defined based on geographic issues, market segments, or association with other companies.
e) Corporate Process: Processes that are centralized with defined rules and procedures that must be followed by all Business Divisions. The processes are: (a) Finance; (b) Legal; (c) People; (d) Audit; (e) IT; (f) Engineering; and (g) Industrial.
f) Risks: Factors or events that can cause impact and exposure not aligned with Gerdau's business objectives.
g) Environmental risk: Related to the exposure of the company's operations which have impacts on the environment, either by the extraction of natural resources or by the effect of productive processes on natural systems.
h) Corruption risk: Noncompliance with legal practices or company policies, procedures, and guidelines, resulting from internal or external behaviors that are illegal.
i) Strategic risks: Related to those that impact the business' goals and successes.
j) Financial risk: Related to economic performance, and linked to corporate finances, such as profitability, indebtedness, return, liquidity, indexes, etc.
k) Operational risks: Facts that can impact in losses due to failure, deficiencies or noncompliance of any internal processes involving persons or systems directly related to company operations.

l) Political risk: Related to the participation with activities, decisions, events and or political-economic conditions that can significantly affect the profitability and exposure of the company.
m) Regulatory risk: Related to the company's ability to monitor, interpret, act, and anticipate laws and regulations in the markets in which it operates.
n) Reputational risk: Damages to the company´s reputation, consequent to an adverse event even if the company is not found guilty.
o) Technological risk: Related to cyber-attacks, data leakage, and system misuse that supports administrative and operational processes.

## 4. GUIDELINES

### 4.1 Risk Identification and Treatment:

4.1.1 The Risk Management structure at Gerdau is operated in a decentralized manner, to take advantage from technical knowledge and the profile of professionals of each area. Those responsible for risk management in the BD and Corporate Processes must identify and address risks that may affect the Company's objectives. There is a consolidation of information related to critical risks treated by BD's and Corporate Processes, and a report to the Corporate Risk Committee.

4.1.2 When a risk presents the probability of high impact materialization, it is an obligation of the Processes Managers to identify controls to mitigate and monitor the risk, as well as to report all matters to the managers, upper levels as appropriate, and areas impacted.

4.1.3 Risks should be identified and evaluated, considering the probability of occurrence and the impacts on the company's business and image, as well as, being in compliance with the laws where the company conducts business. Mitigation actions must be compatible with the degree and exposure of such risk(s).

4.1.4 For operational risks, considering the analysis of cost *versus* risk exposure, the “Three Lines Model” must be established, defined by the global and independent organization “The Institute of Internal Auditors - IIA”:

a) 1st line: control environment with routine and control activities, procedures, approval levels, systemic blocks, access restriction, and reconciliations.
b) 2nd line: management activities, monitoring, process analysis, accountability, management of internal controls, and
c) 3rd line: carrying out internal and/or external audits in all processes.

4.1.5 In the 1st line is a process which must formalize routines and controls in official Guidelines, with the definition of procedures, responsibilities, and limits of approval to mitigate operational risks, financials, regulations, environmental, image and frauds.

4.1.6 In the 2nd line, in addition to the role of process managers monitoring their risks, there are support areas for improving the control environment:

- The Internal Controls area should analyze the environment of controls, processes and risks, evaluate changes, perform assessments in accordance with the Sarbanes-Oxley Act (SOX), propose improvements and report results.
- The Compliance area must ensure an integrity and compliance program for activities with exposure to risks related to ethical guidelines, non-compliance with laws, regulations, rules, and anti-corruption practices. The activity includes training for the dissemination of the Code of Ethics, Conduct and the Guidelines; records monitoring, Ethics Helpline, and periodic evaluations.

4.1.7 The company provides an anonymous and confidential Ethics Helpline , which is available to all employees and third parties, where complaints are filed and controlled by the Corporate Compliance area and handled by the appropriate area(s), with all significant occurrences reported to the Board.

4.1.8 In the 3rd line, the Internal Audit is responsible to evaluate the control environment independently, based on an annual work plan, considering, mapping and risk analysis, the results of audits performed, the results of the Sarbanes-Oxley certification tests, risk history in other locations, and information received from process managers.

4.1.9 Risks assessment must be analyzed by Business Divisions and Corporate Processes. Managers are responsible for the evaluation of internal or external risks, which can or will represent loss, impact to the company's image, strategic business plans and operations, and/or economic sustainability.

4.1.9.1 Main risks to be considered:

a) Economic: Economic Crisis / slowdown, Cyclical demand
b) Political: Government policies; Social risks; changes in laws and regulations
c) Financial: Inflation; Interest rate; Credit risk; Exchange Rate Variation; Capital management (relation between financial debts and equity); Liquidity Risk; Exposure of the capital market; Financial cost of capital
d) Strategy: Mergers, acquisitions, divestitures; new business; market and competitors; trading barriers; confidentiality of information
e) Reputation: Communication; Image; Relationship with stakeholders
f) Environmental: Environmental legislation; environmental liabilities; relationship with community
g) Operational and Technological: Supply risks; Energy; Equipment and productive capacity; Costs management; Information and Control Systems
h) Human Resources: Succession and retention; Culture and Organizational Climate; Union movements
i) Regulatory: Adherence to Laws and Regulations; Ethics and Compliance.

4.1.9.2 It is the responsibility of each area within the company's business operations, divisions, and locations to identify and monitor any potential risk of exposure, identify potential scenarios, and monitor external information which can create a risk, implement KPIs, hire technical analysts (when necessary); identify discrepancies and causes of a risk; map the organizational climate to eliminate risk exposure, and enforce company's policies, procedures, and governance structure.

4.1.9.3 Process Managers are responsible for assessing any and all risks using tools, planning, tracking budget, results and future scenario assessments.

4.1.9.4 In all new business evaluations, divestments of an operation, relevant changes in routines or objectives, revisions of plans, the responsible manager must evaluate the impacts, and identify any potential for present or future risks.

## 5. ORGANIZATIONAL STRUCTURE IN RISK MANAGEMENT

In accordance with definitions per item 4.1.1, follow the Company entities involved in the risk assessment process.

### 5.1 Business Divisions and Corporate Processes Committees

The Business Divisions, responsible for mills, mines, productive centers, and Corporate Processes have Committees composed by groups of managers responsible to report and treat critical subject and risks. In addition, they are responsible for managing the risks from their operations, ensuring proper treatment. Examples: Business Divisions Committee; Credit Committee, Finance Committee, Investments Committee, Industrial Committee, etc.

### 5.2 Risk Committee

The Risk Committee is responsible for evaluating a consolidation of the critical risks and treated in its operations (item 5.1). This Committee is responsible for ensuring that all the main Business Divisions and Corporate Processes perform their analysis and that critical risks are being adequately addressed. In addition to the assessment of this summary of the Company's risks, they are also responsible for periodically evaluating other risk indicators arising from information provided by Internal Audit, Compliance, Information Security and Legal:

- Status of assessments on controls arising from the Sarbanes Oxley Act;
- Main audit results on operational risks;
- Evolution and treatment of incidents from the Ethics Channel;
- Integrity Program and Compliance topics;
- Image risk;
- Risks related to security information;
- Legal contingencies;
- And any other identified risks that need to be reported to the Risk Committee.

### 5.1 Fiscal Council (Audit Committee)

Independent inspector committee, acting in under specific functions of the Audit Committee, attributing to those described in Article 13 of the Company's Bylaws, as well as monitoring the responsibilities and work performed of internal and external auditors, SOX results, and when appropriate, supporting risk management.

This policy was reviewed and approved at a meeting of the company's Board on May 04, 2022.

********