RISK MANAGEMENT POLICY

1. PURPOSE

Springs Global Participações SA ("Company"), with the purpose of providing greater security to its shareholders and the continuity of its business, presents its Risk Management Policy ("Policy"), aiming to formalize and disclose the principles, guidelines and responsibilities for the purpose of identifying, controlling and mitigating the risks to which the Company is exposed.

The Policy is intended to be a mechanism to help identify, assess, forecast and monitor the risks to which the Company is subject, standardizing the risk control and management activities that must be performed at all levels of the Company and in the stages of your business processes.

2. SCOPE

This Policy is applicable to the Company in all its macro-processes and operations, and its respective employees and administrators must comply with it.

3. RISK CATEGORIES

3.1 Strategic Risks

They are those associated with the Company's strategy in the pursuit of value creation, protection and growth. They are caused by changes in the external environment, such as political, economic and social, market, competitors, mergers and acquisitions, reputation and image, availability of resources, innovations and portfolio of products and/or services and changes in the rules applicable to the market.

3.2 Operational Risks

These are those associated with the Company's operation, which affect operational efficiency and the effective and efficient use of resources, which make the exercise of the Company's activities inappropriate and are associated both with the operation of the business, for example, industrial, sales, commercial, technology; as to the management of business support areas, such as accounting, controllership, controls, supplies, occupational health and safety, environment and union relations.

3.3 Financial Risks

They are those arising from unexpected effects in the economic, political and market trends that may reflect on consumer behavior, interest rates, inflation, financial investments, among others, and may include market, credit and liquidity risks.

3.4 Legal and Compliance Risks

These are the risks of imposition of legal or regulatory sanctions, financial or reputation loss that the Company may suffer as a result of non-compliance with laws, agreements, rules and regulations, as well as its own internal policies and procedures. These include risks in the scope of labor lawsuits and tax matters, fraud in financial statements and misappropriation of assets, corruption, among others.

3.5 Succession Risks

Are those related to the continuity of the Company; is associated with the risk of key employees leaving the Company before carrying out the succession, which can make the implementation of the Company's strategic plans difficult and have an adverse effect on the Company.

SPRINGS GLOBAL

4. GUIDELINES

The Company is committed to the dynamics of risk management, in order to preserve and develop its values, assets, reputation, competitiveness, business continuity and ensure compliance with the goals established in its strategic planning.

The objective of risk management is to understand them, assess and define response actions so that any losses are foreseen and reduced, with a view to maintaining risks at acceptable levels. Risk analysis should assist the decision-making process at the Company's different management levels. The Company's approach is to integrate risk management into the day-to-day conduct of its business through a structured process.

5. PROCESS

5.1 Risk Identification and Classification

At this stage, the Company identifies events that could impact its objectives and strategy. The risks to which the Company is exposed can be identified through a series of instruments, including:

- Risk questionnaires: professionals in the Company's leadership position are asked to fill out specific questionnaires to indicate possible risks to which the Company is exposed (risk owners). Risk scenarios are observed and cataloged;
- Interview cycles: risk scenarios are identified and discussed with certain employees. Results are also documented as part of the assessment; and
- Process audits: the Company's processes are audited and evaluated in order to verify any risks to which it is exposed. In this process, risk matrices are created or updated. Such records contribute to the identification of risks within the Company, functioning as a source of possible threats/weaknesses.

After collecting information through these instruments, the Company develops a Risk Map.

The risks described in the Risk Map may be updated considering the following aspects:

i. New scenarios (internal, political, economic, among others);
ii. Results of audits, interviews, questionnaires, observations and other activities; and/or
iii. Evolution of the integrity and risk mitigation culture.

5.2 Risk Analysis

Once the identification and classification of risks are carried out, those that are most relevant for treatment are defined. For analysis, the following aspects are considered:

- Impact/consequences that the identified risk can generate, such as potential for financial losses, degradation of the Company's image, legal penalties, among other negative results.
- Probability/vulnerability of the occurrence, considering the complexity and robustness of the existing internal controls for that risk.

The risk profile is delineated by combining both aspects.

5.3 Defining and implementing response actions

Based on the identified, assessed and analyzed risks, the Company, under the coordination of the Governance Officer, defines and recommends response actions, considering the following hypotheses:

i. Eliminate risk, that is, redefine business objectives and/or strategies;

ii. Mitigate the risk, that is, intensify the level of management and/or improve internal controls, and identify the residual risk, after implementing the management improvements;
iii. Accepting the risk, that is, taking no further action and continuing to monitor the risk, especially when it is not possible or practical to respond to the risk; or
iv. Passing on the risk, transferring the responsibility to third parties (e.g. in the risk of fire, the cost of the claim can be transferred to insurers).

These recommendations are broken down into detailed actions, pilots, tests, validations and necessary adjustments to ensure the effectiveness of the treatment and control of the risks to which the Company is exposed.

Based on the definition of risks and recommendations given by the Governance Officer, the Company's business areas must implement action plans in order to ensure proper treatment. The implementation of activities, actions and response deadlines are monitored by the Governance Officer and periodically reported to the Audit Committee.

5.4 Monitoring and Communication

The Governance Officer is responsible for monitoring and continuously improving the risk management process and for periodic communication with the Managers of the business areas, the Audit Committee, and the Board of Directors. Additionally, the Governance Officer must communicate, in a timely manner, the risk events that present a tendency to occur and/or possible extrapolation of limits, for discussion in the appropriate forums and levels

The Internal Audit is responsible for assessing the quality and effectiveness of the risk management and internal control processes, providing periodic reports to the Audit Committee, in order to ensure that the culture of transparency, accountability and awareness of risks is being properly implemented by the Governance Officer.

The Company must annually review the risks and assess the adequacy of the operating structure and internal controls for risk management.

6. RESPONSIBILITIES

The Company's Risk management is carried out following the “Three Lines of Defense” model. The First Line of Defense is made up of managers from the business areas and those directly responsible for the processes, according to the risks they manage. The Second Line of Defense is made up of the control structures, which must equip first-line managers for the correct management of risks and opportunities. The Third Line of Defense is made up of the Internal Audit, which will act with an independent eye to verify the effectiveness of the model. The Internal Audit may, at the Company's discretion, be outsourced and performed by an independent auditor registered with CVM.

6.1 Board of Directors

It is responsible for the governance of the risk management process, and has the following attributions:

i. Approve the policies, guidelines, risk matrix, exposure limits and any changes;
ii. Define an appropriate risk tolerance, prioritizing risks and approving mitigation plans;
iii. Supervise and approve risk response plans, when necessary;
iv. Ensure operational autonomy to the Audit Committee, approving its own budget to cover expenses with its operation;

v. Establish a risk management culture; and
vi. Assess the adequacy of the operational structure and internal controls for risk management

6.2 Audit Committee

The Audit Committee, an advisory body to the Board of Directors, with operational autonomy and its own budget approved by the Board of Directors, is responsible for:

i. Assess and monitor the Company's exposure to risks that may affect its sustainability;
ii. Give an opinion on the hiring and dismissal of independent audit services;
iii. Evaluate the quarterly information, interim statements and financial statements;
iv. Oversee risk management, compliance, internal controls and Internal Audit activities;
v. Direct the reports made by the Internal Audit to the Board of Directors;
vi. Assess, at least annually, whether the structure and budget of the Audit Area are sufficient for the performance of its functions;
vii. Assess the effectiveness of the Company's risk management model and suggest solutions to improve internal risk management processes to the Board of Directors;
viii. Recommend to the Board of Directors the review or implementation of changes, prioritizations and additions to the Company's risk matrix;
ix. Evaluate and monitor compliance and effectiveness of this Policy and other internal policies of the Company and recommend corrections/improvements necessary to the Board of Directors; and
x. Coordinate and monitor whistleblower channel activities, ensuring autonomy, secrecy, confidentiality, and an environment free from retaliation.

6.3 Governance Officer

The Governance Officer belongs to the Non-Statutory Executive Board, the position may be accumulated by a Statutory Officer, is responsible for the risk management process, in addition to the Compliance and Internal Controls function, reporting to the Executive Board for administrative matters, and to the Audit Committee, with regard to its risk management, compliance and internal controls functions, and has the following attributions:

i. Implement the Company's strategies approved by the Board of Directors in relation to Risk Management;
ii. Establish and coordinate the Company's risk management structure and process, in accordance with the guidelines, the risk matrix and the exposure limits provided for in this Policy;
iii. Implement this Policy through the dissemination of tools and good practices;
iv. Conduct a periodic review of this Policy and submit any suggestions to the Board of Directors or Audit Committee;
v. Suggest, evaluate and monitor the guidelines, the risk matrix, the limits and impacts of exposure to risks;
vi. Monitor and communicate the perception of exposure to the main risks, according to the risk matrix;
vii. Propose limits for risk exposure and suggest, assess, implement and monitor action plans for risk mitigation;
viii. Coordinate the risk assessment process together with the Audit Committee;
ix. Communicate, in a timely manner, risk events that tend to occur and/or possible extrapolation of limits, for discussion in the appropriate forums and authority;
x. Disseminate the risk management culture;

xi. Evaluate and review the Company's internal control system;

xii. Prepare and update the register of people identified as Related Parties, pursuant to the Company's Related Party Transaction Policy; and

xiii. Participate in the investigation of whistleblowing channel activities and analysis of disciplinary measures to be applied as a result of violations of the Company's Code of Ethics and Conduct.

The accumulation of compliance, internal controls and corporate risk functions with operational activities is prohibited.

6.4 Managers of the business areas

The managers of the business areas of the Company’s subsidiaries are directly responsible for risk management, reporting to the Executive Board, in general, and to the Governance Officer, specifically with regard to the matters under their responsibility, and their duties :

i. Identify and manage the risks of the respective business areas and processes in accordance with the risk limits;

ii. Communicate, in a timely manner, to the Company's Governance Officer, risk events that show a tendency to occur and/or possible extrapolation of risk limits; and

iii. Implement and monitor action plans for risk mitigation and monitor corrective actions in the respective areas and processes.

6.5 Internal Audit

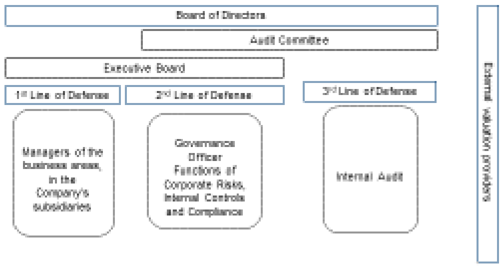
The Company's Internal Audit, whose activities are reported to the Board of Directors through the Audit Committee, has the following duties:

i. Assess the quality and effectiveness of the Company's risk management, control and governance processes; and

ii. The other activities approved by the Board of Directors.

The Internal Audit must have a structure and budget considered sufficient for the performance of its functions, as assessed by the Audit Committee at least once a year.

Organizational Chart of the Risk Management Structure



7. TERM

This Policy was approved by the Board of Directors, effective as of fiscal year 2022 and may only be modified by resolution of the Company's Board of Directors.

São Paulo, December 27, 2021.