RISK MANAGEMENT POLICY

LOG COMMERCIAL PROPERTIES E PARTICIPAÇÕES

1. PURPOSE

LOG ("Company") is committed to using the best corporate governance practices aligned with its mission, vision, values and strategic objectives to preserve and drive value to all stakeholders.

Risk management is a critical element for a good corporate governance, as it helps reduce uncertainties when defining strategies and objectives, making results feasible.

The purpose of this Risk Management Policy ("Policy") is to establish guidelines to be followed during the integrated corporate risk management, so that all decisions are made through a transparent process, reducing the company's exposure to risks and ensuring the fulfillment of strategic objectives.

2. SCOPE

This policy is applicable to all company's organizational levels that make up the risk management process, either directly or indirectly, the Board of Directors, Senior Administration, Committees, and other Company employees.

3. GUIDELINES

The Company is committed towards maintaining a robust and integrated governance model through the risk management dynamics, helping the Company drive value and preserve its assets and reputation, while keeping risks at acceptable levels.

LOG's approach is to integrate risk management to its strategies and daily business activities, ensuring that events with significantly destructive potential become well known. To do so, the following guidelines are adopted:

- Risk management process aligned to the Company's strategy, corroborating with its efforts to develop sustainable business pillars;
- Premises adopted according to market best practices, as determined by Brazilian and international regulations;
- Structured risk management process adopted to ensure that risks, and their impacts, are taken into account during decision-making process;
- Proactively managing risks associated to business, management and support processes in a wide-reaching manner, keeping them at exposure levels aligned with the Company's risk profile;
- Corporate risk management actions aligned across all corporate sectors and departments, covering all managers and employees;
- Independence of the risk management process ensured and the segregation of duties between risk takers, responsible of implementing risk mitigation controls and responsible for controls monitoring; and
- Transparency and accountability ensured towards all of LOG's stakeholders regarding the Company's primary risks, along with the means to address them.

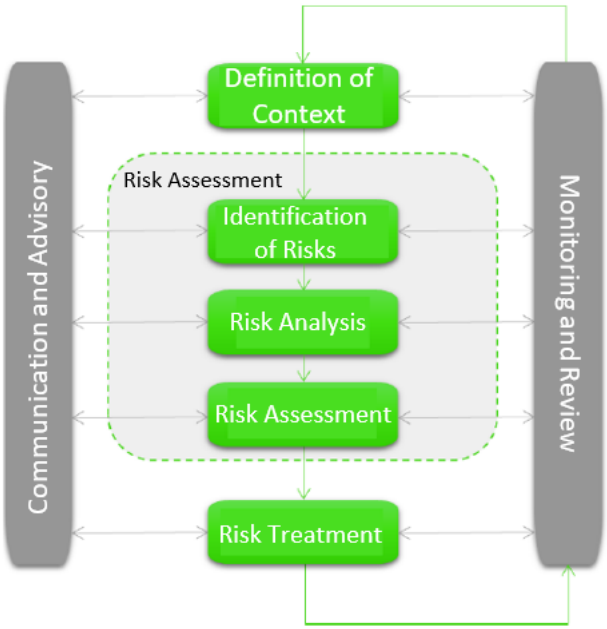
4. RISK MANAGEMENT PROCESS

LOG's risk management process was defined according to the best practices worldwide (COSO ERM and ISO 31.000), with the following goals:

- Aligning the risks appetite with the Company's strategy;
- Providing integrated responses to a variety of risks;

- Involving all representatives in our structure;
- Standardizing concepts and practices;
- Optimizing risk response decisions;
- Ensuring compliance to corporate governance;
- Ensuring dynamic and efficient flow of information;
- Increasing transparency for stakeholders, market analysis and credit agencies.

The process steps are defined as follows:



4.1 CONTEXT DEFINITION

The Board of Directors and Senior Administration are responsible for defining Company strategic objectives (long-term) and goals (short- and medium-term). The context (including scope and criteria) to be considered in corporate risk management will be defined according to the results expected from strategic planning, the influence of internal and external environments, and willingness to take risks. In addition, the Risk Management department will leverage the Company's value chain, policies, standards, and procedures.

4.2 RISK IDENTIFICATION

This step consists of studies on available sources of information (be them internal or external) that could contribute to discussions about the key events capable of impacting the fulfillment of corporate objectives. The purpose of this step is to map the risk events to which LOG is exposed and that could affect the Company's strategy and objectives.

The process to identify risks will take place through a set of activities in different organizational levels, including process mapping activities, interviews with business areas managers, reports from the compliance hotline, discussions with advisory committees (Compliance Committee and Audit Committee), internal and external audit reviews, management assessments and benchmarks with companies from the same industry and of similar sizes. This step will also consider external factors (economic, business,

environmental, political, social and, technological), as well as internal (infrastructure, people, processes, and technology) factors.

In order to standardize the risk management process, LOG adopted a corporate risk dictionary (unified risk base), including a corporate risk portfolio that classifies and categorizes risks in a language that is common to all business areas, considering the Company's characteristics and context. This dictionary divides the risks in five different natures:

- **Strategic**: risks of losses resulting from failure of the adopted strategies, considering business dynamics and competition, changes to the policies and economic conditions in Brazil and abroad, as well as environmental, social and governance issues.
- **Operational**: risks of losses resulting from failure, deficiencies or inadequacies in internal and personal processes and systems, or resulting from external events.
- **Financial**: risks of losses resulting from market fluctuations that impact the company's assets, as well as risks related to customers' and payment sources' credit capacity, and the Company's liquidity with financial organizations.
- **Compliance**: risks of losses resulting from legal and/or regulatory sanctions imposed upon the organization due to failure to comply with laws, regulations, standards and internal procedures, compromising the Company's reputation.
- **Cyber**: risks of losses resulting from failure, deficiency or inadequacies in maintaining confidentiality, integrity and availability of information, networks and systems, as well as of all individuals interacting with them.

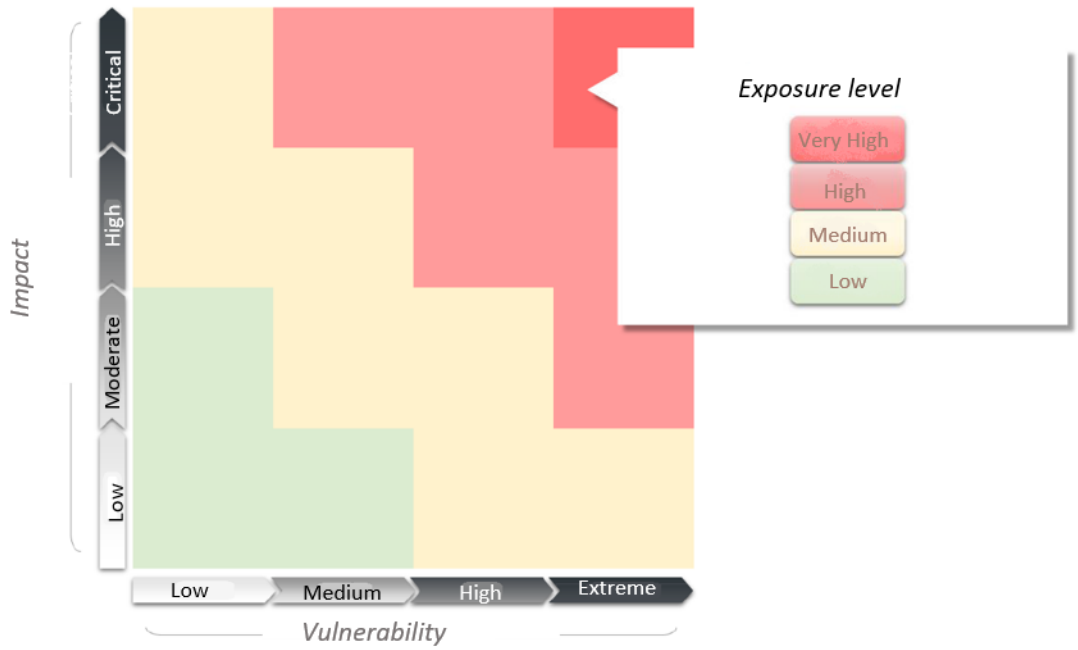
4.3 RISK ANALYSIS

This step consists in assessing the Company's exposure to internal and external risk factors. The risks must be analyzed along with the risk owners, control areas (second line of defense) and other company departments, when applicable and according to their capacity for contribution. This will help properly identify risk sources, the areas and processes affected (either directly or indirectly), causes and potential consequences that could adversely affect the Company's goals and/or strategic objectives.

4.4 RISK EVALUATION

Risks are evaluated according to their impact and vulnerability. This assessment indicates the exposure level of each identified risk. Risks may be classified as very high, high, medium, or low, as per the heat map.

The risks map also represents the Company's willingness to take risks, according to impact and vulnerability attributes.



Impact

Impact analysis requires the use of quantitative (financial measurement) and qualitative (reputation and image; strategic elements; compliance; operational health and safety) risk assessment attributes, divided by scales.

The impact must be classified (as low, moderate, high, or critical) according to the type of analysis, that is, whether the impact will be measured using quantitative means (applicable when historical data on risk materialization or risk value is available) or qualitative means (applicable when historical data on risk materialization or risk value accuracy is unavailable). For the latter, we will use the worst-case scenario and professional judgment as basis to assess the impact.

Vulnerability

When assessing vulnerability, we will consider the occurrence history, executives' perception, how far action plans were implemented, the current control structure and professional judgment.

Vulnerabilities are classified as low, medium, high, or extreme, representing the level of exposure to risk according to aspects such as control efficiency, maturity of internal control structure, process/risk exposure regularity, complexity of the activities, degree of changes to processes and response to risks.

General Risk Assessment

The General Risk Assessment involves **identifying**, **analyzing** and **assessing** risks, structurally reflecting how executives perceive the primary aspects of managing the risks involved in the Company's operations, areas/business processes and characteristics.

The internal and external origins of the Company's business strategies and objectives are mapped and monitored to ensure that any materialized risks become known, allowing them to be managed at an acceptable level.

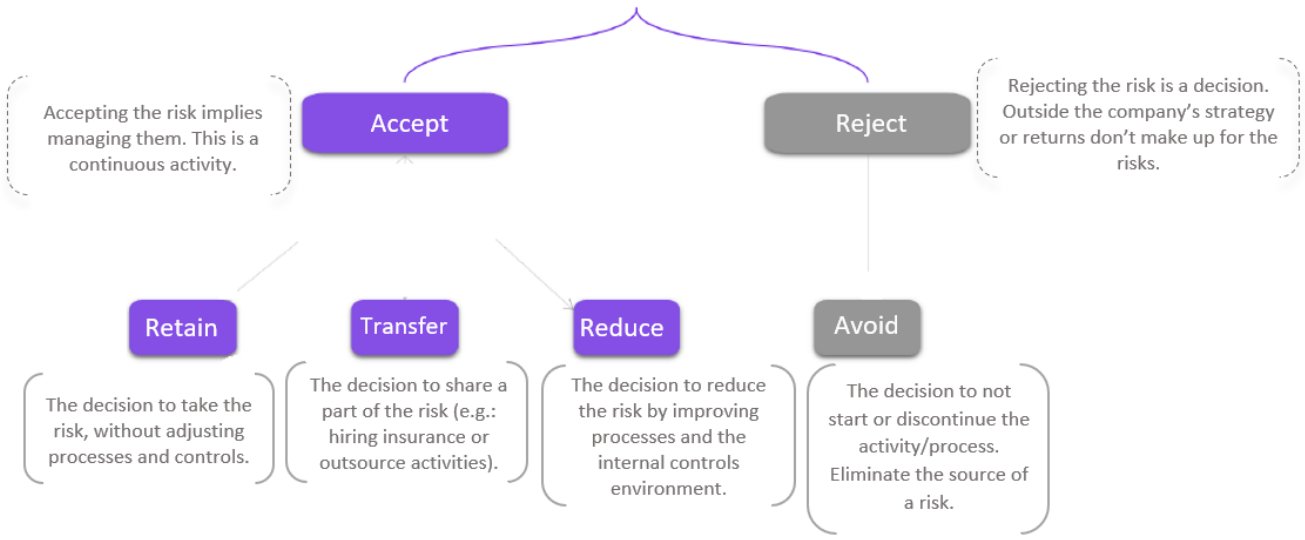
The assessment is updated yearly in order to identify any changes in the environment that could affect how business objectives are fulfilled. All identified changes must be recorded in the Company's corporate risk analysis document.

4.5 RISK TREATMENT

In this step, management is responsible for defining a response for identified risks, in order to bring the exposure down to a level that is acceptable by the Company, varying according to willingness to take risks.

Treatment must also consider the best way to balance the reduction of exposure levels and associated costs, along with how the decision could affect other departments, processes, systems, etc.

Treatment possibilities include:



If the choice is made to accept/retain the risk, monitoring metrics must be established. In cases when the decision is to reduce risk exposure (transferring or reducing), action/mitigation plans must be defined and monitored through Key Risk Indicators (KRIs), risk owners and deadlines.

4.6 MONITORING AND REVIEW

The monitoring and review step involves checking, supervising, critically observing, and implementing improvements by identifying changes in the required or expected performance level. It is important that the monitoring process takes place in all aspects of risk management, in order to:

(i) ensure controls and management practices are efficient in their design and operation;
(ii) obtain information that could improve the risk assessment process;
(iii) improve the process by analyzing events, changes, trends, successes, and failures;
(iv) identify changes in external and internal contexts that could have influenced prior responses and priorities;
(v) identify emerging risks.

4.7 COMMUNICATION AND CONSULTATION

The communication and consultation step involves creating and maintaining continuous and interactive processes, so that all stakeholders can share, provide or obtain information, contributing towards improvements to the Company's risk management activities.

5. ROLES AND RESPONSIBILITIES

Risk management is a continuous, transparent process, for which everyone in all organizational levels share responsibility, be it strategic, tactical or operational. All employees must know the risks of their activities and manage them according to concepts and guidelines found in this policy and its complementary documentation.

Below are the roles and responsibilities of the Company's risk management process representatives:

Board of Directors

- Establishes the Company's risk guidelines;
- Approves the Company's Risk Management Policy and future revisions;
- Provides feedback on risk management operational structure changes and approves suggestions of changes, if needed;
- Supervises the Company's Risk Management and Compliance activities;
- Works and interacts with the Audit Committee to ensure the established risk guidelines are fulfilled; and
- Periodically approves the risks map and indicators.

Executive Board

- Supports decisions by the Board of Directors and the Audit Committee regarding risk mitigation;
- Implements Company strategies and guidelines approved by the Board of Directors, respecting them and ensuring all employees respect their definitions;
- Subsides resources to implement effective internal controls and risk mitigation strategies;
- Ensures a periodic training schedule on conduct and ethics for the Company administration and employees, along with the Compliance department; and
- Maintains an effective internal controls and Compliance environment.

Audit Committee

- Assesses and monitors the Risk Management process and the Company's exposure to risks;
- Assesses the key risks reporting process;
- Ensures risks are properly estimated and reviews key risk management;
- Submits the consolidated risk assessment results to the Board of Directors;
- Oversees and ensures the fulfillment of: (i) laws and standards that are applicable to the Company's business and activities; (ii) the Code of Conduct; and (iii) the rules, regulations, policies, and internal guidelines;
- Ensures adequacy, improvement and operation of the Company's internal controls system;
- Maintains and disseminates the Company's commitment towards management focused on the pillars of corporate governance, sustainability and ethics;
- Fights against all forms of corruption;
- Issues recommendations on situations with potential conflict of interest between Company-related parties;
- Investigates reports coming from the compliance hotline or from some other means in an impersonal manner, respecting the integrity of the reporting party and the individuals being reported, as per the Company's Compliance Policy.

Finance Committee

- Assesses and defines the Company's financial strategies related to loans and financing, identifying financial risks the Company may be exposed to; and
- Submits the financial risk assessment results to the Board of Directors.

Compliance Committee

- Assesses questions and ethical dilemmas that may emerge at LOG;
- Oversees, requires and maintains, along with the Audit Committee, the fulfillment of: (i) laws and standards that are applicable to the Company's business and activities; (ii) the Code of Conduct; and (iii) the rules, regulations, policies, and internal manuals;
- Fights against all forms of corruption and/or improper benefits, along with the Audit Committee;
- Issues recommendations on situations with potential conflicts of interest that expose the Company to a compliance risk; and
- Assesses, along with the Compliance department, conduct deviations and violations of internal standards that may be identified or reported, either through monitoring activities or through reports from the compliance hotline.

Management

Managers at the Company's different departments are responsible for:

- Ensuring risk management remains operational, implementing preventing and corrective actions for identified risks;
- Identifying risks proactively, reporting them to senior leadership;
- Contributing towards providing information that subsidize the assessments by the Audit Committee; and
- Developing processes, procedures, training, and means of communication that allow the consistent dissemination of the Company's risk management activities.

6. MISCELLANEOUS

The Board of Directors shall be responsible for assessing this Policy's adequacy and applying changes as needed.

This Policy shall go into effect upon approval by the Board of Directors, and shall remain in effect indefinitely, until decided otherwise.

Any changes to this Risk Management Policy shall be approved by the Board of Directors.

7. STATUTORY BASIS/REFERENCE DOCUMENTS

ISO 31.000:2018 - Risk Management Guidelines;

COSO ERM:2017 - Corporate Risk Management Integrated with Strategy and Performance;

UK HM Treasury:2004 - The Orange Book - Management of Risk - Principles and Concepts

IBCG Corporate Risk Management:2017 - Evolution of governance and strategy/Brazilian Institute of Corporate Governance.

8. DEFINITIONS, CONCEPTS AND ACRONYMS

Risk apetite: refers to the risk of exposure levels that the Company is willing to accept in order to fulfill its short-, medium- and long-term corporate objective.

COSO (Committee of Sponsoring Organizations of the Treadway Commission): a private, non-profit organization founded in the US in 1985, dedicated towards improving reliability of financial reports by applying ethics and efficacy when fulfilling Internal Controls.

Risk Dictionary: an information base that defines and standardizes the descriptions of risks, along with their categories and nature.

Risk Factors: events that may lead to risks if not properly managed.

Impact: likely consequence of the emergence of a risk, measured in financial and/or non-financial terms.

Risk Map (or Heat Map): a graphic representation of the exposure to the impacts of a risk, comparing them to the vulnerability of the identified risks.

Risk Ruler: a means to classify exposures that help the Company establish management priorities, how the Company is positioned regarding the Risks and the appropriate forums for management and monitoring. Four classification levels are used: “Low”, “Moderate”, “High”, and “Critical”.

Risk Response: how the Company positions itself upon identifying a risk. The choice of an appropriate response occurs in two instances. The first is when a decision is made to avoid (i.e., a decision to not start or discontinue the activity that originates the risk) or to accept. The second is when a decision is made to accept, that is, assuming (not taking any mitigation actions, but rather monitoring factors that could influence the increase of exposure) or mitigate (addressing the actions to remove the source of the risk or changing vulnerabilities and/or impact).

Risk: an uncertainty effect capable of how objectives are fulfilled, capable of influencing a positive deviation from the expected, representing an opportunity or a negative deviation, or representing a threat.