ITAÚSA

Grandes **marcas**, grande **história**, grande **futuro.**

CNPJ 61.532.644/0001-15
A Publicly-Held Company

RISK MANAGEMENT POLICY

1. PURPOSE

This Risk Management Policy ("Policy") sets out the guidelines to be followed in the Risk management process of Itaúsa S.A. ("Itaúsa" or "Company") in order to identify, assess, prioritize and handle these Risks, thereby perpetuating the business.

2. TARGET AUDIENCE

The provisions provided herein apply to the Company and its entire management (members of the Board of Directors and Board of Officers), members of the Fiscal Council, members of the Board advisory committees, members of the Board of Officers' advisory councils, and employees.

3. CONCEPTS

- **General Risk Analysis:** process of identifying, analyzing, classifying, prioritizing and treating risks, including a cycle of interviews with management members and supervisors to capture the internal perception of risks to which the Company is exposed, in addition to updating the Company's Risk methodology.
- **Risk Appetite:** degree of exposure to Risks that the Company is willing to tolerate in order to achieve its objectives and create value for its stockholders.
- **Compliance:** designation used in the prevention and detection of any failure to comply with domestic and foreign laws and regulations, which may be committed by the Company's management members, employees and business partners.
- **Controls:** policies, rules, procedures, activities and mechanisms implemented to ensure that the objectives of businesses are achieved and that undesirable events are prevented or detected and corrected.
- **Risk Factor:** situation that can potentiate the occurrence of a Risk.
- **Risk Management:** activities undertaken with the purpose of identifying, classification, formalizing, monitoring and/or managing identified Risks. Risk Management should be aligned to the Company's objectives, strategies and business.
- **Impact:** result of an event to which the Company may be exposed due to its activities.
- **Key Risk Indicators (KRI's):** metrics for assessing or monitoring the Company's exposure to its Risks.

- **3 Lines Model:** identifies structures and processes that help in the achievement of goals and strengthen governance and Risk management.
- **Risk Map:** a graphical representation of the qualitative and quantitative classification of Risks, considering the possible Impact and probability of their materialization.
- **Action Plan(s):** definition of corrective actions to reduce the exposure to residual Risks, based on the identification of deficiencies during the evaluation cycle of the Control/Risks environment.
- **Response(s) to Risk(s):** the decision that will be made following the identification of Inherent Risk or evaluation of the Control environment of the residual Risks, for the purpose of fostering discussion and ensuring the efficiency of Itaúsa's internal controls environment.
- **Risk(s):** threat of events or actions that may impact the achievement of the Company's goals. It is inherent in any activity and may affect the assets, results, reputation or continuity of businesses.
- **Risk Tolerance:** limit of the level of Risk or uncertainty that the Company supports to achieve its goals.
- **Inherent Risk:** Risk that exists in the process before being treated/mitigated as to its probability of occurrence and Impact.
- **Residual Risk:** Risk that remains after the Company has implemented Controls or Action Plans to reduce the probability of occurrence and mitigate its Impact.
- **Risk Owner:** the person or department with responsibility and authority to manage a Risk in the first line and support the definition and implementation of Action Plans for Risk mitigation or remediation.
- **Vulnerability:** level of exposure of the Company to the Risk, considering the current environment of internal Controls.

4. PRINCIPLES AND GUIDELINES

The purpose of the corporate Risk Management principles and guidelines is to reinforce Itaúsa's commitment to act in compliance with regulatory requirements and best practices, aligning its business with the Company's strategy. It also has the role of defining the responsibilities of employees and management members in Risk Management, ensuring that governance guidelines are complied with and strengthening the Risk philosophy and culture in the Company.

4.1. Control Activities

A set of actions, policies, rules, procedures and systems for safeguarding the Company's assets, ensuring that its Risks are known and suitably mitigated.

Control activities should be carried out at all levels of the Company and at various stages of the corporate processes.

4.2. Risk Management Structure

In line with the best market practices, Itaúsa has an organized structure in charge of the application of the Risk management process described herein, at different levels of the organization, as detailed in item 5 of this Policy.

The Company adopts the 3 Lines Model of the International Institute of Auditors (IIA) in corporate Risk Management, where the business areas, as well as the Compliance and Corporate Risk department, Internal Audit, Committees, Councils, Board of Officers and Board of Directors act in an integrated manner:

- 1st line: business supervisors, who are knowledgeable of and manage their risks, and are responsible for defining and implementing Action Plans for risk mitigation in order to ensure the proper process management;
- 2nd line: the Compliance and Corporate Risk department, which assists the 1st line in identifying risks and related causes and consequences. Responsible for the Risk Management process, using market methodologies and the best market practices; and
- 3rd line: the internal audit function, which is independent to assess the controls carried out by the 1st line and the adequacy of Risk Management.

4.3. Stages of Risk Management:

4.3.1. Risk Identification

The Risks to which the Company is exposed must be reviewed at least once a year, and documented and formalized on a structured basis so that they may be known and suitably handled. The General Risk Analysis process must otherwise take place twice a year.

These Risks must be classified in accordance with their nature and origin, as shown below:

- **Strategic:** Risks associated with the governance and decision-making process of management and that may result in a significant loss of the Company's economic value. They may also have a negative impact on the Company's revenue or capital due to faulty planning, adverse decisions made, Itaúsa's inability to implement proper strategic plans and/or changes in its business environment.

  These are risks that go beyond the internal environment of the Company and its Investees, also taking into consideration relationships with external stakeholders and their perceptions and values. They include external factors, such as political and social and economic risks, market behavior, legislative changes and unforeseen events. Additionally, themes focused on business goals, the Company's image, its environmental, social and climate management, people and its ethical and conduct standards are considered strategic.

- **Financial:** Risks that may result in losses of funds by the Company, broken down into the following categories:

  * Liquidity risk: represented by the possibility of the Company not being able to honor its commitments on the due date or only meeting them by incurring in

significant losses. This risk may also be classified as a cash flow risk, given the possibility of mismatches between payments and receipts affecting the Company's payment capability.

- Market risk: this Risk measures the likelihood of an economic loss arising from changes in market Risk Factors to which the prices of assets, liabilities and derivatives are sensitive. The time horizon for analysis is typically short-term and includes Risks associated with foreign exchange variation, interest rates, equities prices and commodity prices.
- Credit risk: the possibility of losses arising from the Company's failure to receive amounts contracted with third parties as a result of their financial inability.

- **Operational:** Risk associated with the Company's infrastructure (processes, people and technology), affecting the operating efficiency and the effective and efficient use of its resources.
- **Regulatory:** Risk associated with the non-compliance with the legislation applicable to the sector of activity as well as legislation in general (environmental, labor, civil and taxation/ fiscal).
- **Technology:** Risk associated with the possibility of an internal or external threat exploring the vulnerabilities of an asset, thus affecting the confidentiality, integrity and availability of systems and information.

The identification stage comprises the corporate Risks inherent in the Company's activities, including outsourced services. Identification can occur at any time, from the design of a new process to its operationalization and have the participation of all those involved in the process at different levels. Causes (Risk Factors, consequences and Risk Owners) must also be defined).

4.3.2. Risk Analysis

This stage involves the verification of causes (Risks Factors) and consequences of Risks, as well as the probability of these consequences effectively arising.

4.3.3. Risk Assessment

Risk assessment involves dynamic and interactive processes that should: (i) verify which Risks require treatment; and (ii) determine the priority for implementation of said treatment. To this end, the Company adopts Impact and Vulnerability criteria that are used to define the Risk Map:

Impact considers the Management's guidelines in relation to possible financial (loss), strategic, image/reputation, operational, legal/regulatory aspects and effects on their investors and on the Company's securities. Vulnerability considers the magnitude of Itaúsa's exposure to several external and internal factors, that is, it considers the probability of Risk occurrence based on the robustness of its internal Control environment.

The final classification of the Company's degree of exposure to each Risk will be defined based on the combination of Impact and Vulnerability, as follows:

- **Critical:** Risk with critical or high Impact and probable or very probable Vulnerability.
- **High:** Risk with critical, high or medium Impact and possible, probable or very probable Vulnerability.
- **Medium:** Risk with critical, high, medium or low Impact and remote, possible, probable or very probable Vulnerability.
- **Low:** Risk with medium or low Impact and remote or possible Vulnerability.

This classification will result in the Risk Map that will help Company to prioritize the Risk treatment.

4.3.4. Risk Treatment

The risks identified must be addressed according to their criticality. Responses to Risks must consider the possible cost/benefits arising from legal, regulatory or any other requirements that may prove material to the Company, and will comprise the following alternatives for Risk treatment:

a) **Accept:** no action is taken to influence the probability of occurrence and/or severity of the Risk. Risks with impact below the cost/benefit of their management may be maintained, as long as they are known and accepted by the Audit Committee, in line with the Risk Appetite defined by the Board of Directors. However, ongoing monitoring measures must be established to ensure that, in the case of a change in the scenario that justifies changing the way the risk is treated, the Company implements said proper treatment.

b) **Mitigate:** actions are taken to reduce the probability of materialization and/or severity of the Risk. This response involves the improvement or creation of controls and improvements in processes, with the definition of Risk Owners and implementation deadlines, in addition to the establishment of monitoring measures aimed at reducing the probability of risk occurrence and the Impact in the case the Risk materializes.

c) **Transfer:** actions are taken to reduce the exposure to Risk by transferring it in whole or in part to third parties, such as by taking out insurance, outsourcing, hedging, etc.

d) **Eliminate:** In the event it is decided that the Company does not wish to coexist with the Risk under current conditions. It suggests that no response would be able to reduce the Risk to an acceptable level. In this case, the process that has generated the Risk must be discontinued.

4.3.5. Risk Monitoring

The purpose is to ensure the effectiveness and suitability of internal Controls and obtain information which provides the basis for improvements in the Risk management process. Monitoring should be conducted through ongoing and impartial evaluations.

Key Risk Indicators (KRI's) are monitoring tools used to follow up the exposure limits established by the Company, as well as the Action Plans defined by the 2nd line together with the Risk Owners.

Monitoring is important to follow up whether the Risk degree has changed, identify the possible need for additional treatment and ensure the effectiveness of the Company's Risk Management.

4.3.6. Information and Communication

The purpose is to communicate clearly and objectively to all stakeholders the results of all stages of the Risk management process in order to contribute to the understanding of the current situation of the effectiveness of the Action Plans and to raise awareness and provide capacity building for the risk management culture in the Company.

5. RESPONSIBILITIES

5.1. Board of Directors:

- define the level of the Company's Risk Appetite and Risk Tolerance, based on the principles and guidelines established herein;
- approve the Company's Risk Management Policy and its future revisions; and
- approve, as proposed by the Audit Committee, the Risk Map and the prioritization of Risks, Response to Risk plans, when risks are above the Company's Risk Appetite, as well as their revisions.

5.2. Audit Committee:

- propose to the Board of Directors the Company's Risk Appetite and Tolerance level;
- monitor Risk Management (whether risks are identified by the Board of Officers or reported by the Compliance and Corporate Risk department) as provided for in this Policy;
- validate the Company's Risk consolidation report, submitting it to the Board of Directors;
- monitor the Response to Risk plans for risks that are above the Company's Risk Appetite, reporting them to the Board of Directors; and
- opine on suggestions for changing or suggest changes to this Policy and recommend improvements to the Board of Directors, should it be deemed necessary.

5.3. Board of Officers:

- ensure the operation of the 3 Lines model in the Company's Risk Management process;
- approve the methodology to be used for carrying out the Risk Management process;
- approve the critical and high Risk Action Plans proposed by the business areas for Risk mitigation purposes;
- systematically carry out the Risk Management, including Key Risk Indicators (KRI's), as well as the stage of implementing Risk mitigation actions;

- periodically evaluate the suitability of the operational structure of Risk Management to check for its effectiveness; and
- approve the Company's Risk consolidation report prepared by the Compliance and Corporate Risk department.

5.4. Business Areas:

- act directly in the Risk Management of their own area, privileging: the risk identification, assessment, treatment and monitoring, according to the guidelines of this Policy;
- perform, together with the 2nd line, the Risk assessment process (Self-Assessment);
- propose and implement Action Plans for Risk treatment, in line with the Compliance and Corporate Risk department;
- actively report to the Compliance and Corporate Risk department any risks not previously identified and any changes that may impact Risk Management, such as changes in processes or Controls, new business, divestitures of a certain operation, significant changes in routines or objectives, and planning reviews;
- develop, together with the Compliance and Corporate Risk department, Key Risk Indicators (KRI's), classification criteria and limit proposals;
- report to the Board of Officers any information related to their Risk management and compliance activities; and
- approve the rules and procedures guiding individual initiatives for the implementation of Risk management concepts in their area of activity in order to ensure that the Responses to Risks are carried out.

5.5. Compliance and Corporate Risk Department:

- propose responsibilities related to Risk Management activities, as well as authorization levels for approval and scopes of activities;
- provide tools, systems, infrastructure and governance to support the Company's Risk management;
- develop the Risk Management methodology and submit it for approval to the Board of Officers through the Audit and Risk Council;
- raise awareness among the 1st line of the importance of Risk Management and the inherent responsibility of the Company's management members and employees;
- coordinate the Risk Management activities with the 1st line areas, maintaining independence in the exercise of their functions;
- Develop, together with business supervisors, models and/or Risk Indicators for monitoring Risks, classification criteria and limit proposals;
- prepare periodic consolidated Risk reports of the Company, submitting them to the Board of Officers, through the Audit and Risk Council, and to the Audit Committee;

- support process supervisors in the drawing up of Action Plans required for Risk treatment and ensure the implementation of these Action Plans;
- disseminate the knowledge and culture of Risk Management in the Company;
- report the information related to their Risk management activities to the Audit and Risk Council and the Audit Committee; and
- enable the internal audit work to ensure its reporting to the Board of Directors.

5.6. Internal Audit:

- verify, independently and periodically, the adequacy of the processes and procedures for Risk identification and management, according to the guidelines established in this Policy and internal regulations; and
- submit to the Board of Directors the results of the assessments of the Risk Management system and the effectiveness of internal Controls.

_____