ITAÚSA

CNPJ 61.532.644/0001-15
A Publicly Held Company

RISK MANAGEMENT POLICY

(approved by the Meeting of the Board of Directors held on May 4, 2017, amended on May 14, 2018 and revision on February 22, 2021)

1. PURPOSE

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

2. TARGET AUDIENCE

This Policy applies to the Company and its entire management (members of the Board of Directors and officers), members of the Fiscal Council, members of advisory committees to the Board of Directors, members of the advisory commissions to the Board of Executive Officers and other employees.

The respective Risk management policies of Itaúsa's controlled companies should contemplate the considerations formulated herein, reflecting their eventual procedural particularities of management and the complexity of their operations. The controlled companies, which do not have their own policy, should adhere to the terms of this Policy, in alignment with their respective management structures.

3. CONCEPTS

- **Risk Appetite:** degree of exposure to Risks, which the Company is willing to tolerate in order to achieve its objectives and create value for its shareholders.
- **Compliance:** designation used in the prevention and detection of failure to comply with domestic and foreign laws and regulations, which may be committed by members of management, employees and business partners of the Company.
- **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.
- **Risks Management:** activities undertaken with the purpose of identifying, classifying, formalizing, monitoring and/or managing the identified Risks. Risk management should be aligned to the Company's objectives, strategies and businesses.
- **Impact:** result of an event to which the Company may be exposed due to its activities.
- **Risk Indicators (KRI's):** metrics for evaluating or monitoring the Company's exposure to its Risks.

- **3 Lines Model:** identifies structures and processes that help in the achievement of objectives and strengthen governance and Risk management.
- **Risk Map:** graphical representation of the qualitative and quantitative classification of Risks, considering possible Impact and probability of their materialization.
- **Action Plan(s):** definition of corrective actions in order to reduce exposure to the residual Risks, based on the identification of the deficiencies during the evaluation cycle of the Control/Risks environment.
- **Response(s) to the Risk(s):** decision that will be taken following identification of the 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, which may impact the attainment of the Company's objectives. It is inherent to any activity and may affect the assets, results, reputation or continuity of the businesses.
- **Risk Tolerance:** limit of the level of Risk or uncertainty that the Company supports to achieve its objectives.
- **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 area with responsibility and authority to manage a Risk in the first line and support the definition and implementation of Action Plans for mitigation or remediation of the Risk.
- **Vulnerability:** level of exposure of the Company to Risk considering the environment of internal Controls in force.

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 the regulatory requirements and best practices, aligning its business with the Company's strategy. In addition, it also has the role of defining the responsibilities of employees and Administration in Risk Management, ensuring that governance guidelines are complied with and strengthening the Risk philosophy and culture in the Company.

4.1. Control Activities

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

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

4.2. Risk Management Structure

In line with best market practices, Itaúsa maintains an organized structure for 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 Line Model of the International Institute of Auditors (IIA) in corporate Risk Management, where the business areas, the Compliance and Corporate Risk area, Internal Audit, Committees, Commissions, Board of Executive Officers and Board of Directors act in an integrated manner.

- 1st line: business managers, who have knowledge and management of their Risks, as well as the responsibility to define and implement Action Plans for their mitigation, in order to ensure the adequate management of processes;
- 2nd line: the Compliance and Corporate Risk Area, which assists the 1st line in the identification of Risks, causes and associated consequences. Responsible for the Risk Management process, it uses methodology and best market practices; and
- 3rd line: internal audit, which is independent to assess the controls executed by the 1st line and the adequacy of Risk Management.

4.3. Stages of Risk Management:

4.3.1. Identification of the Risks

The Risks to which the Company is subject, must be identified periodically, documented and formalized so that such Risks may be known and suitably handled. These Risks should be categorized in accordance with their nature and origin as shown below:

- **Strategic:** Risks related to the taking of decisions by management and which can generate substantial losses in the economic value of the Company. In addition, the Risks can have a negative Impact on revenue and on the capital of the Company due to deficient planning, the adopting of adverse decisions, the inability of Itaúsa to implement its appropriate strategic plans and/or any changes in its business environment.
- **Financial:** Risks, which if materializing, result in losses of financial resources by the Company, subdivided into the following categories:
  - Liquidity Risk: reflects the possibility of the Company being unable to honor its commitments on time, or only doing so with heavy losses. This Risk can also be classified as cash flow Risk given the possibility of mismatching between payments and receivables, affecting the Company's payment capacity.
  - Market Risk: this Risk measures the possibility of economic loss generated from the variation in market Risk Factors to which the prices of the assets, liabilities and derivatives are sensitive. The time horizon for analysis is typically short-term and includes a variation Risk: exchange rate, interest rates, share prices and commodity prices.
  - Credit Risk: is the possibility of losses resulting from the non-receipt of contractual amounts from third parties due to their economic-financial incapacity.
- **Operational:** Risks relating to the infrastructure of the Company (processes, people and technology), which affect the operational efficiency and effective and efficient use of its resources.

- **Regulatory:** Risks related to non-compliance with the legislation applicable to the sector of activity as well as legislation in general (environmental, labor, civil and taxation/ fiscal
- **Cyber:** Risk related to the possibility of an internal or external threat to exploit Vulnerabilities of an asset, impacting the confidentiality, integrity and availability of systems and information.

The identification stage contemplates the corporate Risks inherent to the Company's activities, including outsourced services. The 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. The causes must also be defined (Risk Factors, consequences and those responsible for the Risks).

4.3.2. Risk Analysis

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

4.3.3. Evaluation of the Risks

The 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.

The Impact considers the Management's guidelines in relation to possible financial aspects (loss), strategic, image/reputation, operational, legal/regulatory and reflection on the Company's securities. The Vulnerability considers the magnitude of Itaúsa's exposure to several external and internal factors, that is, it considers the probability of occurrence of the Risk 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 according to the combination of Impact and Vulnerability, as follows:

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

This classification will result in the Risk Map which will help Company in the prioritization of the treatment of the Risks.

4.3.4. Treatment of the Risks

The identified Risks should be handled in accordance with their criticality. The Sustainability and Risks Commission should decide how to respond to the Risks and define the instruments for protecting the Company, at the same time balancing the effects of the Response to Risk against eventual cost/benefits due to legal and regulatory requirements or any other requirements which may prove material to the

Company. The Sustainability and Risks Commission shall be guided by the following alternatives for handling Risks:

- **Accept:** no action is undertaken to influence the probability of occurrence and/or severity of the Risk. Risks the Impact of which is less than the cost/benefit of their management may be maintained conditional on being known and accepted by the Sustainability and Risk Commission, in line with the Risk Appetite defined by the Board of Directors. However, continuous monitoring measures must be established in order to ensure that, in case there is a change in the situation that justifies changes in the Risk treatment, the Company implements said treatment.
- **Reject**: should it is be decided that the Company does not wish to coexist with the Risk under current conditions, the Sustainability and Risk Commission shall adopt one of the following initiatives:
  - Act: 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 responsible persons and implementation deadlines, in addition to establishing Risk Indicators (KRI's) for monitoring
  - Plan: define actions or Controls that reduce Vulnerability or Impact in case of Risk materialization
  - Monitor: there is no need to define an action or Control for the Risk. Periodic monitoring is carried out to reassess its Impact and Vulnerability classification.

4.3.5. Monitoring of the Risks

To ensure the effectivity and suitability of the internal Controls and obtain information which provides the basis for improvements in the Risk management process. Monitoring should be conducted through continuous and impartial evaluations.

The Risk Indicators (KRI's) are monitoring tools to follow 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 degree of Risk 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

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 provide awareness and capacity building for the risk management culture in the Company.

5. RESPONSABILITIES

5.1. Board of Directors:

- to define the level of the Company's Risk Appetite and Risk Tolerance, based on the principles and guidelines established herein;
- to approve the Company’s Risks Management Policy and its future revisions;

- to approve, by proposal of the Board of Executive Officers, the Risk Map and the prioritization of Risks, as well as their revisions;
- to supervise and approve Risk Response plans, when necessary;
- to supervise and opine about the evaluation of the effectivity of the policies, Risk management systems and internal Controls and approve eventual suggestions for alterations, should these be deemed necessary.

5.2. Board of Executive Officers:

- to propose to the Board of Directors the Company's Risk Appetite and Tolerance level;
- to ensure the functioning of the 3 Line model in the Company's Risk Management process;
- to perform Risk Management (whether identified by the Board of Executive Officers itself or reported by the Compliance and Risk Area) as provided for in this Policy;
- to validate the Company's Risk consolidation report, submitting it to the Board of Directors;
- to monitor the Action Plans for the mitigation of exposure to Risk, as well as to define the respective responsible persons and implementation deadlines;
- to opine on the evaluation of the effectivity of the policies, Risks and Internal Controls management systems and to submit their findings for the examination of the Board of Directors; and
- to opine on suggestions for altering or suggest alterations to this Policy and recommend to the Board of Directors suggestions for improvement, should be deemed necessary.

5.3. Sustainability and Risks Commission:

- to approve the methodology to be used for conducting the Risks Management process;
- to approve the critical and high Risk Action Plans proposed by the business areas for Risks mitigation;
- systematically, to monitor the Risks Management, including Risk Indicators (KRI's), as well as the stage reached for implementing the actions established for Risks mitigation;
- periodically, to evaluate the effectiveness of the policies, Risk management systems and internal Controls, and submit this evaluation for the examination of the Board of Executive Officers;
- periodically, to evaluate the suitability of the operational structure of Risks Management in the verification of its effectiveness and recommend to the Board of Executive Officers suggestions for improvements, should these be deemed necessary;
- to approve the Company's Risk consolidation report prepared by the Compliance and Corporate Risk area, submitting it to the Board of Executive Officers; and
- to assess exceptions, possible violations and cases omitted from this Policy and refer them to the Board of Directors for their resolution and/or approval, such

communication being sent simultaneously to the science of the Board Executive Officers.

5.4. Business Areas:

- to act directly in the Risk Management for their area, privileging: identification, evaluation, treatment and monitoring, according to the guidelines of this Policy;
- to perform, together with the 2nd line, the Risk assessment process (Self-Assessment);
- actively report to the 2nd line changes that may impact Risk Management, such as changes in processes or Controls, new business, divestments of a certain operation, relevant changes in routines or objectives, and planning reviews;
- to ensure the implementation of Action Plans established for the treatment of Risks;
- to develop, together with the Compliance and Corporate Risk Area, Risk Monitoring Indicators (KRI's), classification criteria and limit proposals;
- to report to the Sustainability and Risks Commission information relating to their activities of Risk management and compliance;
- to communicate to the Compliance and Corporate Risks Area on a timely basis as to Risks, hitherto not identified, whether new or otherwise;
- to approve the rules and procedures guiding individual initiatives for the implementation of the concepts of Risk management in their area of activity in order to ensure that the response to the Risks is executed; and
- to detail the Action Plan, aligning it to Compliance and Corporate Risks Area and implementing it pursuant to the priorities set out therein.

5.5. Internal Audit

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

5.6. Compliance and Corporate Risks Area:

- to propose responsibilities related to Risk Management activities, as well as authorization levels for approval and scopes of activities;
- to provide the tools, systems, infrastructure and governance that support the Company's Risk management;
- to develop the Risk Management methodology and submit it for approval to the Sustainability and Risk Commission;
- raise awareness of the 1st line about the importance of Risk Management and the inherent responsibility of the Company's managers and employees;
- to coordinate the Risk Management activities with the 1st line areas, maintaining independence in the exercise of their functions;
- to develop with business managers models and/or Risk Indicators for monitoring Risks, classification criteria and limit proposals;

- to prepare periodic consolidated Risk reports of the Company, submitting them to the Sustainability and Risks Commission;
- to support the process managers in the drawing up of Action Plans necessary for the treatment of Risks and ensuring implementation of the Action Plans;
- to disseminate the knowledge and culture of Risk Management in the Company;
- to report the information related to their Risk management activities to the Sustainability and Risk Commission; and
- to enable the internal audit work to ensure its reporting to the Board of Directors.
