2024

SURA

ASSET MANAGEMENT

OC-ADR-PO001

Operational Risk Management Policy

OPERATIONAL RISK MANAGEMENT SYSTEM

Version: **3**
Last Updated: **May 2024**
Approved by: **Board of Directors**
Responsible Area: **Enterprise Risk Management**
Information Classification: **Confidential**
Code: **OC-ADR-PO001**

Introduction and Objective

The activities of SURA Asset Management and its subsidiaries (hereinafter referred to as "the Company") are exposed to various types of risks that may result in financial losses, regulatory non-compliance, or damage to the Company's name and reputation. These risks must be adequately managed to ensure the Company's long-term sustainability.

The Company references the definitions established by international standards and guidelines of regulatory or control entities regarding the management of Operational Risks, allowing us to obtain benefits in terms of operational efficiency and effectiveness, as well as providing criteria for the design and implementation of a methodology that reasonably establishes our risk appetite and tolerance in processes.

This policy is part of the Company's Internal Control System, which is based on the principles of self-control, self-management, and self-regulation.

The objective of this document is to provide the framework of guidelines for the Company's Operational Risk Management System, defining the activities that allow us to ensure the identification, measurement, control, and monitoring of Operational Risks, Business Continuity Risks, and Information Security Risks in order to manage the risks that may affect the Company and maintain its level of exposure within the defined risk appetite.

Scope and Framework

The guidelines contained in this document apply to all employees and third parties (clients, service providers or partners) operationally and/or functionally involved in the Company's processes, projects, or initiatives, regardless of the work modality.

This policy encompasses Operational Risk Management, including: operational risks, availability risks (business continuity), fraud and corruption risks, technological risks, cybersecurity risks, and information risks.

Specifically, availability risks include the definition, implementation, testing, and maintenance of Business Continuity , incorporating elements of prevention and emergency response, crisis scenario management, contingency plans, and the ability to return to normal operations. Information risks include the procedures and resources to effectively manage Information Security (confidentiality, integrity, and

“This document is the property of SURA Asset Management. Any use, disclosure, or reproduction of this document, in whole or in part, is prohibited without prior written”

availability) and information quality (effectiveness, efficiency, and reliability).

Key Roles and Responsibilities of Governing Bodies

In order to implement, operate, maintain, and improve the management of the Company's Operational Risks, the roles and responsibilities of the different governing bodies are defined as follows:

Company's Board of Directors' Risk Committee:
The general functions of the Board of Directors' Risk Committee are defined in the document "Regulations of the Risk Committee of SURA Asset Management, S.A." and in the documents of each of the Company's companies. Specifically, the following responsibilities are held:

i. To promote, at the organizational level, a risk management culture by setting policies and guidelines for the implementation of the Operational Risk Management System.
ii. To periodically monitor the operational risk profile, as well as the monitoring of the Company's main risks.
iii. To decide on the need to take measures, and if necessary, to follow up on their application and effectiveness, when aware of:
   - Material variations in the Company's operational risk exposures, including deviations from the thresholds and limits defined in the Operational Risk Management Manual.
   - Weaknesses in the implementation of the Company's operational risk management, considering the business plan, risk appetite, and risk profile of each.
iv. To adopt the necessary measures for the annual evaluation of the effectiveness of operational risk management.
v. To provide the necessary resources to implement and maintain, effectively and efficiently, the Operational Risk Management System.

"This document is the property of SURA Asset Management. Any use, disclosure, or reproduction of this document, in whole or in part, is prohibited without prior written"

vi. All other functions included in the board of directors' regulations.

Area responsible for the Company's risk management:

i. To ensure compliance with the provisions defined in the local and corporate regulations and policies, in accordance with the processes and nature of the risks faced by the Company.
ii. To process, review, and update operational risk policies, manuals, and procedures whenever required and present them to the defined governing bodies, ensuring alignment with corporate definitions and guidelines.
iii. To manage each of the stages and elements of the operational risk management process, in order to ensure that they are within the defined risk appetite, ensuring their alignment with corporate definitions and guidelines.
iv. To promote a risk management training and culture among all Company employees, in coordination with the corresponding areas of the organization and corporate guidelines, so that each employee has the necessary knowledge for the management of the risks associated with their activities.
v. To have the necessary communication and reporting mechanisms that guarantee adequate risk management within the Company and compliance with control entities, in accordance with the established governing bodies and decision-making instances.
vi. All other functions that the Board of Directors and/or the Board of Directors' Risk Committee consider necessary to assign.

Company's Risk Management Committee:

The Company has a regional Committee with quarterly meetings, made up of leaders and representatives of local risk teams, which is responsible for:

i. Monitoring the operational risk appetite framework by country and Company, in order to maintain the level of risks within the thresholds established by the Company.
ii. Monitoring the implementation and compliance of the operational risk management system in the Company, evaluating compliance with policies, the early warning system, and the operational risk management manual.

iii. Evaluating, at least once a year, the effectiveness of the corporate operational risk management framework and presenting the results of this evaluation to the Board of Directors, along with the proposal of the measures that may be necessary.

iv. To report promptly when material changes are identified in the Company's operational risk exposures and situations that lead to modifications in the Operational Risk Appetite Management Framework, and in the Company's business plan.

The Company must establish, implement, and maintain an Operational Risk Management System, according to its structure, size, and activities, including support activities, whether carried out directly or through third parties, that allows for the identification, measurement, control, and monitoring of Operational Risks.

General Guidelines for Operational Risk Management

i. The Company must establish, implement, and maintain an Operational Risk Management System, according to its structure, size, and activities, including support activities, whether carried out directly or through third parties, that allows for the identification, measurement, control, and monitoring of Operational Risks.

ii. The area responsible for risk management must maintain records and documents of all stages and elements of the operational risk management process.

iii. The area responsible for risk management must keep all reporting and control levels informed regarding the management of Operational Risks according to the defined periodicity.

iv. The area responsible for risk management implements and maintains clearly established communication channels for risk reporting.

v. The area responsible for risk management is responsible for developing a periodic awareness, dissemination, and training plan to provide periodic training on risk management to employees, suppliers, and business partners.

vi. The processes defined in the Company and its activities must be aligned with the objectives set in terms of Operational Risk Management,

“This document is the property of SURA Asset Management. Any use, disclosure, or reproduction of this document, in whole or in part, is prohibited without prior written”

Governance

The approval of this policy is the responsibility of the Company's Board of Directors' Risk Committee, upon recommendation of the Risk Committee or equivalent bodies. Any modification must be approved by these same governing bodies. Any exception to compliance with this policy must be reviewed by the Corporate Risk Management Management and reported to the corresponding governing bodies.

Disclosure and Update

All persons involved in the management of the Company's Operational Risks must know and apply this Policy, complying with what is established herein.

The area responsible for risk management is in charge of the administration of this Policy and, to that extent, will manage its compliance, disclosure, and updating with the areas involved in the Company. It will be updated in accordance with legal provisions, organizational changes, or other aspects that may affect the guidelines described herein.

This Policy shall come into effect as of its adoption by the Boards of Directors or equivalent bodies.

This policy repeals the following documents:

- Suampogro102 – Business Continuity Policy v1.0 – August 2014
- Suampogro100 – Operational Risk Management (ORM) Policy v1.2 - August 2016.
- Suampogro101 - Technological Risk Management (TRM) Policy – October 2021

“This document is the property of SURA Asset Management. Any use, disclosure, or reproduction of this document, in whole or in part, is prohibited without prior written”