PO-PROC-001
POLICIES FOR OPERATIONAL RISK MANAGEMENT

MACROPROCESS
COMPREHENSIVE RISK MANAGEMENT

PROCESS
OPERATIONAL RISK AND INTERNAL CONTROL MANAGEMENT

Approvals		
Process Owner	Paula Andrea Orozco Botero	Helber Alonso Melo Hernández
Title	Internal Control Director	Risk Vice President

Policies "Process Map" V1

TABLE OF CONTENTS

1 CHAPTER I - POLICIES

1.1 GENERAL POLICIES

Operational Risk Management is subject to the guidelines established in the Comprehensive Risk Management System "SIAR".

Through its Operational Risk Management policies, the Bank's Board of Directors establishes general guidelines that must be complied with within the Bank to prevent or mitigate losses resulting from human error, process inadequacies, technology failures, or external events.

1.1.1 Proportionality

Operational Risk Management must be directly related to the Bank's operating model, organizational structure, and size.

1.1.2 Commitment

The Bank's Board of Directors and Senior Management are committed to appropriate management and control of the risks arising from the performance of its corporate purpose and recognize Operational Risk Management as a tool that guides managers and employees in the administration and oversight of this type of risk within the Bank as an integral part of its business activity.

1.1.3 Operational risk management culture

Operational Risk Management seeks to enhance understanding of the operational risks that may affect the Bank's operations, as well as the tools to prevent or mitigate their occurrence. Operational Risk Management supports the establishment of the measures required to reduce losses associated with operational risks, improve the Entity's controls and processes, through systematic identification, measurement, control, and monitoring of risks.

Accordingly, Operational Risk Management is a fundamental element in reinforcing the institutional commitment to a solid risk management culture within the Bank, based on the principles of operational quality, productivity, efficiency, and operational resilience as a guiding framework for excellence in execution and the continuous improvement of the Bank's activities.

1.1.4 Responsibilities

The Board of Directors approves the risk appetite, the policies, and the operational risk management model in accordance with the Comprehensive Risk Management System "SIAR". It also oversees Management to ensure that the risk appetite, policies, processes, and other model components are effectively implemented.
Operational risk roles and responsibilities are defined under the three lines methodology, whereby the areas responsible for the Bank's processes (operational, commercial, and business support) are responsible for the identification and assessment of operational risks, the design of controls, and operational risk management. The Risk Vice Presidency and its support areas are responsible for the governance of the operational risk management model, and for providing guidance and monitoring to support its effective implementation, while the internal and external control bodies conduct the independent evaluation of the model and its implementation.

The three lines must include outsourced activities within the scope of their evaluations.

The administration and oversight of operational risks constitute an integral part of the activities carried out by each of the Bank's employees.

It is the responsibility of the Bank, through the Risk Vice Presidency and its support areas, to know, comply with, and enforce the applicable legal provisions currently in force, as well as the guidelines established in the Corporate Policy for Operational Risk Management, issued and updated by Grupo Aval.

1.1.5 Business Continuity

The Bank maintains continuity plans to ensure its operational capacity in the event of material and/or reputational impacts affecting the availability of critical business processes and/or events that may affect the ordinary course of operations.

The Bank has defined, implemented, tested, and maintained, in accordance with its structure, size, corporate purpose, and support activities, business continuity management, which includes elements for prevention and emergency response, crisis scenario management, contingency plans, and the capacity to resume the Bank's normal operations.

The Bank's business continuity plans comply with the following minimum requirements:

a. They must pass the necessary tests to confirm their effectiveness and efficiency.
b. They must be communicated to all relevant stakeholders.
c. They must cover at least the following aspects: identification of risks that may affect operations, activities to be carried out when failures occur, alternative operating procedures, and return to normal operations.

1.2 POLICIES REGARDING THE STAGES OF OPERATIONAL RISK MANAGEMENT

Operational risk management is carried out through the following stages:

- Risk identification
- Risk measurement
- Risk control
- Risk monitoring and evaluation

These stages must be applied continuously to maintain ongoing monitoring of the identification, analysis, and assessment of operational risk, considering the evolution of risks arising from changes in the environment or changes in the Bank's processes, and thereby prevent unexpected losses or impacts on the Bank's trust and reputation.

The identification, measurement, control, and monitoring of operational risks are carried out by each process owner with the advisory support of the Risk Vice Presidency and its support areas, under a uniform methodology that allows systematic and comprehensive assessment. The applicable methodology is defined in this Manual. The results of applying the methodology to the processes form the Bank's operational risk map.

When the need to outsource activities or processes is identified as part of the Bank's strategies and plans, an operational risk analysis must be conducted before outsourcing. Depending on the criticality of the processes, the risks associated with service provision must be identified, the required control activities must be established, as well as the corresponding measures for verifying compliance with these measures and for managing operational risk as part of the monitoring and evaluation of third parties.

Risk and control assessments of processes must be performed when:

- A process is designed, redesigned, or undergoes maintenance. In this case, risk and control assessment is carried out once a complete definition of the new processes to be executed is available.
- Reports are received from internal or external control bodies related to the process.
- Risks inherent to the process materialize, or external risk events become known that may affect the process.
- The scheduled periodic review is carried out.

1.2.1 Risk identification

Operational risk identification is carried out across all macro-processes and procedures within the Bank's value chain, as defined by the area responsible for the Bank's processes, considering internal and external risk factors, to identify possible events that may generate losses from this type of risk and anticipating their potential occurrence.

Operational risks are identified and assessed at the sub-process level and must include risks arising from contracts and service agreements with third parties that support the Bank's processes.

Before the launch of any process, product, service, or channel, or any related modification, operational risks associated with such implementation must be identified and assessed to establish controls that mitigate the Bank's risks.
Evaluations conducted by control bodies, as well as materialized risk events, must serve as inputs for identifying new operational risks or to validate, refine, complement, or reformulate existing risks or their causes.

Process owners are responsible for comprehensively assessing operational risk for all new processes, activities, products, and systems, and for maintaining continuous monitoring to confirm that no significant changes have occurred in the processes. This is an ongoing responsibility of all process owners, who must inform the Operational Risk Management Unit of significant process changes that may affect the existing risk assessment and risk profile.

1.2.2 Risk measurement or assessment

Risk evaluation and risk levels are determined using assessment criteria designed to estimate the impacts that operational risk would generate if it materialized. These operational risk evaluation criteria are defined in accordance with the level of risk the Bank is willing to accept and are approved by the Board of Directors. Inherent and residual risks are classified according to the evaluation criteria.

When data are available through sources such as the database of materialized events, process indicators or statistics, or findings from reports issued by control bodies, measurement must be conducted quantitatively; in cases where no historical records on the risk are available, measurement shall be qualitative.

1.2.3 Risk control

Control must be established based on the analysis of the risk and/or its causes, the type of risk, and the inherent risk level, considering, among other factors, the following aspects:

- The favorable cost-benefit relationship in relation to the expected outcome.
- Emphasis on preventive controls over detective or corrective controls. Preventive controls act on the causes of risks and therefore reduce their likelihood of occurrence. Detective or corrective control influence the effects of the risk and reduce its impact.
- Preference for key automated controls, to the extent that, according to the Bank's priorities, these can be implemented.

- The adequacy of the control framework, that is, whether controls individually or in combination can manage the risks.
- The required timeliness of controls.

The Process Owner shall monitor the effectiveness of the established measures or controls once they are operational, as part of the ongoing monitoring of compliance with the day-to-day responsibilities of the process or through periodic control monitoring.

Process owner areas and internal and external control bodies shall ensure consistency between what is documented and how controls are operated.
Evaluations conducted by internal and external control bodies, as well as materialized risk events, must serve as input for:

- Validating and updating the rating of control design and execution.
- Assessing the need to redesign existing controls or design new controls.
- Taking corrective actions in response to deviations in their application.

Controls that do not meet prevention and/or mitigation characteristics shall be subject to an action plan aimed at mitigating, reducing, sharing, or accepting the risk, in accordance with the Bank's established requirements and accepted risk profiles.

1.2.4 Monitoring

The Bank must conduct overall monitoring of Operational Risk Management, including the monitoring of the Bank's operational risk profile and risk appetite in accordance with the guidelines established in the Comprehensive Risk Management System "SIAR".

1.3 POLICIES REGARDING THE ELEMENTS OF OPERATIONAL RISK MANAGEMENT

1.3.1 Organizational structure

The Bank must define the organizational structure required for the proper operation and maintenance of operational risk management, considering the responsibilities of the governance, administration, and control bodies established under current SIAR regulations and the policies and procedures contained in this manual.

The Bank must ensure that operational risk management functions are assigned to personnel with subject-matter expertise and adequate experience to fulfill their responsibilities.

1.3.2 Control bodies

Control bodies are responsible for conducting independent evaluations of Operational Risk Management, to confirm its proper functioning or identifying opportunities for improvement or potential failures in the management system. The results shall be reported in accordance with the SIAR guidelines.

1.3.3 Processes and documentation

The Bank, through the Risk Vice Presidency and its support areas, shall establish the processes for the development of Operational Risk Management. The policies, methodologies, and processes of Operational Risk Management must be documented, kept up to date, and made available to all areas and employees involved in operational risk management.

The Bank must maintain documentation evidencing the application of the risk management methodology.
Non-compliance with the obligations set forth in Operational Risk Management, section 1.3.9 of this document, shall give rise to the applicable disciplinary measures in accordance with the Internal Labor Regulations.

1.3.4 Event recording

An operational risk event registry shall be established and updated based on at least the data and criteria established by the Financial Superintendence of Colombia. The Bank shall define the necessary mechanisms to analyze and evaluate operational risk events to adopt the appropriate measures to prevent the occurrence of new events.

1.3.5 Accounting disclosure

Losses that affect the income statement must be recorded in operational risk expense accounts in the period in which the loss materialized.

Recoveries related to operational risk that affect the income statement must be recorded in income accounts in the period in which the recovery materialized.

1.3.6 Technological infrastructure

The Bank shall maintain technological tools that support compliance with the policies and procedures established by the Bank in this matter and that allow appropriate operational risk management. In this regard, the Bank adopts the use of corporate tools defined by Grupo Aval for common risk management across the banks, as well as any others that the Bank deems necessary or appropriate. The scope and timelines for the implementation of these tools will be defined according to institutional capabilities and priorities, as well as the availability of required financial resources and the cost/benefit ratio of the tools.

1.3.7 Training

Training sessions shall be conducted on the topics that comprise Operational Risk Management, targeting all Bank employees and to third parties supporting the Entity's processes, at least on an annual basis, as well as to new employees during the induction process, third parties under contractual relationships performing functions for the Bank, and those who, due to their responsibilities, must have specialized knowledge regarding the administration and oversight of operational risk. In all cases, evaluation mechanisms shall be applied to determine the effectiveness of the training delivered.

1.3.8 Information disclosure

The necessary reports and information flows shall be established to support proactive operational risk management by all participants in the operational risk management model.

The Bank's work in relation to operational risk management shall be disclosed in accordance with the guidelines established in SIAR.

1.3.9 Measures for non-compliance with operational risk management

The Risk Vice Presidency and its support areas shall monitor compliance with the responsibilities and procedures of Operational Risk Management and shall communicate the results to process owners and their immediate supervisors to support the adoption of appropriate improvement measures.

Internal and external control bodies, through their periodic visits to different areas, shall conduct independent evaluations of compliance with the policies, procedures, and controls related to Operational Risk Management, to detect deviations and recommend the necessary corrective actions.

The procedures to be followed in the event of non-compliance with commitments related to operational risk management must be aligned with the provisions set forth in the Internal Labor Regulations. When non-compliance involves third parties linked to the Bank, the provisions defined for contractual breach shall apply.

1.4 ORGANIZATIONAL STRUCTURE

1.4.1 Structure for Risk Management

The Bank's Operational Risk Management is led by the Risk Vice Presidency and its support areas, with the involvement of all Bank employees.

1.4.2 Functions and Responsibilities

The following functions and responsibilities apply to the governance, administration, and control bodies defined by the Bank for the proper administration and oversight of Operational Risk:

Board of Directors

- Approve the specific policies related to Operational Risk Management, as well as their periodic review and updating.
- Monitor and provide feedback on the Bank's operational risk profile, as well as on the quantification of capital requirements for such risk, based on the reports submitted by the legal representative and/or President to the Board of Directors.

Non-Financial Risk Committee

The responsibilities of this Committee are defined in the Regulations of the Bank's Non-Financial Risk Committee, and are applicable to Operational Risk Management.

Risk Vice Presidency – Legal Representative

- Lead the development and updating of Operational Risk Management, and submit relevant updates to the legal representative.
- Submit the Operational Risk Policy and its updates for approval by the Board of Directors.
- Establish guidelines for the design and maintenance of methodologies, tools, models, and procedures for Operational Risk Management.
- Periodically report the evolution and relevant aspects of Operational Risk Management to the President of the Bank.
- Propose updates to Operational Risk Management to the Bank's Presidency.
- Evaluate the reports submitted and take corrective actions on Operational Risk Management.
- Submit a report, at least semi-annually, to the Board Risk Committee and the Non-Financial Risk Committee on the evolution of operational risk, the controls implemented

and the monitoring performed, as well as the preventive and corrective actions implemented or planned and the identification of the responsible areas.

Operational Risk Management Unit

- Define and keep methodologies, tools, and procedures up to date, tools, and procedures for operational risk administration and oversight.
- Develop and implement the Bank's internal and external operational risk reporting system.
- Manage the operational risk event database.
- Coordinate the collection of information to populate the operational risk event registry, ensuring compliance with the criteria defined by the Financial Superintendence of Colombia to maintain a high-quality event database for determining operational risk exposure.
- Establish and monitor the Bank's risk appetite, operational risk profile, and operational risk exposure value; evaluate the control measures adopted; and prepare reports on the development of Operational Risk Management for the President, the Non-Financial Risk Committee, and the Board Risk Committee.
- Submit Operational Risk Management reports to the Non-Financial Risk Committee.
- Propose roles and responsibilities related to operational risk management for the different areas of the Bank, including outsourced activities, to support appropriate operational risk management.
- Monitor the effectiveness of controls associated with risks rated as high.
- Continuously monitor compliance with policies and procedures related to Operational Risk Management, propose the corresponding updates and/or modifications, and ensure the proper functioning of Operational Risk Management.
- Monitor the follow-up of operational risk management action plans.
- Develop, together with the relevant area, the Bank's training programs related to Operational Risk Management.
- Train and advise areas on the proper use of methodologies, tools, and processes of Operational Risk Management.
- Periodically monitor the content of information databases and ensure the implementation of necessary corrective actions.
- Coordinate, consolidate, validate, and monitor the budget of operational risk accounts.
- Follow up on the actions undertaken by process owners and risk managers, providing the necessary advisory support.
- Periodically report the results and management of Operational Risk Management to Vice Presidents and Process Owners.
- Prepare the Operational Risk Management Manual and its updates.
- Prepare and submit the Quarterly Report on the Current Status of Operational Risk for the Bank to the Corporate Risk Vice Presidency, under the format designed by Grupo Aval.
- Promptly inform the Grupo Aval Corporate Risk Vice Presidency about operational risk events that materialize with significant impact or frequency.

- Promote the development of training and communication strategies for Operational Risk Management.
- Ensure that the operational risk event registry complies with criteria of timeliness, integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality of the information contained therein.
- Develop policies, procedures, strategies, methodologies, models, thresholds and/or limits, controls, contingency plans, the business continuity plan, and the early warning and monitoring indicators framework for Operational Risk Management.

Bank Process Areas

- Support operational risk managers and/or process owners in updating and documenting the controls under their responsibility.
- Assist process owners and/or Operational Risk Managers in defining, developing, and implementing action plans required for effective operational risk management.

Vice Presidencies and Departments Reporting Directly to the Presidency

- Ensure and promote the application of policies, standards, methodologies, processes, and monitoring schemes defined for the management of operational risks in the processes under their responsibility.
- Maintain awareness of the operational risk profile of their processes and promote the adoption of risk treatment measures to manage them appropriately, considering the information reported by the Operational Risk Management Unit.
- Participate, within their area of competence, in verifying the quality performance of the controls established within the Bank, in order to identify and prevent risks in their area.
- Approve the definition and tolerance level of the indicators established for operational risk monitoring.
- Approve and promote the design of action plans developed to prevent and/or mitigate operational risks.
- Promote among employees in their areas the completion of training related to Operational Risk Management.

Process Owners

- Prepare and approve the operational risk matrices for the processes under their responsibility.
- Certify the operational risk matrices for the processes under their responsibility.
- Assess the effectiveness of the control measures used to mitigate residual risks.
- Ensure the reporting of operational risk events within their processes, analyze them, and monitor their follow-up.
- Define and monitor operational risk indicators and the risk profile of the processes under their responsibility.
- Manage prevention and/or mitigation measures for operational risks that materialize.

- Ensure the quality and consistency of information reported to the Operational Risk Management Unit.
- Establish the commitments, action plans, and improvement plans required for the effective development of Operational Risk Management, manage their execution, and ensure compliance.
- Appoint operational risk managers required within the processes under their responsibility, where applicable.
- Disclose the results and evolution of Operational Risk Management within their area to the relevant authorities.
- Ensure that employees within their area and external suppliers supporting their processes complete training on Operational Risk Management.
- Evaluate the effectiveness of contingency plans and the business continuity plan.
- Establish measures to mitigate risks associated with outsourced activities or processes under their responsibility related to service delivery and ensure compliance for monitoring and evaluation of the third party.

All Bank Employees

All Bank employees are involved in operational risk management, as any employee may identify potential risks or operational risk events. Therefore, all Bank employees have the following responsibilities regarding Operational Risk Management:

- Comply with the policies, standards, processes, procedures, and controls established to contribute to the reduction or appropriate maintenance of risk levels.
- Strengthen the control environment both within their respective area and within the Bank as a whole.
- Report in a timely manner any events related to Operational Risk Management, whether actual or potential, in accordance with the terms established in this document.
- Identify any change that may impact the operational risks associated with their assigned activities and communicate it promptly to the Process Owner, the Risk Manager, and/or their direct supervisor.
- Participate in the training and education processes provided by the Bank.

CHANGE LOG

Version History			
Version #	**Publication date**	**Description of changes**	**Professional**
1	07/07/2021	Creation of the SARO Policies document under the new architecture structure.	Katerin Mancipe
2	05/30/2023	The document is updated in accordance with the guidelines of the SIAR document.	Jeisson Hernández
3	09/17/2024	The Policy is modified by updating the organizational structure illustration, the name of the Comprehensive Risk Management to Risk Vice Presidency, and Consolidated Committee to Board of Directors Risk Committee in accordance with Board of Directors Minutes 2789 dated March 21, 2024.	Sebastian Andrade C
4	12/13/2024	The policy is modified as follows: Removed: The functions of the presidency, incorporated under the Risk Vice Presidency functions. Legal Representative. References to subsidiary control mechanisms. The detailed organizational chart of operational risk management, replacing it with a general reference to the organizational structure supporting operational risk management. The champion role is eliminated and the responsibilities of the risk manager and reporter are transferred to the operational risk guidelines. Specific area names, replaced with general references as follows: VP risk support areas, area responsible for Bank processes, and area responsible for training processes. Added or supplemented: Business continuity and training section. Functions of the Risk Vice President. Legal representative, area responsible for operational risk management.	Jahir Morales
5	11/18/2025	Update due to change of process owner and reassignment of Subprocess Manual.	Jenny Pabón