POLICY

For

Managing Risk Over Financial Reporting

MACROPROCESS

Manage Risk Systems

Approvals	
Process Owner: Luz Patricia Chitiva Lozano	Dr. Helber Alonso Melo Hernández
Title: Operational, Strategic and Subsidiary Risk Manager	**Title:** Risk Vice President

TABLE OF CONTENTS

1. OBJECTIVE

This document has been prepared with reference to the Corporate Compliance Manual for SOX Law and the Corporate Policy for the Integrated Risk Management Administration of Grupo AVAL.

2. GENERAL POLICIES

Through this Policy, the Bank's Board of Directors establishes the guidelines that must be followed to maintain an effective internal control system over the Bank's financial statements.

The Board of Directors and the Bank's Senior Management are committed to compliance with the SOX Law so that, through appropriate risk management and administration, material misstatements in the financial statements—whether due to fraud or error—are prevented or detected in a timely manner, and the necessary remediation measures are taken.

The Bank is responsible for complying with and enforcing the policies, guidelines, and methodologies established in the SOX Law Corporate Compliance Manual, as well as the instructions issued by Grupo AVAL on this matter. The Bank is also responsible for communicating these documents to its subsidiaries, guide them in their adoption, and monitor compliance with them. In all cases, consideration must be given to the specific characteristics of the activities carried out by the Bank and each subsidiary.

The risk appetite, tolerance level, and risk capacity regarding the Bank's financial reporting are established considering the criteria defined in the internal Risk Appetite Framework (RAF). The Bank's President ensures that financial reporting risk management is implemented throughout the Bank and that it is consistent with the risk appetite and tolerance levels adopted.

The Bank adopts COSO 2013 (Committee of Sponsoring Organizations of the Treadway Commission) as the reference framework for financial reporting risk management.

Roles and responsibilities for financial reporting risk are defined under the three lines model, as follows: I. Risk management by each business line. II. A risk management function. III. Independent review, in accordance with the Integrated Risk Management Framework Policy of Grupo AVAL.

The Bank's President appoints the area responsible for leading, implementing, and coordinating compliance with the SOX Law, promoting the adoption of a robust culture of financial reporting risk management within the Bank.

3. RISKS

The Bank evaluates financial reporting risks annually and submits proposed changes to Grupo AVAL. The SOX compliance scope (entities, accounting accounts, and processes — including their naming), the SOX Risk Inventory, and the inherent risk rating are defined annually by Grupo AVAL and are not subject to modification by the Bank.

The Bank updates financial reporting risks before the end of the first calendar half-year of each year in accordance with the scope and SOX Risk Inventory defined by Grupo AVAL.

4. CONTROLS

SOX controls are established based on the analysis of the Bank's financial reporting risks, identifying key or critical activities both at a cross-functional level within the Bank and at the level of each process, required to prevent or detect errors or potential fraud in the initiation, recording, processing, reporting, or disclosure of the Bank's financial statements.

The identification and design of SOX controls are performed by each process owner in which the risk is present, with the guidance and support of the Bank's SOX team, considering the Control Baselines, the control design guidelines defined in the SOX Compliance Corporate Manual, instructions from Grupo AVAL, and applicable best practices, in line with the Bank's operational and technological environment. SOX controls must include activities designed to protect the integrity, accuracy, and validation of information processed, sent, and received from third parties that affect the Bank's financial statements.

Process owner areas, as part of their day-to-day process responsibilities, are responsible for ensuring the effectiveness of the established SOX controls and for identifying changes in SOX controls arising from new processes, activities, products, and systems, and for reporting them promptly to the Bank's SOX team so that these changes can be evaluated and controls can be updated or created, as applicable.

All deficiencies associated with the design or operation of SOX controls identified through evaluations by internal and external control bodies must be managed and remediated in a timely manner by process owners. At the end of each semiannual evaluation period, the Bank must classify and analyze deficiencies to determine their individual or combined impact, determine whether the risk materialized, and assess the need to adopt additional measures that provide reasonable assurance regarding the Bank's internal control over financial reporting.

5. MONITORING

The SOX-designated area appointed by the Presidency conducts ongoing monitoring of compliance with the SOX Law methodology established in the Bank's Corporate SOX Compliance Manual.

On a quarterly basis, the results of financial reporting risk management are presented to the Non-Financial Risk Committee, composed of Vice Presidents and Managers reporting directly to the Presidency and responsible for processes within the SOX scope, to ensure that corrective actions are taken as appropriate.
The actions to be implemented when SOX indicator results exceed established thresholds are presented to the Bank's Board Risk Committee together with the corresponding action plans.

5.1. CERTIFICATION OF THE INTERNAL CONTROL SYSTEM OVER FINANCIAL REPORTING

Each year, the Bank must certify to Grupo AVAL the effectiveness of its Internal Control System over Financial Reporting.

The Bank's certification must be submitted together with the certifications of its subsidiaries, formalized by email to the corporate office.

6. RESPONSIBILITIES

The SOX compliance process requires oversight by the Bank's senior management and its subsidiaries, as well as the establishment of roles and responsibilities for each phase of the process, across each department and function involved, to support the success and sustainability of the process.

Senior management commitment and sponsorship are required for the following reasons:

- By its nature, the SOX Law affects many of the Bank's departments and subsidiaries, and Grupo AVAL directly.
- Some employees may perceive SOX compliance efforts as being associated only with financial, accounting, or internal audit functions, rather than with all processes and the Bank's internal control system.
- Completing the SOX process annually requires significant time and resources from the Bank.

Banco Popular has structured its risk-related functions and responsibilities, following the methodology defined in the three lines model for Risk and Control Management, according to the Corporate Policy for Integrated Risk Management Administration, which defines:

1. <u>First Line – Business Line Management:</u> corresponds to the operational, commercial, and support areas that manage the business.
2. <u>Second Line – Independent Operational Risk Function.</u>
3. <u>Third Line – Independent Review:</u> corresponds to Comptrollership Management, which is responsible for reporting its findings to the Board Audit Committee.

The general activities of each key participant in the process are detailed below:

6.1. BOARD OF DIRECTORS

- Maintain overall responsibility for compliance with the Sarbanes-Oxley Act across the Bank and its subsidiaries.
- Ensure that management has implemented an adequate internal control system over the preparation and presentation of Financial Statements.
- Remain informed of the scope defined by management for compliance with SOX requirements each year.
- Receive relevant information regarding any fraud or any significant internal control failure affecting financial statements.
- Be informed of the conclusions of the evaluation of internal control over financial reporting.

6.2. AUDIT COMMITTEE OF THE BOARD OF DIRECTOR

- Provide information on the SOX review process when requested by the Grupo AVAL Audit Committee.
- Receive and analyze relevant information on any fraud incident or significant internal control failure, evaluate Management's follow-up, and report such matters to the Grupo AVAL Audit Committee.
- Request that the Internal Audit, External Audit, and SOX teams keep it informed of the results of their independent validations of the design and operation of key controls.
- Review the Bank's Financial Statements before their submission.
- Evaluate whether Management is implementing an appropriate "Control Culture," communicating the importance of internal control and risk management.
- Maintain communication with the Grupo AVAL Audit Committee on matters deemed relevant, related, among others, to:
    - Recommendations on guidelines, policies, principles, models, and methodologies that, in their opinion, should be applied in matters of internal control.
    - Evaluation of whether Management is implementing an adequate "Control Culture," communicating the importance of internal control and risk management.
    - Evaluation of the effectiveness of internal control and risk management, and consideration of whether recommendations made by internal and external auditors have been implemented by Management.
- Review the effectiveness of the Whistleblowing System (Ethics Line) to monitor compliance with standards, regulations, internal policies, and industry standards, as well as the results of investigations and management follow-up (including disciplinary actions) of any fraudulent act or non-compliance.

- Receive periodic reports from the Comptrollership Management regarding complaints received through the Ethics Line that have a material impact on the Bank's financial statements, strategies, operations, or reputation.
- Issue recommendations based on the results of Internal and External Audits.
- Ensure that significant findings and recommendations made by internal auditors, as well as management's proposed response, are received, discussed, and properly managed.

6.3. PRESIDENT AND FINANCIAL VICE PRESIDENT

- They are responsible for the effectiveness of the Internal Control System over the processes and controls under their responsibility.
- Promptly inform the President and Financial Vice President of Grupo AVAL of the results of the internal control assessment, especially regarding any matters that could affect the Entity's internal control.
- They are co-responsible for the completion, signing, and reporting of the compliance certification regarding the evaluation and validation of the effectiveness of the Bank's internal control to Grupo AVAL, and must ensure that such certification is properly supported with the corresponding evidence.
- Analyze reports from internal and external audits to identify potential impacts on their processes and controls and take the respective corrective actions.
- Follow up on the prior-year RDC and ensure corrective actions are implemented in a timely manner.
- Notify the SOX Officer and Risk areas about changes in operations, risks, or responsible parties.
- Appoint the Bank's SOX Officer and provide the human and technical support required to perform their duties, as well as define an appropriate succession plan for the Bank's SOX Officer role, ensuring the continuous training of this officer.
- Actively participate in the Bank's Consolidated Risk Committee to monitor process progress, results, and remediation plans when necessary.
- Ensure that all necessary remediation plans are properly and promptly implemented to minimize the risk of errors in the financial statements.
- Obtain, through the SOX Team, the certifications of the Bank's subsidiaries, in order to support their own certification to Grupo AVAL.

6.4. VICE PRESIDENTS AND MANAGERS (N+1) – SOX CONTROL OWNERS

- Be responsible for the effectiveness of internal control over the processes under their responsibility.
- Actively participate in the Regulatory Risk Committee and the Consolidated Risk Committee convened within the Bank.
- Monitor the progress of the SOX roadmap in the processes under their responsibility, as well as its outcomes.

- Ensure that all process owners or control owners under their supervision continuously verify that the controls designed to mitigate risks remain valid, documented, communicated, and monitored.
- Design and implement monitoring within the processes under their responsibility that enables the identification of failures in control execution, ensuring that key controls over financial reporting are executed consistently as designed.
- Analyze reports from internal auditors, external auditors, statutory auditors, and other supervisory and control bodies to identify situations that could indicate control failures under their responsibility, determine their impact, and report them to the Bank's SOX Officer.
- Follow up on the RDC (Control Deficiency Report) for the processes under their responsibility and ensure that required corrective actions are implemented in a timely manner.
- Ensure that their work teams (Control Owners) remain trained in SOX-related topics.

6.5. PROCESS OWNERS OR SOX CONTROL OWNERS

- Design and implement the necessary controls to mitigate the risks associated with their responsibilities, with the support of the SOX Team, ensuring their implementation and continuous execution.
- Act as the primary owners of their respective process/control to ensure proper documentation thereof; therefore, they are responsible for understanding the associated risks, implementing controls to mitigate them, and providing evidence of their effectiveness.
- Know and understand the risks and controls under their responsibility and their importance within the overall process.
- Provide evidence-related information of the controls under their responsibility to internal and external supervisory and control bodies, in a complete and timely manner.
- Ensure that the financial information they generate is consistent, accurate, and complete from its determination through the final presentation of the Financial Statements and their disclosures.
- Inform the SOX Team and the Vice President of their area of any training needs related to Internal Control and the SOX process.
- Inform the SOX Officer, SOX Team, and the Vice President of their area about changes made to control activities, processes, or information systems, so that the SOX Risk and Key Control Matrix can be updated. Perform control monitoring (self-assessments, cross-reviews, etc.) to ensure that controls are properly executed, by continuously verifying that the controls designed to mitigate risks are in place, documented, communicated, monitored, and executed consistently throughout the entire period.
- Design, with the support of the SOX Team, appropriate remediation plans and implement them immediately.
- Remain informed of the results of control design and validation testing, and participate in the discussion of such results.

- Understand the results of independent testing by internal and external auditors, design and implement the necessary remediation plans.
- Promptly inform the SOX Officer and/or SOX Team when any failure in control effectiveness is identified as a result of control execution.
- Ensure, through an appropriate delegation scheme for all employees in the area, the continuous application of controls and their respective documentation throughout the period.
- Request the updating of controls under their responsibility in the SOX Matrix and inform the SOX Officer / SOX Team and the Vice President of their area whenever, during the year, they identify changes in risks or controls.
- Conduct an adequate, sufficient, and timely handover in the event of temporary or permanent departure of employees who execute SOX controls.

6.6. SOX TEAM

- Support the Financial Vice President in documenting key matters to be considered in SOX planning, and assist the Corporate SOX Officer in identifying qualitative aspects that should be considered when defining the scope.
- Support Process Owners / Control Owners in control rating. Advise Process Owners / Control Owners on identifying all controls required to reasonably mitigate key SOX risks.
- Ensure that communications and guidelines issued by Grupo AVAL are understood and applied in the Bank and its subsidiaries, through the subsidiaries' SOX Officers.
- Act as the first point of contact within the Bank for coordinating tasks to be performed in compliance with the evaluation of internal control under SOX regulations.
- Follow up on actions taken by process/control owners to ensure control design effectiveness.
- Identify and manage SOX training needs within the Bank. Share SOX knowledge within the organization.
- Provide ongoing support to Process/Control Owner Managers in the continuous improvement of the internal control system over financial reporting, and in the updating of the SOX Matrix, addressing changes in the business and audit recommendations.
- Ensure that process owners annually update control documentation in the matrix and retain evidence of such updates through forms, minutes, etc., and support process owners in maintaining and formalizing the SOX Matrix.
- Consolidate and monitor the progress and results of SOX work within the Bank. If relevant issues that could affect the certification are identified, inform the Corporate SOX Officer, the Vice President of Finance, and the President of the Bank.
- Analyze SOX work progress and report to the Corporate SOX Officer, identified deficiencies, and other matters that may be considered key for the SOX evaluation.
- Support Process Owners and Control Owners in the design of remediation plans.
- Prioritize, together with process owners, the remediation of deficiencies.
- Follow up on the remediation of all identified deficiencies, both in design and operation, to ensure their timely implementation by the Bank.

- Participate in the semiannual closing process for quantifying the deficiencies of the Bank and its CSCs (Spanish acronym) and in the identification of compensating controls, supporting Process Owners.
- Prepare the Bank's Control Dashboard for reporting to Grupo AVAL and monitor the management of its subsidiaries through their dashboards.
- Evaluate and report the Bank's progress and results using the format designed by Grupo AVAL for reporting purposes.
- Support the President and Vice President of Finance of the Bank in issuing the SOX 404 compliance certification.
- Maintain SOX process information at the Bank in a complete, accurate, and secure manner, and develop and establish mechanisms to ensure that documentation of control validation testing is properly safeguarded within the Bank.
- Ensure that all relevant process information required under the Group's evaluation methodology is stored in the repository defined by the Bank.
- Follow up on deficiencies not remediated in the immediately preceding year.
- Ensure the integrity and accuracy of the RDC, including impact quantification and probability of occurrence.

6.7. COMPTROLLERSHIP MANAGEMENT

- Obtain an understanding of the processes and/or controls to be validated through applicable auditing standards and best practices for internal control over financial reporting.
- Perform and document the independent evaluation of the design of controls, based on its judgment and the work plan approved by the Audit Committee of the Board of Directors.
- Perform the independent validation of the effectiveness of controls in accordance with the work plan approved by the Audit Committee of the Board of Directors.
- Communicate the results of its independent evaluations to the bodies designated within the Bank.

6.8. HUMAN TALENT CARE AND DEVELOPMENT MANAGEMENT

- Responsible for the induction process for new employees using the SOX Virtual Course prepared by the Bank's SOX Team
- Responsible for reporting SOX training needs they may identify, so they can be included in the annual training plan.
- Structure ongoing SOX training plans in coordination with the Bank's SOX Team.

6.9. VALUE CHAIN AND OPERATIONAL EXCELLENCE MANAGEMENT

- Responsible for advising the Process Owner in the design, updating, and documentation of the Bank's internal processes and related documents, in accordance with the request submitted by the Process Owner.
- Responsible for publishing and disseminating of the Bank's internal processes and related documents in the Virtual Library.

CHANGE LOG

VERSION HISTORY		
Version #	**Publication date**	**Description of change**
1	08/04/2022	The document "Policy for Managing Risk over Financial Reporting" is created under the macro process "Administer Risk Systems", associated with the process "Manage Risk over Financial Reporting – SOX".
2	12/15/2023	Update of the corporate SOX Policy, which was approved by the Board of Directors of Grupo Aval in its session of June 07, 2023.
3	09/02/2024	Change of title to Risk Vice President and renaming of Committees, in accordance with the approval given in Board of Directors Minutes 2789 dated March 21, 2024.