ENTERPRISE RISK MANAGEMENT SYSTEM POLICY

RISK MANAGEMENT MACROPROCESS

Banco Popular

2026

TABLE OF CONTENTS

1. INTRODUCTION

The Enterprise Risk Management System (ERMS) reflects the Bank's commitment to optimizing the processes used to consolidate the measurement and monitoring of the risks to which it is exposed in carrying out its corporate purpose, thereby improving the accuracy and timeliness of corrective actions.
The Bank is committed to strengthening its risk management capabilities in order to safeguard its financial soundness and support value creation for the Institution.

Within this framework, the implementation of the ERMS serves as a core mechanism for aligning the business plan with risk management. It also enables timely and comprehensive management of the risks inherent in the conduct of the Bank's business through the adoption of methodologies for risk identification, measurement, control, and monitoring. This provides both an enterprise-wide and specific view of the Bank's risk profile, thereby supporting more informed and appropriate decision-making.
The ERMS is based on leading risk management practices under the following reference frameworks:

- **Basic Accounting and Financial Circular (CBCF)** (External Circular 100 of 1995), **Chapter XXXI – Enterprise Risk Management System (ERMS)**, and its respective appendices.
- **Committee of Sponsoring Organizations of the Treadway Commission (COSO)** – **Enterprise Risk Management (ERM)**.
- **Basel Committee on Banking Supervision (BCBS)**.
- **PwC Risk Management Framework**.

2. PURPOSE

To establish a system that integrates the diverse risks monitored by the Bank through consolidation and governance methodologies that support their effective management, taking into account the impact that each risk management system has on the conduct of the Bank's business, with the objective of maintaining an appropriate risk-return balance.

3. SCOPE

The policies and guidelines set forth in this document constitute a governance framework and serve as a standing reference for all areas of the Bank.

Direct employees and temporary agency workers are responsible for complying with the provisions set forth in this document.

The Enterprise Risk Management System (ERMS) encompasses the management of the risks applicable to Banco Popular in accordance with the regulations issued by the Financial Superintendence of Colombia. It also provides guidelines for the Bank's subsidiaries, considering their nature, corporate purpose, and the risks applicable to their respective businesses.

4. RISK MANAGEMENT PRINCIPLES

The Bank's fundamental principles for optimizing risk management are designed to promote and strengthen a sound institutional risk-management philosophy that minimizes risk and maximizes value in the conduct of its operations, in accordance with applicable regulations and the requirements established by the supervisory authorities.

- **Governance and Oversight Principle:** The Bank ensures that an appropriate governance structure is in place to guarantee effective control and oversight,

clearly defining the roles and responsibilities associated with each stage of the risk management process.

- **Transparency and Perspective Principle:** The Bank ensures that risk management is carried out in accordance with the policies and procedures established by the Institution, which are communicated together with the processes implemented within the Integrated Risk Framework.
- **Adaptability Principle:** The Bank periodically reviews and evaluates the appropriateness of its risk management methodologies and policies to ensure that they remain dynamic and responsive to internal and external changes.
- **Security Principle:** The Bank establishes risk policies and limits that are consistent with its defined risk appetite, the regulations in force, Grupo Aval's Corporate Risk Policy, and the Bank's business objectives.
- **Zero Tolerance for Bribery and Corruption Principle:** The Bank is committed to a zero-tolerance policy toward corruption in any form. It promotes a culture of preventing and combating corrupt practices and conducts its business and operations in accordance with the highest ethical standards and in compliance with applicable laws and regulations.
- **Priority Principle**: For the Bank and its subsidiaries, compliance with applicable regulations and protection of the Institution's reputation—particularly with respect to events related to money laundering and terrorist financing—shall prevail over the achievement of commercial objectives or any other institutional or personal interest.

5. THREE LINES MODEL

The Bank's risk management framework is based on the Three Lines Model

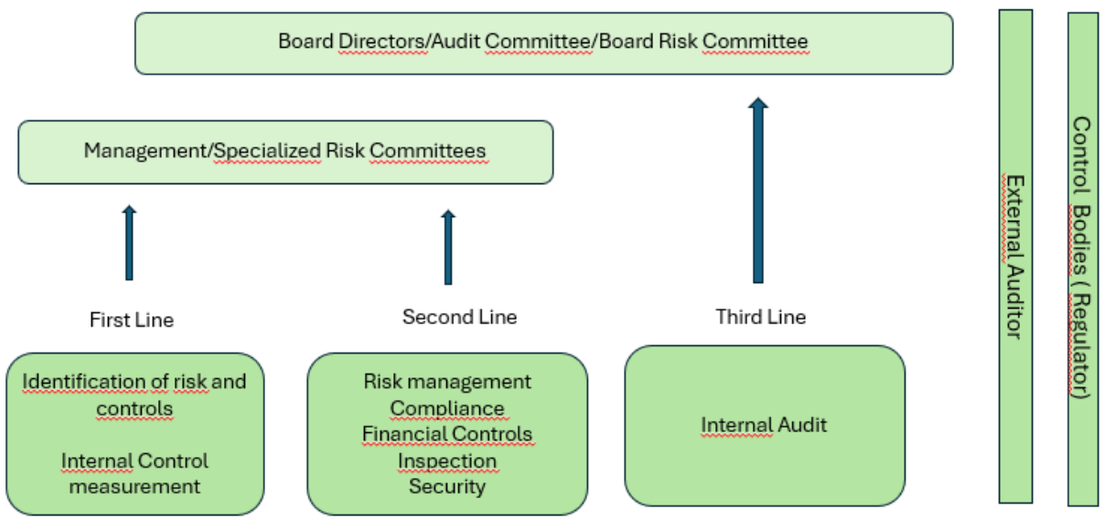

Figure 1 – Three Lines Model

- **First Line:** As the process owner, it is responsible for identifying, measuring, and controlling risks, it owns them and is responsible for their administration. It recognizes and manages the risks assumed in the performance of its activities and is responsible for implementing preventive and/or corrective actions to address process and control deficiencies.
- **Second Line:** It is responsible for supporting the measurement and control of the Bank's risks through an appropriate methodology, as well as monitoring the effectiveness of risk controls and issuing the corresponding reports, independently from the activities performed by the first line. It assists and/or advises process owners in risk management by facilitating and monitoring the implementation of effective risk management practices by the first line. Likewise, it is responsible for monitoring the security of information assets, a function that must be carried out with functional and organizational independence.
- **Third Line:** It performs its functions independently, reports directly to the Institution's highest level of management, and maintains an active reporting line to the corporate governance bodies. It is responsible for conducting risk-based audits and reviews, providing assurance over the control framework, and verifying that

the policies approved by the Board of Directors exist and are effectively implemented.

6. ERMS (Enterprise Risk Management System) POLICIES

To achieve the objectives of the Enterprise Risk Management System (ERMS), the following policies are established in accordance with leading practices:

- The Bank manages a diverse range of risks that are grouped according to their nature and the types of processes from which they arise, in order to develop specialized methodologies for risk identification, measurement, control, and management. The management of each type of risk is supported by independent management and governance models, all of which operate within the framework of the Enterprise Risk Management System (ERMS).
- The ERMS shall be directly aligned with the Bank's strategies, objectives, business plan, capital and liquidity levels, the management of interest rate risk in the banking book (IRRBB), the Bank's and its subsidiaries' Risk Appetite Framework (RAF), the operating model, the organizational structure, and the size of the Institution.
- The ERMS shall promote ongoing dialogue with Senior Management on risk management by establishing actions that maintain an appropriate balance between profitability and risk.
- Senior Management is committed to the effective governance of the Enterprise Risk Management System and the risks identified during its implementation. In addition, it shall recognize the ERMS as the guiding framework for executives and employees in the risk governance and management throughout the Bank.
- The ERMS includes a description of the objectives, methodologies, models, controls, and limits applicable to the level of consolidated risks that the Institution is willing to assume.
- The Risk Appetite Framework (RAF) forms an integral part of the ERMS, and any update to either shall require the review and potential amendment of the other.
- Senior Management shall communicate the ERMS and its components to the Board of Directors, the Risk Committee, the External Auditor, and throughout the Bank, with the objective of reinforcing a risk-aware culture and adopting preventive and/or corrective measures in the event of non-compliance.
- The Bank shall seek to maintain alignment and balance between its commercial strategies and the actions undertaken in relation to risk management.
- The Bank maintains business continuity plans to ensure its ability to operate in the event of material operational and/or reputational impacts affecting the availability of critical business processes and/or other events that may disrupt the ordinary course of business.
- The Enterprise Risk Management System (ERMS) includes communication and reporting guidelines addressed to the various governance bodies.
- The ERMS shall be reviewed and evaluated at least once a year to ensure its continued suitability and effectiveness, taking into account the results of assessments conducted by internal and external oversight bodies, regulatory and corporate changes, and macroeconomic or other prevailing conditions that may have an impact on risk management.
- The Bank shall establish guidelines for managing, communicating, and approving intragroup transactions and transactions involving affiliates and related parties.
- The internal control framework shall be aligned with the provisions of the Enterprise Risk Management System (ERMS).
- Based on the information available, the Bank shall cooperate with the supervisory and oversight authorities by providing any information requested in relation to the ERMS.
- As part of its external-environment assessment, the Bank identifies emerging risks and monitors them in accordance with the corporate guidelines and the provisions of the ERMS.
- The ERMS policies and the processes derived from them shall be mandatory for all direct employees of the Bank and temporary agency workers at every organizational level.

- All Bank employees shall identify and report any actual or potential conflicts of interest related to the ERMS in accordance with the provisions of the Bank's **Code of Ethics and Conduct**.
- The Bank shall develop an annual training plan to enable all employees to strengthen their competencies in risk management.
- Information shall be handled in accordance with the provisions of the **Code of Ethics and Conduct** approved by the Bank's Board of Directors.

7. GOVERNANCE STRUCTURE

The Enterprise Risk Management System (ERMS) is supported by an organizational structure with roles and responsibilities that are clearly defined, documented, communicated, and understood across the Bank.

7.1. Organizational Structure

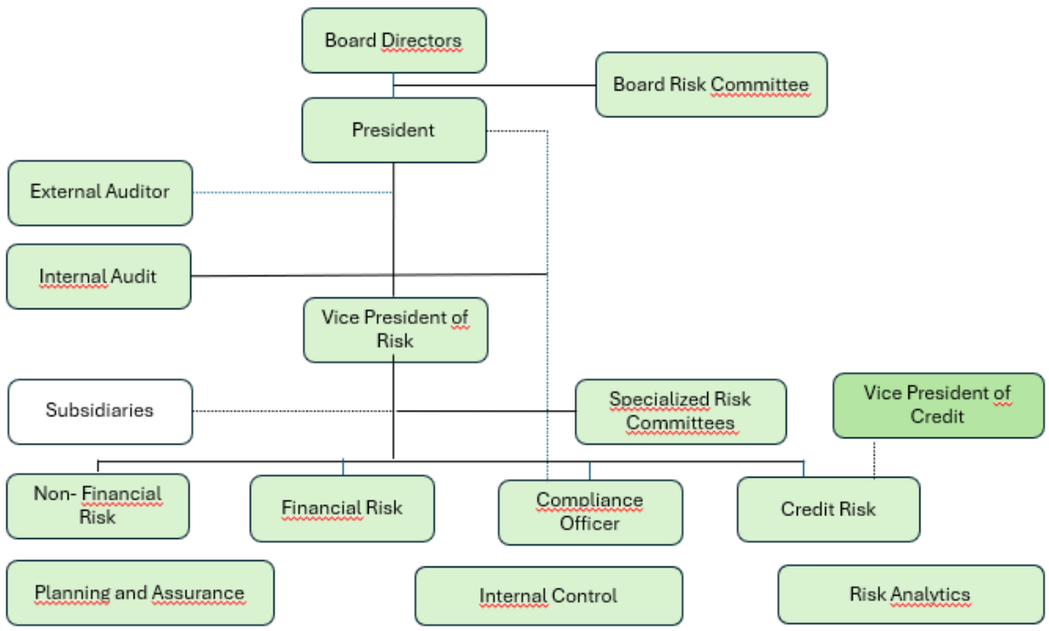

Figure 2 – Organizational Structure

The Bank's Board of Directors is the highest authority responsible for the approval and oversight of compliance with the Enterprise Risk Management System (ERMS), taking into account the recommendations of the Board Risk Committee and the Specialized Risk Committees. These Committees are primarily responsible for assisting the Board of Directors in fulfilling its oversight responsibilities with respect to the Institution's risk management.

7.2. Risk Management Model

Conceptual Framework

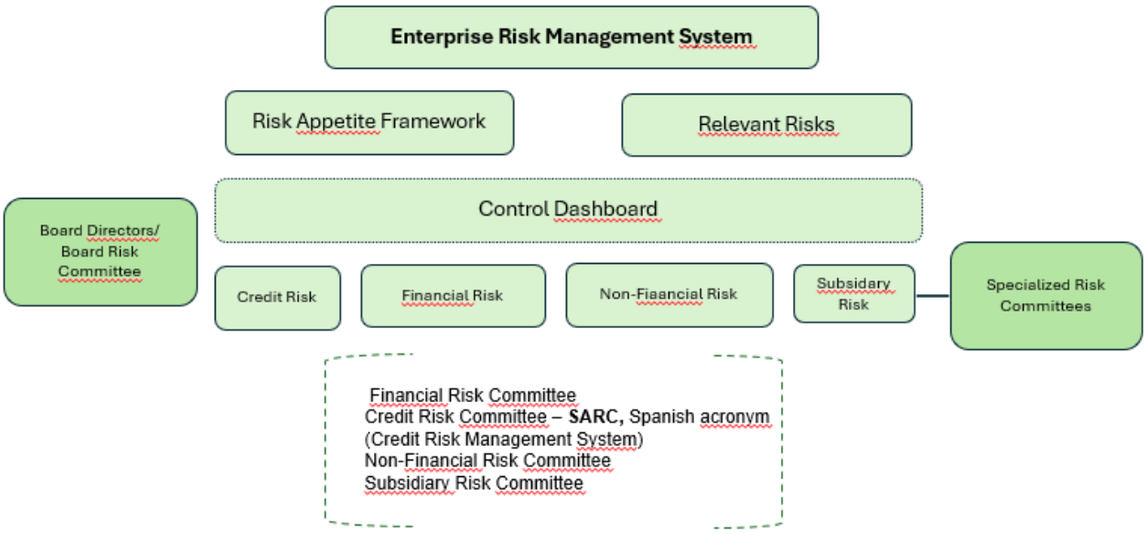

Figure 3 – Conceptual Framework

7.2.1 Specialized Risk Committees

Each of the risks managed by the Bank is monitored by a Specialized Risk Committee. The governance of each Committee is documented in its respective charter or bylaws, and its functions and operating rules are established as determined by Management.

a. Credit Risk Committee – SARC, Spanish acronym (Credit Risk Management System)

b. Financial Risk Committee

c. Non-Financial Risk Committee

d. Subsidiary Risk Committee

The Bank's functional structure includes specialized units dedicated to its principal risk management systems. These structures reflect the diversity of risk types and the methodologies required to identify, measure, and monitor each type of risk.

Accordingly, the Bank has organized its functional areas and grouped risks as follows:

a) Credit Risk:
This area comprises specialized units that define the Bank's credit risk appetite, based on the establishment of lending and measurement criteria determined in accordance with the Bank's target market and its value proposition.

b) Financial Risk:

- Market Risk: Responsible for supporting the definition of policies, guidelines, methodologies, and control procedures for managing the risks associated with the portfolios administered by Treasury, with the aim of optimizing the risk-return relationship, as well as managing interest rate risk in the banking book (IRRBB).
- **Liquidity Risk**: This unit supports the definition of policies, guidelines, methodologies, and control procedures for managing the Bank's liquidity risk.
- **Interest Rate Risk in the Banking Book (IRRBB)**: Responsible for supporting the definition of policies, guidelines, methodologies, and control procedures for managing the Bank's interest rate risk in the banking book.

c) Non-Financial Risks:
These units support the definition of policies, guidelines, methodologies, and control procedures for the management of Operational Risk, Cybersecurity, Information Security, Fraud Prevention Management, Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Risk Management, Bribery Risk and Anti-Corruption Measures, Fraud Risk and/or Misstatements in Financial Reporting (SOX Framework), Emerging Risks, Strategic Risks, Conduct Risk, and Country Risk.

d) Subsidiary Risks:

This area supports alignment of the subsidiaries' risk management through the issuance of risk governance guidelines and methodologies. It also performs periodic analyses and monitoring of significant matters relating to risk management and country risk associated with the exposure arising from each subsidiary's equity investments abroad.

Each of these functional units has its own organizational structure, governance framework, risk identification, measurement, and monitoring methodologies, as well as its own alerting and control systems. They operate autonomously and generate the inputs required for the Enterprise Risk Management System governed by this Policy. In turn, decisions based on the integrated view of risks inform these specialized systems, ensuring that they contribute to a common risk management strategy and remain aligned with the Bank's defined risk appetite.

The Enterprise Risk Management System includes cross-functional structures that support analytical functions, strategy, assurance, and internal control. The System also includes planning capabilities to ensure compliance with work plans, information analysis, compliance with supervisory authorities, coordination with the first and third lines of defense, the Bank's subsidiaries, and the execution of the integrated risk management model.

FUNCTIONS

The responsibilities related to the Enterprise Risk Management System (ERMS) of the Bank's principal governance bodies are described below.

7.2.2 Board of Directors

In addition to the responsibilities inherent to this governance body, the Board of Directors shall perform the following duties and responsibilities with respect to the ERMS.

Risk Management

a. Approve the Institution's business plan and oversee its implementation.

b. Approve and oversee compliance with the Risk Appetite Framework (RAF), the ERMS policies, the general exposure and concentration limits, the risk governance structure, and the strategies for managing: (i) risks, (ii) capital, (iii) liquidity, and (iv) conflicts of interest and their disclosure, including any updates thereto. For this purpose, the Board shall verify that these are consistent with the Institution's risk profile and risk appetite, business plan, nature, size, complexity, and diversity of its activities, as well as the economic environments and markets in which it operates.

c. Approve: (i) the guidelines governing the internal reports to be submitted to the Board regarding risk management, and (ii) the liquidity contingency plan, including any updates thereto.

d. Approve the measures to be implemented and monitor their implementation and effectiveness when: (i) increases in risk exposure result in breaches of the regulatory and/or internal thresholds or limits established by the Institution or non-compliance with the Risk Appetite Framework (RAF); (ii) weaknesses are identified in the ERMS that impair effective risk management in light of the economies and markets in which the Institution operates, its capital and liquidity levels, the regulatory framework, the business plan, and the Institution's risk profile and risk appetite; and (iii) corrective and improvement actions are required after the preceding governance levels have been exhausted.

e. Review the results of Market Risk, Liquidity Risk, Credit Risk, and Interest Rate Risk in the Banking Book (IRRBB) stress tests and approve the measures or action plans to be implemented to mitigate the identified risks based on those results.

f. Monitor, at least annually, the effectiveness and adequacy of the Enterprise Risk Management System (ERMS) in ensuring appropriate risk management and its alignment

with the business plan and the economies and markets in which the Institution operates and approves any necessary improvement actions.

g. Grant prior approval for the reclassification of a position from the trading book to the banking book, or vice versa, when such reclassification arises from an identified hedging strategy. The reclassification shall become effective only after thirty (30) business days from the date of its approval. This provision neither implies nor permits the reclassification of investments for valuation and accounting purposes, which are governed by the rules set forth in the Investment Valuation Chapter of the Basic Accounting and Financial Circular (CBCF). In all cases, the hedging strategies to be implemented shall be consistent with the criteria established in Chapter XVIII of the CBCF.

h. Approve and monitor the Bank's material risks.

i. Ensure the appropriate independence of the various control functions involved in the implementation and management of the Enterprise Risk Management System (ERMS).

j. Approve the maximum exposure limit, expressed as a percentage of regulatory capital, both on an individual and consolidated basis.

k. Review and issue opinions regarding the Country Risk Report and the results of country risk stress tests, to be considered as part of the decision-making process.

Resources

a. Appoint the members of the Board Risk Committee, approve its charter, and define its responsibilities.

b. Approve, at least annually, the training policy and budget for personnel forming part of the Institution's risk governance structure, as well as the guidelines on ethics, conduct, and internal control related to the Enterprise Risk Management System (ERMS).

Ensure that the management of the Enterprise Risk Management System (ERMS) is supported by information systems and tools appropriate to the complexity and volume of the information being analyzed.

d. Provide the resources necessary to implement, maintain, and ensure the effective and efficient operation of the Enterprise Risk Management System (ERMS).

The decisions adopted by the **Board of Directors** in exercising the above responsibilities shall be documented in the minutes of the corresponding meeting and shall include the appropriate supporting rationale.

7.2.3 Board Risk Committee

The Board Risk Committee is a specialized, technical, and advisory body whose primary purpose is to support the Bank's Board of Directors in fulfilling its oversight responsibilities with respect to risk management, including the identification, measurement, control, and consolidated monitoring of the risks to which both the Bank and its subsidiaries are exposed, within a holistic framework that promotes an institutional culture centered on prevention.

The Committee shall perform the following responsibilities:

a. Monitor the Institution's risk profile and risk appetite, evaluate their consistency with the business plan and the capital and liquidity levels, report the principal findings to the Board of Directors, and issue the corresponding recommendations as appropriate.

b. Evaluate the development of the Bank's consolidated risk management framework and the Risk Appetite Framework (RAF), based on the business model, and submit any proposed changes or updates to the Board of Directors for its consideration and approval.

c. Advise the Board of Directors on transactions, events, or activities, including entry into new markets, that may: (i) affect the Institution's risk exposure and risk profile; (ii) constitute deviations from the business plan, risk appetite, or internal and regulatory limits; or (iii) compromise the viability of the business.

d. Review the Enterprise Risk Management System (ERMS) Policy at least once a year and submit any proposed amendments to the Board of Directors for approval.

e. Advise the Board of Directors regarding the status of the Institution's risk culture.

f. Assess the adequacy of the business continuity plan and contingency plans.

g. Report to the Board of Directors on its analysis of the reports received from the function responsible for risk management, in accordance with the frequency required by applicable regulations.

h. Verify that consolidated risk management models are in place and effectively implemented, ensuring compliance with regulations applicable to the Bank and the policies established by the Board of Directors.

i. Review the consolidated risk dashboard, monitor compliance with established risk limits, and review the proposed action plans in the event that such limits are exceeded.
j. Propose strategies, models, and methodologies that facilitate the consolidated measurement of the Bank's risks together with those of its subsidiaries.

k. Monitor the economic environment and its impact on the integrated risk management models.

l. Conduct periodic evaluations of the Enterprise Risk Management System (ERMS) and the Risk Appetite Framework (RAF) to assess their effectiveness, recommend any necessary modifications or adjustments, and submit them to the Board of Directors for approval.

m. Oversee updates and changes to the risk governance framework.

n. Evaluate the Bank's risk management.

o. Monitor the management of the Bank's material risks.

p. Report to the General Shareholders' Meeting, where appropriate, on matters within its scope of responsibility that are raised by shareholders.

q. Review and assess the integrity and adequacy of the Company's risk management function.

r. Review the adequacy of the economic and regulatory capital, where applicable, for each company and its allocation among the different business lines and/or products.

s. Review risk limits and risk reports, issuing the corresponding recommendations to the Board of Directors and/or the Audit Committee.

t. Propose the Company's risk policy to the Board of Directors.

u. Systematically assess the Company's overall risk strategy and policies, as reflected in the establishment of limits by risk type and business, with the level of granularity established for business lines, corporate or economic groups, customers, and areas of activity.

v. Analyze and assess the Company's day-to-day management of risk in terms of limits, risk profile (expected loss), profitability, and capital map (capital at risk).

w. Analyze and evaluate the Company's risk control systems and tools.

x. Recommend any improvements it considers necessary in the infrastructure and the internal risk control and management systems.

y. Submit to the Board of Directors proposals regarding the delegation framework for the approval of the various types of risk that are to be assumed either by the Board itself or by lower levels within the organization.

z. Report to the Board of Directors on transactions requiring its authorization when such transactions exceed the approval authority delegated to other levels of the Company.

aa. At the request of the Board of Directors, report on transactions that require the Board's authorization pursuant to law, regulations, or internal or external provisions.

bb. Assess and monitor the recommendations issued by the supervisory authorities in the exercise of their oversight functions.

cc. Promote the enhancement of the Company's risk management framework toward an advanced model that supports the establishment of a risk profile aligned with its strategic objectives and enables monitoring of the degree to which the risks assumed remain consistent with that profile.

dd. Review and submit recommendations to the Board of Directors regarding the Country Risk Report and the results of country risk stress tests.

ee. Perform any other duties assigned by the Board of Directors.

7.2.4 President and/or Legal Representative

Under the direction and oversight of the **Board of Directors**, the **Legal Representative** shall implement and monitor compliance with the business plan and the Enterprise Risk Management System (ERMS). Accordingly, at a minimum, the Legal Representative shall perform the following duties and responsibilities:

Risk Management

a. Submit to the Board of Directors for approval the business plan, the Risk Appetite Framework (RAF), the ERMS policies, the general exposure and concentration limits, the risk governance structure, and the strategies for managing: (i) risks, (ii) capital, (iii) liquidity, and (iv) conflicts of interest and their disclosure, including any updates thereto. The Legal Representative shall also ensure compliance with these matters.

b. Submit to the Board of Directors for approval: (i) the guidelines governing the internal reports to be presented regarding risk management, and (ii) the liquidity contingency plan, including any updates thereto.
c. Approve the **Enterprise Risk Management System (ERMS) Manual** and the business continuity and contingency plans. The latter shall address the risks associated with interconnectivity with other financial market infrastructures, supervised entities, and/or third-party service providers.

d. Ensure that the contingency and business continuity plans are included in the budget to facilitate their timely implementation.

e. Monitor the adequacy of the Enterprise Risk Management System (ERMS) to ensure that it effectively manages risks and remains aligned with the Institution's risk profile and risk appetite, business plan, nature, size, and complexity, as well as with the applicable regulatory framework and the economic and market conditions in which the Institution operates.

f. Periodically review the composition, characteristics, and level of diversification of the Institution's assets, liabilities, capital, liquidity, and funding strategy.

g. Ensure that the operational risk event register complies with the principles of integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality of the

information contained therein, and that an appropriate procedure exists for maintaining and updating such register.

h. Promote the quality and consistency of information.

Resources

a. Allocate the financial resources necessary for the management of the Enterprise Risk Management System (ERMS) and the Risk Appetite Framework (RAF), ensuring that such management is supported by information systems and tools appropriate to the complexity of the processes under control.

b. Ensure that all operational areas have the tools, operational processes, and knowledge necessary to identify, report, and monitor the risks associated with their respective activities.

c. Promote the availability of qualified personnel to perform the Institution's risk management functions.

Reporting and Information

a. Report quarterly to the **Board of Directors** on the Institution's performance, financial condition, and the issues identified in risk management, together with the corresponding recommendations.

b. Promptly inform the **Board of Directors** of: (i) any changes or deviations from the business plan and the Risk Appetite Framework (RAF); and (ii) any situation or risk event that may compromise the viability of the business or public confidence, while ensuring that the appropriate corrective measures and/or improvement actions are implemented.

c. Promptly inform the **Financial Superintendence of Colombia (SFC)** of any situation or risk event that compromises the viability of the business or public confidence, as well as the causes giving rise to such event and the measures to be implemented to correct or address the situation.

d. Notify the **Financial Superintendence of Colombia (SFC)** in writing within ten (10) business days following the authorization referred to in item **g** of subsection **7.2.2**.

7.2.5 Vice President of Risk and/or Legal Representative

Risk Management

a. Prepare, together with the Legal Representative, the Risk Appetite Framework (RAF), the Enterprise Risk Management System (ERMS) Manual, and any updates thereto.

b. Develop policies, procedures, strategies, methodologies, models, thresholds and/or limits, controls, contingency plans, business continuity plan, and the framework of early warning and monitoring indicators for the Risk Appetite Framework (RAF). Submit any relevant updates to the Legal Representative.

c. Evaluate, in coordination with the other areas involved in risk management, the contingency and business continuity plans, the Institution's risk exposure and risk management, any deviations from established risk limits and the risk appetite, and their consistency with the Institution's capital and liquidity levels. Such evaluation shall include the risks inherent in new activities and/or markets, as well as their impact on the Institution's risk profile and risk management framework.

d. Monitor the influence of the funding positions and funding characteristics of related parties on the Institution's liquidity risk.

e. Issue opinions regarding transactions that do not comply with the Institution's established risk policies, controls, and/or limits, or with the applicable regulatory framework, and report such transactions as promptly as possible to the Legal Representative and the heads of the corresponding business units.

f. Conduct stress tests to determine the Institution's potential risk exposures under a range of scenarios and design the measures or action plans required to mitigate the identified risks based on the results obtained.

g. Compare the results of the stress tests against the Institution's risk appetite levels, identify the corresponding risk mitigation actions, and report the results to the **Board of Directors**, the **Legal Representative**, and the **Risk Committee**.

h. Administer the operational risk event register and coordinate the collection of information for such register. Based on this information, generate reports and analyses that support effective risk management.

i. Design and submit, for approval by the **Board Risk Committee** and subsequently by the **Board of Directors**, the methodology for the identification, definition, monitoring, and control of **Strategic Risks**.

Reporting and Information

a. Report to the Board of Directors, at least quarterly, on the nature and level of the Institution's risks and their consistency with the risk appetite and the Institution's capital and liquidity levels, including potential outcomes under severe but plausible stress scenarios. In all cases, the Board of Directors shall be promptly informed of any significant increase in risk exposure and its impact on the Institution's current and future capital and liquidity levels.

b. Report monthly to the **Legal Representative** and the **Risk Committee** on the Institution's risk exposure, including, at a minimum, a breakdown of the specific exposure associated with each material activity and each type of risk, any deviations from the established limits, and, where applicable, their consistency with the Institution's capital and liquidity levels.

   Reports on **liquidity risk exposure** shall include the quantification of cash flow mismatches or imbalances compared with the amount of liquid assets available to the Institution, placing particular emphasis on transactions conducted with entities within the financial conglomerate and with related parties, as well as sensitivity analyses and stress testing under severe but plausible scenarios.

c. Report to the Board of Directors, the Risk Committee, and the Legal Representative, at least semiannually, on the evolution of operational risk, the controls implemented, the monitoring activities performed, and the preventive and corrective actions implemented or to be implemented, together with the area responsible for such actions.

d. Report to the **Legal Representative** and the heads of the business units:

   i. At least once each business day, depending on the type of business or activity, on the status of market risk and liquidity risk.

   ii. On a weekly basis, on market risk levels, the conditions of the transactions executed, and, in particular, any breaches of established limits, unusual transactions or transactions executed outside prevailing market conditions, and transactions involving affiliates and related parties.

e. Ensure that the **Board of Directors**, the **General Shareholders' Meeting**, and the **Risk Committee** are informed in a timely and appropriate manner regarding:

   i. Any breaches of the Risk Appetite Framework (RAF), internal and/or regulatory thresholds and limits, together with the proposed corrective measures.

ii. Changes in the local and international economic, political, and market environment that may affect the Institution's current or future risk profile and/or compromise compliance with the limits and policies established under the Enterprise Risk Management System (ERMS).

iii. The risks inherent in new activities and/or markets and their impact on the Institution's risk profile, risk management framework, and capital and liquidity levels.

f. Report, in a timely and clear manner, to the General Shareholders' Meeting and the heads of the business units the issues identified in risk management, together with the corresponding recommendations.

7.2.6 Vice Presidencies – Functional Units Representing the First Line

The roles and responsibilities of the Vice Presidencies, in their capacity as the functional units comprising the **first line of defense** within the Enterprise Risk Management System (ERMS), are as follows:

a. Participate in the identification and definition of strategic risks, monitoring metrics, controls to prevent their materialization, and the action plans to be implemented.

b. Update the information related to the indicators for which they are responsible and periodically submit such information to the **Vice President of Risk Management**.

c. Ensure the consistency and quality of the information provided to the **Vice President of Risk Management**.

e. Monitor the ERMS indicators, controls, or action plans under their responsibility and ensure compliance with the established policies.

f.

e. Promptly identify and escalate to the **Vice President of Risk Management** any non-compliance with the limits established under the ERMS.

f. Submit to the **Board Risk Committee** the action plans or improvement measures required as a result of the monitoring of the risks to which the Bank is exposed and/or participate in Committee meetings whenever requested.

g. Implement and ensure compliance with the recommendations and/or action plans issued by the **Board of Directors**, the **President**, the **Chief Risk Officer (CRO)**, or the **Board Risk Committee** during the review of the Enterprise Risk Management System (ERMS).

h. Promptly identify and escalate to the **Vice President of Risk Management** any alerts indicating potential non-compliance with the limits established under the **Risk Appetite Framework (RAF)**, as well as the potential materialization of risks.

i. Assess the impact of risks on the business plan and use this information as an input for the Bank's budget planning process.

j. Participate in the identification and definition of strategic risks and compliance limits, taking into consideration the business and capital plans, the Institution's risk capacity, and its compensation programs.

k. Prepare annual reports, or ad hoc reports as required, containing macroeconomic analyses to support the Bank's risk management activities.

l. Ensure the integrity of, and full compliance with, the policies established under the Enterprise Risk Management System (ERMS) and the Risk Appetite Framework (RAF).

7.2.7 Internal Audit

The **Internal Audit** is responsible for:

a. Periodically evaluating the effectiveness of, and compliance with, the Enterprise Risk Management System (ERMS), or whenever circumstances require its review, and reporting the results of such evaluation to the function responsible for risk management, the Legal Representative, the Audit Committee, and the Board of Directors, including the follow-up on recommendations, improvement actions, and compliance with the audit plan. This evaluation shall expressly cover, at a minimum, the transactions and liquidity flows to and from related parties.

b. Monitoring the implementation of recommendations and the remediation of deficiencies identified in risk management as a result of assessments conducted by the **Financial Superintendence of Colombia (SFC,** Spanish Acronym**)** and the internal audit function, as well as the action plans and corrective measures adopted by the Institution.

c. Informing the **Financial Superintendence of Colombia (SFC)** of any material situations that may affect the continuity or development of the business, as well as any corrective or improvement actions that have not been addressed by the Institution.

The evaluation conducted by the internal audit function with respect to the Enterprise Risk Management System (ERMS) shall reflect changes in the operating environment and in the Institution's risk profile and shall be based on the risks to which the Institution is exposed.

7.2.8 External Auditor

Without prejudice to the responsibilities assigned under other legal provisions, the External Auditor shall include within its audit plan a periodic evaluation of compliance with the Enterprise Risk Management System (ERMS) and shall prepare an annual report setting out the conclusions reached during the evaluation and review process. Such report shall be incorporated into the audit opinion on the financial statements.

These reports shall be made available to the Financial Superintendence of Colombia (SFC).

Likewise, the **External Auditor** shall promptly inform: (i) the General Shareholders' Meeting or its equivalent, (ii) the Board of Directors, (iii) the Legal Representative, (iv) the Audit Committee, and (v) the **Financial Superintendence of Colombia (SFC)** of any material irregularities identified in connection with compliance with the Enterprise Risk Management System (ERMS), as well as any deficiencies in the internal control framework.

The report shall be properly documented and shall include the results obtained, the recommended actions, and the Institution's response to the observations made.

8. METHODOLOGY

The methodology established by the Bank for the design and implementation of the Enterprise Risk Management System (ERMS) was developed in accordance with international leading practices established by the framework established by **COSO Enterprise Risk Management (Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management (ERM))**.

The methodology is structured to operate in a cyclical and dynamic manner, continuously informing management decision-making and to the quantitative and qualitative analysis of the information managed by the Institution.

Its design incorporates the stages required by the Financial Superintendence of Colombia (SFC): Identification, Measurement, Control, and Monitoring.

Figure 4 below illustrates the structure of the methodology.

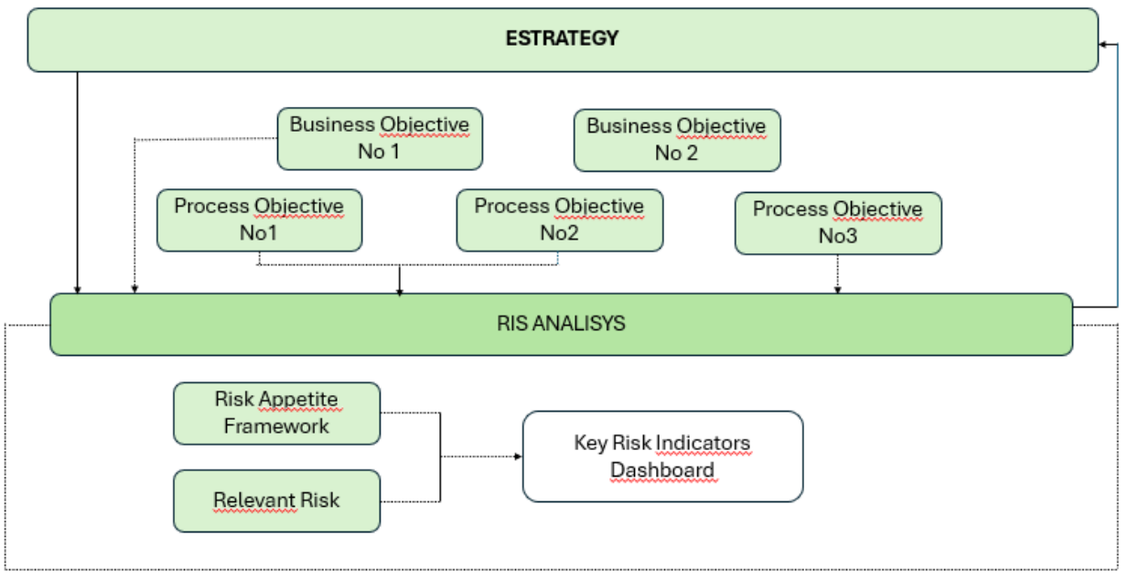

Figure 4 – Methodology Structure

8.1 Identification

For the identification of the risks to be monitored under the **Enterprise Risk Management System (ERMS)**, the Bank adopts a hybrid approach that combines the two methodologies most commonly used for risk identification: **Top-Down** and **Bottom-Up**, as described below.

Bottom-Up:
This approach seeks to identify risks at the process level that may have a significant impact on the Bank, taking into account both the process management perspective and the historical documentation of materialized risks. This approach enables the Bank to identify operational weaknesses and address them through appropriate management actions.

Top-Down:
This approach seeks to identify the main risks that may affect the economic, financial, or socio-political environment at the global, national, and industry levels in order to understand the bank's vulnerability to potential changes in the global and local environments. These risks manifest in one of the following categories:

- Economic
- Social
- Political
- Environmental
- Regulatory
- Technological
- Strategic

Integrated Approach

The integrated approach is intended to provide a comprehensive and detailed view of the principal risks faced by the Bank by combining the **Bottom-Up** approach—which identifies risks at the process level based on employees' knowledge and the historical record of risk events—with the **Top-Down** approach, which identifies emerging risks affecting the economy.

The objective of this methodology is to consolidate the risks that may hinder the achievement of the Bank's strategic objectives or, although initially affecting only process-level or business objectives generate significant levels of exposure that could lead the Bank into scenarios affecting its operational or financial continuity, as illustrated in Figure 4.

A comprehensive and consolidated view of risks is particularly important within the context of strategic planning, as it supports the achievement of the Bank's strategic objectives. Because strategic planning typically covers a longer-term horizon, assumptions regarding future conditions are inherently more uncertain and may become invalid during the planning period. Consequently, the Bank requires the continuous updating and monitoring of both internally materialized risks and emerging risks that may affect its operations.

Once the integrated approach is implemented, the identification stage produces two components: material risks and the risks associated with the Bank's risk management systems. Both components are monitored and controlled through a dashboard of indicators that serves as a risk portfolio to support Senior Management's understanding and oversight.

8.2 Measurement and Control

The risks included in the Bank's Risk Appetite Statement, or RAF risks, are subject to specific measurement and control methodologies, which are described in the Risk Appetite Framework and the Risk Appetite Statement documentation.

Under the Operational Risk Management Methodology, the Bank's exposure and the mechanisms designed to mitigate or minimize the likelihood and impact of the materialization of inherent risks associated with the Bank's activities are assessed.

The identification of material risks comprises two phases: the first is exploratory and investigative, and the second is a consensus-building phase. Both are led by the team of the Vice President of Risk Management, resulting in the identification of the set of risks on which Senior Management will focus its efforts.

The methodologies for the measurement and control of these risks are described in the Material Risks Appendix.

8.3 Monitoring

Periodically, in accordance with the dynamics of the identification and control processes carried out by the responsible areas, the indicators associated with the Risk Appetite Framework (RAF) are updated, and their performance is monitored through a corporate risk dashboard.

The results of the integrated risk management process are presented by the **Vice President of Risk Management** to the **Board Risk Committee** and the **Board of Directors**.

When deviations from established limits or unusual indicator behavior are identified, the corresponding actions, as applicable, shall be evaluated and submitted to the appropriate governance body.

Material risks are monitored by each responsible area in accordance with the assignments established in the **Risk Matrix**. These risks are supported by a series of controls and indicators that are periodically presented to the **Board Risk Committee** and/or the **Board of Directors**.

In the event of deviations or unusual indicator behavior, the corresponding actions, as applicable, shall be evaluated and submitted to the appropriate governance body, in accordance with the provisions of the **Material Risks Appendix**.

9. COMMUNICATION AND TRAINING

The **Board of Directors**, through the **Board Risk Committee**, the **Specialized Risk Committees**, and the departments responsible for managing each risk, ensures that communication plans for the **Enterprise Risk Management System (ERMS)** are in place.

The clarity and understandability of these communication plans are essential to fostering the Bank's risk culture.

The communication activities described herein shall be conducted at least once a year, except when special circumstances require the disclosure process to be repeated.

To ensure the effective implementation and operation of the **Enterprise Risk Management System (ERMS)**, the following documentation shall be maintained:

a. **ERMS Manual**, which includes the stages, policies, strategies, procedures, methodologies, responsibilities, and functions of the risk governance framework, updated and approved by the appropriate governing bodies.

b. Minutes of the **Board of Directors** meetings approving the **Enterprise Risk Management System (ERMS)** policies and any updates thereto.

c. Risk models.

d. The business continuity plan and contingency plans.

e. The early warning system and the other indicators implemented to monitor each risk, as well as the actions, corrective measures, and improvement initiatives implemented in response to breaches of established limits or the activation of alerts.

f. Reports prepared by the various risk governance bodies and officers regarding risk management, together with any other documents supporting the monitoring of such management.

g. The **Code of Ethics and Conduct**.

h. The operational risk event register.

The Bank maintains verifiable records and an information retention, custody, and security plan, ensuring that such information may be accessed only by duly authorized personnel.

These procedures are aligned with the current **Information Security Manual**, which applies across all of the Bank's processes.

9.1 Internal Information Comunication

The Bank prepares periodic reports to monitor its integrated risk management activities through reports submitted to the **Board Risk Committee** and the **Board of Directors**, which are documented in the minutes of the meetings of these governing bodies.

The Board Risk Committee shall report to the Board of Directors through reports issued after each meeting.

The **Risk Reporting Guidelines** addressed to the **Board Risk Committee** and the **Board of Directors** shall be followed.

Monthly	Market Risk Report – Liquidity Risk – Banking Book Interest Rate Risk, Indicators and Alerts. Comprehensive Risk Management Integrated Report and other reports upon request.

Quarterly	***SARLAFT, Spanish acronym (Money Laundering and Terrorist Financing Risk Management System), Report.***
Semi-Annual	***Operational Risk Management Report, ABAC Report, Cybersecurity and Information Security Report, Relevant Risk Monitoring Report, Country Risk Report.***
Annual	***DAR Indicator Recalibration, FATCA Report, Annual Risk Report and Relevant Risk Proposal.***
On Demand	***Credit Risk Report.*** ***Board of Directors approvals: Risk Policies, LAFT Segmentation, Others.***

Table 1 – Internal Information Disclosure

Where necessary, additional reports may be issued or reports may be prepared more frequently.

Periodic training programs shall be developed to communicate relevant information on the Enterprise Risk Management System (ERMS) and any applicable updates to those responsible for risk management, with the objective of reinforcing a risk-aware culture throughout the organization.

The design and delivery of these training programs are the responsibility of the **Vice Presidency of Risk Management**, with the support of the **Vice Presidency of Human Talent Experience**.

9.2 External Information Comunication

The **Vice President of Risk Management** is responsible for ensuring the timely and appropriate preparation of the reports required by external supervisory, oversight, and regulatory authorities, credit rating agencies, and other relevant stakeholders, in accordance with the prescribed format, deadlines, and requirements established by such entities.

In compliance with **Article 97 of the Organic Statute of the Financial System (EOSF)** and the other applicable legal provisions governing this matter, the Bank provides the public with the information necessary for the market to assess its risk management practices.

The Bank ensures that the information disclosed is consistent with its size, complexity, nature, and risk profile.

10. TECHNOLOGICAL INFRASTRUCTURE AND INFORMATION SYSTEMS

In accordance with the nature and scale of its operations, the Bank maintains information systems that support the operation of the **Enterprise Risk Management System (ERMS)**, as well as a data system that provides a comprehensive view of risks and facilitates the generation of reports to support informed decision-making and compliance with applicable regulatory requirements.

Within this system, the data aggregation process is carried out using, as inputs, the pre-calculated **Risk Appetite Framework (RAF)** indicators generated by each of the Bank's risk management functions and its subsidiaries, thereby providing a comprehensive view of the Bank's risk profile.

The implemented information system includes:

- Information governance and data quality.
- Procedures for the management and storage of information to ensure its confidentiality, security, quality, availability, integrity, consistency, and consolidation.
- Updated, sufficient, and timely information on risk management.
- Data aggregation and reporting guidelines based on the following principles:
    - **Governance:** Risk data aggregation and risk management reporting shall be based on the guidelines established by the **Board of Directors**.
    - **Accuracy and Integrity:** Risk data shall be accurate and reliable and, to the greatest extent possible, aggregated through automated processes.
    - **Completeness:** All significant risk data across the Institution shall be identified and aggregated. At a minimum, such data shall be available by risk type, business activity, asset type, economic sector, geographic region, and intragroup transactions, as well as transactions with affiliates and related parties.

The documentation supporting the **Enterprise Risk Management System (ERMS)** establishes both general and specific guidelines for the effective management of each risk category.

11. MAINTENANCE AND UPDATING

The **Enterprise Risk Management System (ERMS)** shall be reviewed periodically (at least once a year) and whenever necessary to ensure that it remains current and appropriate to the Bank's circumstances.

The **Vice President of Risk Management** is responsible for ensuring that the policies, methodologies, and process guidelines remain updated.

Whenever amendments to the **Enterprise Risk Management System (ERMS)** are required, the **Vice President of Risk Management** shall submit the proposed modifications and updates to the **Board of Directors** for approval, following the prior recommendation of the **Board Risk Committee**, and shall be responsible for updating the Manual and communicating any changes.

12. ALIGNMENT WITH SUBSIDIARIES

To obtain a comprehensive understanding of the risk management practices of Banco Popular's subsidiaries, a set of risk indicators has been established for each risk category, tailored to the business activities of each subsidiary and aligned with the Bank's corporate framework.

To support this process, an information architecture and technological infrastructure have been established to facilitate the management and monitoring of these indicators.

The management of the risks inherent to each subsidiary's business activities is the responsibility of the respective subsidiary. Nevertheless, corporate-level guidelines are issued to strengthen the risk management practices of the subsidiaries.

Accordingly, the Vice President of Risk Management has the necessary procedures to monitor these indicators. Such procedures are submitted to the Board Risk Committee for its review and approval.

13. APPENDICES

The following are the main documents that form an integral part of the Enterprise Risk Management System (ERMS):

- **A-PAE-0002** – Risk Appetite Framework (RAF)
- **A-PAE-0007** – Risk Appetite Statement (RAS)
- **A-PAE-0001** – Methodology for the Measurement of Material Risks
- **Operational Risk Management Policy**
- **Market Risk Management Policy**
- **Liquidity Risk Management Policy**
- **Interest Rate Risk in the Banking Book (IRRBB) Management Policy**
- **General Provisions of the Credit Risk Management System (SARC)**
- **Conduct Risk Policy**
- **Country Risk Policy**
- **A-PAE-0011** – Risk Reporting Guidelines

CHANGE LOG

VERSION HISTORY

Version #	Publication Date	Description of Change
1	04/08/2021	The document is created to present the policies associated with the integrated risk model.
2	07/13/2021	The document is updated to adjust the description of Article Three – permanent guests, and Article Six – Quorum.
3	08/05/2022	The document is updated as follows: The title of the Comprehensive Risk Manager position is adjusted. The responsibilities of the Board of Directors Risk Committee are included. The Consolidated Risk Committee bylaws are removed and documented independently, while responsibilities are retained within the structure chapter. The name of the report "DAR Indicator Control Dashboard" is adjusted.
4	04/13/2023	The name and content of the document are updated in compliance with External Circular 018 of 2021. The Comprehensive Risk Management System (SIAR, Spanish acronym) document is restructured based on the latest version of the Integrated Risk Model.
5	04/25/2024	Regulatory Risk Committee merged with the Non-Financial Risk Committee. Consolidated Risk Committee eliminated. SARM and SARL Committees unified into the Financial Risk Committee. Title of Comprehensive Risk Management changed to Risk Vice Presidency throughout the document. Section 13 Annexes added. Changes approved in Board of Directors Minutes 2789 dated March 21, 2024.
6	12/13/2024	Sections 5 (Three Lines Model), 7.2.1 (Specialized Risk Committees), and 7.2.6 (Functional Unit Vice Presidencies Representing the First Line) are updated in accordance with management requirements.
7	02/21/2025	Section 7.2.1 Specialized Risk Committees is updated, including country risk management within the Non-Financial Risk Committee. Section 7.2.1 Specialized Risk Committees is updated, including country risk management within the Subsidiary Risk Committee regarding capital investment risk exposure in each subsidiary's foreign operations. Section 7.2.2 is updated regarding the functions of the Board of Directors in risk management. Section 7.2.3 Board of Directors Risk Committee is updated, including responsibility for the country risk report recommendation. Section 13 includes the Country Risk Policy annex. Changes approved in Board of Directors Minutes No. 2812 dated January 27, 2025.