Comprehensive Risk Management Framework

Table of Contents

1. Overview ... 3
2. Scope ... 4
3. Purposes ... 5
4. General Considerations ... 6
   - 4.1 About the Comprehensive Risk Management Governance Framework ... 6
   - 4.2 Setting the context ... 6
5. Organizational Structure ... 8
6. Organizational Model - The Three Lines of Defense ... 11
7. Roles and Responsibilities ... 12
   - 7.1 Board of Directors ... 12
   - 7.2 Senior Management (Executive Committee) ... 12
   - 7.3 Risk Policy and Assessment Committee (CPER) ... 13
   - 7.4 Executive Vice Presidency of Comprehensive Risk Management ... 13
   - 7.5 Internal Audit ... 15
8. Comprehensive Risk Management Definitions ... 16
   - 8.1 Definition of Comprehensive Risk Management ... 16
   - 8.2 Definitions and terms applicable to Comprehensive Risk Management: ... 16
9. Types of Risk ... 18
10. Stages of Comprehensive Risk Management ... 21
11. Risk Management Tools ... 23
12. Comprehensive Risk Management Committees ... 25
13. Risk Appetite Framework ... 27
    - 13.1 Appetite, Tolerance and Capacity ... 27
    - 13.2. Risk Appetite Statement ... 28
14. Rules for Use of the Comprehensive Risk Management Framework ... 31
    - 14.1 Compliance and Interpretation ... 31
    - 14.2 Review and Update ... 31
    - 14.3 Distribution ... 32

1. Overview

Risk Management plays a fundamental role in the strategy of Banco Latinoamericano de Comercio de Comercio Exterior, S.A. (hereinafter referred to as "the Bank"), as it guarantees the solvency and sustainable development of the entity, based on the objectives established and that they are in line with the Bank's mission and risk appetite.

For an effective management with an integral vision, the Bank, through the Comprehensive Risk Management Department, has the structure, as well as policies, manuals and procedures designed to identify potential events that may affect it, all of which must be in line with its business risk profile, taking into account the complexity and volume of its operations.

As part of the framework, a risk appetite statement is established, which represents the balance between the ability to assume risk and the associated business opportunities.

As a result, the Bank has a robust governance framework for the effective management of its risk profile, based on the division of responsibilities among the three lines of defense, a solid committee structure, and a risk culture embedded throughout the organization.

2. Scope

The Comprehensive Risk Management Framework (hereinafter referred to as the "Document") has been prepared by the Executive Vice President of Comprehensive Risk Management and approved by the Board of Directors through the Risk Policy and Assessment Committee ("CPER") in order to establish the principles and foundations for adequate Comprehensive Risk Management within the Bank, and compliance with this Document is mandatory for the parties involved.

3. Purposes

The purpose of this document is to define an adequate framework for the proper Comprehensive Risk Management within the Bank, based on the best practices and the Agreement No. 008-2010 of the Superintendency of Banks of Panama ("SBP"), as amended by Agreement No. 009-2017, which incorporates the concept of "Social and Environmental Risk", and Agreement No. 011-2022, which adds the "Climate-Related Risk", which are mandatory for the parties involved in the risk management process.

- Be consistent with the rules, standards, principles and regulatory requirements related to risk management. In this regard, the Comprehensive Risk Management Framework is consistent with:
  - "International Convergence of Capital Measurement and Capital Standards" (hereinafter "Basel")
  - "Enterprise Risk Management – Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO").
  - International Standardization Organization – 31000:2018 Standard (Risk Management)
  - "Generally Accepted Risk Principles" ("GARP")
  - Agreement No. 8-2010 of the Superintendency of Banks of Panama, "Whereby provisions on Comprehensive Risk Management are established", as amended by Agreement No. 009-2017 and Agreement No. 011-2022
  - Agreement No. 005-2011 of the Superintendency of Banks of Panama "Corporate Governance"
  - Agreements issued by the Superintendency of Banks of Panama regarding the different risks that must be managed by the Risk Unit, and other applicable regulations.
  - Bank's Bylaws.
  - Risk Policy and Assessment Committee ("CPER") Charter
  - Policies, Manuals and other documentation related to the different risks that are managed by the Bank's Comprehensive Risk Management area.
- Clearly define the general guidelines under which risks are identified, monitored, controlled, mitigated and reported within the Bank.
- Actively contribute to the achievement of the Bank's objectives and strategies, and increase operational efficiency by reducing losses from risk events and optimizing control systems.
- Provide a means for senior management to communicate, drive and maintain an effective risk culture within the Bank.

- Clearly define the roles and responsibilities for comprehensive risk management within the Bank, thereby establishing an organizational structure that promotes the appropriate management of integral risk.

4. General Considerations

4.1 About the Comprehensive Risk Management Governance Framework

The Comprehensive Risk Management Framework is intended to provide all employees of the Bank with a comprehensive understanding of the concepts and scope of risk management, roles and responsibilities, as well as its management guidelines, and where any risk is identified in accordance with the provisions of Agreement No. 008-2010 (as amended), and encompasses the set of processes and procedures implemented in the Bank designed to provide reasonable assurance regarding the achievement of the objectives approved by the Board of Directors.

The Bank manages its risks in a comprehensive manner, based on international best practices and standards in risk management, such as Basel, as well as COSO and ISO 31000, which cover the objectives of management in terms of effectiveness and efficiency of operations, ensuring its reliability, establishing and recommending the development, implementation and continuous improvement of a benchmark framework whose purpose is to integrate the risk management process in the direction, strategy and planning, processes, policies, values and culture of the entire organization and compliance with laws and regulations, both national and international.

República de Panamá
Superintendencia de Bancos

ACUERDO No. 008-2010
(de 1 de diciembre de 2010)

"Por medio del cual se dictan disposiciones sobre Gestión Integral de Riesgos"

LA JUNTA DIRECTIVA
En uso de sus facultades legales, y

CONSIDERANDO

BANK FOR INTERNATIONAL SETTLEMENTS

International Organization for Standardization ISO 31000

4.2 Setting the context

It is necessary to obtain an overview of the organization and the risks inherent in its market segment. All general information about the organization should be gathered to better understand its mission, strategies, values, etc., which will help ensure consistency and coherence between the strategic objectives for comprehensive risk management and the organization's mission.

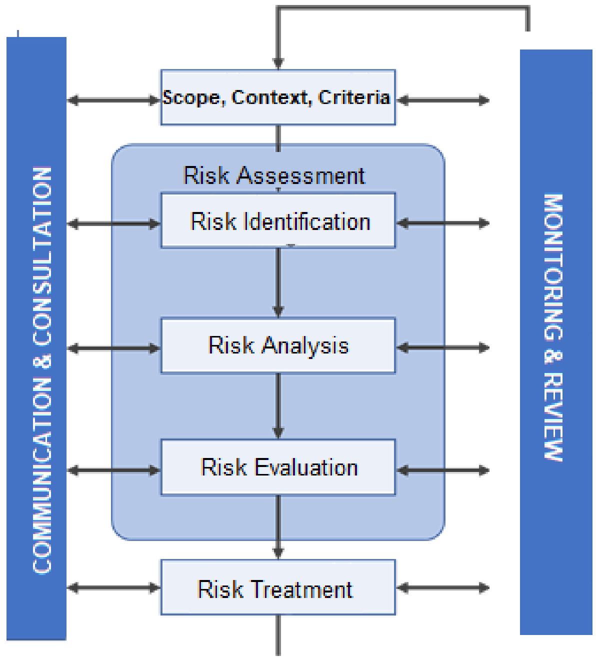
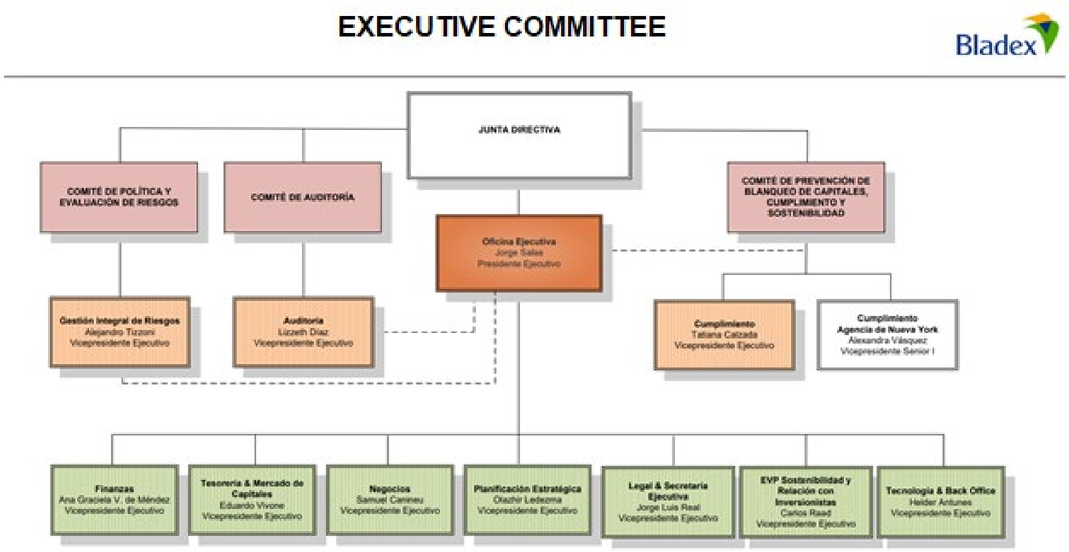


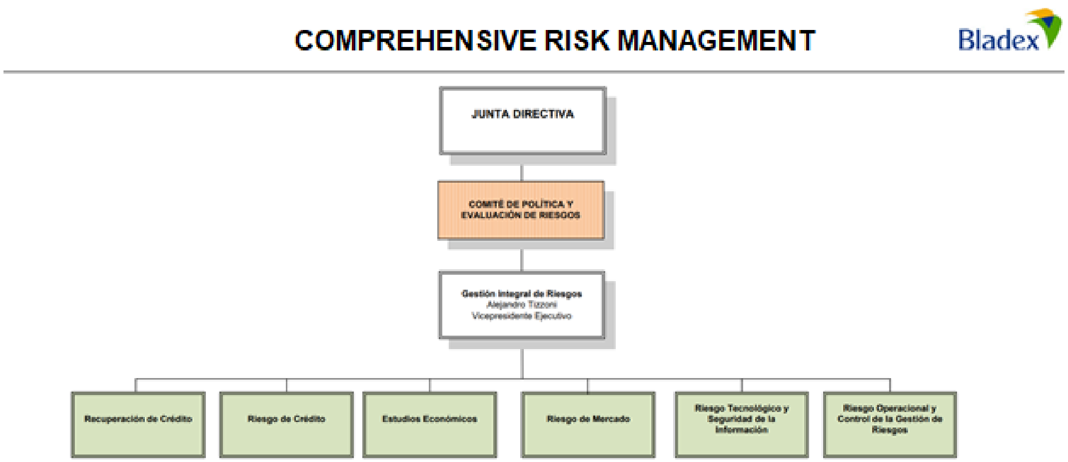
Diagram Source: ISO 31000

5. Organizational Structure

The organizational chart below describes the overall organization of the Bank, although for the purposes of this document only some of the parts directly related to Comprehensive Risk Management are identified and described.



Specifically, the organization of the Executive Vice Presidency of Comprehensive Risk Management is as follows to align with the Comprehensive Risk Management Framework:



The organizational chart should provide clear guidance on the activities of not only the Comprehensive Risk Management Vice Presidency, but also the Business, Support and Internal Audit Vice Presidencies.

Legal risk management (legal business risk/regulatory risk) and money laundering management are the responsibility of the Legal and Compliance departments. Comprehensive Risk Management is kept informed of these areas, but is not directly involved in their management.

In accordance with Corporate Governance standards, the Bank has adopted policies to ensure the integrity and efficiency of the management processes for each of its risks.

In addition, it has adopted frameworks or manuals and their operationalization through procedures, guidelines and various documents that define the manner in which the comprehensive risk management process is governed, with the aim of promoting a risk management culture that flows through all levels of the organization according to the size and complexity of its operations and services. The policies and manuals are listed below:

- CPER Charter
- Operational Risk Management Policy
- Operational Risk Management Manual
- Business Continuity Plan
- General Information Security and Cybersecurity Policy
- Information Security and Cybersecurity Manual
- IT Risk Management Manual

- Portfolio Monitoring and Recovery Policy
- Independent Credit Review Policy for the New York Agency Commercial Portfolio
- Credit Risk Management Policy
- Credit Risk Management Manual
- Environmental and Social Risk Management Policy
- Credit Committee Charter
- Market and Liquidity Risk Management Policy
- Market and Liquidity Risk Management Manual
- Investment Portfolio Risk Management Policy
- Country Risk Management Policy
- Country Risk Management Manual
- Reputational Risk Management Policy
- Fraud Risk Management Policy
- Corporate Insurance Management Policy
- Model Risk Management Policy
- Credit Reserve Methodology
- Legal Risk Manual *(managed by the Legal Department)*
- Documentation and other legal policies *(managed by the Legal Department)*
- Manual for the Prevention of Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction *(Managed by the Compliance department, and the document approved by the Anti-Money Laundering, Compliance and Sustainability Committee)*

In this sense, the Bank's organizational structure supports comprehensive risk management in the following ways:

- A clear separation between the business lines and the risk unit.
- Mechanisms for communication and disclosure of the scope and results of the process.
- Personnel with the necessary knowledge and skills to perform their duties.
- Information technology commensurate with the sophistication of the methodologies and activities involved.

6. Organizational Model - The Three Lines of Defense

All employees who perform tasks in the Bank are directly responsible for the inherent risks, and it is therefore clear, not only in this Document, but also in the Bank's policies, that the first line of defense in the prevention of undesirable risks lies with the Business and Support Area officers.

Business and Support Areas	Comprehensive Risk Management	Internal Audit
Responsible and Executor	Management and Monitoring	Verification
• Made up of process owners and risk managers • Monitors risks associated with their processes • Involved in compliance with the Bank's risk governance framework	• Facilitates and monitor the application of effective risk management practices by Business and Support Areas • Assists risk managers in setting the Bank's target risk exposures	• Fully independent, reporting to the Audit Committee of the Board of Directors • Evaluates the risk management process • Performs control testing

In addition, once the activities in the Business and Support Areas have been carried out and monitored by the Vice Presidency of Comprehensive Risk Management, it is necessary to verify both the risk management process and the activities of the Vice Presidency of Comprehensive Risk Management through internal audits.

Thus, having clearly conceptualized the roles of the so-called “Three Lines of Defense” in best practices, we can proceed to analyze the structure of the Vice Presidency of Comprehensive Risk Management within this combination of activities between the Vice Presidencies of Business, Support and Internal Audit.

It is a fundamental principle of the Bank and comprehensive risk management that the Board of Directors and Senior Management be responsible for creating an organizational culture that places a high priority on risk management and effective compliance with operational controls at all levels of the Bank.

Therefore, the organizational structure that Bladex has decided to adopt with respect to comprehensive risk management will take into account the basic rules established by Basel for the governance of entities, which are essentially the following:

- The involvement of the Board of Directors and Senior Management in the management and definition of risk strategies;
- The independence of the risk units, and in this case of the Vice Presidency of Comprehensive Risk Management, and of the Business and Support units. This independence will be subject to review by the supervisor (Pillar II); and

- The involvement of Internal Audit in the review of the Comprehensive Risk Measurement and Management model (without direct participation in its active management).

7. Roles and Responsibilities

7.1 Board of Directors

- Establish the bank's acceptable risk profile, which requires knowledge and understanding of the risks to which the Bank is exposed.
- Appoint the members that compose the CPER.
- Approve, based on Senior Management's proposals, the necessary resources for the adequate development of the Comprehensive Risk Management in order to have the appropriate infrastructure, methodology and personnel.
- Ratify the approval of the policies and structures of risk limits for the different operating and business areas of the Bank.
- Grant the Executive Vice President of Comprehensive Risk Management sufficient authority, hierarchy and independence with respect to the rest of the Bank's staff, as well as the power of veto in decisions related to the Bank's integral risk.
- Submit annually to the Superintendency of Banks a certificate of compliance with Agreement 008-2010, as amended.
- Approve the Bank's Risk Assessment Report on Money Laundering, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction, in accordance with Agreement 001-2017.

7.2 Senior Management (Executive Committee)

- Ensure consistency between operations and defined risk tolerance levels.
- Be aware of the level of risk assumed by the Bank.
- Establish review programs by the Risk Management Unit and the business units regarding compliance with objectives, procedures and controls in the conduct of operations, as well as exposure limits and risk tolerance levels.
- Ensure that the Executive Vice President of Comprehensive Risk Management has an adequate budget to perform its functions.
- Ensure that adequate systems are in place to store, process and manage information.

- Ensure that training and continuing education programs are established for the staff of the Executive Vice President of Comprehensive Risk Management and for all persons involved in operations involving risk to the Bank.
- Establish procedures to ensure an adequate flow, quality and timeliness of information between the business units and the Executive Vice President of Comprehensive Risk Management for all those involved in operations involving risk for the Bank.

7.3 Risk Policy and Assessment Committee (CPER)

- Monitor risk exposures and compare such exposures against the tolerance limits approved by the Board of Directors. The CPER shall consider, among other aspects it deems relevant, the impact of such risks on the stability and solvency of the Bank.
- Evaluate the performance of the Executive Vice President of Comprehensive Risk Management, which shall be duly documented.
- Report to the Board of Directors the results of its assessments of the Bank's risk exposures.
- Approve the limits, strategies and policies that contribute to effective risk management, as well as the scenarios and the time horizon in which limit overruns or exceptions to policies may be accepted, subject to the approval of the Board of Directors, and the possible courses of action or mechanisms by which the situation may be regularized.
- Develop and propose risk management models and methodologies.
- Propose contingency plans to be submitted to the Board of Directors for approval.
- The functions and requirements established in the policies that make up the Comprehensive Risk Management Framework.

7.4 Executive Vice Presidency of Comprehensive Risk Management

Its primary function is to monitor risks, assist in the design of policies and procedures, monitor compliance, and alert the CPER or the appropriate body to risks that may require additional controls.

The Executive Vice Presidency of Comprehensive Risk Management shall perform the following functions:

- Identify, assess and comprehensively control all risks relevant to the Bank. For such purpose, it may:
  - Have risk measurement models and systems that are commensurate with the level of complexity and volume of its operations and that accurately reflect the value of positions and their sensitivity to various risk factors.

  - Ensure that the necessary information to be used in the risk measurement models and systems is provided by the responsible areas and is available in a timely manner.
  - Evaluate the above models and systems on an ongoing basis and report the results to the Risk Policy and Assessment Committee.
  - Depending on the complexity and volume of its operations, conduct a periodic back-testing program, comparing the internal model's estimates of exposures by risk type with the actual results observed for the same measurement period, and make the necessary corrections, modifying the model if deviations occur and documenting them.
  - Ensure that any deficiencies identified with respect to the quality, timeliness and completeness of the information used by Risk Management are reported to the areas responsible for its preparation and control.
- Perform exposure estimates by risk type.
- Present to the CPER, at least quarterly, for its consideration, the tools and techniques used to identify and analyze risks, as well as the methodologies, models and parameters used to measure and control the different types of risks to which the Bank is exposed.
- Monitor compliance with global and specific limits, as well as acceptable tolerance levels by type of risk.
- Provide the CPER with information on:
  - Exposure to the various risks relevant to the Bank, with the periodicity established.
  - The impact of the entity’s risk-taking on capital adequacy, taking into account sensitivity analysis under different scenarios (stress testing), including extreme events.
  - Deviations from exposure limits and established risk tolerance levels. This information must be provided promptly to Senior Management and business line managers, as well as to the Risk Committee or other appropriate body.
  - Proposals for corrective actions to be taken as a result of deviations from approved exposure limits and risk tolerance levels.
  - The historical development of the risks assumed by the entity.
- Investigate and document the causes of deviations from established risk exposure limits.
- Direct the reduction of observed exposures and, where appropriate, the modification of global and specific risk exposure limits and risk tolerance levels.
- Continually analyze and evaluate the assumptions and parameters used in the required analyses.
- Perform any other function required by the CPER or the competent body.

- Prepare the Bank's Risk Assessment Report on Money Laundering, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction, in accordance with the provisions of Agreement 001-2017, and submit it first to the Money Laundering, Compliance and Sustainability Committee for approval and then to the Board of Directors for approval.

7.5 Internal Audit

- Internal Audit will evaluate compliance with the procedures used for comprehensive risk management and the effectiveness of the controls established in the comprehensive risk management framework.

8. Comprehensive Risk Management Definitions

One of the objectives of the Comprehensive Risk Management Framework is to establish a "Common Language" within the Bank, ensuring that all employees utilize consistent definitions to facilitate the interpretation of results and decision-making.

This section contains the definitions of the main terms related to the "Comprehensive Risk Management Framework," as shown below:

8.1 Definition of Comprehensive Risk Management

The definition of Comprehensive Risk Management used by the Bank shall be that established by the Superintendency of Banks of Panama in Agreement No. 008-2010 (as amended).

> *"Comprehensive Risk Management is defined as the process by which the Bank identifies, measures, monitors, controls, mitigates, and informs the operating areas within the bank of the various types of risk to which it is exposed, based on the size and complexity of its operations, products, and services."*

8.2 Definitions and terms applicable to Comprehensive Risk Management:

- **Senior Management:** Members of the Executive Committee and responsible for the management of each area.
- **Internal Environment:** The Bank's internal environment, which establishes the framework for personnel to comprehend and manage risks, encompassing risk management principles, risk appetite, integrity, ethical values, and the operational context.
- **Risk Appetite:** The level of risk that the Bank is willing to accept in relation to the expected return.
- **Risk Capacity:** The maximum level of risk that the Bank is willing to accept in pursuit of its objectives.
- **Application Controls:** Procedures programmed into applications and related manual procedures to ensure the integrity and accuracy of information processed.
- **Manual Controls:** Controls performed manually without the assistance of computers.
- **Goal Setting:** The action by which Senior Management establishes objectives to be achieved by the Bank in a given period of time, following specific parameters for the achievement of desired results.
- **Risk Assessment:** Analysis of the probability of occurrence and impact of risks on an inherent and residual basis to determine how they should be managed.
- **Event:** An internal or external event that affects the achievement of established objectives.

- **Comprehensive Risk Management:** In accordance with Agreement 008-2010 of the Superintendency of Banks of Panama (as amended), Comprehensive Risk Management is understood as the process by which the Bank identifies, measures, monitors, controls, mitigates and informs the operational areas within the Bank of the different types of risks to which it is exposed according to the size and complexity of its operations, products and services.
- **Event Identification:** Actions that allow knowledge of both external and internal events that may affect the achievement of established objectives.
- **Impact:** Result or effect of an event.
- **Reporting and Communication:** Process by which relevant information is identified, captured, and communicated in appropriate formats and at appropriate times to enable people to fulfill their control responsibilities. Effective communication also extends to Senior Management and the Board of Directors.
- **Common Language:** A set of commonly used words or terms whose meanings should be understood throughout the organization.
- **Lines of Defense:** The three lines that the Bank has in place to prevent the occurrence of intolerable risk events.
- **Monitoring:** Ongoing action to follow the operation of the comprehensive risk management framework and determine the need for changes, if any, through routine activities as well as specific assessments, such as those performed by Internal Audit.
- **Opportunity:** The occurrence of an event that has a positive impact on the probability of achieving established objectives.
- **Probability of Occurrence:** The likelihood that an event will occur.
- **Risk Response:** Actions taken by the Bank to avoid, accept, reduce or share risk and to align risk with the defined risk appetite and tolerance.
- **Risk:** The possibility that an event will occur and adversely affect the Bank's ability to achieve its objectives.
- **Inherent Risk:** Risk faced by the Bank in the absence of any action to mitigate it.
- **Residual Risk:** Risk that remains after management action to mitigate its impact and/or probability of occurrence.
- **Reasonable Assurance:** A concept that indicates that a comprehensive risk management framework, however well or poorly designed, cannot provide absolute assurance of the achievement of established objectives given existing inherent limitations.
- **Risk Tolerance:** Acceptable deviation from risk appetite.

9. Types of Risk

The Bank establishes a common definition of the different types of risk in accordance with the provisions of Agreement No. 008-2010 of the Superintendency of Banks of Panama, as amended, and other Agreements applicable by this Superintendency. The Bank's different types of risk are defined below:

- **Credit Risk:** The possibility that the Bank may suffer losses and that the value of its assets may decrease as a result of the failure of its borrowers to comply, in a timely manner, with the terms and conditions agreed upon in the credit agreements.

- **Counterparty Risk:** The possibility that a counterparty to a financial contract to which the Bank is a party may be unable to meet its financial obligations, causing the Bank to incur a loss.

- **Liquidity Risk:** The possibility of economic loss to the Bank due to difficulties in liquidating assets or obtaining funding under normal conditions.

- **Market Risk:** This is the risk of loss arising from adverse movements in the prices of products in the financial markets where positions are held, in relation to trading portfolio transactions. It consists mainly of price risk, interest rate risk and foreign exchange risk.

  - **Price Risk:** The possibility of economic loss resulting from adverse changes in the market price of a financial instrument or from the uncertainty of the price at a given time.
  - **Interest Rate Risk:** The possibility of economic loss resulting from adverse movements in interest rates.
  - **Foreign Exchange Risk:** The possibility of economic loss resulting from changes in foreign exchange rates.

- **Operational Risk:** The possibility of incurring losses due to deficiencies, failures or inadequacies of people, processes, technology, infrastructure or the occurrence of external events. This definition includes legal risk related to such factors.

  - **Legal Risk:** The possibility of incurring a loss as a result of non-compliance with rules, regulations or procedures, as well as the effect of contractual provisions. Legal risk also arises from malicious, negligent or involuntary actions that affect the formalization, effectiveness or execution of contracts or transactions.

- **Reputational Risk:** The possibility of incurring economic losses due to damage to the Bank's reputation. This includes, among other things, the impact of money laundering.

- **Country Risk:** The possibility of incurring losses from adverse changes in the economic, social and political environment or from natural disasters in the countries in which the Bank or its customers operate. Country risk includes, but is not limited to, transfer risk, political risk and sovereign risk.

    - **Transfer Risk:** The general inability of borrowers in a particular country to meet their financial obligations due to the unavailability of the currency in which the obligation is denominated, regardless of the particular financial position of the borrower.
    - **Political Risk:** Political risk refers to, among other things, the possibility of war, civil unrest and other situations of a purely political nature.
    - **Sovereign Risk:** The possibility that the sovereign borrower of a particular country will be unable or unwilling to meet its financial obligations.

- **Contagion Risk:** The possibility of losses that the Bank may suffer, directly or indirectly, as a result of adverse events in companies within its own economic group or in companies engaged in similar activities in the market where it is located or in the financial system of another country.

- **Strategic Risk:** The possibility of incurring losses as a result of decisions taken by the Bank's Senior Management in connection with the creation of sustainable competitive advantages. It is related to failures or weaknesses in the analysis of the market, the trends and uncertainties of the environment, the Bank's key competencies, and the process of value creation and innovation.

- **IT Risk:** The possibility of economic losses from an event related to the technological infrastructure, access or use of technology, which affects the development of the Bank's business processes and risk management by threatening the confidentiality, integrity, availability, efficiency, reliability, compliance or timeliness of information.

- **Concentration Risk:** A high level of exposure that could result in losses to the Bank that could affect its solvency or ability to continue operations. Concentrations of risk may arise in assets, liabilities, or off-balance sheet activities.

- **Social and Environmental Risk:** The possibility that the Bank incurs losses due to negative environmental and social impacts caused by the granting of loans for project financing, as well as by activities originating from the environment in which it operates and having a significant impact on the economic, social or environmental system.

- **Climate-related Risks:** These are the actual or potential negative impacts that may result from climate change or efforts to mitigate climate change. These impacts include economic and financial consequences for a company or organization. These risks can be categorized as physical, transition, and liability risks.

- **Physical Risks:** The general inability of borrowers in a particular country to meet their financial obligations due to the unavailability of the currency in which the obligation is denominated, regardless of the particular financial position of the borrower.
- **Transition Risk:** It refers to, among other things, the possibility of war, civil unrest and other situations of a purely political nature.
- **Climate-related Legal Liability Risks:** The possibility that the sovereign borrower of a particular country will be unable or unwilling to meet its financial obligations.

▪ **Model risk:** The set of potential adverse consequences resulting from decisions based on incorrect results or reports from models or their inappropriate use. Errors in a model may include simplifications, approximations, incorrect hypotheses, poor design, or deficiencies in the data used in the model. Inappropriate use refers to the use of models in contexts for which they were not designed and in which they are not valid.

▪ **Fraud risk:** An intentional act or omission designed to deceive others, resulting in loss to the victim and/or gain to the perpetrator.

10. Stages of Comprehensive Risk Management

The Comprehensive Risk Management process, , based on the indications of the Superintendency of Banks of Panama, as well as best practices, includes the following stages:

- **Identification:** The Identification process occurs in an analysis by Senior Management assisted by the Executive Vice President of Comprehensive Risk Management in which events are identified that, if they occur, could affect the Bank's ability to achieve its objectives. In this way, events with a negative impact are categorized as risks, and such risks, under our Comprehensive Risk Management Framework, must be evaluated and monitored.

Level 1 Risk	Level 2 Risk	
Credit	▪ Impact ▪ Counterparty	▪ Country ▪ Concentration
Market and Liquidity	▪ Price ▪ Liquidity	▪ Interest Rate ▪ Exchange Rate
Operational	▪ Internal Fraud ▪ External Fraud ▪ Customers, Products and Corporate Practices ▪ Management Information Deficiency ▪ Model Deficiency	▪ Legal ▪ Labor Relations and Workplace Safety ▪ Process Execution, Delivery and Management ▪ Business Interruption and Systems Failure ▪ Damage to Tangible Assets
Money Laundering and Terrorist Financing	▪ Customers ▪ Products and/or Services ▪ Geography	▪ Channels ▪ Employees
Business	▪ Reputation ▪ Environmental and Social (ESG)	▪ Strategic ▪ Climate

- **Measurement:** The Comprehensive Risk Management area is responsible for the development and maintenance of a variety of risk management techniques suitable to support the operations of the different business lines and the measurement of capital at the institutional level. These include, among others, the use of models and stress tests.

- **Mitigation:** Once the risks inherent in the Bank's environment have been identified and assessed, it is the responsibility of Senior Management and the CPER to decide whether the risk should be accepted, shared, avoided or transferred in order to reduce its consequences and impact. The following are examples of strategies that may be implemented depending on the type of mitigation sought.

Category	Strategy
Avoid	▪ Decide not to promote a new activity, product or service that could give rise to risks. ▪ Renounce an area, product or service.
Share	▪ Take out insurance against unexpected major losses (damage insurance). ▪ Contractual agreements with suppliers, customers or business partners.
Reduce	▪ Diversify products or services. ▪ Establish tolerance levels. ▪ Design controls.
Accept	▪ Set aside reserves to cover potential losses. ▪ Accept risk if it fits within existing risk tolerances.

- **Monitoring and Control:** Ensures that business activities are conducted within approved policies and limits and are consistent with the Bank's strategies and risk appetite. Any non-compliance in this regard is reported to Senior Management, the CPER or the Board of Directors, depending on the limit in question.

- **Reporting:** The Executive Vice President, of Comprehensive Risk Management is responsible for providing the Board of Directors, the CPER and Senior Management with risk reports to assist them in understanding the Bank's risk profile. Risk reporting is an additional element of risk measurement across products and businesses to ensure compliance with policies and limits, and to provide a mechanism for communicating the amounts, types and sensitivities of the Bank's various risks.

11. Risk Management Tools

Risk management includes tools consistent with the Comprehensive Risk Management Framework and is integrated with the Bank's strategic and business planning processes.

- **Policies**
  - Policies are based on recommendations from the members of Senior Management responsible for risk management, internal audit and the business units.
  - Policies take into account industry best practices and regulatory requirements.
  - They are aligned with the Bank's risk appetite and establish the Bank's operational limits and controls.
  - Key risk policies are approved by the Board of Directors, either directly or through the Risk Policy and Assessment Committee (CPER) or the Anti-Money Laundering, Compliance and Sustainability Committee or the Financial and Business Committee.

- **Limits**
  - These are the risk control activities within the tolerance levels set by the Board of Directors, the CPER and Senior Management. They also serve to define the various responsibilities for key tasks within the risk-taking process and the level or conditions under which transactions may be approved or executed.

- **Processes and Procedures**
  - Guidelines issued to implement and operationalize policies. In general, they describe the types of services, the total exposure for each service and the conditions under which the Bank is prepared to carry out its activities.
  - They are related to the identification, assessment, documentation, reporting and control of risks.

- **Models**
  - Quantitative methods, systems or approaches that apply statistical, economic, financial or mathematical theories and assumptions to process input data and produce quantitative estimates.

Models support the Bank's objectives and are fundamental in the risk measurement phase.

- **Stress Testing**

- Stress testing programs allow the Bank to estimate the potential impact of significant changes in market conditions, the credit environment, liquidity requirements and other risk factors on its earnings, capital and liquidity.

▪ **Back Testing**

- Back testing is a validation technique that tests the results of a predictive model against historical data. Its application to the Bank's various models ensures that their evolution is constant and allows parameters and assumptions to be adjusted so that they do not become outdated.

12. Comprehensive Risk Management Committees

The Bank has a well-established risk control structure that includes an active and committed Board of Directors supported by an experienced Senior Management team and a centralized risk management group that is independent of the business lines. Decision-making is centralized in a number of senior and executive risk management committees. The committee structure is designed to ensure alignment of risk objectives, risk tolerance and risk resources.

The following are the committees on which the Executive Vice Presidency of Comprehensive Risk Management participates:

- **Risk Policy and Assessment Committee (CPER):** This Committee reviews and evaluates the Bank's exposure to the various risks it faces in its business management, including the quality and profile of credit assets, the exposure to market risks, and the analysis of operational risks, taking into account the legal risks of the products offered by the Bank, within the limits of the risk levels the Bank is willing to assume in accordance with the relevant policies.

- **Assets and Liabilities Committee (ALCO):** Responsible for monitoring and managing the Bank's liquidity, interest rate and currency mismatches, and coordinating disbursement and funding activities to optimize earnings and manage risk.

- **Credit Committees:** Approve requests for new credit limits, annual credit limit renewals, maturity extensions and/or changes to these economic group and/or individual credit limits for all regions and business areas, including Treasury. It comprises both the Management's Credit Committee (CCA) and the Board's Delegated Credit Committee (CCD).

- **Executive Committee:** This Committee is responsible for directing and carrying out the administrative management of the Bank, based on the delegation of powers by the Board of Directors in matters of approval of expenditures, investments and human resources.

- **Management and Monitoring Committee:** Reviews the situation of those customers in category 6 or worse, in the process of restructuring and/or in impaired condition that require a review of their structure, strategy, guarantees, exit plan, among others.

- **Operational Risk Committee:** The body responsible for overseeing the management and control of operational risks within the Bank.

- **IT Risk and Information Security Committee:** The body responsible for overseeing the management and control of risks arising from the use and management of technology, information security and cybersecurity within the Bank.

- **Country Risk Committee:** Reviews and recommends to the CPER changes in the rating and the amount of the country limit and conditions of use of the countries in which Bladex operates. Monitors the economic, political and social situation of countries in Latin America in which the Bank has financial exposure or potential business.

- **Technology Committee:** Ensures that the Technology Department delivers the expected benefits (products and services) in accordance with the business strategy.

- **Data Operating Committee:** Proposes, approves and oversees activities related to the identification, assessment and management of the quality and use of data included in the Governance Model.

- **Project Portfolio Committee:** Follows up and receives information on the status of each project and the Bank's strategy.

- **Anti-Money Laundering, Compliance and Sustainability Committee:** Assists the Board of Directors in fulfilling its oversight responsibilities with respect to the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, and is responsible for providing strategic direction to the organization's compliance program.

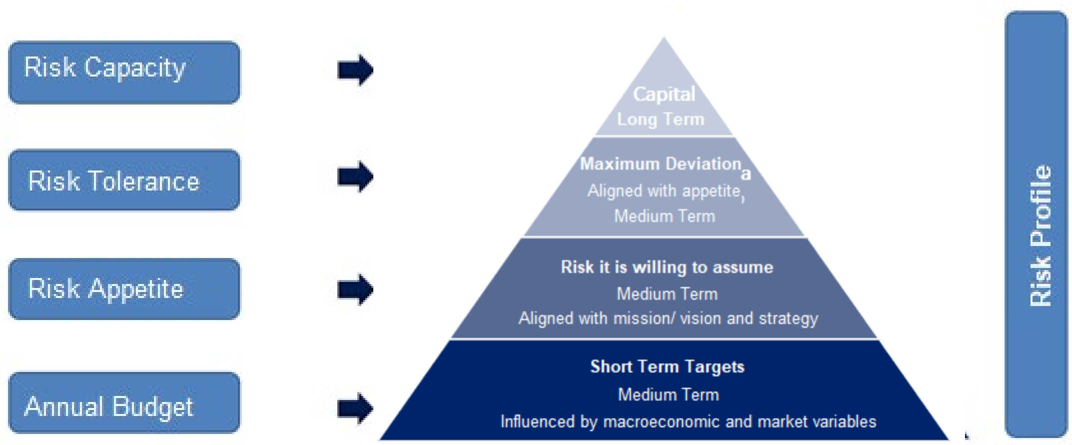
Comprehensive Risk Management, which is an integral part of all the Bank's decision-making and follow-up processes, involves several committees that are not described in this document, but whose composition and functions are described in the Bank's Corporate Governance Manual.

13. Risk Appetite Framework

13.1 Appetite, Tolerance and Capacity

Risk appetite represents the balance between the Bank's capacity to take risks and the business opportunities associated with those risks. It is expressed through limits on quantitative metrics and qualitative indicators that measure the Bank's risk exposure or profile by risk type, portfolio, segment and business line, both under current and stressed conditions. These risk appetite metrics and limits are articulated in axes that define the positioning that the Bank wishes to adopt or maintain in the development of its business model:

- The solvency position the Bank wishes to maintain.
- The volatility in the profit and loss account that it is willing to accept.
- The minimum liquidity position the Bank wishes to maintain.
- The maximum level of concentration that the Bank considers reasonable to assume.

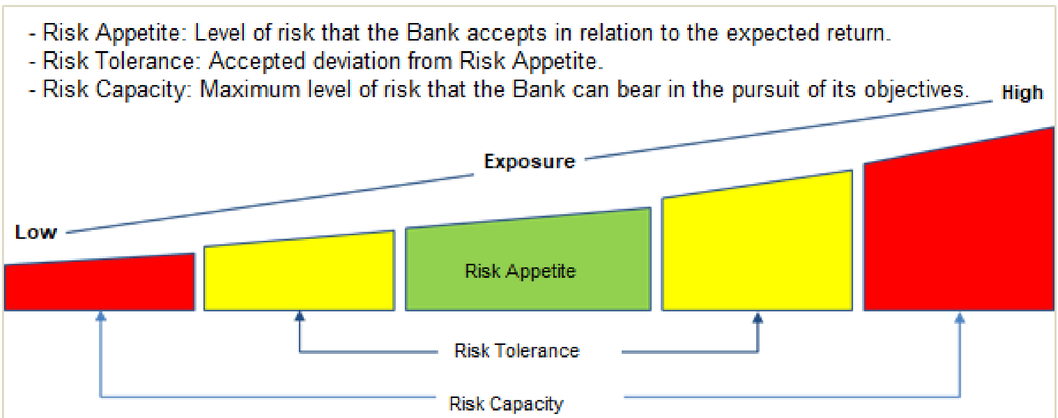


The Risk Appetite Framework should be integrated with planning processes that ensure that the Bank's strategy is consistent with the risk it is willing to take.

The relationship between the Risk Appetite Framework and Business Management is as follows:

- The Risk Appetite Framework is integrated into the decision-making process, while risk management and mitigation strategies are aligned with the purpose of achieving business objectives.
- The Bank has set a target for its risk-adjusted return to exceed its cost of capital in order to create value from the sum of the returns of its various businesses.

- Any transaction proposed as an exception to the established limits must represent a differentiated business opportunity and must receive the necessary approvals from the bodies empowered to approve such exceptions.
- Appetite is used for normal conditions, it must be aligned with the strategy, it is recalibrated at least every 12 months and in a stress scenario ("black swan" type Covid-19) it is expected that these indicators will be sensitized.



The review and updating of Risk Appetite indicators is an ongoing exercise:

- As new metrics are defined, they will be measured and presented on a quarterly basis.
- The metrics are defined by management and discussed and approved by the Risk Management Committee.

13.2. Risk Appetite Statement

Bladex declares that it has an appetite for a medium residual risk profile based on sustainable growth to achieve a balanced portfolio, but with a low tolerance for operational risks that could interrupt our services, as well as regulatory non-compliance.

This statement underscores a balanced approach that recognizes the need for growth while emphasizing the importance of regulatory compliance and operational stability.

“CAMELS" Metrics
(Capital Adequacy, Asset, Management Capability, Earnings, Liquidity, Sensitivity)

Axes	Description	Value
a) Capital	Capital Adequacy (SBP)	Appetite: 14% Tolerance: 13.5%
	Basel III Capital	Appetite: 16% Tolerance: 15.5%
	RAC (Risk Adjusted Capital) S&P	Appetite: 11% Tolerance: 10%
	Country Concentration (Low)	Group: 100% Individual: 25%
	Country Concentration (Normal)	Group: 75% Individual: 20%
	Country Concentration (Moderate)	Group: 50% Individual: 17.5%
	Country Concentration (Difficulty)	Group: 25% Individual: 7.5%
	Country Concentration (Doubtful)	Group: 10% Individual: c/c
	Customer Concentration (Top 20)	Appetite: 40% Tolerance: 45%
	Customer Concentration (Top 50)	Appetite: 65% Tolerance: 70%
	Customer Concentration (Top 100)	Appetite: 85% Tolerance: 90%
	Operating Environment (Moody’s)	Appetite: 7.0 Tolerance: 7.5
	Operating Environment (Fitch)	Appetite: 9.0 Tolerance: 9.5
	Operating Environment (S&P)	Appetite: 6.5 Tolerance: 7.0
	Duration	Appetite: 14m Tolerance: 16m
	Main 20 / Tier 1	Appetite: 2.7x Tolerance: 3.1x
	Trade Short Term	Appetite: 55% Tolerance: 45%
	Reserves (Stage 1 and 2) / Loan Portfolio	Appetite: 1.0% Tolerance: 0.5%
c) Management	Data quality (first 6 “entities”)	Appetite: 90% Tolerance: 80%
	Project Execution (Deviation from Critical Path)	Appetite: 0% Tolerance: 5%
	Operational (Global Limit)	Appetite: USD 4.5MM Tolerance: USD 2.25MM

Axes	Description	Value
	Operational (Loss Limit)	Appetite: USD 0.9MM Tolerance: USD 1.8MM
	Information Security (Vulnerability Risk Level)	Appetite: <240 Tolerance: <349
	Information Security (Cybersecurity Score)	Appetite: >90 Tolerance: >87
	Information Security (Phishing)	Appetite: <4% Tolerance: <7%
	Employee Fraud	Appetite: 0 Tolerance: 0
	Supplier Fraud	Appetite: 0 Tolerance: 0
	Fraudulent Transfers	Appetite: 0 Tolerance: 0
d) Earnings	ROE	Appetite: 15% Tolerance: 13%
	ROA	Appetite: 1.75% Tolerance: 1.5%
	Efficiency	Appetite: 28% Tolerance: 30%
e) Liquidity	Coverage of liabilities due in the next 30 days with liquid assets (LCR SBP)	Appetite: 120% Tolerance: 100%
	% Top 20 Depositors	Appetite: 64% Tolerance: 70%
	Liquidity / Performing Assets	Appetite: 17% Tolerance: 15%
	Net Gap / 90d Liabilities	Appetite: 5% Tolerance: 5%
f) Sensitivity	(NII) +/- 200bps	Appetite: USD 10MM Tolerance: USD 10MM
	(EVE) +/- 200bps	Appetite: 2.5% Tier 1 Tolerance: 2.5% Tier 1

14. Rules for Use of the Comprehensive Risk Management Framework

14.1 Compliance and Interpretation

The integrity and good judgment of the Bank's professionals is a key aspect in the application of the policies described in this Document. All employees involved in the Bank's Comprehensive Risk Management process must be aware of and act in accordance with the policies set forth herein.

Likewise, employees who are required to comply with the Comprehensive Risk Management Framework must understand the spirit and purpose of the Framework in order to apply their reasoning and rationale to situations that may not have been foreseen in this Document.

Any doubt regarding the interpretation and application of the Comprehensive Risk Management Framework should be referred to the Executive Vice President of Comprehensive Risk Management for clarification.

14.2 Review and Update

The Comprehensive Risk Management Framework is a document that needs to be updated and adapted according to the situations that the Bank goes through, such as:

- Changes in applicable regulations
- Changes in business strategy
- Access to new markets, products or technological developments that introduce new risks
- Changes in risk structure or limits
- Changes in organizational structure
- Changes in the infrastructure of the IT systems used that involve automation of manual processes
- Regulatory changes
- Recommendations from committees of the Board of Directors, Internal Audit and/or External Audit.

The responsibility for updating this Comprehensive Risk Management Framework lies with the Executive Vice Presidency of Comprehensive Risk Management, with the support of the Vice Presidencies of Credit Risk Management (Origination), Credit Risk Management (Monitoring and Recovery), the Vice Presidency of Country Risk Management, the Vice Presidency of Market and Liquidity Risk Management, Vice Presidency of Operational Risk Management and Business

Continuity, Vice Presidency of IT Risk Management and Information Security, and Vice Presidency of Management of Other Non-financial Risks.

Except in the circumstances described above in this section, the Executive Vice President of Comprehensive Risk Management shall, on an annual basis during the fiscal year, request information from the members of the Executive Committee regarding matters to be considered under the Comprehensive Risk Management Framework and, if necessary, shall make the appropriate changes to the Framework and then submit it to the Board of Directors for review and approval.

14.3 Distribution

The Comprehensive Risk Management Framework, once approved, will be made available through the electronic disclosure tool for policies and procedures on the Bank's Corporate Intranet ("Bladexpoint").