I. OBJECTIVE

To raise awareness on risk management among Banco de la República's (BanRep) suppliers with the purpose of strengthening their knowledge of the risks and practices inherent in their processes to ensure adequate delivery of the products and services to BanRep as per their contractual agreement.

II. CONTENT

1. Key concepts
2. Integrated Risk Management at Banco de la República de Colombia (BanRep, the Central Bank of Colombia).
3. BanRep's Key Elements for Risk Management
4. Banrep's Comprehensive Risk Management Contact

1. KEY CONCEPTS

1.1 Key Concepts

- **Comprehensive Risk Management:** Enterprise Risk Management (ERM) refers to the identification, measurement, monitoring, control, and reporting of risk types in all categories and their interrelationships affecting the performance and continuity of an organization's processes.
- **Risk:** Effect of uncertainty on objectives .
- **Operational Risk:** It is the possibility that the institution incurs losses due to deficiencies, failures, or inadequate operation of processes, technology, infrastructure or human resources, as well as the occurrence of external events associated with them, including legal risks .
- **Third Party Risk – Suppliers:** Risk of incurring losses arising from non-compliance or deficiencies in the provision of services to the institution by third parties.
- **Risk Event:** A fact or change that may affect the achievement of the institution's objectives. In terms of operational risk, it refers to an event or change that can generate financial or reputational impacts to the institution.

1.2 Main Risks associated with Third-Party Management

- **Operational:** Losses due to deficiencies, failures or inadequate operation of processes, technology, infrastructure, or human resources, as well as the occurrence of external events associated with them.
- **Money Laundering and Terrorism Financing:** Risk of an institution being used to make assets from criminal activities appear to be lawful or to channel resources into terrorist activities. Asset Laundering: A set of activities aimed at concealing the illicit origin or at giving the appearance of legality to resources obtained from the execution of illicit activities. Terrorism Financing: A set of activities aimed at channeling licit or illicit resources to promote, defray, or sponsor terrorist individuals, groups, or activities.
- **Unavailability:** Risk of incurring losses resulting from the interruption of internal processes resulting from the unavailability of human resources, information, technology, or infrastructure belonging to the Bank or of external sources.
- **Information Security and Cyber Risk:** Information Security: Risk of incurring losses arising from the impairment of the integrity, confidentiality, or availability of information from the institution. Cyber Risk: Risk of incurring losses resulting from failures, unauthorized, or misguided use of the Bank's information systems or from cyber-attacks.
- **Legal:** Risk of incurring losses arising from penalties or indemnities resulting from non-compliance with regulations or contractual obligations. This includes third parties acting on behalf of the institution.
- **Reputational:** Risk of negative impairment of the trust/credibility of the institution by one or more of its stakeholders in terms of integrity, technical or operational capacity, or compliance. It is a consequence of the materialization of other risks.

1.3 Risk Management Cycle

In the development of its processes, especially those directly related to the services provided by its suppliers, it is important to identify, measure, treat, control, and monitor the risks associated with the following processes:

ID: At this stage, the aim is to determine the risks (current and potential) inherent (without controls) to the processes and/or activities that the institution develops or plans to develop.

Measurement: Its objective is to determine the level of exposure of the risks, supported by the measurement of their probability of occurrence and potential impact.

Treatment: To establish risk management measures to make decisions regarding the management of residual risks.

Control and Monitoring: Carry out follow up on the risk profile through different mechanisms with the purpose of taking timely measures (continuous improvement) to prevent and correct deviations from risks and from the risk management system.

1.4 Main Risks and Controls in Third-Party Management - Third-Party Life Cycle and Risk Management

During the stages of the life cycle of third parties, different risks can materialize at BanRep. Therefore, it is important to exercise control practices during the different stages:

Types of Risks R1. Operational Risk - Fraud

Proposed Controls:

- C1. Good Governance Schemes
- C2. Code of Ethics and Conduct
- C3. Segregation of Duties

Types of Risks: R2. AL / TF

Proposed Controls:

- C1. Policies to prevent risks of AL and TF
- C2. Periodic checklist verification (third parties, employees, customers, etc.)

Types of Risks: R3. Operational Risk - Failures and Errors

Proposed Controls:

- C1. Dual Controls
- C2. Automatic Controls
- C3. Segregation of Duties

Types of Risks: R4. Unavailability

Proposed Controls:

- C1. Continuity Plans
- C2. Redundancy Schemes and Alternate Contingencies

Types of Risks: R5 Information Security and Cyber Risk

Proposed Controls:

- C1. User Administration
- C2. Confidentiality Agreements
- C3. Access Controls
- C4. Vulnerability Scanning
- C5. Erasing Data

IMPORTANT: For the proper management of these risks, it is important that all our suppliers have a risk management system, or at least an adequate control environment that ensures that the different high-level and operational controls are applied, establishing treatment strategies to minimize exposure to risks that may affect the delivery of the service provided to its customers.

2. COMPREHENSIVE RISK MANAGEMENT AT *BANCO DE LA REPÚBLICA*

2.1 Scope

Comprehensive Risk Management is carried out through the administration of the following subsystems:

Risk management subsystems may have individual policies that provide guidelines for the particular management of risks within a risk process or type according to their scope. These policies fall within the umbrella of the Bank's Comprehensive Risk Management System.

2.2 Risk Taxonomy

The Comprehensive Risk Management at Banco de la República covers all mission and corporate processes, areas, branches and agencies, all the Bank's employees, **suppliers and third parties** related to BanRep. It is cross-sectional to the risk typologies established in the following taxonomy:

2.3 “Three Lines of Defense” Model

Comprehensive Risk Management is supported in a three-line defense model that allows to identify, manage, control, and monitor BanRep's risks through a scheme of weights and balances, with an independent risk unit that reports functionally to the highest level of the organization .

3. BANREP’S KEY ELEMENTS FOR RISK MANAGEMENT

3.1 Code of Conduct

The Bank has a Code of Conduct, which is a compendium of internal regulations that establish and develop the principles and values that govern the performance of the functions of the employees at BanRep.

In turn, it is a frame of reference for individuals and legal persons with whom BanRep has some contractual relationship regarding the conduct expected of BanRep’s employees. Therefore, it is important for suppliers to be aware of the Code of Conduct and to adopt the provisions set out therein.

Our Values

- **INTEGRITY:** We act with independence, accountability, honesty, consistency, transparency, and a sense of public assets.
- **EXCELLENCE:** We commit to quality results in a timely, dynamic, and efficient manner, regarding both services to the economy and internal processes.
- **SUSTAINABILITY:** We contribute to generating positive economic, social, and environmental impacts with a long-term vision.
- **INCLUSION:** We value differences, welcome diversity, act equitably, and listen to different opinions and points of view.
- **RESPECT:** We offer a dignified and cordial treatment to all people, recognizing and valuing all efforts, contributions, and achievements.

3.2 Practices for handling conflicts of interest, presents, or invitations by suppliers

Suppliers should be aware of the Code of Conduct at BanRep, particularly the guidelines established therein for conflicts of interest , presents, or invitations from third parties:

- Refrain from making payments or disbursements or any kind of retribution to BanRep’s employees.
- Validate and monitor relationships that may generate conflict of interest situations for the subscription and during the execution of a contract with BanRep.

- Not offering gifts, favors, prizes, preferential deals, invitations, or trips, among others, that compromise or may give the appearance of compromising an employee's judgment and independence for decision-making.
- To inform BanRep of any conflict of interest of an employee of BanRep in charge of a contract through the established reporting channels: Sección de Atención a la Ciudadanía.

3.3 Comprehensive Risk Management

Risk events are incidents that represent the materialization of a risk or that alert of potential risks, and are generated by failures in internal processes, technology, infrastructure, people, or events generated by external sources.

As a supplier for Banco de la República, in an event that may affect the provision of services or the performance of the contract, BanRep must be notified in the person of the employee in charge of the contract as soon as possible by e-mail: dgrp-riesgos@banrep.gov.co, with description of the event, its causes, and actions taken for mitigation.

4. BANREP'S COMPREHENSIVE RISK MANAGEMENT CONTACT

Should you have any questions or concerns regarding risk management at your institution, your relationship as a supplier to Banco de la República, or about BanRep's Comprehensive Risk Management System, or if you wish to report any risk events to us, please e-mail us at:

dgrp-riesgos@banrep.gov.co

We will be happy to respond to your concerns.