Report on the status of Banco de la República (the Central Bank of Colombia) Internal Control System - First half of 2023

AUTHORS AND/OR EDITORS Internal Control Department
Status of the Bank's Internal Control System: **100%**

Publication Date: Thursday, 20 of February 2025 General Conclusion on the Evaluation of the Internal Control System

- Are all components operating together in an integrated manner? (Yes / in process / No) (Justify your answer):

Yes. According to the independent evaluation performed on the design and operation of the relevant controls related to the principles or guidelines established for each of the five components of the Internal Control Standard Model "Control Environment," "Risk Assessment," "Control Activities," "Information and Communication," and "Monitoring Activities," in accordance with the format and instructions provided by the Civil Service Administrative Department for the evaluation of the internal control system, pursuant to the provisions of its External Circular 100-006 of 2019 and Article 156 of Decree Law 2106 of 2019, it was found that the aforementioned components of the model exist and are operating together in an integrated manner.

Likewise, it was observed that these components operate transversally in Banco de la República, and that together with the three-line model implemented by the Bank, they allow the control of the risks to which the Bank is exposed in order to achieve its objectives.

- Is the internal control system effective for the objectives evaluated? (Yes / in process / No) (Justify your answer):

Yes. The Internal Control System of Banco de la República is effective, since each of the components of the Internal Control Standard Model and principles or guidelines related to each component are present and operating, as per the independent evaluation carried out in accordance with the format and instructions provided by the Civil Service Administrative Department for the evaluation of the internal control system, and the provisions of its External Circular 100-006 of 2019 as well as Article 156 of Decree 2106 of 2019. No control failures were identified that could have any impact on the Bank's internal control system.

- Within its Internal Control System, the Bank has an institutional framework (lines of defense) that allows it to make decisions regarding control (Yes / in process / No) (Justify your answer):

Yes. The governance framework, control architecture, and risk management of Banco de la República are based on the Three-Line Model, in which the following lines participate: i) a strategic line made up of the Board of Directors, the Administrative Council, the Audit Committee, the Risk Committee, the Institutional Committee for Internal Control Coordination, and Top Management; ii) the first line, made up of all business units and process leaders whose main role is risk-taking and self-control and who are responsible for risk mitigation and the effectiveness of operational controls; iii) the second line, made up of the Office for Risk Management and the Legal Department, whose main role is to manage and improve the Bank's integrated risk system and monitor risk management independently from the first line; and iv) the third line, made up of the Internal Control

Department, whose main role is to plan, direct, and organize the independent verification and evaluation of the Bank's Internal Control System.

In addition, the Bank has a "fourth line" made up of the Auditor General's Office (which exercises its function independently), an external financial audit, and the different control, supervision, and oversight agencies.

These lines operate in a coordinated manner with clear lines of communication and reporting for decision-making regarding risks and control, and each one contributes from its role to the maintenance and strengthening of the Bank's Internal Control System.

1. Component: Control environment
   - Is the component present and working? Yes
   - Level of compliance with the component: **100%**
   - Estado actual: Explicación de las debilidades y/o Fortalezas:
     - **Strengths:** *Banco de la República* (the Central Bank of Colombia) remains committed to integrity and promotes the ethical behavior of its employees through the disclosure and periodic follow-up of compliance with the Code of Conduct. Procedures for the management of potential conflicts of interest have been designed, implemented, and disclosed. The Bank has procedures for its suppliers to declare the non-existence of disqualifications and incompatibilities in the contracting processes. An anti-fraud strategy has also been designed and implemented, which includes a statement on "zero tolerance" for illicit acts. Per this strategy, the Bank also formulated the Anti-Corruption and Citizen Services Plan (PAAC, in Spanish) and as mentioned in the risk assessment component, this contains the activities for monitoring and reviewing corruption risk management, which by 2023 was aimed at strengthening the culture of prevention, detection, and response to illicit acts, promoting actions to fight corruption, and improving the interaction between the Bank and citizens through the improvement of service, transparency, and reporting mechanisms.

       In addition, the Bank designed and implemented the *Sistema Informático de Atención al Ciudadano*, SIAC (Citizen Services Informatic System) as a technological tool for the management of requests, complaints, claims, suggestions, and reports (PQR in Spanish). The Bank has also implemented policies, guidelines, and controls for the mitigation of cybersecurity risks and the protection of information assets, including privileged information, which include the use of technological tools and permanent monitoring schemes. The Bank completed the implementation of the new *Sistema de Atención al Ciudadano*, SAC (Citizen Services System), as detailed in the Information and Communication component.
     - The Bank is committed to staff competency and has designed and implemented policies and procedures for staff selection, performance evaluation, and termination processes. It also establishes annual training plans, which are monitored through the Training Committee. The governing bodies establish the strategic objectives, as well as those responsible for them, the schedule for their fulfillment, and indicators under the SMART methodology through which the achievement of these objectives is monitored.
     - In addition, it adopted a process-based management model, as well as the Three-Line Model, which establishes clear roles, responsibilities, and reporting and accountability lines for the management of controls and risks. The model includes: i) a strategic line made up of the Board of Directors, the Administrative Council, the Audit Committee, the Risk Committee, the Institutional Committee for Internal Control Coordination, and Top Management; ii) the first line, made up of all business units and process leaders; iii) the second line, made up of the Office for Risk Management and the Legal Department; and iv) the third line, made up of the Internal Control Department. In addition, the Bank has a "fourth line" made up of the Auditor General's Office (which exercises its function independently), an external financial audit, and the different control, supervision, and oversight

agencies. The Internal Control System is evaluated and supervised by the Institutional Committee for Internal Control Coordination and the Audit Committee, through which it is monitored and its improvement is ensured. The Risk Committee approves the policies of the Integrated Risk Management System (IRMS), defines the risk appetite, tolerance, and exposure limits, approves the methodologies that support the IRMS, and follows up on integrated risk management through periodic reports from the second line.
    - The Bank has defined policies and procedures related to the induction process for new staff members to strengthen their integration into the culture and to promote employee performance.
    - During the first half of 2023, the Bank has continued implementing the controls related to the Control Environment component.
    - **Weaknesses:** No weaknesses were identified.

- Level of compliance with the component presented in the previous report: **100%**
- Status of the component presented in the previous report:
    - **Strengths:** *Banco de la República* (the Central Bank of Colombia) remains committed to integrity and promotes the ethical behavior of its employees through the disclosure and periodic follow-up of compliance with the Code of Conduct. Procedures for the management of potential conflicts of interest have been designed, implemented, and disclosed. The Bank has procedures for its suppliers to declare the non-existence of disqualifications and incompatibilities in the contracting processes. An anti-fraud strategy has also been designed and implemented, which includes a statement on "zero tolerance" for illicit acts. In accordance with this strategy, the Bank also formulated the Plan Anticorrupción y de Atención al Ciudadano, PAAC (Anti-Corruption and Citizen Services Plan) and designed and implemented the *Sistema Informático de Atención al Ciudadano,* SIAC (Citizen Services Informatic System) as a technological tool for the management of requests, complaints, claims, suggestions, and reports (PQR). The Bank has also implemented policies, guidelines, and controls for the mitigation of cybersecurity risks and the protection of information assets, including privileged information, which include the use of technological tools and permanent monitoring schemes. During the second half of 2022, the Bank completed the implementation of the "new citizen services system", as detailed in the "information and communication" component.
    - The Bank is committed to staff competency and has designed and implemented policies and procedures for staff selection, performance evaluation, and termination processes. It also establishes annual training plans, which are monitored through the Training Committee. The governing bodies establish the strategic objectives, as well as those responsible for them, the schedule for their fulfillment, and indicators under the SMART methodology through which the achievement of these objectives is monitored.
    - In addition, it adopted a process-based management model, as well as the Three-Line Model, which establishes clear roles, responsibilities, and reporting and accountability lines for the management of controls and risks. The model includes: i) a strategic line made up of the Board of Directors, the Administrative Council, the Audit Committee, the Risk Committee, the Institutional Committee for Internal Control Coordination, and Top Management; ii) the first line, made up of all business units and process leaders; iii) the second line, made up of the Office for Risk Management and the Legal Department; and iv) the third line, made up of the Internal Control Department. In addition, the Bank has a "fourth line" made up of the Auditor General’s Office (which exercises its function independently), an external financial audit, and the different control, supervision, and oversight agencies. The Internal Control System is evaluated and supervised by the Institutional Committee for Internal Control Coordination and the Audit Committee, through which it is monitored and its improvement is ensured. The Risk Committee approves the policies of the Integrated Risk Management System (IRMS), defines the risk appetite, tolerance, and exposure limits, approves the methodologies that support the IRMS, and follows up on integrated risk management through

periodic reports from the second line.
    - During the second half of 2022, the Bank defined policies and procedures related to the induction process for new staff members to strengthen their integration into the culture and to promote the performance of its employees.
    - **Weaknesses:** No weaknesses were identified.

- Final component progress: **0%**

2. Component: Risk assessment
    - Is the component present and working? Yes

    - Level of compliance with the component: **100%**
    - Current status: Explanation of weaknesses and/or strengths:
        - **Strengths:** The Bank has implemented the Integrated Risk Management System (IRMS) through a policy approved by the Risk Committee and disclosed to all employees, defining the guidelines that make up the Management System, understood as the set of policies, limits, methodologies, and monitoring and control schemes established by the Bank to manage the organization's risks and support decision-making. It is considered a fundamental pillar to support the Bank's strategic and operational decision-making and is based on the Three-Line Model. The risk subsystems of the model develop policies for each of them: financial, operational, information and cyber risk, money laundering and terrorist financing, conduct, compliance, environmental, and third-party risk. The scope of the IRMS is transversal to all mission and corporate processes, areas, branches, and agencies. The IRMS assigns roles and responsibilities under the Three-Line Model and defines the following stages for risk management: i) Identification; ii) Measurement or valuation; iii) Risk control and treatment; and iv) Monitoring through reports.
        - The Risk Committee periodically follows up on the progress and status of the integrated Risk Management System through reports made by the second line and, on a consolidated basis, through the Financial and Non-Financial Risk Reports. Actions are taken on reports related to risk materialization, establishing improvement plans subject to follow-up. The third line performs independent evaluations of risk management by the first and second lines, establishing improvement plans that are subject to monitoring by the Audit Committee. The methodologies for operational risk management consider the construction of matrices that are periodically reviewed to determine changes in processes due to internal or external factors, as well as changes in controls.
        - Process-Based Management allows for a clear identification of the mission and corporate processes along with their objectives. The strategic planning process considers the relationship of the strategic objectives with the objectives at the level of mission and support processes, as well as project objectives for the adequate evaluation of their risks and the definition of control activities. The strategic objectives are monitored by Senior Management through indicators to ensure compliance. The Bank continues to strengthen its risk governance; therefore, it consolidated the Financial Risk Department to operate as a second transversal line for the management of the Bank's financial and consolidated risk monitoring, with the definition of a policy for financial risk management and with defined work plans for the implementation of the risk model. The roles of the first and second lines regarding Cybersecurity and Information Security risk were reviewed and established.
        - The Bank regularly follows-up and monitors Cybersecurity as one of its risk priorities, which includes the analysis of its security posture reporting to the Risk Committee. For the first half of 2023, improvements have been made as per the results of an external expert assessment on Cybersecurity Posture to strengthen the process control framework. The Bank made adjustments to its IRMS and the Operational Risk Management System to align with the new provisions of the Financial Superintendency of Colombia (SFC in Spanish) - External Circular 018 of 2021 - Risk Management System for Excepted Entities (SARE, in Spanish), and also strengthened risk

management through the introduction of improvements in the governance of management of Operational Risk Events (EROs in Spanish), monitoring, and reporting. At the same time, the Bank's business continuity policies as well as the functions of the bodies and roles involved in the process were reviewed, updated, and approved by the Risk Committee.
    - The Anti-Corruption and Citizen Services Plan (PAAC in Spanish) is prepared annually by the Office for Risk Management, which contains the activities for monitoring and reviewing the corruption risk management. For 2023, the plan was aimed at strengthening the culture of prevention, detection, and response to illicit acts, promoting actions to fight corruption, and improving the interaction between the Bank and the citizens through the improvement of the mechanisms for assistance, transparency, and reporting. It includes the activity plans for strengthening the direct domestic mechanisms for the prevention, detection, and response to acts of corruption, the socialization of the Bank's corruption risk map, the strengthening of the Bank's Citizen Services System, the management of PQR for citizens and the promotion of transparency in its management. The PAAC is subject to periodic monitoring by the third line.
    - In the first half of 2023, the Risk Committee approved the methodologies for reporting the Bank's individual financial risks, structural risk, and Balance Sheet Stress. It also approved the Third-Party Risk Management System, which includes policies, roles, and responsibilities, and the methodology for defining critical third parties. Likewise, it established and approved the training plan on Integrated Risk Management for the 2023 fiscal year, and the governance for environmental risk management.
    - **Weaknesses:** No weaknesses were identified.

- Level of compliance with the component presented in the previous report: **100%**
- Status of the component presented in the previous report:
    - **Strengths:** The Bank has implemented the Integrated Risk Management System (IRMS) through a policy approved by the Risk Committee and disclosed to all employees, defining the guidelines that make up the Management System, understood as the set of policies, limits, methodologies, and monitoring and control schemes established by the Bank to manage the organization's risks and support decision-making. It is considered a fundamental pillar to support the Bank's strategic and operational decision-making and is based on the Three-Line Model. The risk subsystems of the model develop policies for each of them: financial, operational, information and cyber risk, money laundering and terrorist financing, conduct, compliance, environmental, and third-party risk. The scope of the IRMS is transversal to all mission and corporate processes, areas, branches, and agencies. The IRMS assigns roles and responsibilities under the Three-Line Model and defines the following stages for risk management: i) Identification; ii) Measurement or valuation; iii) Risk control and treatment; and iv) Monitoring through reports.
    - The Risk Committee periodically follows up on the progress and status of the integrated Risk Management System through reports made by the second line and, on a consolidated basis, through the Financial and Non-Financial Risk Reports. Actions are taken on reports related to risk materialization, establishing improvement plans subject to follow-up. The third line performs independent evaluations of risk management by the first and second lines, establishing improvement plans that are subject to monitoring by the Audit Committee. The methodologies for operational risk management consider the construction of matrices that are periodically reviewed to determine changes in processes due to internal or external factors, as well as changes in controls.
    - Process-Based Management allows for a clear identification of the mission and corporate processes along with their objectives. The strategic planning process considers the relationship of the strategic objectives with the objectives at the level of mission and support processes, as well as project objectives for the adequate evaluation of their risks and the definition of control activities. The strategic objectives are monitored by Senior Management through indicators to ensure compliance.

The Bank continues to strengthen its risk governance; therefore, it consolidated the Financial Risk Department to operate as a second transversal line for the management of the Bank's financial and consolidated risk monitoring, with the definition of a policy for financial risk management and with defined work plans for the implementation of the risk model. The roles of the first and second lines regarding Cybersecurity and Information Security risk were reviewed and established.

- The Bank regularly follows-up and monitors Cybersecurity, which includes the analysis of its security posture, reporting to the Risk Committee, as one of its risk priorities. For the second half of 2022, an external expert assessment on Cybersecurity Stance was conducted to strengthen the control framework of the process. The Bank made adjustments to its IRMS and the Operational Risk Management System to align with the new provisions of the Financial Superintendency of Colombia (SFC in Spanish) - External Circular 018 of 2021 - Risk Management System for Excepted Entities (SARE) that comes into force in June 2023, and also strengthened risk management through the introduction of improvements in the governance of management of Operational Risk Events (EROs in Spanish), monitoring, and reporting. At the same time, the Bank's business continuity policies, as well as the functions of the bodies and roles involved in the process, were reviewed, updated, and approved by the Risk Committee.
- The Anti-Corruption and Citizen Services Plan (PAAC in Spanish) is prepared annually by the Office for Risk Management, which contains the activities for monitoring and reviewing the management of corruption risks. For 2022, the plan was aimed at strengthening the culture of prevention, detection, and response to illicit acts, promoting actions to fight corruption, and improving the interaction between the Bank and the citizens through the improvement of the mechanisms for assistance, transparency, and reporting. It includes the activity plans for corruption risk management, for reports and dialogues and incentives with citizens, mechanisms for transparency and access to public information. It also contains the corruption risk matrix. The PAAC is subject to periodic monitoring by the third line.
- **Weaknesses:** No weaknesses were identified.

- Final component progress: **0%**

3. Component: Control activities
   - Is the component present and working? Yes

   - Level of compliance with the component: **100%**
   - Current status: Explanation of weaknesses and/or strengths:
     - **Strengths:** he Bank has established guidelines through the Process-Based Management Model and the Integrated Risk Management Model for the design of manual and automatic controls under criteria of adequate segregation of duties, adequate mitigation of related risks, considering the conditions of each process, changes in the same, and applicable regulations. Through policies and procedures documented in circulars and disclosed to all employees, roles, responsibilities, and details of the control activities that must be performed at the process level are established. Likewise, the units permanently update policies, standards, and procedures, reviewing and redefining controls to mitigate identified risks to acceptable levels.
     - Relevant general controls over Information Technology and controls for Cybersecurity risks have been designed. Guidelines have been established for the administration of roles and profiles in corporate applications, with general guidelines for user management, establishing, among other aspects, the creation of role and profile matrices for each application. The matrices are managed by the areas that own the corporate applications and are prepared jointly with the Information Security Department.
     - Other management systems have been incorporated into the Bank's control structure, such as the quality management systems applicable to several mission processes. Process-Based Management

and the Integrated Risk Management Model and its risk subsystems (financial, operational, information and cyber risk, money laundering and terrorist financing, compliance, environmental and third-party risk), as well as the Continuity Management System, allow the establishment of control activities that are monitored by the second line.
    - The Internal Control Department performs independent evaluations on the design and operation of controls in accordance with the annual plan of activities approved by the Audit Committee. Likewise, the Bank's Auditor General's Office evaluates the design and effectiveness of control activities.
    - **Weaknesses:** No weaknesses were identified.

- Level of compliance with the component presented in the previous report: **100%**
- Status of the component presented in the previous report:
    - **Strengths:** The Bank has established guidelines through the Process-Based Management Model and the Integrated Risk Management Model for the design of manual and automatic controls under criteria of adequate segregation of duties, adequate mitigation of related risks, considering the conditions of each process, changes in the same, and applicable regulations. Through policies and procedures documented in circulars and disclosed to all employees, roles, responsibilities, and details of the control activities that must be performed at the process level are established. Likewise, the units permanently update policies, standards, and procedures, reviewing and redefining controls to mitigate identified risks to acceptable levels.
    - Relevant general controls over Information Technology and controls for Cybersecurity risks have been designed. Guidelines have been established for the administration of roles and profiles in corporate applications, with general guidelines for user management, establishing, among other aspects, the creation of role and profile matrices for each application. The matrices are managed by the areas that own the corporate applications and are prepared jointly with the Information Security Department.
    - Other management systems have been incorporated into the Bank's control structure, such as the quality management systems applicable to several mission processes. Process-Based Management and the Integrated Risk Management Model and its risk subsystems (financial, operational, information and cyber risk, money laundering and terrorist financing, compliance, environmental and third-party risk), as well as the Continuity Management System, allow the establishment of control activities that are monitored by the second line.
    - The Internal Control Department performs independent evaluations on the design and operation of controls in accordance with the annual plan of activities approved by the Audit Committee.
    - **Weaknesses:** No weaknesses were identified.

- Final component progress: **0%**

4. Component: Information and communication
    - Is the component present and working? Yes
    - Level of compliance with the component: **100%**
    - Current status: Explanation of weaknesses and/or strengths:
        - **Strengths:***Banco de la República* (the Central Bank of Colombia) has internal communication policies, which establish its governance framework, and define the roles, responsibilities, and procedures related to requests for communication campaigns. The Bank has different mechanisms through which it develops the principle of citizen participation so that citizens may exercise social control and evaluation. The Sistema de Atención al Ciudadano, SAC (Citizen Services System) is a mechanism that, in addition to the channels, establishes the policies of interaction with citizens, continuous improvement, transparency, timely management, streamlining of procedures, and institutional collaboration for the management of rights to petition submitted by citizens (PQR:

petitions, requests for information, inquiries, complaints/claims, and reports), as well as for reports of acts of corruption by users, suppliers, contractors, employees and, in general, any citizen.

- The Bank completed the implementation of the "new citizen services system" for the assistance and relationship with citizens, supported by a technological solution in the cloud and an integral solution under a CRM (Customer Relationship Manager) type tool that facilitates and improves the management of petitions, requests for information, complaints, and claims, suggestions (PQR), compliments, and complaints, according to the requirements identified with the areas, current regulations, and best practices, as well as for the control and monitoring of the management of PQR and complaints in terms and traceability. This led to the updating of internal procedures and guidelines in this area.
- The Bank has designed policies and procedures related to Public Information Management Tools that develop, among others, the roles and responsibilities in the publication and disclosure of public information on the Bank's website and in the State's information systems, the guidelines for the publication of information on the Bank's website, and the procedure for updating the Information Management Tools, all in accordance with the Transparency Law and the provisions of the Colombian Ministry of ICT (Mintic). It classifies this information as available public information or confidential or classified public information. Within the management instruments, there is a Document Management Program (PGD in Spanish), the Index of Classified and Confidential Information (IICR in Spanish), the Registry of Information Assets (RAI in Spanish), and the Information Publication Scheme (EPI in Spanish).
- There is an inventory of the minimum public information required by transparency standards. The Bank has established policies and procedures related to roles and responsibilities for the fulfillment of its obligations regarding the collection, storage, use, circulation, and deletion of personal data contained in databases, as well as the security measures applicable to the treatment of databases containing personal data, in particular with the handling of information security incidents to protect confidential and classified information. The Code of Conduct establishes guidelines on the protection of the Bank's sensitive information by employees. The Bank also has defined policies and procedures on information security and cybersecurity, aimed at protecting the Bank's strategic assets that depend on or use information and communication technologies. Control activities are carried out on the integrity, confidentiality, and availability of data and information defined as relevant.
- The Bank develops and implements technical controls that facilitate the management of information and internal and external communication in a secure manner, supported by technological tools. Employees responsible for the creation and publication of internal and external communications must ensure compliance with the Policies for: i) Internal Communication and ii) Editorial Portals and Disclosure Media; which include a governance framework and iii) the criteria established in the Handbook of Usability and Accessibility Standards of the Institutional Site , such as: Classification or confidentiality, compliance with obligations and rights of third parties, blackout period, restricted use, copyright, text attributes of publications, and gender-inclusive language. There are guidelines on those responsible for authorizing the publication of content in social networks and other means of dissemination by the Bank's areas. The Bank has guidelines on spaces for communication with the public to disseminate the institution's messages using social networks: Facebook (Banco de la República) and Twitter (@BancoRepublica), @banrepcultural, @MuseoBanRep, @ConciertosBR). Likewise, it has a disclosure and communications plan that seeks to define an effective communication strategy in order to achieve the understanding and internalization of the strategic plan by employees, applying the Internal Communication Policy and the Editorial Policy for Portals and Disclosure Media.
- The Bank has strengthened the guidelines for the governance of portals and digital media, seeking to develop activities that achieve a more user-friendly, accessible, and usable portal, with an intuitive navigation, and easy to search. In addition, the internal guidelines on active transparency were

updated: publication and disclosure of public information and information management tools. The information management processes were strengthened by updating the Document Management Manual regarding the conservation of the Bank's documents.
    - In the first half of 2023, the Bank updated the general guidelines that must be complied with to publish and disclose public information through portals and disclosure media, in order to disseminate information related to the Bank's mission activity and services. It also defined and communicated the roles, responsibilities, and requirements for creating, updating, and deleting contents in the portals and disclosure media.
    - **Weaknesses:** No weaknesses were identified.

- Level of compliance with the component presented in the previous report: **100%**
- Status of the component presented in the previous report:
    - **Strengths:** *Banco de la República* (the Central Bank of Colombia) has internal communication policies that establish its governance framework, and define the roles, responsibilities, and procedures related to requests for communication campaigns. The Bank has different mechanisms through which it develops the principle of citizen participation so that citizens may exercise social control and evaluation. The *Sistema de Atención al Ciudadano*, SAC (Citizen Services System) is a mechanism that, in addition to the channels, establishes the policies of interaction with citizens, continuous improvement, transparency, timely management, streamlining of procedures, and institutional collaboration for the management of rights to petition submitted by citizens (PQR) (petitions, requests for information, inquiries, complaints/claims, and reports), as well as for reports of acts of corruption by users, suppliers, contractors, employees and, in general, any citizen.
    - During the second half of 2022, the Bank completed the implementation of the "new citizen services system" for the assistance and relationship with citizens, supported by a technological solution in the cloud and an integral solution under a CRM (Customer Relationship Manager) type tool that facilitates and improves the management of petitions, requests for information, complaints, and claims, suggestions (PQR), compliments and complaints, according to the requirements identified with the areas, current regulations, and best practices, as well as for the control and monitoring of the management of PQR and complaints in terms and traceability. This led to the updating of internal procedures and guidelines in this area.
    - The Bank has designed policies and procedures related to Public Information Management Tools that develop, among others, the roles and responsibilities in the publication and disclosure of public information on the Bank's website and in the State's information systems, the guidelines for the publication of information on the Bank's website, and the procedure for updating the Information Management Tools, all in accordance with the Transparency Law and the provisions of the Colombian Ministry of ICT (Mintic). It classifies this information as available public information or confidential or classified public information. Within the management instruments, there is a Document Management Program (PGD), the Index of Classified and Confidential Information (IICR), the Registry of Information Assets (RAI), and the Information Publication Scheme (EPI).
    - There is an inventory of the minimum public information required by transparency standards. The Bank has established policies and procedures related to roles and responsibilities for the fulfillment of its obligations regarding the collection, storage, use, circulation, and deletion of personal data contained in databases, as well as the security measures applicable to the treatment of databases containing personal data, in particular with the handling of information security incidents to protect confidential and classified information. The Code of Conduct establishes guidelines on the protection of the Bank's sensitive information by employees.
    - The Bank also has defined policies and procedures on information security and cybersecurity, aimed at protecting the Bank's strategic assets that depend on or use information and communication technologies. Control activities are carried out on the integrity, confidentiality, and availability of

data and information defined as relevant. The Bank develops and implements technical controls that facilitate the management of information and internal and external communication in a secure manner, supported by technological tools.
    - Employees responsible for the creation and publication of internal and external communications must ensure compliance with the Policies for: i) Internal Communication and ii) Editorial Portals and Disclosure Media; which include a governance framework and iii) the criteria established in the Manual of Usability and Accessibility Standards of the Corporate Portal; such as: Classification or confidentiality, compliance with obligations and rights of third parties, blackout period, restricted use, copyright, text attributes of publications, and gender-inclusive language. There are guidelines on those responsible for authorizing the publication of content in social networks and other means of dissemination by the Bank's areas. The Bank has guidelines on spaces for communication with the public to disseminate the institution's messages using social networks: Facebook (*Banco de la República*) and Twitter (@BancoRepublica), @banrepcultural, @MuseoBanRep, @ConciertosBR). Likewise, it has a disclosure and communications plan that seeks to define an effective communication strategy in order to achieve the understanding and internalization of the strategic plan by employees, applying the Internal Communication Policy and the Editorial Policy for Portals and Disclosure Media.
    - In the second half of 2022, the guidelines for the governance of portals and digital media were strengthened, seeking to develop activities that achieve a more user-friendly, accessible, and usable portal, with an intuitive navigation, and easy to search. In addition, the internal guidelines on active transparency were updated: publication and disclosure of public information and information management tools. The information management processes were strengthened by updating the Document Management Manual regarding the conservation of the Bank's documents.
    - **Weaknesses:** No weaknesses were identified.

- Final component progress: **0%**

5. Component: Monitoring
    - Is the component present and working? Yes
    - Level of compliance with the component: **100%**
    - Current status: Explanation of weaknesses and/or strengths:
        - **Strengths:** The Bank's internal control system is monitored by governance bodies such as the Audit Committee and the institutional Committee for Internal Control Coordination. Periodic independent evaluations are carried out by the Internal Control Department, the Auditor General’s Office, and an external auditing firm whose scope is the financial audit. As a result of these evaluations and in the event of identified deviations, improvement plans are established with the appropriate hierarchical levels to mitigate risks.
        - The results of the evaluations, as well as the follow-up of compliance with the improvement plans, are reported to the Audit Committee and the Institutional Committee for Internal Control Coordination, where their impact on the Bank's internal control system is reviewed. Reports from external oversight, supervision, and control bodies are also considered and, when applicable, in the event of possible observations in these reports, improvement measures are implemented and followed up.
        - The Audit Committee annually approves the Internal Control Department's work plan and periodically supervises its implementation during the year. The Institutional Committee for Internal Control Coordination evaluates the functioning of the Internal Control System and follows up on the commitments made by management.
        - The Risk Committee approves the policies of the Integrated Risk Management System (IRMS), defines the risk appetite, tolerance, and exposure limits, approves the methodologies that support the IRMS, and periodically follows up on the status of the Integrated Risk Management System

implemented by the Bank, which has been strengthened and is considered a fundamental pillar to support strategic and operational decision-making. Risk monitoring is performed periodically by the aforementioned Committee through second line risk reports. See the "risk assessment" component.
    - In the first half of 2023, the Bank has maintained and strengthened its internal control system monitoring scheme. The monitoring performed by the second line has been significantly strengthened. The third line has been strengthening its internal control system monitoring function by applying the risk-based approach considered in its annual work planning approved by the Audit Committee. The Audit Committee and the Institutional Committee for Internal Control Coordination continue to supervise and monitor the Bank's control scheme in accordance with their Bylaws.
    - **Weaknesses:** No weaknesses were identified.

- Level of compliance with the component presented in the previous report: **100%**
- Status of the component presented in the previous report:
    - **Strengths:** The Bank's internal control system is monitored by governance bodies such as the Audit Committee and the institutional Committee for Internal Control Coordination. Periodic independent evaluations are carried out by the Internal Control Department, the Auditor General’s Office, and an external auditing firm whose scope is the financial audit. As a result of these evaluations and in the event of identified deviations, improvement plans are established with the appropriate hierarchical levels to mitigate risks. The results of the evaluations, as well as the follow-up of compliance with the improvement plans, are reported to the Audit Committee and the Institutional Committee for Internal Control Coordination, where their impact on the Bank's internal control system is reviewed. Reports from external oversight, supervision, and control bodies are also considered and, when applicable, in the event of possible observations in these reports, improvement measures are implemented and followed up.
    - The Audit Committee annually approves the Internal Control Department's work plan and periodically supervises its implementation during the year. The Institutional Committee for Internal Control Coordination evaluates the functioning of the Internal Control System and follows up on the commitments made by management.
    - The Risk Committee approves the policies of the Integrated Risk Management System (IRMS), defines the risk appetite, tolerance, and exposure limits, approves the methodologies that support the IRMS, and periodically follows up on the status of the Integrated Risk Management System implemented by the Bank, which has been strengthened and is considered a fundamental pillar to support strategic and operational decision-making. Risk monitoring is performed periodically by the aforementioned Committee through second line risk reports. See the "risk assessment" component.
    - In the second half of 2022, the Bank has maintained and strengthened its internal control system monitoring scheme. The monitoring performed by the second line has been significantly strengthened. The third line has been strengthening its internal control system monitoring function by applying the risk-based approach considered in its annual work planning approved by the Audit Committee.
    - **Debilidades:** No se identificaron debilidades

- Final component progress: **0%**

Fuente: https://d1b4gd4m8561gs.cloudfront.net/en/transparency/internal-control-system-report/first-half-2023