

## **Specific Policy to Prevent and Combat Money Laundering, the Financing of Terrorism, Financing of the Proliferation of Weapons of Mass Destruction and Corruption**

1. Area responsible for the matter: Institutional Security Unit – USI.
2. Regulation: Law 9.613/1998, Law 12.846/2013, Law 13.260/2016, Law 13.810/2019, CMN Resolution 4.557/2017, BCB Circular Letter 3.978/2020, CVM Resolution 50/2021, Susep Circular Letter 612/2020, and BCB Resolution 44/2020 are relevant regulations.
3. Review frequency: at least annually, or extraordinarily, at any time.
4. Introduction and Concept:
  - 4.1. This Policy guides the behavior of Banco do Brasil. Entities Related to Banco do Brasil (ELBB) are expected to define their directions based on these guidelines, considering the specific needs and the legal and regulatory aspects applicable to them. This policy guides Banco do Brasil's actions with respect to preventing and combating money laundering, the financing of terrorism, financing of the proliferation of weapons of mass destruction and corruption and is part of the list of policies associated with operational risk management at Banco do Brasil. The criteria, requirements, standards, and procedures arising from this Policy are defined in internal normative instructions (IN).
  - 4.2. For the purposes of this Policy, we consider the following definitions:
    - 4.2.1. Senior Management: According to Article 11 of Banco do Brasil's Bylaws (ESBB), the management bodies of Banco do Brasil include the Board of Directors and the Executive Board. The latter comprises the Steering Board and other officers, as specified in Article 24 of the ESBB.
    - 4.2.2. Money laundering: concealing or disguising the nature, origin, location, disposition, movement or ownership of assets, rights or amounts arising directly or indirectly from a criminal offense.
    - 4.2.3. Financing of terrorism: allocation of funds to terrorists, terrorist organizations or terrorist acts. Funds can be sourced legally or illegally.
    - 4.2.4. Corruption: harmful acts committed by legal entities against the domestic or foreign public administration, that threaten domestic or foreign public assets; against the principles of public administration; or against international commitments assumed by Brazil, defined by Law 12.846/2013 as: promising, offering or giving, directly or

indirectly, an undue advantage to a public official, or to a person related thereto; demonstrably financing, funding, sponsoring or, in any way, subsidizing the practice of the unlawful acts foreseen in the Law; demonstrably using an intermediary individual or legal entity to hide or conceal the real interests or the identity of the beneficiaries of the acts practiced; frustrate or defraud, through adjustment, combination or any other act, of the competitive nature of a public bidding procedure; preventing, disturbing or defrauding the performance of any act of a public bidding procedure; removing or seeking to remove a bidder through fraud or offering of an advantage of any kind; defrauding a public bidding process or a contract arising therefrom; fraudulently or irregularly creating a legal entity to participate in a public bidding process or enter into an administrative agreement; fraudulently obtaining undue advantage or benefit from modifications or extensions of agreement entered into with the public administration, without authorization in the law, in the bid invitation notice or in the respective contractual instruments; or manipulating or defrauding the economic-financial balance of agreements entered into with the public administration; hindering the investigation or inspection activities of public bodies, entities or agents, or intervening in their activities, including in the scope of the regulatory agencies and the inspection bodies of the national financial system.

- 4.2.5. Bribery: an illicit act that consists of inducing someone to perform a certain act in exchange for money, material goods, or other private benefits.
- 4.2.6. Facilitation payment: refers to the payment of small amounts of money or promises of other benefits for the personal benefit of a public official, most often at a low hierarchical level, for the purpose of accelerating a given process. It differs from bribery in that the process in question would be done anyway but would take longer than desired.
- 4.2.7. Financing of the proliferation of weapons of mass destruction: consists of the direct or indirect provision of funds, by any means, for the purpose of providing financial support, supply, or collection of funds intended for use in the proliferation of weapons of mass destruction. Weapons of mass destruction are defined as devices capable of causing intentional damage on a large scale, such as nuclear, chemical, biological, or toxin weapons.

## 5. Statements:

- 5.1. We repudiate and do not tolerate acts of corruption, bribery, extortion, kickbacks, fraud, money laundering, terrorism financing, financing of the proliferation of weapons of mass destruction and any other unlawful practices.
- 5.2. We do not authorize any kind of facilitation payment.



- 5.3. We prevent money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption practices in doing business in Brazil and abroad, in accordance with the national legislation, with the legislation in force in each country where we operate, and with the legislation of transnational scope.
- 5.4. We operate in line with the international commitments assumed by the Brazilian Federal Government with regard to preventing and combating money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption, in compliance with the legislation in force.
- 5.5. We encourage and participate in joint actions, within the scope of the National Financial System, to prevent and combat money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption.
- 5.6. We adopt procedures in the relationship with public entities, to inhibit the practice of acts of corruption.
- 5.7. We adopt practices and controls to prevent and combat money laundering and the financing of terrorism in line with the Wolfsberg Group's principles for correspondent banking.
- 5.8. We use parameters established by law for registering transactions and identifying those considered indications of money laundering, terrorism financing or financing of the proliferation of weapons of mass destruction, in the development of automated systems for monitoring transactions performed.
- 5.9. We use specific parameters for monitoring financial transactions that may be indications of corruption.
- 5.10. We keep records related to the procedures of preventing and combating money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption in compliance with the legislation in force.
- 5.11. We adopt procedures in the development of products and services to inhibit their use for unlawful practices related to money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption.
- 5.12. We conduct internal risk assessment to identify and measure the risk of using our products and services for money laundering, the financing of terrorism, the financing the proliferation of weapons of mass destruction and corruption, considering the risk profiles of: customers; Banco do Brasil, including the business model and the geographical area of operation; operations, transactions, products and services, covering all distribution channels and the use of new technologies; and the activities performed by employees, partner institutions, suppliers and bank correspondents.
- 5.13. We do not accept the movement of funds through anonymous current

accounts or those linked to fictitious holders.

- 5.14. In analyzing the operations, we assess the instruments used, the way they are performed, the frequency, the parties and amounts involved, the customer's financial capacity and economic activity, and any indication of irregularity or illegality involving the customer or its operations, for the purpose of detecting signs of money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction or corruption.
- 5.15. We condition the initiation and maintenance of business relationships with customers who are Politically Exposed Persons on the authorization of senior management.
- 5.16. We adopt due diligence procedures to mitigate the risks of money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption, according to the activity, jurisdiction and agents involved.
- 5.17. We adopt restrictive measures regarding doing business and maintaining business relationships with customers, suppliers and partners when circumstances reveal evidence of involvement in acts related to money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction or corruption, in compliance with the legislation in force.
- 5.18. We condition the maintenance of correspondence relations with other banks to the existence, in the scope of those banks, of mechanisms for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, and contracting to the inexistence of an administrative or judicial conviction in the sanctions of Law 12.846, dated 08/01/2013.
- 5.19. When maintaining business relationships with partners and suppliers, we consider the existence, within the scope of these third parties, of mechanisms to prevent corruption.
- 5.20. We have adopted procedures to monitor the process of preventing and combating money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction by senior management, ensuring their commitment to the effectiveness and continuous improvement of the policy, procedures and internal controls required, as defined in our internal procedures and institutional roles and responsibilities.
- 5.21. We exchange information between control areas to comply with regulatory obligations, adhering to the guidelines established by the Information and Cybersecurity Policy.
- 5.22. We maintain specific channels for receiving complaints, including anonymous ones.
- 5.23. We investigate indications and accusations of acts of corruption practiced



- by direct agents or third parties, for the benefit or interest of the Bank, against the public administration, in accordance with the legislation in force.
- 5.24. We investigate indications and accusations of acts of corruption practiced by direct agents or third parties, against the assets, principles and commitments undertaken by the Bank, in accordance with the legislation in force.
- 5.25. We conduct, in a confidential manner, the registration, analysis and communication processes of financial operations with signs of money laundering, the financing of terrorism or the financing of the proliferation of weapons of mass destruction to the competent authorities, including in relation to customers, as well as the processes related to the investigation of suspected acts of corruption.
- 5.26. We preserve the identity of the whistleblowers as anonymous.
- 5.27. We repudiate any acts of reprisal or retaliation against good-faith whistleblowers who choose to identify themselves.
- 5.28. We adopt measures to protect good-faith whistleblowing employees in relation to facts arising from their reports.
- 5.29. We notify the competent authorities regarding operations or proposed operations that, in the form of the current legislation, characterize signs of money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption.
- 5.30. We collaborate with the public authorities in investigations related to acts harmful to the public administration that result from our activities, in compliance with the legislation in force.
- 5.31. We adopt criteria for hiring and employee conduct, with a focus on preventing and combating money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption.
- 5.32. We request that our suppliers adopt criteria for hiring and monitoring employee conduct, with a focus on preventing and combating money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption.
- 5.33. We maintain a specific employee training program on preventing and combating money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and corruption.
- 5.34. We request that the bank correspondents who provide services to the Bank carry out training in preventing and combating money laundering and the financing of terrorism.
- 5.35. We do not maintain relationships or conduct financial transactions with designated entities or individuals. Additionally, we take timely and discreet steps to make the assets of natural and legal persons sanctioned by the United Nations Security Council unavailable.

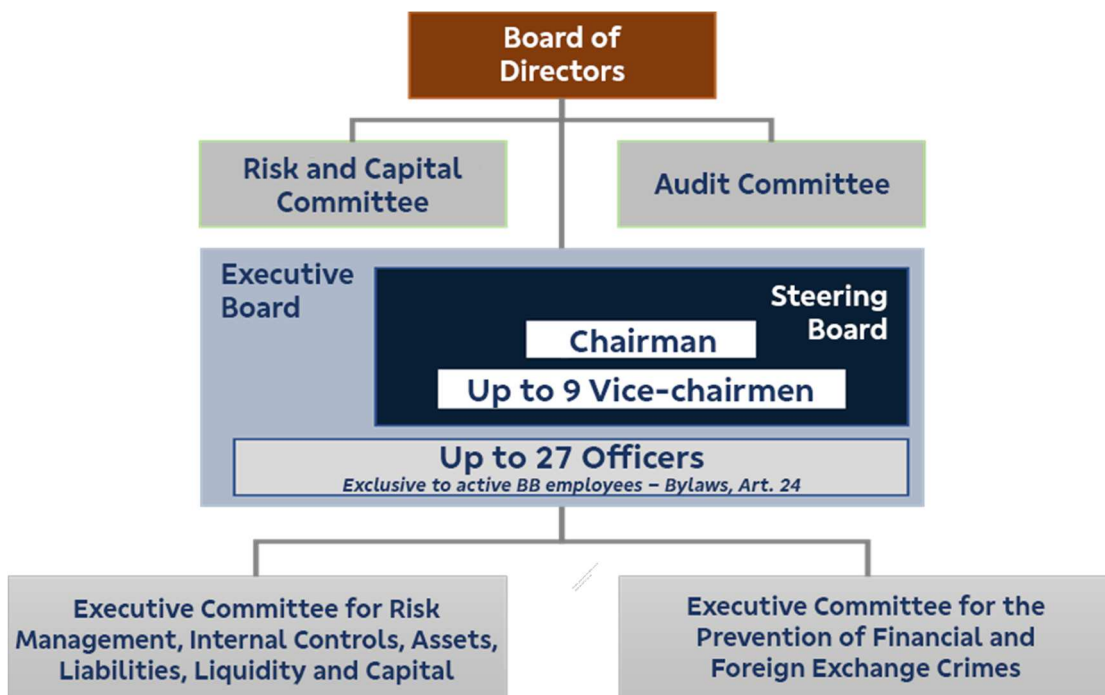


5.36. We submit the process of preventing and combating money laundering and the financing of terrorism, financing of the proliferation of weapons of mass destruction, and corruption to an independent auditing company on an annual basis.

Last review date: 04/10/2025.

## Roles and Responsibilities of Banco do Brasil’s AML/CFT Process

1. To comply with the Regulations, the roles and responsibilities of Banco do Brasil’s organizational agents are herein outlined
  - 1.1. This is simplified graphic representation of BB’s risk management and money laundering governance:



### 1.2. Board of Directors

- 1.2.1. The Board of Directors (BoD), an independent collegiate decision-making body, is formally established in Article 18 of BB’s Bylaws (“ESBB”). Its powers are described in Article 21 of the ESBB and Article 5 of its Internal Regulations.
- 1.2.2. The Board of Directors has strategic, guiding, elective, and supervisory duties, as provided by law and the Bylaws, and does not include operational or executive functions (Internal Regulations of the BoD, Article 3).
- 1.2.3. Regarding roles and responsibilities in the prevention of money laundering and risk management, the Board of Directors is responsible for approving BB’s Policies, including those related to the topics covered in this section.
- 1.2.4. Article 5, items XXIII to XXXIV of the Board of Directors’ Internal Regulations, establishes specific duties inherent to the risk management process.

### **1.3. Risk and Capital Committee**

- 1.3.1. According to Article 35 of the ESBB, the Risk and Capital Committee (Coris) is a collegiate body that reports to the Board of Directors. Its purpose is to advise the Board on matters related to risk and capital management.
- 1.3.2. Coris operates on a permanent basis, with prerogatives, attributions, and duties outlined in the applicable legislation and regulations. Its work is governed by its Internal Regulations.
- 1.3.3. Article 5 of Coris' Internal Regulations details the committee's duties regarding risk and capital management.

### **1.4. Audit Committee**

- 1.4.1. The Audit Committee (Coaud), established as an advisory body to the Board of Directors by Article 33 of BB's Bylaws, holds the responsibility of advising the BoD on its auditing and supervisory functions.
- 1.4.2. Coaud operates on a permanent basis, with its prerogatives, attributions, and duties outlined in the applicable legislation and regulations. In addition to those specified in the ESBB, its activities are governed by its Internal Regulations.
- 1.4.3. Article 5 of Coaud's Internal Regulations details the committee's duties concerning its auditing and supervisory functions.

### **1.5. Executive Board and Steering Board**

- 1.5.1. The Executive Board of BB comprises both the Steering Board and other Executive Officers, as stipulated in Article 24 of the ESBB.
- 1.5.2. The Steering Board (SB) is a fundamental component of BB's corporate governance structure, formally established in the ESBB. It is an integral part of the Executive Board and consists of the Chairman and Vice-chairmen (ESBB, Article 24, Paragraph 11).
- 1.5.3. As outlined in Article 29 of the ESBB, among its various responsibilities, the Steering Board is tasked with enforcing BB's Policies, including those pertaining to money laundering prevention and risk management. Additionally, it holds the authority to decide on the establishment, dissolution, and operation of committees within the Executive Board.
- 1.5.4. Article 7 of SB's Internal Regulations of the Board of Directors delineates specific powers for the Vice-Chairman of Internal Controls and Risk Management.

## **1.6. Executive Committee for Risk Management, Internal Controls, Assets, Liabilities, Liquidity and Capital – CEGRC**

1.6.1. CEGRC operates as a committee reporting directly to the Steering Board. Its membership comprises Vice-chairmen, and its primary purpose is to provide advisory support to the board concerning Risk Management, Internal Controls, Assets, Liabilities, Liquidity, and Capital-related matters.

## **1.7. Executive Committee for the Prevention of Financial and Foreign Exchange Crimes – CEPI**

1.7.1. CEPI is a committee under the steering Board, consisting of members of the Executive Board. Its purpose is to advise the board on matters related to the prevention of financial and foreign exchange violations.

## **1.8. Institutional Security Unit**

1.8.1. The Unit's specific responsibilities include:

- 1.8.1.1. Identifying rules and regulations applicable to prevent and combat money laundering, terrorism financing, financing of the proliferation of weapons of mass destructions, and corruption;
- 1.8.1.2. Developing and proposing the Specific Policy for Preventing and Combating Money Laundering, Terrorism Financing, Financing of the Proliferation of Weapons of Mass Destructions, and Corruption, along with the necessary instruments and actions for identifying, controlling, mitigating, and monitoring these activities;
- 1.8.1.3. Creating strategies, standards, norms, procedures, and performance indicators related to preventing and combating money laundering, terrorism financing, financing of the proliferation of weapons of mass destructions, and corruption;
- 1.8.1.4. Classifying clients by their risk level regarding ML/CFT;
- 1.8.1.5. Conducting prior analysis of new products, services, and technologies to mitigate ML/CFT risks;
- 1.8.1.6. Continuously monitoring Banco do Brasil's client base to identify individuals on the United Nations Security Council (UNSC) lists;
- 1.8.1.7. Ensuring compliance with UNSC sanctioning resolutions;
- 1.8.1.8. Monitoring adherence to the strategies, standards, norms, and procedures for preventing and combating money laundering, terrorism financing, financing of the proliferation of weapons of mass destructions, and corruption;

- 1.8.1.9. Controlling the accuracy of the system parameters for monitoring financial transactions that might indicate money laundering, terrorism financing, or financing of the proliferation of weapons of mass destructions;
- 1.8.1.10. Evaluating the effectiveness of the policies, strategies, standards, norms, procedures, instruments, and actions developed for preventing and combating money laundering, terrorism financing, financing of the proliferation of weapons of mass destructions, and corruption;
- 1.8.1.11. Preparing Banco do Brasil's Internal Risk Assessment for Money Laundering, Terrorism Financing, Financing of the Proliferation of Weapons of Mass Destructions, and Corruption;
- 1.8.1.12. Analyzing and reporting any detected or proposed operations that may indicate money laundering or terrorism financing to the relevant regulatory bodies;
- 1.8.1.13. Reporting to the Securities and Exchange Commission (CVM), if applicable, the non-occurrence of such operations or situations in the previous calendar year;
- 1.8.1.14. Developing guidelines for Related Entities (ELBB) regarding the prevention and combat of money laundering, terrorism financing, financing of the proliferation of weapons of mass destructions, and corruption.

## **1.9. Internal Controls Board**

- 1.9.1. Responsible for regulating and supervising the Internal Controls and Compliance System;
- 1.9.2. Compliance Risk Manager, as established in the Line of Defense Framework;
- 1.9.3. Responsible for preparing the Report on the Evaluation of the Effectiveness of the AML/CFT Policy, Procedures and Internal Controls and the Verification of the Internal Risk Assessment in ML/CFT of Banco do Brasil;
- 1.9.4. Responsible for the Follow-up Report on the AML/CFT Action Plan aimed at resolving the flaws identified in the Report on the Evaluation of the Effectiveness of the AML/CFT Policy, Procedures and Internal Controls and the Verification of the Internal Risk Assessment in ML/CFT of Banco do Brasil.

**1.10. Credit Board**

- 1.10.1. Responsible for the Specific Client Identification Policy and the process of identifying and registering Banco do Brasil clients;
- 1.10.2. Manager of the client registration information system, including the BB client registration database and the registration notes database;
- 1.10.3. Standardizer of the rules and procedures for collecting, verifying, validating, and updating client registration information;
- 1.10.4. Monitors the quality of the databases and the data sent to external bodies.

**1.11. Fundraising and Investments Unit**

- 1.11.1. Coordinates processes related to suitability and oversees the investor registration process.

**1.12. Risk Management Board**

- 1.12.1. Responsible for identifying risks associated with Banco do Brasil's businesses and processes;
- 1.12.2. Develops models, methodologies, processes, standards, procedures, and instruments to ensure Banco do Brasil's alignment with banking regulations;
- 1.12.3. Security Risk Manager, as established in the Lines of Defense Framework.

**1.13. Legal Board**

- 1.13.1. Responsible for providing legal advice on matters related to the requirements and regulations of standardizing, inspection, and control bodies within the scope of the AML/CFT process, as well as issues related to the management of Banco do Brasil's business and processes.

**1.14. Culture and People Management Board**

- 1.14.1. Responsible for managing ethics and disciplinary control, promoting organizational culture, overseeing corporate education, and handling the personnel admission process.

**1.15. Procurement, Infrastructure and Assets Board**

- 1.15.1. Responsible for prospecting, hiring, registering, managing relations, and supervising suppliers, as well as managing third-party risk.

**1.16. Physical and Digital Channel Service Unit**

1.16.1. Responsible for managing internal and third-party channels, as well as systematizing operational risk controls and hiring criteria for BB Correspondents.

**1.17. Holdings and Strategic Partnerships Unit**

1.17.1. Responsible for overseeing Banco do Brasil Related Entities (ELBB) governance and managing actuarial, contagion, and strategic risks within the BB Conglomerate framework.

**1.18. Digital Business Board**

1.18.1. Responsible for overseeing third-party risk management in partnerships related to the development of digital businesses.

**1.19. Internal Audit**

1.19.1. As the third line of defense entity, it is responsible for conducting independent activities based on a systematic and disciplined approach. Its purpose is to evaluate the processes established to mitigate the risk of Banco do Brasil's involvement in money laundering, terrorist financing, and corruption. Additionally, it aims to enhance the effectiveness of risk management, control, and governance processes.

**1.20. Strategic Units as a whole in their first-line defense responsibilities**

1.20.1. Responsible for preventing and combating the use of the Conglomerate's products and services for the practice of ML/CFT and encouraging the participation of its employees in training events on preventing and combating money laundering, terrorist financing, financing the proliferation of weapons of mass destructions and corruption.

**1.21. Business Units in the Country**

1.21.1. Responsible for managing customer relations, collecting and verifying documents for customer record preparation, and updating registration data within their scope of responsibility;

1.21.2. Responsible for providing information on the "Know Your Customer Principle" during the analysis of transactions or situations exhibiting atypicalities that may raise suspicions of ML/CFT.

**1.22. Business and Operations Support Services Center Brasília (Cenop Serviços BSB)**

- 1.22.1. Responsible for analyzing transactions or situations exhibiting atypicalities that may raise suspicions of ML/CFT.

**2. Documents prepared to comply with AML/CFT regulations****2.1. Specific Policy for Preventing and Combating Money Laundering, Terrorism Financing, Financing of The Proliferation of Weapons of Mass Destructions, and Corruption**

- 2.1.1. This document is a component of the Bank's Governance Structure, serving as a guide for the development of functions and behavioral standards within the institution.
- 2.1.2. Responsible Entity: Institutional Security Unit

**2.2. Banco do Brasil's Internal Risk Assessment for Money Laundering, Terrorism Financing, Financing of The Proliferation of Weapons of Mass Destructions, and Corruption**

- 2.2.1. This document outlines the methodology for identifying and quantifying the risk associated with the use of products and services in money laundering, terrorist financing, financing of the proliferation of weapons of mass destructions, and corruption. It encompasses various risk profiles, including those of BB's clients, the institution itself (including its business model and geographical area of operation), operations, transactions, products, services, distribution channels, use of new technologies, activities conducted by employees, as well as those of suppliers, partners, correspondents, and other institutions in relationship with BB.
- 2.2.2. Responsible Entity: Institutional Security Unit.

**2.3. Report on the Evaluation of the Effectiveness of the AML/CFT Policy, Procedures and Internal Controls and the Verification of the Internal Risk Assessment in ML/CFT**

- 2.3.1. This document has been prepared in alignment with the directives set forth in Bacen Circular Letter No. 3,978/2020 and CVM Resolution No. 50/2021.
- 2.3.2. Responsible Entity: Internal Controls Board

#### **2.4. Follow-up Report on the AML/CFT Action Plan regarding the flaws identified in the Report on the Evaluation of the Effectiveness of the AML/CFT Policy,**

##### **Procedures and Internal Controls and the Verification of the Internal Risk Assessment in ML/CFT**

- 2.4.1. This document has been prepared in alignment with the directives set forth in Bacen Circular Letter No. 3,978/2020.
- 2.4.2. Responsible Entity: Internal Controls Board.

#### **2.5. “Know Your Client” Guidebook**

- 2.5.1. This document serves as a comprehensive consolidation of rules and procedures established to prevent the Institution from being exploited for illicit or fraudulent activities, including money laundering, terrorist financing, financing of the proliferation of weapons of mass destructions, and corruption.
- 2.5.2. Responsible Entities: Institutional Security Unit and Credit Board.

#### **2.6. “Know Your Employee” Guidebook**

- 2.6.1. This document serves as a comprehensive consolidation of the standards and processes adopted by Banco do Brasil to ensure adequate knowledge about its employees. The primary purpose is to facilitate the identification of employees who may be involved in illicit or fraudulent practices, such as money laundering, terrorism financing, financing of the proliferation of weapons of mass destructions, and corruption. Ultimately, the protocol aims to prevent the bank from incurring potential image and reputational risks.
- 2.6.2. Responsible Entities: Institutional Security Unit and Culture and People Management Board.

#### **2.7. “Know Your Supplier” Guidebook**

- 2.7.1. This document sets out a comprehensive set of rules and processes designed to prevent the intentional or unintentional use of Banco do Brasil for illicit or fraudulent purposes, including money laundering, terrorist financing, financing of the proliferation of weapons of mass destructions, and corruption.
- 2.7.2. Responsible Entities: Institutional Security Unit and Procurement, Infrastructure and Assets Board