



MISSIONDAY:1985

HOLD

W

36000  
37500  
38500  
42000  
50000  
60000

CAM:A2

**CCB BRASIL**  
CONGLOMERATE'S  
**GUIDE OF BEST**  
**PRACTICES**

VISION:

ROTATION-BALANCE-SPEED  
CONNECTED

SUMMARY: ZONE:A

Anonymous

Guest:Code:M5w098da43001-2923k-32223-o98319

MISSIONDAY:1985

ONLINE · R

90-5-RPM

36-5-RPM

40-5-RPM

Anonymous:A

OPERATIONAL RISK CONTROL DATA PRIVACY UNLAWFUL ACT PREVENTION BUSINESS CONTINUITY MANAGEMENT COMPLIANCE

**CCB BRASIL CONGLOMERATE'S**

**GUIDE OF BEST PRACTICES**

COMPLIANCE ETHICAL VALUES INFORMATION SECURITY BUSINESS CONTINUITY MANAGEMENT SELF-REGULATION

## Summary

<b>1. Brief message from the Board of Directors</b> .....	04
CCB Brasil Conglomerate's values, Compliance, full adherence of the Institution to the Brazilian legislation and ways to protect and strengthen the compliance culture and the Bank's corporate image.	
<b>2. The importance of this document</b> .....	05
Legal determinations to financial institutions, contract obligations, sanctions, and responsibilities with the education of the internal public, clients, and suppliers / service providers.	
<b>3. How to use this guide</b> .....	06
Information contained herein, normative resolutions, form of availability and complementary documents.	
<b>4. Applicable legislation</b> .....	07
Compliance which must be ensured by everyone keeping a relationship with CCB	
<b>4.1 – Compliance at Conglomerate CCB Brasil</b>	
<b>4.2 – Data Privacy and Protection Program at Conglomerate CCB Brasil</b>	
<b>4.3 – Information Security at Conglomerate CCB Brasil</b>	
<b>4.4 – Risk Management at Conglomerate CCB Brasil</b>	
<b>4.5 – Business Continuity Management at Conglomerate CCB Brasil</b>	
<b>4.6 – Unlawful Act Prevention at Conglomerate CCB Brasil</b>	
<b>4.7 – Bank Self-Regulation at Conglomerate CCB Brasil</b>	
<b>5. Important links</b> .....	59
A direct link to some of the channels whose content is complementary to this guide.	
<b>6. Acronyms</b> .....	60
The meaning of acronyms included herein.	
<b>7. Glossary</b> .....	62
Definition of terms and more technical expressions to assist in fully understanding this guide.	

Transparency and responsibility:  
in practice, this is the **PRACTICE**.

## Brief message from the Board of Directors

1

CCB Brasil Conglomerate's Guide of Best Practices is a document that was prepared under the strictest norms of conduct and integrity and shall govern each and every relationship of the institution, both internally and externally.

It is oriented and developed from the values described in the Institution's Code of Ethics and Conduct, technical principles determined by its managers and extensive legislation, must be equally complied with by everyone on all levels of the Organization, without hierarchical distinction, as well as by all those who are connected to the Institution.

It is the duty of every employee to pass on the content presented herein to every supplier / service provider aiming at reducing the risks to all and providing a perfect division of responsibilities in compliance with the laws.

Full compliance leads to strengthening the corporate image, increasing the notion of sustainability, and perpetuating the business. Integrity, transparency, and respect to norms are essential for the balance in the work environment and relationship with suppliers / service providers, in addition to encouraging the creation of a virtuous circle of healthy habits, with positive repercussions inside and outside Conglomerate CCB Brasil.

**Conglomerate CCB Brasil Board of Directors**

## The importance of this document

2

The guidelines in this Guide of Best Practices aims at orienting CCB Brasil Conglomerate's stakeholders regarding the protection of their assets and awareness for the prevention, detection, and identification of occasional irregularities. The Compliance content presented herein is based on legal determinations and recommendations from Central Bank of Brazil and Febraban, among other institutions, and has its due legal support and protection.

It is important to highlight its consultive role as strategic support in managing resources and passing on the culture and values in CCB Brasil Conglomerate's mission and vision. In other words, Compliance goes beyond the fundamental idea of regulatory conformity in order to reach different governance aspects as a whole.

Legal or regulatory sanctions deriving from misuse of or noncompliance with the provisions and norms herein, such as image risks, reputational damage, or financial loss, are regarded as irreparable damages to the institution's material and non-material property. Thus, all employees, regardless of the position they hold, as well as those who have a relationship with the institution, are responsible for the full and effective compliance with this guide.



## How to use this guide

This document includes the most important normative resolutions that were released for ensuring responsible business conduct on every relationship level at Conglomerate CCB Brasil. They are essential for fully complying with internal and external regulations, thus preventing the risk of punitive administrative measures and legal or regulatory sanctions. Furthermore, the correct use of this guide creates certainty in the performance and growth of strategic values, thus safeguarding the Institution from reputational or financial losses.

For the purpose of facilitating access to the original volumes of the norms, the sources are indicated at the end of each chapter to dive deeper into the themes dealt with herein. The main document links are available at the end of the six chapters of this CCB Brasil Conglomerate's Guide of Best Practices.

It is worth pointing out that, in addition to fully reading this document, it is essential that every employee spread the conformity culture across every context of the Institution, including the external public, for the broad perception of ethical values in which Conglomerate CCB Brasil is grounded. Should any question regarding the terms used herein come up, there is a glossary at the end, so that no information escapes the reader.



## Applicable legislation

Find below, didactically and concisely sorted into six topic sets, the general lines of the current norms and legislations that are applicable to the respective internal provisions of Conglomerate CCB Brasil. **Read them carefully.**

- 4.1 Compliance at Conglomerate CCB Brasil
- 4.2 Data Privacy and Protection Program at Conglomerate CCB Brasil
- 4.3 Information Security at Conglomerate CCB Brasil
- 4.4 Risk Management at Conglomerate CCB Brasil
- 4.5 Business Continuity Management at Conglomerate CCB Brasil
- 4.6 Unlawful Act Prevention at Conglomerate CCB Brasil
- 4.7 Bank Self-regulation at Conglomerate CCB Brasil



# 4.1 Compliance at Conglomerate CCB BRASIL



*Compliance, corporate and internal control policies.*

## WHAT IS COMPLIANCE?

The compliance term comes from “to comply” in English and means “to be in conformity with”. It is the main principle of corporate governance and aims at neutralizing the so-called conformity risks, meaning those arising from noncompliance with the law, norms, guidelines (either national or international) or commitments made concerning the codes of self-regulation.

Executive Board of Conglomerate CCB Brasil is who establishes the internal Compliance structure, its implementation and maintenance, in addition to defining its guidelines and establishing its practices for the purpose of mitigating risks.

Conformity Governance must include the Board of Directors, Chief Executive Officer (CEO), Chief Risk Officer (CRO), Chief Compliance Officer (CCO) and the Risk and Compliance Executive Board and it is up to every employee at Conglomerate CCB Brasil, in addition to those who are connected to the institution, to be responsible for full and effective compliance.

## WHAT IS COMPLIANCE USED FOR?



In addition to the natural compliance with the law, Compliance is basically used for spreading and implementing the conformity culture throughout all areas of the Institution. Thus, this results in an example of conduct that every employee and others with whom the Institution is connected, particularly the top management, must support and establish its guidelines. Several other benefits arise from it, such as:

**VALUING** the awareness of the importance of this policy's guidelines by stakeholders, including employee, clients, partners, suppliers/service providers, governments and the society;

**PROMOTING** risk reduction on all business levels, from operational to strategic;

**APPROACHING** regulatory and supervisory agencies, trade associations, as well as independent and internal auditors;

**CONSTANTLY CORRECTING** items related to nonconformity with prompt fulfillment of and compliance with the law;

**ASSISTING** the Risk and Compliance Executive Board and the entire conformity structure in their assignments related to information and sharing the conformity culture;

**AIDING** the business areas with the awareness and observance of rules issued by external regulatory agencies and internal norms, while pointing out their impact.

## HOW DOES COMPLIANCE APPLY TO CONGLOMERATE CCB BRASIL?



The Conformity Policy formalizes the Conglomerate CCB Brazil Board of Directors' guidelines and establishes the internal Compliance structure, its implementation and maintenance. Its purpose is to seek adherence to measures aimed at achieving institutional goals with internal and external laws and regulations, as well as effectively providing the achievement of such goals.

By performing its roles, Compliance evaluates the regulations received, discloses them to the other possibly impacted divisions, conducts tests of adherence to legislations, self-regulations, and internal norms according to the methodology established and, whenever necessary, follows the action plans and schedules for remedying gaps.

In order to obtain full Compliance, Conglomerate CCB Brasil must provide the allocation of a sufficient number of personnel properly trained and with the necessary experience to perform the activities related to supervising conformity. To that end, the Board of Directors works toward:

**ASSURING** the management, effectiveness, communication and continuity of the conformity policies;

**MAKING SURE** that corrective measures will be promptly applied to correct identified faults;

**CONTINUOUSLY MONITORING** the regulatory environment and disclosing the norms applicable to the performance of areas responsible, meaning to manage the set of internal norms and providing information to employees, and all the others who are connected to the Institution, by widely disclosing them;

**ASSESSING** adherence to the Institution's regulations, and following the changes in the process manuals and other institutional policies referring to conformity while performing activities;

**PREPARING** a report at least on an annual basis containing the summary of the results of conformity-related activities, with their own main conclusions, recommendations and necessary measures, and submitting it to the Risk and Compliance Executive Board, Compliance Committee; to the Internal Audit Committee; and to the Executive Board Committee;

**SYSTEMATICALLY AND OPPORTUNELY COMMUNICATING** the results of conformity-related activities to the Board of Directors;

**INDEPENDENTLY AND AUTONOMOUSLY PERFORMING** with free access to the necessary information for carrying out their attributions.



## WHAT ARE THE EFFECTS OF COMPLIANCE?

Compliance with the regulations in force, as well as with conformity guidelines provided for in a specific policy and other internal norms of CCB Brasil Conglomerate, produces a perennial credibility and transparency effect that is essential for business development, and it must be monitored and supervised according to the Compliance Report, which is issued periodically.

Noncompliance may lead to serious punitive administrative measures, legal or regulatory sanctions, or even result in significant reputational or financial losses.

Law No. 13.506, from November 13th, 2017, which establishes the sanctioning administrative process within the sphere of action of Central Bank of Brazil and that of the Securities and Exchange Commission defines the following as INFRINGEMENT:

**CONDUCTING** in the National Financial System, Pre-purchase Financial Pool System and Brazilian Payment System unauthorized or prohibited operations, or those that are in disagreement with the authorization granted, principles provided for in legal norms and regulations that govern the activity authorized by Central Bank of Brazil;

**OBSTRUCTING** the inspections from Central Bank of Brazil;

**FAILING** to provide Central Bank of Brazil with documents, data or information, which are required to be delivered by legal or regulatory norms;

**PROVIDING** Central Bank of Brazil with incorrect documents, data and information or those that fail to agree with the deadlines and conditions established by legal or regulatory norms;

**ACTING** as the administrator of the Article of Incorporation of financial institutions, institutions supervised by Central Bank of Brazil and those that are part of the Brazilian Payment System (head provision of Article 2 of that Law) without previous approval from Central Bank of Brazil;

**FAILING** to adopt internal controls aiming at preserving the terms of confidentiality provided for in Complementary Law No. 105, from January 10th, 2001;

**NEGOTIATING** securities, financial instruments and other assets, or perform credit or lease-purchase operations at prices that do not match those practiced by the market, to their own detriment or that of third parties;

**SIMULATING** or structuring economically groundless operations aimed at providing or obtaining undue advantages for oneself or third parties;

**DIVERTING** resources of persons mentioned in the head provision of Article 2 of that Law or that of third parties;

**INSERTING** or keeping false or incorrect records or information in financial statements or audit reports of persons mentioned in the head provision of Article 2 of that Law;

**DISTRIBUTING** dividends, pay interest on the stockholder's equity or otherwise compensate shareholders, administrators or agency members provided for in the articles of incorporation or articles of organization of persons mentioned in the head provision of Article 2 of that Law based on results obtained from false or incorrect financial statements;

**FAILING** to diligently and prudently act in conducting the interests of persons mentioned in the head provision of Article 2 of that Law; failing to segregate the activities of persons mentioned in the head provision of Article 2 of that Law from other corporations, controlled companies and affiliated companies, in order to create or help create proprietary confusion; or failing to supervise the acts of administration agencies of persons mentioned in the head provision of Article 2 of that Law, when required to do so;

**FAILING TO COMPLY WITH** legal and regulatory norms of the National Financial System, Pre-purchase Financial Pool System and Brazilian Payment System, determinations of Central Bank of Brazil, as well as their respective deadlines that were adopted based on their competence;



Regarding the calculation of applicable penalties within the administrative scope, in cases of infringement, Resolution No. 131 from Central Bank of Brazil provides for the several parameters to be considered. They vary from the violator's economic capability to the reprehensibility and the duration of the irregular conduct, passing on the number of operations and the degree of damage or danger arising from the offenses.

In the dosimetry of penalties, fine, temporary disqualification, revocation or warning, there are levels according to the type of infraction, institution or activity involved. Some aggravating and mitigating factors, such as recurrence within a period of less than three years or willful misconduct, are also indicated in the norm.

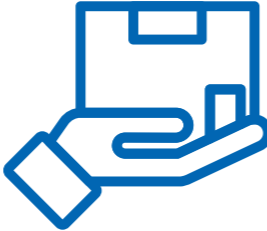
In addition to this, the law determines the values of combinatorial fines set according to the type and size of institutions authorized by BACEN.

We reinforce that, at Conglomerate CCB Brasil, every occasional noncompliance case is subject to infringement, punishment, coercive measures, and alternative solution means applicable to financial institutions, other institutions supervised by Central Bank of Brazil and to Brazilian Payment System members, without prejudice to the responsibilities of the Ethics Committee.

#### REFERENCES IN THIS CONTENT

Law No. 13.506, from November 13<sup>th</sup>, 2017; Resolution CMN No. 4.557, from February 23<sup>rd</sup>, 2017; Resolution CMN No. 4.595, from August 28<sup>th</sup>, 2017; Resolution BCB No. 131, from August 20<sup>th</sup>, 2021; Resolution CMN No. 4.968, from November 25<sup>th</sup>.





## 4.2 Data Privacy and Protection Program at Conglomerate CCB BRASIL

*Responsibility for handling confidential information.*

### WHAT IS DATA PRIVACY AND PROTECTION?

Privacy is provided for in the list of fundamental guarantees and rights, which are defined as constitutionally inviolable. Privacy is an information set about the individual, who can decide to keep it under their exclusive control or communicate the information, by deciding to whom, when, where and under what conditions. Legally, personal data privacy is defined by the LGPD, Lei n°13.709 [General Personal Data Protection Law], which consists of 65 Articles and has been in force in Brazil since 2020. It is a tool aimed at protecting users from damages caused by the breach of these rights or unauthorized use of their data.

The Data Privacy and Protection Program is a compulsory guideline for all the companies belonging to Conglomerate CCB Brasil. Full and effective compliance with that program falls onto administrators, employees, interns, and suppliers/service providers supporting the operation, the maintenance and/or storage of their information, whether they use the Institution's physical facilities and technological infrastructure or not.

Thus, websites, systems, physical or digital documents and cloud-based services, whether they are hosted inside or outside Conglomerate CCB Brasil, are subject to the Institution's control in every environment, whether electronically or manually, real, or virtual.

### WHAT IS THE DATA PRIVACY AND PROTECTION PROGRAM FOR?



The Data Privacy and Protection framework establishes guidelines, instructions, responsibilities, and good practices for creating effective data protection in the Institution. In order to mitigate the risks of personal data handling-related incidents, Conglomerate CCB Brasil acts in such a way so as to:

**PROTECT** the rights and freedom of individuals by guaranteeing the confidentiality of their personal data, and that this data be handled with the utmost seriousness, by requiring from suppliers/service providers the same diligence, discretion and prudence regarding the protection and privacy of information;

**HANDLE** only personal data that is necessary for fulfilling their daily activities, including personal data of employees, suppliers / service provider contracts and commercial partners, among others;

**UNDERSTAND** that personal data comprise the Organization's most precious assets and, thus, adopt permanent, pertinent measures aimed at providing full protection to this information;

**VALUE** the privacy and safety of data on clients, employees, visitors and websites, by handling it with the due respect and always in accordance with the CCB Brasil Conglomerate's Code of Ethics and Conduct and the General Data Protection Law;

**GUARANTEE** that personal information and data only be accessed by properly authorized and qualified personnel, and under no circumstance is it to be provided to, sold to, or shared with third parties without proper authorization for specific procedures, including by court decision, and Conglomerate CCB Brasil reserves the prerogative to destroy it after it is properly used.



**FAVOR** the reading, comprehension, compliance, and sharing of CCB Brasil Conglomerate's data protection policies to suppliers / service providers, commercial partners and any third party either directly or indirectly working with the Institution.

## HOW DOES THE DATA PRIVACY AND PROTECTION PROGRAM APPLY TO CONGLOMERATE CCB BRASIL?



With the creation of the Comitê de Privacidade e Proteção de Dados (CPPD) [Data Privacy and Protection Committee] and Grupo de Trabalho de Privacidade e Proteção de Dados (GTPPD) [Data Privacy and Protection Working Group], two specific scopes were defined for handling topics related to data privacy and protection at Conglomerate CCB Brasil. The Group answers to the Committee, which, in turn, answers to the Data Protection Officer (DPO), whose appointment and data are publicly disclosed. The managers in charge of departments and their respective processes must perform by:

**RESPECTING** the principles of transparency and good practices, in other words, by observing the privacy of holders regarding purpose, need, retention of data, and the appropriate minimization/ cryptography/ anonymization for the protection of the data holder's identity in the case of personal data incident;

**TAKING** the necessary measures for handling data with the best quality possible, by always seeking precision, clarity and relevance in updating the data for its respective purposes;

**KEEPING** records of data handling procedures according to its respective purposes, so that it is possible to guarantee personal data transparency to its holders;

**USING** technical and administrative security measures applicable according to preestablished internal procedures, as well as by adopting preventive measures to mitigate damages and incidents as a result of illegal or unauthorized handling;

**REFRAINING** from handling personal data for unlawful or abusive discriminatory purposes;

**FOLLOWING** the instructions in the specific guide on the topic and its procedures to record every new activity concerning the handling of personal data;

**COMMUNICATING** always how data is handled and, by means of privacy notices, advising who the agent in charge of handling the data is, the purpose for such handling, destination, whether there is shared data use and third parties they are shared with, and above all, about rights and how to exercise them;

**TAKING** proper measures to ensure maximum transparency on exceptional occasions, in which issuing a privacy notice is not possible, for instance, when there is no relation between the handling agent and the holder;

**REFERRING** the specific guide about the handling consent management topic according to each lawfully allowed situation, such as in cases of credit protection, contract performance, fulfillment of legal action, shared data use and health protection, among other hypotheses;

**CAREFULLY CONSIDERING** the so-called sensitive personal data, and only allowing it to be handled in required situations, such as: fulfillment of legal or regulatory obligation; regular exercise of the law (legal, administrative or arbitration processes); specific and clear consent from the holder for specific purposes; health care with procedures carried out by a health professional or health agencies; or holder's fraud and security prevention in electronic identification or registration authentication processes (situations of biometric data collection to access restricted physical locations, bank transactions carried out or confirmed, among others), always making sure that the handling process does not overlap the holder's fundamental rights and freedom;



**MAKING SURE** that apparently ordinary personal data proven to be sensitive, such as product and service consumption analysis, which may reveal or suggest identification by the type of shopping locations, political, religious, sexual preference, etc., be handled as sensitive data;

**HANDLING** data of children and teenagers with increased protection in relation to other personal data. This type of data is not usually handled by Conglomerate CCB Brasil, considering that the products and services they offer do not target this group. Such data can be handled in exceptional cases, in which specific consent from the holder's parents or legal guardians is required, except for cases in which handling is the legal basis for defense in legal, administrative or arbitration processes;

**PROVIDING** holders with the full right of access to their own personal data. Replies to such requests shall be given in a simplified and complete manner, and according to what is provided for by law, within fifteen (15) (fifteen) days from the holder's request, with the exception of commercial and industrial secrets. Furthermore, holders are fully entitled to rectify, cancel, forget, block, oppose their data, in addition to portability or anonymization of their data when overly or unlawfully processed. The holder also shall be entitled to request that their personal data be eliminated when the legal basis for handling comes from consent, except in the cases of retention provided for by law. The holder can also request the portability of their own personal data to another service provider or products upon express request, according to regulation from the Autoridade Nacional de Proteção de Dados (ANPD) [National Data Protection Authority] and regulatory agencies, except in the case of commercial and industrial secrets;

**ALLOWING** international transfer of their personal data in cases in which the level of protection is as appropriate as that of the General Personal Data Protection Law (LGPD) at the country of destination, with previous consultation with CPPD. Every international data transfer, as well as any other personal data handling procedure, must be recorded and submitted to a process of new handling activities defined by the communication guidelines. However, data transfer shall only be allowed if:

⦿ **the controller** offers and guarantees compliance with the principles, holder's rights and data protection regime provided for in the LGPD, by means of contract clauses or global corporate norms;

⦿ **the holder** has offered their specific and clear consent for the transfer, with previous information about the operation's international nature, by clearly distinguishing it from other purposes, according to the consent management guidelines in that policy;

⦿ **ANPD** authorizes the international transfer;

⦿ **the transfer** is necessary for protecting the data holder's or other people's (third parties) vital interests, should the data holder be physically or legally unable to give their own consent;

⦿ **the transfer** results from a commitment made in an international cooperation agreement;

**GUARANTEEING** that the personal data possessed by Conglomerate CCB Brasil is not provided to unauthorized third parties, including relatives or friends of their employees, private organizations and government agencies without the authorization from the Conglomerate, demand from a regulatory agency or court order for such purpose;

**REPORTING** to CPPD every time employees are requested to disclose personal data to third parties, including in the case of demand from a regulatory agency or court order. The participation of employees in specific training sessions that allow them to effectively handle that risk shall be compulsory. All the requests for the provision of data must be supported by extensive documentation and properly stored with the authorization from CPPD;

**MAKING IT COMPULSORY** for employees, partners and third parties to notify Conglomerate CCB Brasil in case of any alteration in the data handling procedure, in order to allow the records to be immediately updated, as per the specific guide on the topic. Conglomerate CCB Brasil is responsible for making sure that every notification about any alteration be recorded, received and properly forwarded to GTPPD;

**RECTIFYING** inaccurate and outdated personal data that has been shared with the Conglomerate, and, in the case of detection, informing the discrepancy in records sent to other departments and third parties, if necessary;

**PROPERLY MAPPING** personal data control and preparing reports according to the privacy norms of the specific guide on the topic;

**TECHNICALLY ASSESSING** the risks related to the impact of the Conglomerate's data handling procedure, by considering and analyzing the deliberations of the Legal and Compliance Department and the techniques in the Relatório de Impacto à Proteção de Dados (RIPD) [Data Protection Impact Report], as described in the specific risk guide, which includes safety, technical and administrative measures, according to the level of risk and respective prioritization;

**VISUALIZING** and considering data privacy and protection at every stage, from the creation to implementation of new products, processes, procedures and systems;

**UNDERSTANDING** this model as a monitoring process for new resources, and making sure that data privacy and protection be complied with throughout every activity created;

**IMMEDIATELY REPORTING** to GTPPD, the possible suspicion of violations and incidents related to handling personal data by Conglomerate CCB Brasil or contractors hired, always following the Incident Management communication channels and guidelines. The GTPPD shall analyze the need for communicating to the Incident Response Group, according to the criticality and complexity of the occurrence and the guidelines established in the Incident Response Policy, which is an integral part of CCB Brasil Conglomerate's documentation. The identification of noncompliance risks shall be reported to the CPPD immediately, so that an independent audit procedure can be requested;

**STORING** for the legal period of time the entire suspicious documentation aiming at internally recording and following occasional security incidents and, in case of urgent questions, directly hiring one of the GTPPD members;

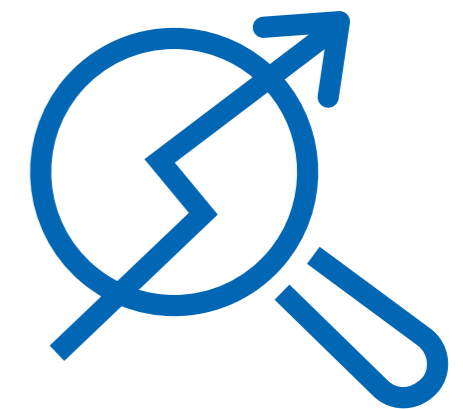
**SUPPORTING** the Privacy Incident Response Policy and taking all measures possible in order to minimize the impacts caused, aiming at recovering the integrity and confidentiality of personal data. To that end, privacy control action plans must be prepared, carried out and monitored;

**CONDUCTING** periodic audits and assessments aiming at guaranteeing that these and other policies related to data privacy and protection be complied with;

**PROVIDING** every employee with the tools for internal procedures and controls, systems, preventive measures, and department activities aiming at keeping the Conglomerate in conformity with norms and compliance with regulations related to personal data privacy and protection. In addition to disclosing information about the Conglomerate's guidelines on the most diverse topics to suppliers / service providers.

## WHAT ARE THE EFFECTS OF THE DATA PRIVACY AND PROTECTION PROGRAM?

The application of every data handling recommendation has a practical effect in preventing, reducing, and mitigating losses arising from information security incidents or privacy contract breaches. Such information admits no negligence since it can directly affect CCB Brasil Conglomerate's information assets. By avoiding it, the trust established among stakeholders is reinforced, reputational damages are eliminated, and the positive perception of the Institution is broadened.



### REFERENCES IN THIS CONTENT

Law No. 13.709/2018 — General Data Protection Law (LGPD).





## WHAT IS INFORMATION SECURITY?

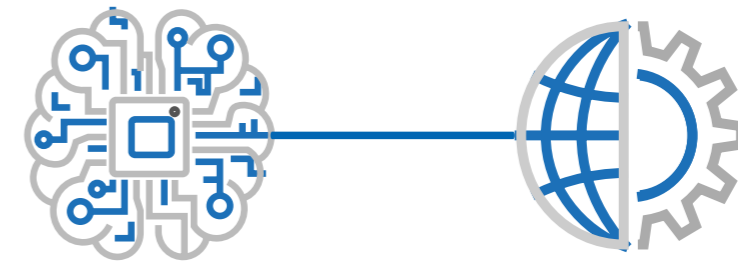
Information Security (InfoSec) is a large protection system of a vast set of information assets. Despite being directly linked to cybernetics and data storage, it has an even wider structure than that of a computational complex, and involves several assumptions and values, such as confidentiality, integrity, availability, authenticity, and legality.

Conglomerate CCB Brasil is responsible for defining and applying the internal policies involving Information Security, as well as for providing support to every asset related to it. Compliance with these norms, responsibility for its constant maintenance and continuous support to security are inherent to the daily jobs and tasks of every employee, third party and supplier / service provider, both internally and externally.

## WHAT IS INFORMATION SECURITY FOR?

Information Security at Conglomerate CCB Brasil aims at responsibly ensuring the confidentiality, availability, and integrity of the information to them entrusted by stakeholders and, in addition to employees, includes investors, third parties and other business partners.

InfoSec policies are applicable to every professional who uses the computer resources and data at Conglomerate CCB Brasil, and make sure that the entire operating system at the Institution is fully functional, thus making it possible to conduct conformity audits with contracts and verify the level of control in the environment in which the information system and personal data protection are entered.



## HOW IS INFORMATION SECURITY APPLIED AT CONGLOMERATE CCB BRASIL?

Information Security at Conglomerate CCB Brasil establishes controls in a way that no third party, supplier / service provider is able to access personal data kept by the Conglomerate without previously signing a data confidentiality agreement. These guidelines must be applied to every area, system, person, and process by the Information Security Division, which is responsible for the Information Security Management at Conglomerate CCB Brasil, and must act by:

**ENSURING** that Conglomerate CCB Brasil is ready in a way to prevent different types of fraud; establishing mechanisms to protect confidential information under their care; promoting the segregation of jobs related to operationalization, control and liquidation, to prevent occasional fraud or operational errors, as well as not allowing the use of privileged information for personal benefit or that of others;

**GUARANTEEING** that laws and norms regulating activities at Conglomerate CCB Brasil be complied with in order to gain adherence to the applicable legislation and regulations;

**PREVENTING** the occurrence of problems or difficulties that affect the security of information under the possession or responsibility of users, and ensuring the security of information generated or managed by the Company and used within any type of relationship scope, whether professional or personal, while observing contract and legal requirements and the organization's norms;

**ASSESSING** the legal requirements applicable to the information under the user's responsibility, as well as the relation between those norms and internal and external controls aimed at promoting adherence to them;

**SECURELY ADMINISTRATING** environments, information, information system assets, and media containing any information belonging to or under the care of Conglomerate CCB Brasil;

**GETTING TO KNOW** the Information Security system, aiming at preventing any type of fraudster from acting or anyone from falling victim to them;

**KEEPING** strict secrecy about each and every piece of information, particularly privileged information, and it is prohibited to use the information for personal gain or that of others;

**SUGGESTING** changes to processes, so that increased protection is brought to the information at Conglomerate CCB Brasil, and report practices that are in disagreement with the Information Security Policies at the Conglomerate, as well as with their Code of Ethics and Conduct or law in force;

**FULLY COMPLYING WITH** the norms contained in the Information Security Policies at Conglomerate CCB Brasil and ensuring that they always be respected, in addition to reporting irregular or suspicious situations to the Company;

**MAKING SURE** that users are aware of the threats that may adversely affect the security of information and orienting and supporting this policy by sharing the security culture. The Information Security Division shall provide training and general

awareness on the topic, so that employees and everyone Conglomerate CCB Brasil have a relationship which can implement and spread their bases according to their need and the specific content to the respective areas;

**MAKING SURE** that every measure is being taken in order to prevent any activity or situation that may expose Conglomerate CCB Brasil to financial, material or human losses, either directly or indirectly, or possible or real, that may compromise their business;

**PROTECTING** the corporate information against disclosure, alteration, exclusion, destruction, and access by unauthorized people, and never placing the information at Conglomerate CCB Brasil or information processes in any risk situation. Every employee and everyone Conglomerate CCB Brasil have a relationship with must sign a term that states their awareness and full adherence to the norms and procedures of CCB Brasil Conglomerate's Information Security Policies and Code of Ethics and Conduct, before they are granted access to any type of information;

**PRESERVING** and storing, within a period of time established by the Company or legislation in force, the information at Conglomerate CCB Brasil accessed only by means of resources dully authorized by the Conglomerate;

**SECURING** and protecting user accounts and their passwords from external access;

**PROMPTLY INVESTIGATING** any possible cause of security problem, incident or risk, and applying all the necessary measures to prevent or minimize damages;

**BEING ATTENTIVE** to keeping workstations monitored, equipped and programmed with log in and passwords for access (log on), with screen block and proper password request to restart, as well as automatic session ending when idle;

**MAPPING** the most critical risk processes, and, along with the person in charge of the process, identify specific security activities to be applied aimed at tightening security and guaranteeing the accuracy of the control and risk prevention activities in the business operations and infrastructure;

**KEEPING** a competent and prepared team to provide the Risk Management Process with an agile pace, by efficiently fighting the occurrence of cases of fraud in the environments at Conglomerate CCB Brasil;

**CONTROLLING** the electronic or physical transfer of information among Conglomerate CCB Brasil, third parties, and suppliers / service providers in a planned manner, in order to guarantee proper protection and storage. Those third parties, since they receive information from Conglomerate CCB Brasil, must

prove that they have policies and practices to ensure availability, integrity, and confidentiality, in addition to the ability to recover the information assets, so that they meet or exceed CCB Brasil Conglomerate's internal policies and practices. A written agreement must be signed as a guarantee of security, and contain clauses for protecting the information in transit against loss, disclosure, and damage that are applied according to the classification of the information, and the nature of the commercial relationship;

**ESTABLISHING** processes and procedures to respond to security breaches, abnormal or suspicious events and incidents aimed at minimizing damages to information assets, and allowing the identification and punishment of offenders, according to the Incident Response Policy. Such processes must be based on the level of risk and be formally documented. This documentation must contain detailed and properly organized instructions for an effective action to fight the causes. The procedures must at least include the identification of the incident source, indications of an intruder in the system, known security loopholes, service interruptions, etc. The post-incident analysis must contain the specifications of and notifications to the internal or external agent, according to the nature and category of the event or incident, so that proper corrective measures are applied;

**INSTALLING** detection and prevention mechanisms that are designed to protect Conglomerate CCB Brasil against malware and viruses. These controls must be included in every information-related asset at the company. Under no circumstance are users to attempt to personally eradicate or clean their workstation after malware-related incidents, and must promptly communicate any virus or malware threat detected on the network computer or related device;

**KEEPING** the conformity with software license agreements, and the acquisition or use of unauthorized software is expressly prohibited at Conglomerate CCB Brasil. Anti-virus software must be installed and configured on every computer, PC, laptop and other related mobile devices, in addition to the network server, electronic mail and internet server to sweep new or old infected files;

**ENSURING** that a communication channel be established, with uninterrupted service, efficiently and autonomously to serve and provide guidance in cases of incidents that may put the information at Conglomerate CCB Brasil, as well as their assets, at risk. Every security incident must be promptly communicated through this channel;

**SHARING** the information security incidents, after reporting them to the Information Security Division, with stakeholders and regulatory institutions. This also applies to incidents communicated by outsourced suppliers / service providers or subcontractors;

**SEPARATING** incompatible functions and responsibilities to minimize improper or unauthorized access to or use of information-related assets in the Company or their commercial processes. Accordingly, test development and production environments must be equally and strategically separated to minimize possible unauthorized changes to the production environment;

**GUARANTEERING** the periodic backup of information assets for the purpose of operation recovery and conformity with the business continuity recovery plans, and such backups must be retained according to commercial and regulatory requirements;

**PERIODICALLY TESTING** the media used for backup regarding its reliability and integrity. The procedures for fully recovering the information must be periodically verified regarding their efficacy and performance. Physical storage media for the backup of documents, data on consumers, clients, administrators, employees, third party information, media types, including electronic mail, must follow the internal information retention guidelines at Conglomerate CCB Brasil;

**PROVIDING** the proper space for creating and keeping information backups whenever necessary. Backups that remain at the location must be stored in environmentally protected physical areas, based on handling requirements defined in the information classification;

**PROVIDING** a proper system to make sure that every standard network equipment password be changed at the time of installation. Conglomerate CCB Brasil is also responsible for providing their equipment with an adequate system to manage access and system passwords, while observing requirements of password complexity, minimum size, and history;

**PROVIDING** all users of the Information Services from Conglomerate CCB Brasil with a unique ID for authentication and the assignment of individual responsibilities. Documented authorization is required so that the user ID is issued;

**MANAGING** system access privileges by following a formal process during the life cycle, from registration to revocation. User profiles must be established in order to line up accesses according to specific needs for the performance of their respective jobs;

**RESTRICTING** administrative access to system resources or similar privileges solely to personnel performing system maintenance services or personnel with related administrative jobs. Privileged access must be solely used for system administrative tasks;

**LINING UP** apps or any other resources at Conglomerate CCB Brasil hosting or providing access to data or internal norms applicable to password management. Users, who were approved and authorized by Conglomerate CCB Brasil to use systems, the network, apps, and the information contained therein, are responsible for protecting their own passwords. User passwords must remain confidential and, under no circumstance are they to be shared, forwarded, or otherwise disclosed.

**NOTIFYING** all users, including those who have remote access to the systems at Conglomerate CCB Brasil, that they are responsible for the security of their own connection to every system and information resource of the company. In line with the Organization's strategy and guidelines, Conglomerate CCB Brasil does not use cloud services. However, either direct or indirect suppliers / service providers may use cloud environments for the provision of services, as long as they follow the steps preestablished in the internal guidelines applied to the practice of security and risk management, which are proportional to the relevance of the services provided. Everyone must always perform according to the CCB Brasil Conglomerate's Information Security guidelines to guarantee the availability, confidentiality and integrity of the information stored, available and accessible in Cloud environment;

**MAKING SURE** that the creation of new products, selection of security mechanisms and goods or technology service acquisition always take into account the balance among the following aspects: risk, technology, cost, quality, speed and impact on the business;

**INCLUDING** the security considerations in every phase of the system development life cycle, particularly to make sure that the security policies at Conglomerate CCB Brasil be approached in a timely manner with cost efficiency;

**IDENTIFYING**, testing, and documenting, before implementation, security applications and systems, so that they do not represent a significant risk. The Information Technology teams must formalize a risk analysis for every new app or

important modification in apps run by Information Security. The results must be documented and made available for later use in security tests and verification stages;

**KEEPING** the bases of the Information Security processes even when the responsibility is outsourced to another organization, by providing periodic audits and seeking to reinforce the certification of their full compliance. The security requirements of Conglomerate CCB Brasil that are related to external parties must be approached and documented in the contract, with clauses always established according to the interests of the Information Security Policies, kept or accessed by suppliers / service providers when managing the Institution's information assets;

**ESTABLISHING** confidentiality agreements with employees, who are to be requested to sign security-related documentation to be provided by the Human Resources Department when they are hired. Such documents must contain the overall security responsibilities. The employees must read them carefully, understand and perform according to the contract conditions applicable to their position. For third parties, the confidentiality agreement must be included in the contracts signed between the parties or separate conditions;

**DEVELOPING** and implementing a comprehensive and specific business continuity strategy for the company's goals and priorities against human or technical faults, or major disasters. It is essential for the proper protection of information assets and critical business processes that, by means of preventive tests and management process audits, Conglomerate CCB Brasil show that they have adequate support capabilities for occasional activity recovery needs, so that they can return to their regular activities as soon as possible;

**IDENTIFYING** and controlling the risks when granting third parties the access to the systems and information assets at Conglomerate CCB Brasil. In cases of the need for consultants, commercial partners, suppliers / service providers or resellers to perform access activities and practices, according to applicable agreements, Conglomerate CCB Brasil reserves the right to conduct on-site audits and inspections within reasonable business timeframes;

**PRESERVE** users' privacy so that all data collected by third parties or shared with third parties that imply the personal identification of users, be properly communicated and authorized by the information owner, except when legal authorization is dismissed. Every piece of information collected and received is used according to the needs specifically indicated on the request for the provision of services, and there are many controls implemented to protect the information against unauthorized access or improper processing.

## WHAT ARE THE EFFECTS OF INFORMATION SECURITY?

By determining strict respect to and follow-up of compliance with their Information Security Policy, CCB Brasil Conglomerate's top management guarantees that all their employees and suppliers / service providers work together toward preventing information confidentiality issues from occurring with the information secrecy in their possession or under their responsibility. This effectively adds to obtaining positive business results, while preserving the quality and credibility, in addition to eliminating risks or reputational losses.



### REFERENCES IN THIS CONTENT

Norm ISO/IEC 17799:2005, ABNT NBR ISO/IEC 27002:2013; Resolution CMN No. 4.893/2021; ISO/IEC 27.001; POG.09.110.



## Risk Management at Conglomerate CCB BRASIL

### 4.4.1 — HOW IS RISK MANAGEMENT APPLIED AT CONGLOMERATE CCB BRASIL?



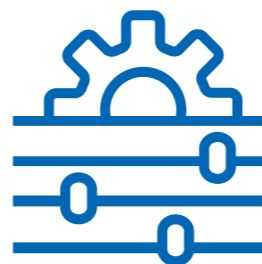
Distributed across the entire management structure at Conglomerate CCB Brasil, Risk Management procedures start with the Board of Directors, go to the Executive Board, and arrive at the Risk Committee, which is coordinated by the CRO and acts in every area of the company. Their role is to preserve the business environment, develop and improve control tools, and monitor crisis situations, by adopting both qualitative and quantitative indicators to anticipate possible situations that may cause negative impacts or impacts that go against the Institution's interests.

Always in line with CCB Brasil Conglomerate's strategic goals, Risk Management is a set of administrative tools that includes models and methodology for technically qualifying processes that aim at preventing and identifying possible risks to the integrity and continuity of the company's business.

By means of specific policies, control guidelines, preventive and corrective measures, Risk Management occurs in distinct stages, by first locating the contexts that are subject to risks and, after identifying them, analyzing, handling, and monitoring them.



As a result of its strategic importance, and in order to provide increased specificity to overall assignments, here are the Risk Management operating modes per area:



● **BOARD OF DIRECTORS** — The Board of Directors is responsible for defining the strategy, risk appetite and control structure for the Institution, in addition to measuring the performance of this management in relation to the goals, by:

**DETERMINING** the structure, responsibilities and controls for managing risks and capital available, and developing and implementing a corporate Enterprise-Wide Risk Management strategy, according to the Institution's risk tolerance;

**COMMUNICATING** the risk strategy, the main policies for its implementation and Risk Management structure to the entire Institution:

For additional information visit: <http://www.br.ccb.com/menu/Institucional/Governanca-Corporativa/Gestao-de-Riscos/Relatorios-de-Gerenciamento-de-Risco-109>

**MONITORING** market trends and potential developments that may be significant when it comes to Risk Management and Capital, and carrying out and proposing changes to the Institution's risk strategies if necessary;

**DEFINING** the specific procedures and approval authority necessary, in case of exceptions to the policies established and/or monitored limits, by considering the measures to be taken in the case of violation of any predefined limit;

**ESTABLISHING** and reviewing the levels of risk appetite expressed in the Risk Appetite Statement (RAS) along with the Risk Committee, the CRO and other Directors;

**APPROVING** and reviewing, at least on an annual basis, the Risk Management policies, strategies and limits, Capital Management policies and strategies, Stress

Test Program, Business Continuity Management Policies, Liquidity Contingency Plan, Capital Plan, and Capital Contingency Plan;

**ENSURING** the adherence to the Institution's Risk Management Policies, their strategy and limits;

**PROPOSING** the prompt correction of possible deficiencies in the Risk and Capital Management structures;

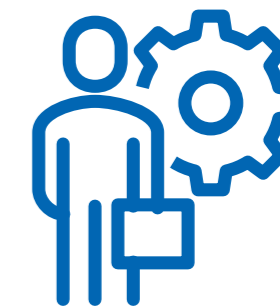
**APPROVING** relevant risk-induced changes to Risk Management policies and strategies, as well as to systems, routines and procedures;

**AUTHORIZING** exceptions to the policies, procedures, limits and levels of risk appetite expressed in the RAS, whenever necessary;

**ENSURING** the adequacy and enough resources for an independent, objective, and effective performance of activities related to Risk and Capital Management;

**PAYING ATTENTION** so that the Institution's compensation structure does not encourage behaviors that are inconsistent with the levels of risk appetite expressed in the RAS, and that levels of capital and liquidity are adequate and sufficient;

**ESTABLISHING** the Risk Committee assignments and spreading the risk culture across the Institution.



● **EXECUTIVE BOARD** — The Executive Board defines the strategies to guide the activities and structures in line with CCB Brasil Conglomerate's values. Board decisions are made by the Executive Board Committee (EBC), which has meetings on at least a monthly basis or when called, and the directors act by:

**DEVELOPING** and implementing the corporate Risk and Capital Management strategy, according to the risk tolerance defined by the Board of Directors;

**DETERMINING** the Institution's Risk Management structure and Risk and Capital Management responsibilities and controls;

**COMMUNICATING** the risk strategy and main implementation policies;

**MONITORING** current market trends and potential advances that may be significant when it comes to Risk Management, and proposing and carrying out changes to the Institution's risk strategies, if necessary;

**DEFINING** the specific procedures and approval authority necessary, in case of exceptions to the policies established and/or monitored limits, by considering the measures to be taken in the case of violation of any predefined limit;

**ATTENDING** and calling meetings, if necessary, for the purpose of monitoring, identifying, assessing, and mitigating risks, by taking into account the existing control environment context, always documenting every decision related to the mitigating action required or acceptance of relevant risks, and when necessary, approving Risk Management-related policies and procedures;

**SUPERVISING** and managing the Bank's risk appetite in a satisfactory manner, in line with the Group's overall risk appetite;

**REPORTING** the material risk event to the Head Office, by organizing opportune and necessary responses and solutions to risk events at the management level, and by reviewing the Bank's Risk Management comprehensive report on a biannual basis.



⦿ **RISK COMMITTEE** — The Risk Committee reports to the Institution's CEO. It is their responsibility to act by:

**PROPOSING** recommendations to the Board of Directors on at least an annual basis;

**ASSESSING** the levels of risk appetite documented in the RAS, as well as strategies for managing them, by taking into account the risks individually and in an integrated manner;

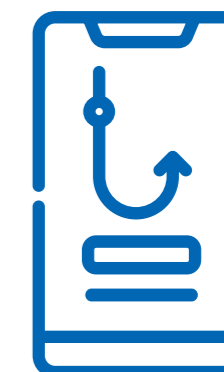
**SUPERVISING** the CRO's conduct and performance, and the compliance with the RAS conditions by the Institution's Board of Directors;

**ASSESSING** adherence to Risk Management processes that were established as policy, and keeping records of their own deliberations and decisions;

**MONITORING** the external business environment, and analyzing the efficacy of the Risk Management procedures and Internal Controls, as well as relevant risk events on the local market;

**PROVIDING** suggestions for the purpose of solving or mitigating risk event impacts, and analyzing other specific topics under their responsibility;

**ORGANIZING** the Risk Committee meeting on a monthly basis or exceptionally, if necessary, by qualifying its members and making sure that meeting minutes comply with the regulatory requirements and the Head Office's guidelines.



⦿ **CRO POSITION** — The Chief Risk Officer is a professional who is directly under the Head Office, with the following responsibilities:

**SUPERVISE** the constant implementation and development of risk management structures, including improvements;

**IMPLEMENT** policies, processes, reports, systems and models that are compatible with the RAS, in addition to strategic goals, promote collaborative risk control mechanism, according to the instructions and guidance from the Head Office;

**MEET** with the Head Office and periodically report to them to meet their qualification requirements, according to the regulation and technical guidelines;

**PROVIDE** proper training on policies, processes, reports, systems and models, even when these models are developed by third parties for the Risk team, and the CRO is not allowed to simultaneously respond to any commercial department;

**OFFER** subsidies and take part in strategic decision-making processes related to Risk Management and, when applicable, to Capital Management, as assistance to the Board of Directors;

**CONTINUOUSLY ORGANIZE** and coordinate the studies necessary for improving control and Risk Management at Conglomerate CCB Brasil.

## WHAT ARE THE EFFECTS OF RISK MANAGEMENT?



The Risk Management at Conglomerate CCB Brasil described herein is the result of effective protection of the Institution's assets within the different risk contexts to which they are exposed: credit, operational, market, etc. Such policies create a virtuous cycle that eliminates operation losses and disruptions. Furthermore, its practice, which is attentive to the smallest details, also cooperates for the full structuring of mechanisms related to measurement, control, and implementation of policies and strategies, with security and high performance.

### 4.4.2 — OPERATIONAL RISK MANAGEMENT WHAT IS OPERATIONAL RISK?

We call operational risk every possibility of loss resulting from unforeseen external events or fault, deficiency, or inadequacy of internal processes, people, or systems.

Operational risk may be associated with possible inadequacies or incorrections on signed contracts, may be linked to sanctions arising from noncompliance with legal provisions, or may even be related to compensations for damages to third parties arising from unforeseen activities developed by any employee.

Operational risk may compromise the goals and efficiency, or services provided, quality of products offered and even the very existence of the companies involved. The efficiency of operational procedures and the strict internal controls in the provision of services considerably reduce the likelihood of an operational risk event occurrence. They can mitigate the possible impacts in the same way, should the events have already occurred. To that end, there is the need to involve every internal and external agent to effectively control them.



## WHAT ARE THE CAUSES OF OPERATIONAL RISKS?

Operational risk generating factors are the internal fragilities and vulnerabilities that make it possible for risks to occur. The cause may be the result of faults from:

**PEOPLE** — when there is incompetence or a lack of ethical conduct in performing their assignments;

**SYSTEMS** — when there is IT infrastructure and architecture errors or a lack of availability for storage and network processing;

**PROCESSES** — when organization-established norms are not followed — flows, development stages, internal norms — or there is no adherence to the legislation in force;

**EXTERNAL ENVIRONMENT** — when unforeseen events occur in the social business environment or the country's regulatory environment.



## HOW IS OPERATIONAL RISK MANAGED?

The proper operational risk management is directly related to the knowledge of the company's existing internal processes. Thus, the company must be permanently kept up to date, particularly when it comes to processes that are seen as critical, by keeping operational risks identified, assessed, monitored, and controlled. To that end, they must:

**IDENTIFY** the operational risks that may impact the Institution's strategic goals, including generating factors (causes) and possible impacts of the operational risk identified;

**MEASURE AND DETERMINE** the potential effect of the operational risk in relation to the likelihood of occurrence and its impact;

**ASSESS** operational risk handling options, conduct additional analyses to better understand operational risks, and keep existing controls up to date;

**MONITOR** possible deficiencies in the operational risk management process;

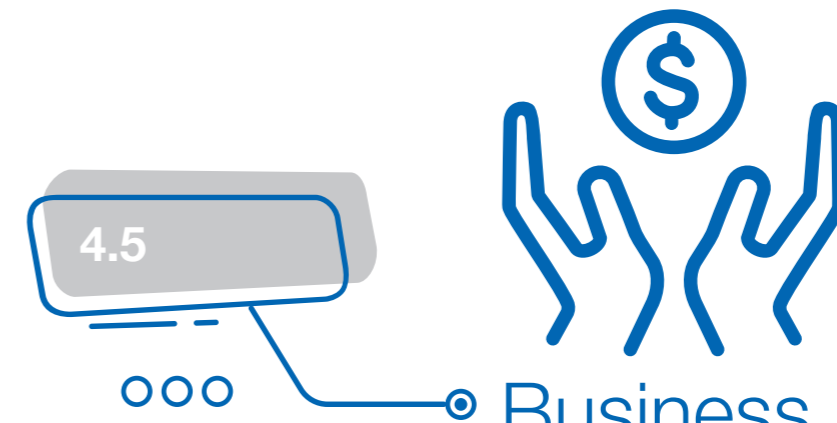
**REPORT AND DISCLOSE** information about operational risks and controls that permeate the Institution's scope, market and regulatory agencies;

**CONTROL AND RECORD** the behavior of operational risks, limits, indicators and operational loss events, as well as implement mechanisms to make sure that operational risk limits and indicators stay within the established levels;

**CREATE AND IMPLEMENT** mechanisms to mitigate operational risks in order to reduce losses to zero.

### REFERENCES IN THIS CONTENT

Bank For International Settlement (BIS). Sound Practices for the Management and Supervision of Operational Risk; Resolution CMN No. 4.557, from February 23rd, 2017; Instituto Brasileiro de Governança Corporativa (IBGC). Corporate Risk Management; ISO 31.000:2018. Risk Management — Guidelines; ISO 31.010:2012. Risk Management — Risk Assessment Process Techniques; ISO Guia 73. Risk Management — Vocabulary; COSO — Corporate Risk Management — Integrated Structure.



## Business Continuity Management at Conglomerate CCB BRASIL

*Business continuity and other administrative responsibilities.*

## WHAT IS BUSINESS CONTINUITY MANAGEMENT?

Business continuity management is the commitment to keep operations running before, during and after an incident, by minimizing the effects caused by the unavailability of their operations or their financial, legal, and regulatory impacts arising from a materialized incident in their critical assets, such as human resources, processes and technologies, which are essential for running their operations.

ISO 22301 is the international norm for business continuity management and is based on the success of the British BS 25999 norm and other regional norms. It was created to protect businesses from possible complications that may prevent Companies from reaching their goals. Interruption incidents include adverse and extreme weather conditions, fires, floods, natural disasters, even robbery, IT service interruptions, employee illnesses, terrorist attacks, etc.

## WHAT IS BUSINESS CONTINUITY MANAGEMENT FOR?

The Business Continuity Management system, by means of ISO 22301, allows the identification of relevant threats to the Company and the critical business roles that can be affected by it. This allows the early implementation of plans that make sure that businesses are not interrupted. The actions include the following:

**IDENTIFYING** and managing current and future threats to their businesses;

**ADOPTING** a proactive attitude to minimize the impact of incidents by implementing and operating controls and measures to manage the capability of handling occasional interruption incidents;

**KEEPING** critical jobs running during a period of crisis;

**MINIMIZING** downtime during incidents and improve recovery time.

## HOW IS BUSINESS CONTINUITY MANAGEMENT APPLIED AT CONGLOMERATE CCB BRASIL?



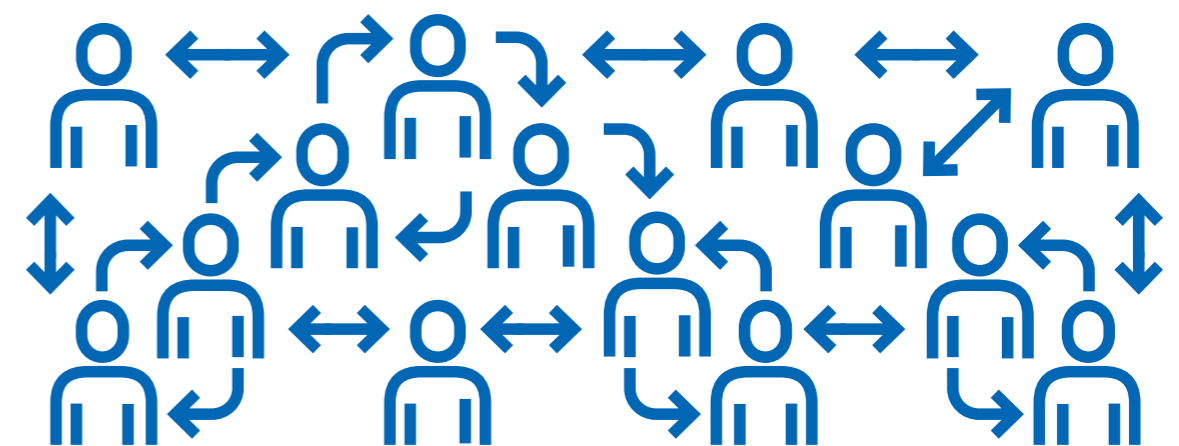
For the proper protection of information assets and critical business processes, it is essential that Conglomerate CCB Brasil, by means of preventive tests and management process audits, prove that they are able to provide support to the possible need for recovering their activities, so that they return to their normal operations as soon as possible.

Conglomerate CCB Brasil have policies and procedures to support Business Continuity Management actions and activities. The plans have a set of detailed procedures to be followed by contingency support teams, which focus on each one of them in different situations.

During recovery moments (beginning of the contingency) and actual recovery (return to normal), the support documentation for carrying out critical activities and procedures in order to show the papers and the responsibilities of teams involved in the Business Continuity process.

For the purpose of fulfilling the Business Continuity Management Plan, periodic exercises are performed to make sure that, in a real contingency situation, Conglomerate CCB Brasil keeps their operations running during the crisis.

These exercises are structured by initially considering the prioritization of critical processes contained in the Business Impact Analysis Report (BIA) of Conglomerate CCB Brasil, and key employees are called upon to take part in them, to test the executability of their routine tasks while seeking to preserve critical assets, human resources, processes, and technologies that are essential to running the operations.





## WHAT ARE THE EFFECTS OF BUSINESS CONTINUITY MANAGEMENT ON BUSINESSES?

By applying the Business Continuity Management good practices, Conglomerate CCB Brasil is able to:

(Operational)

**PREVENT** the total or partial interruption of the activities at the Institution;

(Financial)

**PREVENT** payment fines, indemnifications, court costs and attorney fees; reimbursement for improper charges; operation losses or damages as a result of faults or fraud; among others;

(Legal)

**PREVENT** legal sanctions that hinder the provision of services or running operations at the Institution, administrative, civil, tax and labor processes; among others;

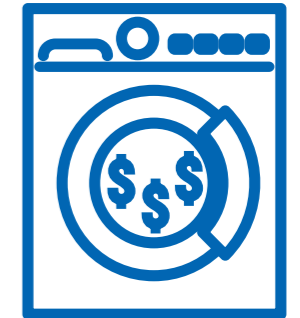
(Image)

**PREVENT** a negative perception of the Institution's image by its customers, media, counterparts, among other stakeholders.

### REFERENCES IN THIS CONTENT

ISO 31.000 of 2009; ISO/IEC 22302; Resolution CMN n° 4.557; POG.05.004

Source: [https:// www.bsigroup.com/pt-BR/ISO-22301-Continuidade-dos-Negocios/ Introducao-a-ISO-22301/](https://www.bsigroup.com/pt-BR/ISO-22301-Continuidade-dos-Negocios/Introducao-a-ISO-22301/)



## 4.6 Unlawful Act Prevention Program at Conglomerate CCB BRASIL

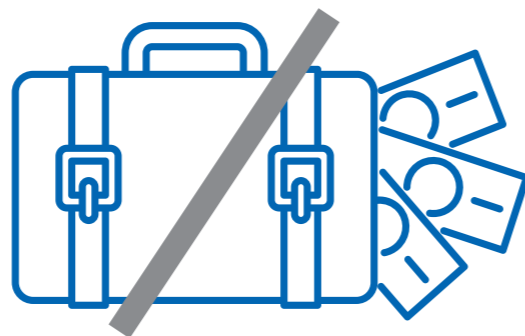
*CCB Brasil Conglomerate's commitment to integrity*

### WHAT ARE UNLAWFUL ACTS?

In practice, we can say that they are any act of disobedience to legal statutes within the civil scope or criminal scope. In the financial system environment, there are several types of fraud, facilitation or cover-up of crimes that make an unlawful act, most of them involve money laundering, corruption, terrorism, or drug trafficking.

### WHAT IS THE UNLAWFUL ACT PREVENTION PROGRAM AND WHAT IS IT FOR?

Every principle that is based on Conglomerate CCB Brasil Conglomerate's Code of Ethics and Conduct — consideration by others, commitment with transparency, compliance with laws and corporate social responsibility — points to the need for acting firmly to prevent unlawful acts.



Financial institutions, since they have a large number of assets coming from transactions made around the globe, have conditions to aid the several crime control authorities in legally tracking and communicating suspicious activities or operations indicating money laundering, corruption, terrorism funding or drug trafficking.

The prevention of unlawful acts is accomplished by means of a set of tools that is essential for protecting financial institutions, which count on the adherence of every public of interest of Conglomerate CCB Brasil. The observance of and compliance with the Integrity Program Guidelines and Money Laundering and Unlawful Act Prevention Policy are indistinctly applied to every hierarchical level at Conglomerate CCB Brasil — administrators, employees, third parties, suppliers / service providers.

## WHAT ARE THE LEGAL SANCTIONS THAT ARE PROVIDED FOR UNLAWFUL ACTS?

The main responsibility of the United Nations Security Council (UNSC) is to keep world peace and safety. According to the Charter of the United Nations, all Member States are obliged to comply with the decisions of the Council. This council takes the lead in determining whether there is a threat to peace or an act of aggression. It invites the parties involved in a controversy to settle it peacefully and recommends adjustments methods or solution terms. In some cases, the Safety Council may resort to the imposition of sanctions or even authorization of the use of force to keep or restore international peace and safety. Sanctions aim at pressuring a State or entity toward fulfilling

the goals established by the Safety Council without resorting to the use of force. Thus, sanctions offer the Safety Council an important instrument for fulfilling their decisions. In Brazil, Law No. 13.810, from March 8th, 2019, also known as the Asset-Freezing Law, establishes the unavailability of funds from people or companies with ties to terrorist activities, according to the list provided by the UN.

The European Union (EU) also has an extensive list of sanctions for situations in which their interference is needed for preventing conflicts, emergency situations and humanitarian crises. Among the retaliations we find a weapon and ammunition embargo, international trade ban, and restricted asset circulation or asset lock, and they can affect governments, organizations, and individuals. Promoting international peace and safety; preventing conflicts; supporting democracy, rule of law and human rights; and defending the international rights principles are the main goals pursued by these negotiations.

Accordingly, the North American Treasury imposes strict sanctions by means of their Office Foreign Assets Control (OFAC). Such sanctions are applicable to countries, individuals or organizations that violate the international trade rules, have ties with terrorism crimes or international drug trafficking, develop activities related to the proliferation of weapons of mass destruction or that in any way threaten the US national security or economic policy.

The Foreign Corrupt Practices Act (FCPA) is a US foreign anticorruption law that was enacted by the US Congress in 1977. It creates civil, administrative, and criminal sanctions to fight against international trade corruption, and is applied to US individuals and companies that, in foreign trade activity, make use of the corruption in foreign governments in order to obtain or retain commercial transactions in that country.

The United Kingdom Bribery Act (UKBA) is regarded as one of the strictest anticorruption laws in the world, and it even punishes private corruption. Like the main existing anticorruption laws, it also enjoys the so-called extraterritoriality, meaning that it is applicable not only to British companies operating on the local market and/or foreign markets, but also to foreign corporations acting in the United Kingdom, in addition to providing for the punishment of individuals and legal entities

for committing one of the four main crimes in the legal text. The fines applicable to individuals and legal entities are limitless, and in the case of individuals, it can be cumulatively or singly applied and is punishable by imprisonment for up to ten (10) years. The directors of companies involved in corruption can be removed from office and suffer impediment processes, resulting in the prohibition of working in the area for up to fifteen (15) years. Failure to prevent bribery was also typified as a corporate crime in the United Kingdom.

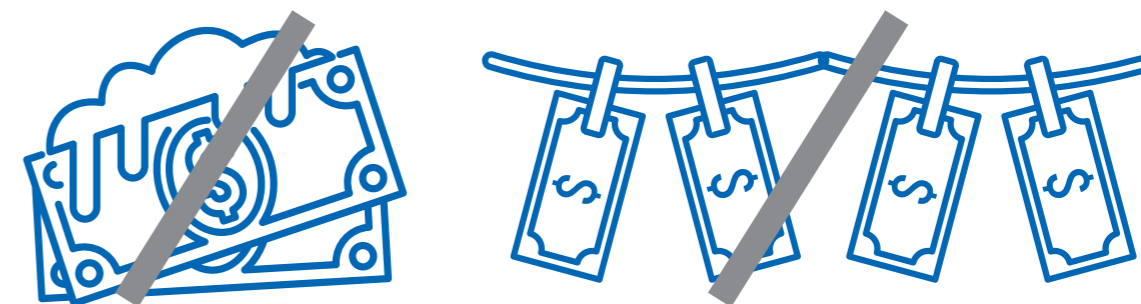
In the case of Brazil, the government created a financial intelligence unit in 1998, Conselho de Controle de Atividades Financeiras (COAF) [Controlling Council of Financial Activities]. On that same date, money laundering was typified by Law No. 9613/98 (with amendments introduced by Law No. 12.683/12), which provides for the prevention of financial system use for unlawful acts. Thus, to conceal or conceal the nature, origin, location, disposition, transaction or ownership of assets, rights, and values directly arising from criminal offense characterize a crime.

In turn, GAFI/FATF develops standards and promotes the effective application of legislative, regulatory, and operational measures against money laundering, terrorism funding, proliferation of weapons of mass destruction and other threats to the integrity of the international financial system. In 2013, the Organized Crime Law was enacted in Brazil, and not only typifies what a criminal organization is within the money laundering context, but also defines the criminal investigation processes, means of evidence collection, correlated criminal offenses and criminal procedures.

Brazilian Federal Law No. 12.846/2013, also known as the "Anticorruption Law", came as a landmark in the legislation for government protection and, indirectly, that of the entire society, by establishing in specific regulation the objective, civil and administrative accountability of legal entities for the practice of acts against the Brazilian and foreign federal governments.

The Law is applicable to corporations, general partnerships, either legally incorporated or not, foundations, legal entities, or individual associations, as well as foreign corporations with a head office, branches, or representation on Brazilian territory, either de facto or de jure corporations, albeit temporally, and provides for objective, civil and administrative accountability of legal entities for the practice of acts against the Brazilian and foreign federal governments.

In 2015, Federal Decree No. 8,420/2015, revoked in 2022 by Decree No. 11,129 regulated such legislation by detailing the mechanisms and procedures of integrity, audits, the application of code of ethics and conduct,



and whistleblowing incentives that should be adopted by companies, which can be the target of inspections conducted by the Controladoria Geral da União (CGU) [Office of the Federal Controller General]. According to the document, the integrity program must be structured, applied, and updated according to the current nature and risks of the activities of each legal entity, which, in turn, must guarantee their constant improvement and adaptation.

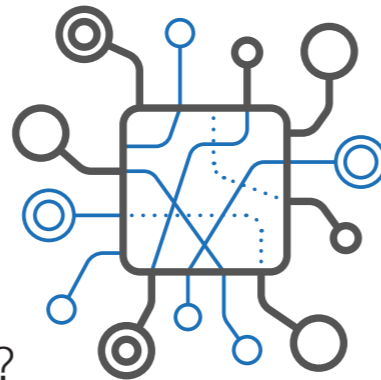
In line with the good practices of corporate governance, in 2016, the International Standardization Organization (ISO) published the ISO 37001:2016 norm – Antibribery Management System, to support organizations in their fight against bribery by means of a culture of integrity, transparency and compliance with laws and regulations applicable, with its requirements, policies, procedures and proper control to deal with bribery risks.

Still in the same year, following the same precautions, the Antiterrorism Law was enacted, and, in addition to typifying terrorism crimes and terrorist organization practice, it equally establishes the applicable punishments, aiming at greater control of unlawful acts.

Accordingly, by consolidating the principles, rules and best national and international practices of ethics and integrity for Corruption Prevention and other harmful acts committed against the Brazilian and foreign federal governments, the bank self-regulation from the Federação Brasileira de Bancos (FEBRABAN) [Brazilian Federation of Banks], in 2019, established a regulation that described the main pillars for structuring and the continuous improvement of the Signatory Financial Institutions Integrity Program.



## HOW IS THE UNLAWFUL ACT PREVENTION PROGRAM APPLIED AT CONGLOMERATE CCB BRASIL?



By consolidating the principles, rules and best national and international practices of ethics and integrity for Corruption Prevention and other harmful acts committed against the Brazilian and foreign federal governments, the Integrity Program at Conglomerate CCB Brasil consists of a set of corporate guidelines to comply with Federal Law No. 12.846, from August 1st, 2013 and with SARB Regulation No. 021/2019.

It is essential that everyone be aware of the importance of preventing money laundering, corruption, terrorism funding, and drug trafficking regarding legal and image risks, to which Conglomerate CCB Brasil may be exposed. Thus, it is worth pointing out everyone's responsibility when performing their activities toward preventing or mitigating unlawful acts at Conglomerate CCB Brasil.

The Conglomerate has teams that are exclusively dedicated to preventing the use of the Institution for unlawful or inappropriate activities, as well as the association of Conglomerate CCB Brasil Conglomerate's image with the practice and/or facilitation of unlawful acts.

Conglomerate CCB Brasil, with the support from Top Management, promotes educational measures regarding the ethical values expressed in their Code of Ethics and Conduct, aiming at increasing the level of adherence to the Program and transparency in the relations with their relationship public. Furthermore, they keep a training platform for employees and, whenever necessary, provide on-site training on the Integrity Program.

They also keep a whistleblower channel, so that each and every situation supposedly involving or characterizing non-compliance with CCB Brasil Conglomerate's Code of Ethics and Conduct can be forwarded to the means of access listed below:

external e-mail:  
**comite.etica@br.ccb.com**

internal e-mail:  
**Ethics Committee**

institution's website:  
**www.br.ccb.com/Fale-Conosco**

Internal channel available on the intranet  
at the pointer "Ethics" (restrict to employees):  
**Talk to the Ethics Committee.**

The procedures for investigation, referral, and treatment of violations, including the necessary deliberations to apply sanctions to offenders, are formalized in specific internal procedures for investigation of ethical violations.

For full compliance with BACEN Resolution CMN No. 4.859, from October 23rd, 2020, which establishes the obligation of a Whistleblower Channel, for dealing with associated demands, manifestations and records, the Company makes the following available: [www.br.ccb.com/denuncia](http://www.br.ccb.com/denuncia) and [www.ccbfinanceira.com.br/atendimento/canal-de-denuncia.php](http://www.ccbfinanceira.com.br/atendimento/canal-de-denuncia.php). It is a constantly open path to every employee, collaborator, third party, client, user, partner, or supplier Conglomerate of CCB Brasil.

Regarding disciplinary measures and procedures to ensure prompt interruption of irregularities or offenses detected, and the immediate remediation of damages caused, we stress that any suspicion or violation must be promptly reported to the Ethics Committee, which will analyze and deliberate on the punishment according to the severity of the offense.

Thus, every Institution representative, employee, intern, and any third party, either direct or indirect, temporary employee, supplier / service provider, consultant, advisor, and agent, contractor, or subcontractor mutually state and guarantee to:

**NOT** pay, offer, authorize and/or promise — either directly or indirectly — any amount, valuable item or undue advantage to any person who is an officer, agent, employee or representative of any government, either national or foreign, or national or foreign agency and organization, or any political party, candidate or government officer, or political party office, or any other person;

**NOT** offer data or receive an advantage or favor with the purpose of obtaining or keeping undue differentiated treatment, in violation of the laws dealing with corruption crimes and practices, and against the government, always complying with laws of money laundering prevention and laws against terrorism funding, drug trafficking and corruption;

**NOT** be excused from observing and complying with the CCB Brasil Conglomerate's Corporate Anticorruption Policy and Code of Ethics and Conduct attentively and fully;

**NOT** accept at any time or under any burden any type of relationship involving countries with embargos and/or restrictions at OFAC, or individuals or legal entities listed or that may be listed on the OFAC Specially Designated Nationals and Blocked Persons List (SDN); or those who are on the UN list; or EU list; or have been restricted by the Brazilian laws, and, in these cases, reporting the reasons for denial to those who are involved.



## WHAT ARE THE EFFECTS OF THE UNLAWFUL ACT PREVENTION?

The procedures and good practices described herein make it possible to increase the probability of detecting bribery, the so-called white-collar crime, and tracking the association with several other crimes with effective success in court proceedings associated, thus drastically reducing the risk of asset losses and severe reputational damages.

The main result of that tight control of possible indication of unlawful acts at Conglomerate CCB Brasil is the elimination of legal and operational conformity risks, such as national or international punishments that may hurt the Institution's image.

Always performing based on this firm positioning of legal conformity, and by the force of their ethical principles established, Conglomerate CCB Brasil believe that banks, as entities that control most of the currency circulation on the planet, work as important tools in building a fairer and less unequal society.

### REFERENCES IN THIS CONTENT

Law No. 12.846/13; Decree No. 11.129/22; SARB Regulation No. 11, from August 1st, 2013; SARB Regulation No. 021, from March 13th, 2019; Law No. 9.613/98; Law No. 13.260/16; Law No. 13.810/19; Resolution BCB No. 44/2020; Circular BCB No. 3.978/2020; Cayman/FATCA/CRS/FCPA/UKBA Legislation.





## Bank Self-Regulation at Conglomerate CCB BRASIL

*Regulatory codes established  
jointly by the industry.*



### WHAT IS BANK SELF-REGULATION?

Self-regulation is an intelligent and broad way to establish a regulatory conduct standard according to each institution's interest, following common references to other institutions. These references include from the definition of legal positions within the scope of ethical conduct of business, consumer protection, socio- environmental responsibilities, and corporate governance to the strictest unlawful act prevention recommendations.

### WHAT IS SELF-REGULATION FOR?

The normative axes of this set of applicable rules were created by the Brazilian Federation of Banks (FEBRABAN), and Conglomerate CCB Brasil, as an associate financial institution, has adhered to the commitments established therein, in a way common to the entire banking system, as a Code of Regulation of the sector. The self-regulation idea is to promote healthy and ethical competition on the market, and guarantee free, clarified, transparent and conscious performance from both sides.

### HOW IS BANK SELF-REGULATION APPLIED AT CONGLOMERATE CCB BRASIL?

Compliance with regulations in force, as well as with the guidelines provided for in this policy and other internal Bank regulations are periodically monitored and inspected both internally and externally. The cases of non-compliance with these norms are regarded as infringement and, without prejudice to the Ethics Committee, are subject to punishment, coercive measures, and alternative means of controversy solution applicable to financial institutions, and other institutions supervised by Central Bank of Brazil, and to Brazilian Payment System members. Such facts will be contemplated in the Conformity Report, which is issued periodically.

For didactic purposes, FEBRABAN dealt with self-regulation by different topics, which are constantly updated on the network in specific documents. See highlighted here, in general, what you will find in each of the regulations in force in the text of the Banking Self-Regulation System (SARB):

**BANK CODE OF ETHICS AND CONDUCT AND SELF-REGULATION** — It establishes the values and principles that govern the document, which are: integrity, equality, respect to the consumer, transparency, excellence, sustainability, and trust. It details the responsibilities and commitments signed by the signatory institutions, scope of the norms presented and overall competences of councils, directors, and commissions.

**SARB nº 001/2008** — RELATIONSHIP WITH THE INDIVIDUAL CONSUMER: I. in the assistance provided at the self-service terminal, on the internet, mobile communication devices, call center and complaints office; II. in the offer and publicity of their products and services; III. in consumer engagement procedures; and IV. in the confidentiality and security of services.

**SARB n° 002/2008** — BANK ACCOUNT NORMS. It presents basic rules regarding transactions, charging fees, and service packages, in addition to reporting risks, security measures and controls for using the services, and also offering a panoramic view on the importance of accurate registration information and the need for updating them with details on possible effects of not doing so.

**SARB n° 003/2008** — CUSTOMER SERVICE (SAC). It defines SAC within the legal scope and goals of the provision of services, from the availability of access to service, service quality and its improvement to following demands within the established deadlines.

**SARB n° 004/2009** — CUSTOMER SERVICE AT BRANCHES. It is about the physical service locations, information, products, and services available there. It deals with priority services, accessibility, and service quality. Furthermore, it also addresses business hours, the service desk, complaints offices, and alternative service channels, among other requirements.

**SARB n° 005/2009** — The offer of and application for DIRECT LOANS TO THE CONSUMERS AND FINANCIAL LEASES FOR THE PURCHASE OF VEHICLES. It provides the guidelines and procedures for the offering and application for loans and leases with purchase options, specifically for the acquisition of vehicles. It deals with the regulation of loan agreements, freedom of choice on the client's part, and several other legal guarantees provided.

**SARB n° 006/2009** — MONITORING OF ADHESION TO SELF-REGULATION NORMS. It verifies its effective application and establishes norms for the supervision and control of procedural acts defined in the self-regulation, its communication and publicity, in addition to disciplinary processes and their mitigation, aggravation, etc.

**SARB n° 007/2011** — Procedures related to the demands recorded on the "LET US KNOW" RECORD CHANNEL. It establishes how the signatories are notified and how service requests are forwarded. It is about how the tool contacts the government channel of the Ministry of Justice, the [consumidor.gov.br](http://consumidor.gov.br).

**SARB n° 008/2011** — Rules for SELF-REGULATION REMOTE ELECTRONIC EDUCATION. It details management and improvement mechanisms to expand the training on e-learning channels. It deals with the regulation of content modules, target audience, and training assessment ways and their deadlines.

**SARB n° 009/2013** — CERTIFICATION PROGRAM OF REAL ESTATE LOAN PROFESSIONALS, OF THE BRAZILIAN ASSOCIATION OF REAL ESTATE LOAN AND SAVINGS ENTITIES (Abecip). It deals with the norms, assessment, and classification in tests for the certification of professionals linked to the important real estate loan sector. It highlights the conducts related to the FEBRABAN Code of Ethics in line with the Abecip certification.

**SARB n° 010/2013** — RESPONSIBLE CREDIT. It clarifies contexts about use limits, content clarity and contract transparency, in addition to publicity and other information made available to clients, by means of either physical or virtual media, in the offer of loans from affiliated institutions.

**SARB n° 011/2013** — PREVENTION OF AND FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FUNDING. It typifies crimes and presents the legislations and regulations available. It presents "Know your Client", which is a set of procedures to help track and identify the funds and clients under suspicion, in addition to dealing with politically exposed people, among other guarantees and security measures.

**SARB n° 012/2014** — LOAN SUMMARY. It defines the basis for the entire relationship between affiliated company and consumer applying for the loan. It focuses on topics such as the definition of margins of values, rates, taxes, insurance, payment installments, burdens, consumer rights, etc.

**SARB n° 013/2014** — LOANS TAKEN REMOTELY. Specifically for revolving loans to individuals, it deals with the transactions made through channels such as telephone, mobile communication devices, self-service ATMs, and the Internet. It also deals with the offer, application, transaction monitoring, waiver, etc.

**SARB nº 014/2014** — The creation and implementation of SOCIO-ENVIRONMENTAL RESPONSIBILITY policies. It exposes the fundamental legal procedures for defining activities linked to governance and sustainability norms of the Socio- Environmental Responsibility Policy (PRSA). In addition to that, it deals with real estate collateral and agricultural loan conditions, among other sector-related topics.

**SARB nº 015/2014** — PAYROLL LOANS. It deals with types of offers, agreements and operations, as well as the obligations of signatory institutions to offer alternatives such as early settlement, right of waiver, monitoring, control, etc.

**SARB nº 016/2015** — SALARY ACCOUNT. It provides all the essential information for opening an account, conditions for gratuity, user rights, portability, restrictions, warnings when breaking bonds, closing an account, etc.

**SARB nº 017/2016** — ADEQUACY OF PRODUCTS AND SERVICES. By seeking the sustainability and harmony of consumer relations in financial transactions, the regulation deals with the adequacy of products and services offered by institutions to specific client profiles, in order to guarantee quality, safety, and sustainability.

**SARB nº 018/2017** — DEALING WITH AND NEGOTIATING DEBTS. It adds to the recovery of the consumer's financial capability in unsecured loan agreements, with the improvement of equity, good faith, and transparency. By granting loans responsibly, the channels of information, negotiation and settlement of agreements are also an effective part of the consumer protection and defense norms.

**SARB nº 019/2018** — CONSCIOUS USE OF OVERDRAFT PROTECTION. It offers important guidance for awareness and transparency when using the conditions and client information regarding installments and settlement of a debt balance and other collaterals, aiming at keeping a healthy and sustainable credit relationship.

**SARB nº 020/2018** — SELF-REGULATION SEAL. It shows to the signatory parties the commitments to be signed with the society, so that seals are granted to their respective institutions according to the levels of adhesion in which they are found — level I, II or III signatory party — and presents the procedures required for maintaining the qualification.

**SARB nº 021/2019** — Integrity program for PREVENTING CORRUPTION AND WRONGFUL ACTS AGAINST NATIONAL OR FOREIGN GOVERNMENTS. It deals with typifying the operational procedures and control, tracking, whistleblowing mechanisms, in addition to disciplinary measures to be observed by signatory financial institutions. It refers to the technical definition of the corruption term and goes as far as implementation procedures, recommended relationships, and preservation of the integrity of affiliated companies.

**SARB nº 022/2019** — COMPLAINTS OFFICES. It emphasizes the need for widespread ombudsman channels, including official SAC decrees. It provides for the management of records of demands, deadlines for responses, management of satisfaction surveys and their relationship with the appropriate target plans of the affiliates, in addition to the constant improvement of their training activities.

**SARB nº 023/2020** — RELATIONSHIP WITH ELDERLY CONSUMERS. It aims at regulating the adequacy of products and services of affiliated companies to this consumer profile in particular. It provides for legally adopting the “Do Not Disturb” procedures, a set of treatment, education, protection measures against abuse, in addition to distinct channels providing services to the elderly.

**SARB nº 024/2021** — On the RELATIONSHIP WITH POTENTIALLY VULNERABLE CONSUMERS. Defines the concept of vulnerable consumers and their characteristics, and the need to create procedures to ensure that the offer of products and services are suitable for this public.

**SARB nº 025/2021** — About PROTECTION OF PERSONAL DATA. It establishes minimum guidelines and procedures for improving the protection of the Holders' Personal Data under the terms of the LGPD and the need to implement a privacy governance program that establishes minimum procedures and good practices for the adoption of effective measures to demonstrate the observance and fulfillment of the protection rules for the Holders' Personal Data.

## WHAT ARE THE EFFECTS OF SELF-REGULATION?



The adoption of a regulation that is common to the entire bank sector results in increased transparency in the relationship among the most diverse Institution partners. Since the resolutions are continuously updated, the commitments signed establish greater competitive equality among the institutions associated, by standardizing the conformity conducts. The easy universal and democratic query, deriving from the same network source, is an important tool for all employees on all management levels, as well as a guarantee that information is always available to clients, investors, third parties, suppliers / service providers and society as a whole, thus making it possible to widely access regulation contexts and contents, such as reducing the risk of damaging the institutional image based on a lack of knowledge on the matter.

### REFERENCES IN THIS CONTENT

FEBRABAN Bank Self-regulation Code

[SARB nº 001/2008](#)

[SARB nº 009/2013](#)

[SARB nº 017/2016](#)

[SARB nº 002/2008](#)

[SARB nº 010/2013](#)

[SARB nº 018/2017](#)

[SARB nº 003/2008](#)

[SARB nº 011/2013](#)

[SARB nº 019/2018](#)

[SARB nº 004/2009](#)

[SARB nº 012/2014](#)

[SARB nº 020/2018](#)

[SARB nº 005/2009](#)

[SARB nº 013/2014](#)

[SARB nº 021/2019](#)

[SARB nº 006/2009](#)

[SARB nº 014/2014](#)

[SARB nº 022/2019](#)

[SARB nº 007/2011](#)

[SARB nº 015/2014](#)

[SARB nº 023/2020](#)

[SARB nº 008/2011](#)

[SARB nº 016/2015](#)

[SARB nº 024/2021](#)

[SARB nº 025/2021](#)

5



Important links

In order to dive deeper into the topics described herein, Conglomerate CCB Brasil suggest reading the original documents below as complementary reading material, since they were the reference for preparing this guide, and are available for public reference. Check them out at:

### CODE OF ETHICS AND CONDUCT

<http://www.br.ccb.com/menu/Institucional/Codigo-de-Etica-127>

### PLD

<http://www.br.ccb.com/menu/Institucional/Governanca-Corporativa/Prevencao-a-Lavagem-de-Dinheiro%2C-a-Corrupcao-e-ao-Financiamento-ao-Terrorismo-188>

### FATCA/CRS

<http://www.br.ccb.com/media/Institucional/guia-fatca-crs-ccb-brasil.pdf>





## Acronyms

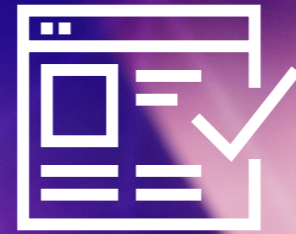
6

- ABECIP** — Brazilian Association of Real Estate Loan and Savings Entities
- ANPD** — National Data Protection Authority
- CCB** — China Construction Bank
- CCO** — Chief Compliance Officer
- CEO** — Chief Executive Officer
- COAF** — Controlling Council of Financial Activities
- CPPD** — Data Privacy and Protection Committee
- CRO** — Chief Risk Officer
- DPO** — Data Protection Officer
- EBC** — Executive Board Committee
- FATCA/CRS** — Foreign Account Tax Compliance Act / Common Reporting Standard
- FCPA** — Foreign Corrupt Practices Act
- FEBRABAN** — Brazilian Federation of Banks
- GAFI/FATF** — Financial Action Task Force
- GTPPD** — Data Privacy and Protection Work Group
- LGPD** — General Data Protection Law
- OFAC** — Office of Foreign Assets Control
- ON** — United Nations
- PDA** — Personal Digital Assistant
- PLD** — Money Laundering Prevention

- PRSA** — Socio-Environmental Responsibility Policy
- RAS** — Risk Appetite Statement
- RIPD** — Data Protection Impact Report
- SAC** — Customer Service
- SARB** — Bank Self-regulation System
- SDN** — Specially Designated Nationals and Blocked Persons List
- IS** — Information Security
- EU** — European Union
- UKBA** — United Kingdom Bribery Act



7



## Glossary

**Asset** — Each and every tangible or intangible good belonging to, administered by or under the responsibility of an institution.

**Information asset** — All data that is stored in possession and under the responsibility of an institution. They are strategic pieces of information, files, system documentation, procedure manuals, continuity plans, training activities, or the entire business support system, the entire base of the operation.

**Software assets** — Apps, systems, development, and utility tools.

**Physical assets** — Computer-related equipment (computers, monitors, laptops, PDAs, flash drives, smartphones, tablets, modems, etc.), communication equipment (routers, PABX, answering machines, landlines, or cell phones, etc.), media (magnetic tapes and disks, optical disks, hard disks, CDs, flash drives, etc.), other technical pieces of equipment (no-breaks, air conditioners, etc.), furniture and its accommodations.

**Self-regulation** — Set of technical norms and rules that are voluntarily and jointly established by institutions belonging to a certain sector for monitoring, inspecting, and creating common ethical references and practices. It is structured from the creation, negotiation and constant updating of documents accepted and signed by all the regulated parties.

**Placement** — Entry into the financial system of funds obtained through unlawful activities, by means of deposits, financial instrument purchase (ex.: CDBs, fund shares, etc.) or the purchase of goods or assets.

**Internal Control Committee** — Committee that aims at advising the Executive Board Committee (EBC) regarding the performance of their assignments related to the adoption of policies and measures oriented to sharing the culture of internal controls, identification, risk mitigation, and conformity with norms applicable to the Institution.

**Compliance** — It is the obligation to comply, be in conformity with laws, guidelines, internal and external regulations, and enforce them, by mitigating the risk pegged to reputational and legal or regulatory risks.

**Conduct** — Display of how a person or institution behaves in society, based on the law, and beliefs, moral and ethical values that they follow or advocate.

**Confidentiality** — Guarantee that certain pieces of information will only be accessed by authorized people.

**Conflict of interests** — Any situation in which a person or institution may have their judgement and decision-making capability affected and may incur the breach of the principle of impartiality and favor personal interests, those of third parties or even those of political or ideological nature to the detriment of the interests and principles of the community where they are.

**Board of Directors** — It is one of the common ways to manage the good practices of corporate governance, and it consists of establishing an organization structure that brings the interests together and lines up strategies in a transparent and autonomous manner. It is also simply called the board and it is to which CEOs report by communicating actions and providing information.

**Corruption** — According to the general legal meaning, it is a crime committed by either government or private company employees that is characterized by offering or obtaining undue advantages or favors in exchange for unlawful gains. It may be either active or passive, internal or external, and the most common types include bribery, kickbacks, nepotism, extortion, influence peddling, use of privileged information for personal purposes or that of friends or relatives, purchase and sale of court judgments, receipt of high value gifts or services, improbity, embezzlement, fraud, collusion, and malfeasance. Corruption affects several sectors of society, compromises an important part of State funds, and threatens political stability and the sustainable development of a nation. Corruption affects transparency and is a threat to the balance, safety, and survival of societies, by weakening institutions and democracy, ethical, and fairness values, in addition to compromising sustainable development.



**Availability** — Prerogative of authorized users to obtain access to information and corresponding systems whenever necessary, within periods and environments approved by the Institution.

**Ethics** — Set of principles and values that guide good conduct in general. It is different from moral, which is based on behavior aspects according to individual, specific views.

**FCPA** — The Foreign Corrupt Practices Act is the Law against Practices of Corruption Abroad which was enacted by US Congress in 1977, and aims at creating civil, administrative, and criminal sanctions in the fight against international commercial corruption. This law applies to North American individuals and companies that, in commercial activities abroad, make use of the corruption affecting foreign governments in order to obtain or retain commercial transactions in the country in question.

**Head Office** — Within the commercial field, this refers to the Parent Company, where their main administrators work. It may also be referred to as Corporate Headquarters.

**Information** — It is an asset that records client data, business data, system configurations, among other pieces of information, which must be classified according to how valuable they are to the Institution. Based on that classification, it must be properly protected regarding the confidentiality, integrity, and availability aspects. The information can be recorded in different ways, such as printed or written on paper, stored on computers, hard discs, CDs, or other types of media, sent by mail or electronic means, exhibited on films, or spoken of during conversations.

**Financial institution** — Legal entity governed by public/private law, as per Law No. 7.492/86, and has as their main or ancillary activity, either cumulatively or not, capturing, intermediating, or investing third-party financial resources in national or foreign currency, or the custody, issuance, distribution, trading, intermediation or administration of securities.

**Integration or reintegration** — Return to the economic system of unlawful funds coming from a seemingly legal way by means of investment in the stock market (ex.: stocks, marketable securities), real estate market, jewelry, productive companies, tourism, artwork, mutual funds, etc.

**Integrity** — Assurance that the information will only be modified by people who are actually authorized to do so, always within the methods approved for such procedure.

**Money laundering** — Practice that is used for covering up illegally obtained financial resources. It is the process in which “dirty” gains obtained from unlawful activities become “clean” gains or are seemingly made legal after several transactions theoretically involving four independent phases, which often occur simultaneously: placement, concealment, integration or reintegration and recycling.

**Concealment** — One or several financial transactions with funds already integrated into the financial system, aiming at concealing illegal funds, which are combined with those of legal origin.

**Recycling** — Thorough cleaning of the traces of the financial transgression by closing bank accounts, withdrawing values, simulating asset transactions. The fight against this practice is extremely important because the social consequences of this type of crime are devastating, since they hurt the formal economy and bring about damages to the financial system, reduce public investments in sectors that benefit society, such as health, safety, and education, among others.

**Signatory party** — Each and every person or institution associated with a certain group, whose principles, values, and attitudes have been previously established in a signed commitment agreement.

**FEBRABAN level I signatory parties** — Financial institutions that signed FEBRABAN's Code of Ethics and Conduct and Self-regulation.

**FEBRABAN level II signatory parties** — Signatory financial institutions that joined at least one of SARB's normative axes.

**FEBRABAN level III signatory parties** — Signatory financial institutions that joined all SARB's normative axes.

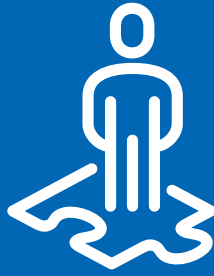
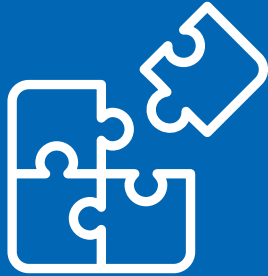
**Information Security** — Preservation of the confidentiality, availability, and integrity of information, as per NBR ISO/IEC 27002 norm.

**Stakeholder** — Interested parties, the so-called groups of interest. They are partners in every segment of society that usually agree with the corporate governance practices performed by institutions, or that take part in defining those practices.

**Terrorism** — Systematic use of acts of terror or unpredictable violence against political regimes, populations, or people, aiming at reaching a political, ideological, or religious end. Resources used for funding terrorism do not necessarily come from criminal activities, which is the prerogative of most money laundering crimes. The operational organization, maintenance, and development of terrorist networks presuppose an activity in continuous evolution, and the simultaneous ongoing search for new and interchangeable methods for obtaining funds and using them via legal and illegal channels, among which are found international commercial corporations, trust funds and offshore companies, stockbrokers, fund transfers via the “hawala” system (via dollar-exchange dealers), or the use of charitable organizations. Financial institutions play a fundamental role in the prevention of and fight against unlawful acts. And the greatest challenge is to identify and repress those increasingly sophisticated operations, and enforce the money laundering, corruption, and terrorism funding prevention policies that were adopted by Conglomerate CCB Brasil, which are in conformity with the legislations, norms, and complementary regulations in force.

**UKBA** — The United Kingdom Bribery Act, which was enacted on July 1st, 2011, is seen as one of the strictest anticorruption laws in the world, and it even punishes corrupt acts in the private sector. Thus, like the main anticorruption laws in action, it also has extraterritoriality, which allows it to be applied not just to British companies performing in local and/or foreign markets, but also to foreign corporations performing in the United Kingdom. It also provides for the punishment of individuals and legal entities that commit any of the crimes described in the legal text.





**CCB**  **中国建设银行**  
China Construction Bank