SmartSuite

Framework / Cybersecurity / Other

BACEN Resolution No. 4,893

Resolution CMN 4,893 requires Brazilian banks to keep a board-approved cybersecurity policy and incident plan and to follow set rules for cloud and data processing contracts.



What it is

Resolution CMN No. 4,893 of February 26, 2021 requires banks and other financial institutions authorized by the Central Bank of Brazil to maintain a board-approved cybersecurity policy and incident response plan, and to follow set rules before contracting cloud and data processing services. It has been in force since July 1, 2021 and replaced Resolutions 4,658 and 4,752.

The National Monetary Council (CMN) issued the Resolution and the Central Bank of Brazil (Banco Central do Brasil, BCB) publishes and supervises it. It does not apply to payment institutions, and since March 1, 2024 not to consortium administrators, securities brokers and dealers, or foreign exchange brokers, which follow BCB Resolution 85 of 2021 (article 1, as amended by CMN Resolution 5,117 of 2024).

At a glance

PUBLISHER
Conselho Monetário Nacional (CMN); supervised by Banco Central do Brasil

TYPE
Regulation

VERSION
Resolution CMN No. 4,893, as amended by CMN Resolutions 5,117 (2024) and 5,274 (December 18, 2025)

EFFECTIVE
July 1, 2021

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Brazil

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893

Why it matters

- **One accountable director** A director must be designated for the cybersecurity policy and for executing the incident response plan, and may hold other roles if there is no conflict of interest (article 7).
- **Board approval and annual review** The board of directors, or the executive board where none exists, approves the policy and the plan, and both are documented and reviewed at least annually (articles 9 and 10).
- **Cloud contracting is regulated** Before contracting relevant cloud or data services, the institution checks the provider's ability to meet legal duties, data access, auditor reports and data segregation (article 12).
- **Regulator access and notice** The BCB must be told of relevant cloud contracts within ten days, and contracts must allow the BCB access to data and documents (articles 15 and 17).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports BACEN Res. 4.893

Policy, Plan and Director Accountability

Record the approved cybersecurity policy, the incident response plan, the designated director and each annual review date (articles 7, 9 and 10).

Article 3 Control Library

Track the fourteen minimum controls against owners, review dates and tests, with a Control record for each (article 3, paragraph 2).

Incident Register and Evidence

Log relevant incidents with cause, impact and effects, and keep supporting files for the five-year availability period (articles 3 and 23).

Penetration and Vulnerability Test Tracking

Schedule the annual independent penetration test and attach results and remediation action plans for the annual report (articles 8 and 22-A).

Cloud Provider Due Diligence

Hold the pre-contract assessment, country and region of processing, ten-day BCB notice date and contract terms for each relevant provider (articles 12 to 17).

Annual Report and Board Reporting

Build a dashboard that assembles the December 31 base-date report inputs for the risk committee and the board's March 31 presentation (article 8).

Common framework mappings

EU DORA | ISO 27001:2022 | ISO 27002:2022 | LGPD | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2 | SWIFT CSCF

Official resources

BACEN Resolution No. 4,893 Full Text

Provides the complete legal text detailing cybersecurity requirements for financial institutions in Brazil.

bcb.gov.br/en/regulation/bacen_resolution_4893_full_text

Banco Central do Brasil Cyber Guidance

Outlines guidelines for implementing cybersecurity measures in line with BACEN Resolution No. 4,893.

bcb.gov.br/en/regulation/cyber_guidance

BACEN Resolution Implementation Guide

Offers guidance on integrating BACEN Resolution No. 4,893 into existing security practices.

bcb.gov.br/en/regulation/implementation_guide

Cybersecurity Risk Management Framework

Defines the framework for managing cybersecurity risks under BACEN regulations.

bcb.gov.br/en/regulation/risk_management_framework

Frequently asked questions

Who must follow Resolution CMN 4,893?

Institutions authorized to operate by the Central Bank of Brazil, such as banks. Payment institutions are outside it, and since March 1, 2024 so are consortium administrators, securities brokers and dealers and foreign exchange brokers, which follow BCB Resolution 85 of 2021 (article 1).

What must the cybersecurity policy and incident response plan contain?

The policy sets security objectives, controls to reduce vulnerability, traceability controls for sensitive information and the handling of relevant incidents, plus guidelines for data classification, service providers and staff awareness (article 3). The plan covers the actions, routines, controls and technology for prevention and response and names the area that records incident effects (article 6).

What is the annual report and who receives it?

The annual report on the incident response plan has a base date of December 31. It covers effectiveness of actions, results of controls, relevant incidents, business continuity test results and penetration and vulnerability test results. It goes to the risk committee, where one exists, and to the board by March 31 of the following year (article 8).

 Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What does the Resolution require before using a cloud provider?

For relevant services the institution assesses service relevance and the provider's ability to meet legal duties, give data access, keep data segregated and provide audit reports. It notifies the Central Bank within ten days of contracting. Providers abroad need an information-exchange agreement between the BCB and the foreign supervisor, or BCB authorization at least sixty days before contracting (articles 12, 15 and 16).

How long must evidence be kept?

The policy, incident response plan, annual report, pre-contract documentation and penetration test results stay available to the Central Bank for five years. Cloud contracts are kept for five years from their end (article 23).

License included / downloadable: Yes The Resolution is a public regulation published by the Central Bank of Brazil and is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/brazil-bacen-resolution-no-4893-cybersecurity-regulation