ManageEngine

Simplify BACEN CMN Resolution 4,893/2021 with ManageEngine IAM and SIEM solutions

BACEN Resolution 4,893/2021 establishes mandatory cybersecurity, incident response, and third-party risk governance requirements for Brazilian banks and financial institutions to protect information assets, ensure operational resilience, and reduce systemic cyber risk across the financial sector.

Achieve BACEN CMN Resolution 4,893/2021 compliance with AD360 + Log360—unified identity governance and access controls, plus real-time threat detection, incident response workflows, and compliance-ready reporting—without added complexity.

Core Principles of BACEN CMN Resolution 4,893/2021

Function	What is it?	Category
Cyber Risk Mitigation Controls – Chapter II, Section I, Art. 3 (II)	Requires institutions to define and implement procedures and controls that reduce exposure to cyber incidents and support overall cybersecurity objectives.	• Cyber Risk Management • Organizational Strategy • Preventive Controls • Security Governance
Information Security & Traceability Controls – Chapter II, Section I, Art. 3 (III)	Mandates specific security controls, including information traceability mechanisms, to protect sensitive and critical information.	• Information Security • Data Protection • Traceability & Auditability • Access Control
Incident Recording & Impact Analysis – Chapter II, Section I, Art. 3 (IV)	Requires maintaining records of relevant cyber incidents along with root-cause analysis, impact assessment, and mitigation tracking.	• Incident Management • Oversight & Monitoring • Risk Analysis • Accountability & Reporting
Cyber Resilience Capability Assessment – Chapter II, Section I, Art. 3 (Para: 1)	Requires cybersecurity objectives to be defined based on the institution's ability to prevent, detect, and reduce cyber vulnerabilities.	• Cyber Resilience • Risk Assessment • Organizational Strategy • Capability Maturity
Baseline Security Control Requirements – Chapter II, Section I, Art. 3 (Para: 2)	Specifies mandatory minimum security controls including authentication, cryptography, intrusion detection, data loss prevention, vulnerability testing, malware protection, access control, network segmentation, traceability, and backups.	• Technical Security Controls • Defense-in-Depth • Access Control & Network Security • Threat Prevention & Detection • Data Protection & Backup
Incident Response & Action Plan – Chapter II, Section III, Art. 6	Requires institutions to establish and maintain an incident response and action plan aligned with the cybersecurity policy.	• Incident Response & Recovery • Governance & Oversight • Operational Readiness • Crisis Management
Third-Party & Cloud Risk Governance – Chapter III, Art. 11	Requires risk management policies to explicitly cover outsourcing decisions, including data processing, data storage, and cloud services, domestically or internationally.	• Supply Chain Risk Management • Third-Party Risk Governance • Cloud & Outsourcing Oversight • Data Residency & Sovereignty • Contractual Risk Controls

How ManageEngine solution helps Brazilian financial institutions stay secure and aligned with CMN Resolution 4,893/2021

ManageEngine Log360

Log360 unifies SIEM, DLP, CASB, and TDIR capabilities with ML-based anomaly detection and rule-based attack detection, delivering centralized visibility, rapid incident response, and audit-ready compliance for organizations operating across on-premises, cloud, and hybrid infrastructures.

- Log correlation and real-time threat detection *[Art. 3 (II)]*
- Tamper-proof audit trails and DLP monitoring *[Art. 3 (III), Art. 3 (Paragraph 2)]*
- Incident management and forensic investigation *[Art. 3 (IV), Art. 6]*
- Ransomware detection and compliance reporting *[Art. 3 (Paragraph 2), Art. 3 (III)]*

Explore Log360

ManageEngine AD360

AD360 is a unified IAM solution that delivers automated identity lifecycle management, access certification, risk assessment, adaptive MFA, secure SSO, approval workflows, UBA-driven identity threat protection, and comprehensive AD, Exchange, and Microsoft 365 audit reporting—all built to strengthen access security and support Zero Trust.

- Automated user provisioning and access reviews [Art. 3 (II), Art. 3 (III)]
- Multi-factor authentication and role-based access [Art. 3 (Paragraph 2)]
- Real-time audit trails and UBA [Art. 3 (III), Art. 3 (IV)]
- Risk exposure management and compliance reporting [Art. 3 (Paragraph 1), Art. 3 (III)]

Explore AD360

Get a personalized demo from our compliance experts and learn how to secure your financial institution while meeting **CMN Resolution 4,893/2021** requirements. **Scan the QR's to book your session.**