TECHNICAL CHECKLIST / CBR CONSULTORIA

Fintech Compliance Checklist

A quick self-assessment guide: the controls regulators and auditors check first at financial institutions.

BACEN 4,893 | LGPD / ANPD | ISO/IEC 27001 | PCI DSS

CBR.Consultoria

Technology & Information Security
2026 Edition

How to use this checklist

A quick, no-nonsense self-assessment

Check what your company already has implemented **and documented** — what "exists in someone's head" doesn't count. At the end, add up the checked items for an honest read of your stage.

Governance | Access | Data | Continuity | Third parties

1 Governance and policy

- [ ] Formal information security policy, approved by leadership.
- [ ] Defined responsibility structure — who owns security, who approves exceptions.
- [ ] Periodic policy review (at least annual), with date and owner on record.
- [ ] Awareness training delivered to all employees, with evidence of participation.

2 Identity and access management

- [ ] Mandatory multi-factor authentication for critical systems and remote access.
- [ ] Periodic permission reviews (who has access to what, and why).
- [ ] Formal offboarding process that revokes access the same day.
- [ ] Least-privilege principle applied — minimum access necessary per role.

3 Personal data and LGPD

- [ ] Up-to-date personal data inventory — where it lives, who accesses it, what it's used for.
- [ ] Documented legal basis for each type of data processing.
- [ ] Incident response process able to notify ANPD within the required deadline.
- [ ] Vendor contracts include data protection clauses.

4 Business continuity

- [ ] Formal business continuity plan (BCP) covering critical systems.
- [ ] BCP test performed in the last 12 months, with a results report.
- [ ] Tested backups — existing isn't enough, you must prove they restore correctly.
- [ ] RTO and RPO defined for each critical system (acceptable recovery time and point).

5 Incident response

- [ ] Documented incident response plan, with clear roles and escalation flow.
- [ ] Incident simulation (tabletop or real) performed in the last year.
- [ ] Notification channel defined for regulators, clients and affected partners.
- [ ] Historical incident log, including low-impact ones, with lessons learned.

6 Third parties and vendor chain

- [ ] Risk assessment applied before contracting vendors with access to critical data or systems.
- [ ] Security contract clauses required from critical vendors, with audit rights.
- [ ] Up-to-date inventory of critical third parties, with a contingency plan if one fails.

Quick read of your result **18 items total**

Up to 8 checked: early stage, prioritize governance and data inventory. 9 to 14: solid foundation, focus on testing what's already on paper. 15 or more: advanced maturity, the next step is formalizing evidence for an external audit.