TECHNICAL PAPER / CBR CONSULTORIA

Security Maturity for Fintechs in 2026

A practical X-ray of the requirements regulators and auditors demand most today — and how to prioritize security investment without stalling operations.

CBR.Consultoria

Technology & Information Security
2026 Edition

01 — Context

Why security maturity became a board-level topic

The regulated financial sector today operates under a volume of requirements growing faster than most internal structures can keep up with. This guide organizes, in practical terms, where to focus effort first.

Fintechs, payment institutions and digital lending platforms share the same challenge: growing fast without leaving gaps that an auditor, a regulator or an attacker could exploit. Pressure comes from several directions at once — Central Bank requirements, LGPD compliance, expectations from partners and investors, and an attack surface that grows with every new product launched.

The most common mistake isn't the absence of controls, but the lack of prioritization: companies spread effort thin across many points and leave gaps exactly where audits and incidents demand most — documented governance, access management and incident response.

3
regulatory fronts generating the most findings in fintechs

3 business days
regulatory deadline for reporting incidents subject to notification to ANPD, subject to specific legislation

01
a documented policy is the item most requested in an initial audit

> This document does not replace legal advice or a formal audit. Its purpose is to provide a structured starting point for prioritizing investment in security and governance.

02 — Regulatory landscape

What each front actually requires

Three fronts account for most of the regulatory scrutiny on technology and security at financial institutions.

Despite different languages, all three essentially require the same thing: living documentation (that reflects the real process, not a generic template), traceability (knowing who accessed what, and when) and proven response capability (having a plan isn't enough — you must show it has actually been tested).

FRONT	WHAT IT REQUIRES IN PRACTICE	WHERE FINTECHS MOST OFTEN FAIL
Central Bank (Res. 4,893)	Formal cybersecurity policy, business continuity plan, relevant incident management and auditable outsourcing contracts.	Policy exists on paper but doesn't reflect the real process; the BCP was never tested.
LGPD / ANPD	Legal basis for each data processing activity, personal data flow mapping, and incident notification within a defined deadline.	No up-to-date data inventory; nobody knows exactly where personal data flows.
ISO 27001 / PCI DSS	An information security management system with a defined scope, risk-mapped controls and evidence of continuous operation.	Controls implemented in isolation, with no periodic review process or formal owner.

The common pattern across the three fronts

Security policy · Access management · Business continuity · Incident response · Third-party management

03 — Maturity model

Four stages of security maturity

Use this model to identify what stage your operation is at today and what changes at the next level.

Stage 1 — Reactive

Security handled case by case, with no formal policy. Decisions depend on one or two people. There's no systematic incident record.

Stage 2 — Documented

Policies and processes exist in writing, but real adherence varies. Audits find gaps between what's on paper and what actually happens.

Stage 3 — Managed

Processes are followed consistently, with defined indicators and owners. The company can demonstrate control evidence to an external auditor.

Stage 4 — Optimized

Security is part of the development cycle and business decisions. Risk metrics feed board decisions. Incident response is tested periodically.

> Most fast-growing fintechs sit between stages 1 and 2 — enough to operate, but not enough to withstand an in-depth audit or a real incident without reputational damage.

04 — Prioritization

Where to start when the budget is limited

Not every fintech has the budget to tackle everything at once. This is the order that tends to generate the most risk reduction per dollar invested.

- [ ] **Data and access inventory.** Without knowing where personal and financial data lives and who accesses it, no subsequent control is reliable.
- [ ] **Documented security policy approved by leadership.** It's the first item any auditor asks for, and the foundation for everything else.
- [ ] **Identity and access management (IAM).** Strong authentication, periodic permission reviews and agile access deprovisioning.
- [ ] **Tested incident response plan.** Having the document isn't enough — you need to simulate an incident and measure actual response time.
- [ ] **Critical vendor and third-party management.** A large share of fintech incidents enter through the supply chain, not through the company's own perimeter.
- [ ] **Business continuity.** A formal plan, with periodic testing, for systems that cannot go down.

Signs it’s time to act

An audit or partner asked for evidence the company didn't have ready; team growth made informal access control unsustainable; a small incident revealed the absence of a response process.

What not to do

Buying a tool before mapping the process; copying another company's policy without adapting it to actual operations; treating security as an IT project isolated from the business.

05 — About this material

Who prepared this document

CBR Consultoria structures, operates and protects technology environments for fintechs and highly regulated businesses — with project management, specialist staffing and incident response, in Brazil and abroad.

CA

Claudio Araujo

Executive Director at CBR Consultoria. More than 31 years of career in Technology and Information Security, working in governance, risk management and regulatory compliance for the financial sector.

Want to apply this model to your operation?

Schedule a free, no-obligation assessment with one of our specialists.