

Build fast. Ship secure. Pass every diligence.

API security, cloud assessment, DevSecOps, TPRM, fraud simulations and regulatory readiness for fintechs.

Three questions every fintech leadership team should be able to answer

Would every API pass an object-level authorisation test today?

Broken authorisation is the leading API risk—and the most common cause of large fintech data exposures.

Could we hand a bank partner a security evidence pack tomorrow?

Banks and NBFCs must oversee fintech partners under RBI's outsourcing and digital lending rules.

Are we ready for DPDP consent and breach duties?

Most DPDP Rules obligations, including breach intimation, take effect in May 2027.

500 mn+

AA consents fulfilled
(Sahamati, Sept 2026)

6 hours

Specified incidents to
CERT-In

180 days

ICT log retention in India

May 2027

Most DPDP obligations
take effect

Built for every fintech model

Lending technology firms and LSPs · Account Aggregators · embedded finance platforms · BaaS and financial API providers · P2P lending platforms · KYC and identity providers · wealthtech and insurtech apps · fintech SaaS vendors.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
RBI Digital Lending Directions (2025)	LSP and DLA obligations; borrower-data restrictions; lender accountability for partners
RBI 2026 NBFC cyber Directions (Jul 2026)	Layer-based requirements for licensed NBFC-AAAs and NBFC-P2Ps; 6-hour reporting
CERT-In · DPDP · partner contracts	6-hour reporting, 180-day logs, consent and privacy safeguards, partner audit rights

WHAT WE DO

API security, cloud, DevSecOps, TPRM, fraud simulation and readiness

API & AppSec

REST, GraphQL, webhook, mobile app and SDK testing; business-logic and authorisation testing.

Cloud Assessment

AWS, Azure and GCP posture, Kubernetes and serverless testing, IAM and secrets reviews.

DevSecOps

SAST, DAST, SCA and secrets scanning in CI/CD; secure code review and threat modelling.

Third-Party Risk

Vendor and SDK assessments, partner questionnaire support, continuous vendor monitoring.

Fraud Simulations

Synthetic identity, deepfake KYC, account takeover and business-logic abuse testing.

Regulatory Readiness

Digital lending alignment, NBFC-AA/P2P cyber readiness, ISO 27001, SOC 2 and DPDPA.

Choose your starting point

Foundation

Pre-launch API and app VAPT, cloud quick review, ISO 27001 / SOC 2 gap review, partner pack. For seed and early-stage fintechs.

Assurance

Release-based testing, DevSecOps and secrets scanning, DPDPA and TPRM, extended-hours SOC. For growth-stage fintechs and NBFC-AAs.

Continuous Resilience

Continuous testing and red teaming, continuous cloud assurance, 24x7 SOC with fraud correlation, Board reporting. For scale-ups.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NICSI for application audit services.

Certified

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped

Every finding mapped to digital lending rules, partners' RBI obligations, CERT-In, DPDP and SOC 2 / ISO 27001.

One connected partner

Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your product, partners, cloud stack and diligence deadlines. We will propose a partner-ready assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220

Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Statistics: Sahamati press release (September 2026); CERT-In Directions; DPDP Rules 2025.