

BANKING CYBERSECURITY

Inspection-ready. Attack-ready. Every day.

Regulatory assurance, VAPT, 24/7 SOC and resilience for commercial, small finance, payments and co-operative banks.

Three questions every bank's leadership should be able to answer

Can we report a cyber incident to RBI within six hours?

RBI's 2026 Directions require reporting on DAKSH within six hours of detection; CERT-In has a parallel 6-hour rule.

Are our critical systems tested as often as RBI expects?

Critical and customer-facing DMZ systems need VA at least every six months and PT at least annually.

Would we spot a mule account or ATM switch attack in time?

RBI expects risk-based transaction monitoring across channels and baseline controls for ATM switch providers.

₹48,021 cr

Frauds reported by banks and FIs in FY26 (RBI)

6 hours

Cyber incident reporting to RBI on DAKSH

Half-yearly

DR drills for critical systems

1 Jan 2027

Revised customer-protection framework applies

Built for every type of bank

Public sector banks · private sector banks · foreign bank branches · small finance banks · payments banks · urban co-operative banks · state and district central co-operative banks · regional rural banks · banking technology providers.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
RBI 2026 Cybersecurity & Technology Risk Directions (Jul 2026)	ITSC and CISO governance, CSOC, six-monthly VA, annual PT, half-yearly DR drills, 6-hour DAKSH reporting
RBI Outsourcing and Authentication Directions (2025)	Vendor and ATM switch oversight; two-factor authentication with a dynamic factor
CERT-In · DPDP · PCI DSS · SWIFT CSP	6-hour CERT-In reporting, 180-day logs in India, privacy safeguards, card and SWIFT controls

Regulatory assurance, VAPT, SOC and resilience

Regulatory Assurance

Gap assessments against RBI's 2026 Directions, IS audit support, PCI DSS, SWIFT CSP and ISO 27001 readiness, Board and ITSC packs.

VAPT & AppSec

Six-monthly VA and annual PT of critical systems; internet, mobile banking and API testing; secure code review.

24/7 Cyber SOC

CSOC with L1-L3 analysts, SIEM, EDR/XDR, SOAR, fraud-signal correlation, anti-phishing and rogue-app monitoring.

Cyber Resilience

Ransomware readiness, backup testing, DR drill observation, Cyber Crisis Management Plan and tabletop drills.

Forensics & Response

Incident triage, evidence preservation, fraud and insider investigations, 6-hour reporting support and RCA.

Third-Party & Privacy

ATM switch, cloud, vendor and fintech partner assessments; DPDPA readiness and DLP.

Choose your starting point

Foundation

Scoped VAPT and retest, gap review against RBI directions, DR readiness check and roadmap. For co-operative banks and banks building a baseline.

Assurance

Six-monthly VA and annual PT, digital channel and API testing, regulatory evidence pack, extended-hours SOC. For mid-sized banks, SFBs and payments banks.

Continuous Resilience

Continuous testing and red teaming, third-party and ATM switch assurance, 24x7 CSOC, Board reporting. For large public and private sector banks.

Why Codec Networks

CERT-In empanelled

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

Certified

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

Regulation-mapped

Every finding mapped to RBI's 2026 Directions, outsourcing rules, CERT-In, DPDP, PCI DSS and SWIFT CSP.

One connected partner

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

Book a scoping session

Share your bank category, critical systems and inspection or audit deadlines. We will propose a regulation-mapped 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: RBI Annual Report 2025-26 (frauds of ₹1 lakh and above, as reported).