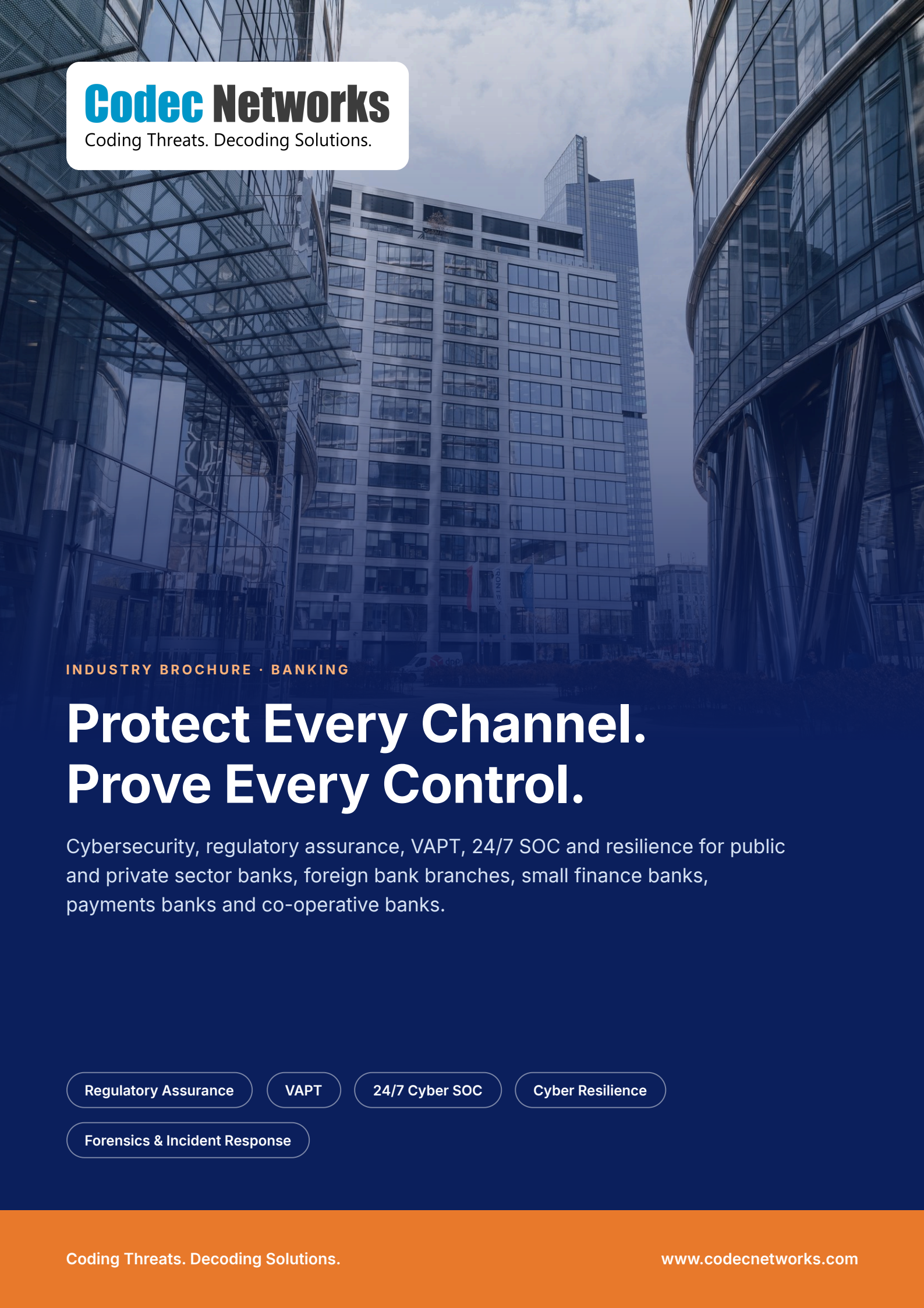




Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · BANKING

Protect Every Channel. Prove Every Control.

Cybersecurity, regulatory assurance, VAPT, 24/7 SOC and resilience for public and private sector banks, foreign bank branches, small finance banks, payments banks and co-operative banks.

Regulatory Assurance

VAPT

24/7 Cyber SOC

Cyber Resilience

Forensics & Incident Response

Coding Threats. Decoding Solutions.

www.codecnetworks.com

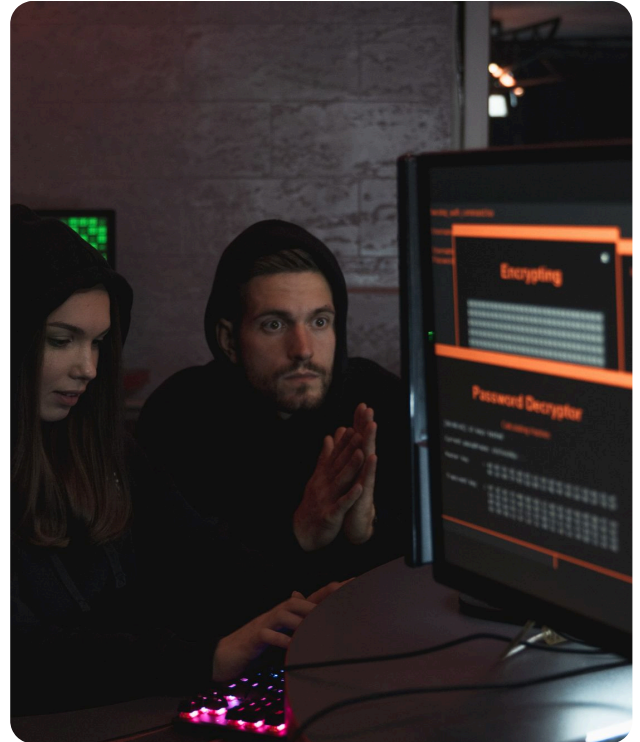
THE CHALLENGE

Banking runs on trust. Attackers know it.

Banks now operate interconnected digital channels, payment rails, partner APIs and legacy core systems—under a new RBI cybersecurity rulebook that took effect in July 2026.

What keeps leadership teams awake

- Account takeover, mule accounts and social-engineering fraud
- Ransomware that halts branches and digital channels
- Third-party and ATM switch provider compromise
- Fintech and co-lending API exposure
- Reporting cyber incidents to RBI within six hours
- Six-monthly VA, annual PT and half-yearly DR drills



₹48,021 cr

Frauds reported by banks and FIs in FY26 (RBI Annual Report)

6 hours

To report cyber incidents to RBI on DAKSH

6-monthly

Vulnerability assessment of critical systems

31 Jul 2026

RBI's new cybersecurity Directions for banks

The rulebook has changed

Instrument	What it means for you
RBI Commercial Banks – Cybersecurity, Technology: Risk, Resilience and Assurance Framework Directions (31 Jul 2026)	ITSC and CISO governance, CSOC, VA every six months and PT annually, half-yearly DR drills, 6-hour DAKSH reporting
Matching 2026 Directions for SFBs, payments banks and UCBs (31 Jul 2026)	Equivalent requirements, with graded levels for urban co-operative banks
RBI Managing Risks in Outsourcing Directions and Authentication Directions (2025)	Vendor oversight, audit and RBI access rights; two-factor authentication with a dynamic factor
CERT-In Directions · DPDP Act & Rules · PCI DSS · SWIFT CSP	6-hour CERT-In reporting, 180-day logs, privacy safeguards, payment-card and SWIFT controls

One partner across every banking channel

Built around our primary proposition for the sector: **regulatory assurance, VAPT, SOC and resilience.**

Regulatory Assurance

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

VAPT & Application Security

- Six-monthly VA and annual PT of critical systems
- Internet, mobile banking and API testing
- Source code review and secure SDLC
- Retesting and closure validation

24/7 Cyber SOC

- CSOC with Level 1–3 analysts
- SIEM, EDR/XDR, SOAR and threat hunting
- Fraud-signal and mule-account correlation
- Anti-phishing and rogue-app monitoring

Cyber Resilience

- Ransomware readiness and backup testing
- DR drill observation and BCP reviews
- Cyber Crisis Management Plan
- Tabletop and crisis-communication drills

Forensics & Incident Response

- Incident triage and evidence preservation
- 6-hour DAKSH and CERT-In reporting support
- Fraud, insider and malware investigations
- Root-cause analysis for regulators

Third-Party & Privacy

- ATM switch, cloud and vendor assessments
- Fintech and co-lending partner reviews
- DPDPA readiness and DLP
- Customer data-flow mapping

Who we serve: 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.

Packaged for how banks actually buy

Eleven Codec Networks bundles apply directly to banks:

B1 Cyber Assessment & VAPT Assurance	B2 Application, API & DevSecOps Security	B3 Cloud, Infrastructure & Zero Trust
B4 Regulatory Cyber Audit & Compliance	B5 GRC, ISO, SOC 2 & PCI DSS Maturity	B6 Data Privacy & DPDPA Program
B7 Managed SOC, MDR & Threat Monitoring	B8 Forensics, Incident Response & Malware RCA	B9 Third-Party & Supply-Chain Risk
B10 Cyber Simulation, Awareness & Tabletop	B11 Emerging Tech, AI & Web3 Security	

Foundation

Co-operative banks, smaller SFBs and banks building a baseline

- Scoped infrastructure VAPT and retest
- Gap review against applicable RBI directions
- Backup and DR readiness check
- Risk register and roadmap

Assurance

Mid-sized private banks, SFBs and payments banks

- Six-monthly VA and annual PT of critical systems
- Internet, mobile banking and API testing
- Regulatory gap assessment and evidence pack
- Extended-hours SOC + IR retainer

Continuous Resilience

Large public and private sector banks

- Continuous testing, red teaming and simulations
- Third-party, ATM switch and cloud assurance
- 24x7 CSOC with L1-L3 coverage
- Quarterly Board, RMC and ITSC reporting

Mapped to your obligations

Requirement	How we help	Bundle
VA at least six-monthly and PT at least annually for critical and customer-facing DMZ systems (RBI 2026 Directions)	Scheduled VA/PT by independent experts, with retest	B1
Application security testing across the lifecycle; source code or escrow for critical applications	Secure code review, application and API testing	B2
CSOC with 24x7 Level 1 monitoring; anti-phishing and anti-rogue-app services	Managed CSOC and brand monitoring	B7
Cyber incidents reported to RBI on DAKSH within 6 hours; CERT-In notified	IR retainer, playbooks and reporting support	B7, B8
DR drills for critical systems at least half-yearly; BCP/DR reviewed annually by the ITSC	DR drill observation, ransomware simulation	B1, B10
Baseline controls for ATM switch providers and third-party IT arrangements	Third-party and ATM switch provider assessments	B9
DLP, data governance and DPDP safeguards	DPDPA programme, data-flow mapping, DLP review	B6

Why banks choose Codec Networks

CERT-In empanelled

Empanelled for information security auditing services; NISCI empanelled for application audit services.

Certified and accountable

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

Mapped to the 2026 Directions

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

Tests the chain, not the link

Technical, process and monitoring tests together—because real attacks combine several weaknesses.

Full stack, one partner

VAPT, audits, CSOC, forensics, privacy and Board advisory stay connected from finding to closure.

Banking-grade expertise

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI and cloud specialists using OWASP, MITRE ATT&CK and NIST CSF.

How we engage

Discover & scope

Bank category, channels, critical systems, third parties and your audit calendar.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next inspection, launch and incident a non-event.

Tell us your bank category, critical systems and deadlines. We will propose a practical, regulation-mapped assessment and assurance plan.

New Delhi

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

Gurugram

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

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003 31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. 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).