

Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · CAPITAL MARKETS & SECURITIES

Protect the Market. Prove Your Resilience.

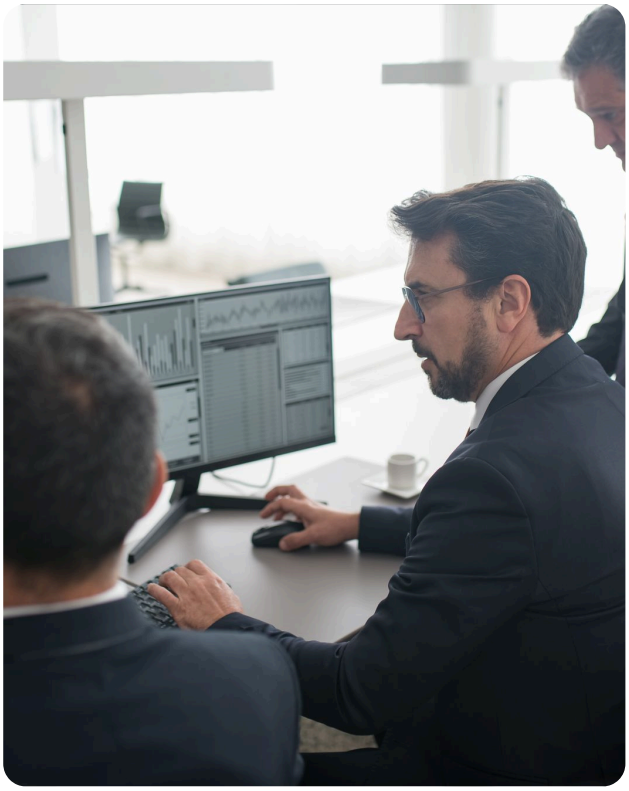
SEBI CSCRF cyber resilience, system audits, trading platform security, cloud audits and 24/7 SOC for exchanges, clearing corporations, depositories, brokers, depository participants and professional clearing members.

- SEBI CSCRF Cyber Resilience
- System Audits
- Trading Platform Security
- Cloud Audits
- 24/7 SOC

THE CHALLENGE

Markets move in milliseconds. So do attackers.

India's securities market now serves crores of investors through apps and APIs—under SEBI's Cybersecurity and Cyber Resilience Framework, which applies to most regulated entities from August 2025.



What keeps leadership teams awake

- Trading account takeover and fake investment apps
- DDoS and outages during market hours
- Ransomware at brokers, DPs and RTAs
- Unauthorised transfers and pledges from demat accounts
- Twice-yearly cyber audits and VAPT by CERT-In empanelled auditors
- Reporting incidents to SEBI and CERT-In within six hours

18.59 cr
Demat accounts at CDSL (30 June 2026)

5
Regulated-entity categories under SEBI CSCRF

6 hours
To report cyber incidents to SEBI and CERT-In

31 Aug 2025
CSCRF compliance date for most REs

The rulebook has changed

Instrument	What it means for you
SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) (20 Aug 2024)	Graded requirements for MIIs, Qualified, Mid-size, Small-size and Self-certification REs; cyber audits and VAPT by CERT-In empanelled auditors; SOC or Market SOC; 6-hour reporting
CSCRF extensions and technical clarifications (2025)	Compliance by 1 Jan 2025 for MIIs, KRAs and QRTAs, and 31 Aug 2025 for other REs; revised thresholds and clarifications
SEBI cloud framework and system audit circulars (2019–2024)	Cloud governance and shared responsibility; system and PCM audits
CERT-In Directions · DPDP Act & Rules	6-hour CERT-In reporting, 180-day logs in India, investor data safeguards and breach duties

OUR SERVICE OFFERINGS

One partner across the trade lifecycle

Built around our primary proposition for the sector: **SEBI cyber resilience, system audits, trading platform security, cloud audits and SOC.**

SEBI CSCRF Compliance

- RE categorisation and gap assessment
- Cyber audits by a CERT-In empanelled auditor
- Cyber Capability Index support
- Board and IT committee reporting

System & PCM Audits

- System audits under SEBI circulars
- Professional clearing member audits
- Findings closure and revalidation
- Evidence packs for SEBI and MIIs

Trading Platform Security

- Trading app, web and API testing
- Algo and OMS/RMS security review
- VAPT with retest and revalidation
- Business-logic and order-flow testing

Cloud Audits

- Assessment against SEBI's cloud framework
- Cloud posture and IAM reviews
- Data protection and exit readiness
- Continuous cloud assurance

24/7 SOC & Response

- Managed SOC or M-SOC readiness
- SOC efficacy measurement
- Threat hunting and red teaming
- 6-hour SEBI and CERT-In reporting support

Investor Data & Privacy

- KYC and investor data mapping
- DPDPA readiness and DLP
- Vendor and RTA data-sharing reviews
- Breach response workflow

Who we serve: stock exchanges · clearing corporations · depositories · stock brokers and trading platforms · depository participants · professional clearing members · custodians · KYC registration agencies · registrars to an issue and share transfer agents · market technology vendors.

BUNDLED SERVICE MODELS

Packaged by CSCRF category

Eleven Codec Networks bundles apply directly to capital market entities:

- **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

Small-size and self-certification REs

- CSCRF categorisation and gap review
- Annual VAPT and cyber audit
- M-SOC onboarding readiness
- Policy pack and roadmap

Assurance

Mid-size REs and growing brokers

- Annual (or half-yearly) cyber audit
- Trading app and API testing
- 24x7 managed SOC
- Cloud framework assessment

Continuous Resilience

MIIs and Qualified REs

- Half-yearly cyber audits and VAPT
- Red teaming and threat hunting
- SOC efficacy and Cyber Capability Index
- Board and IT committee reporting

Mapped to your obligations

Requirement	How we help	Bundle
CSCRF: cyber audit by a CERT-In empanelled auditor—twice a year for MIIs and Qualified REs; annual for most others	CSCRF cyber audit with closure tracking	B4
CSCRF: VAPT by a CERT-In empanelled auditor, with time-bound closure and revalidation	Scheduled VAPT with retest	B1
CSCRF: 24x7 SOC for MIIs, Qualified and Mid-size REs; M-SOC onboarding for smaller REs	Managed SOC and M-SOC readiness	B7
Cyber incidents reported to SEBI and CERT-In within six hours	IR retainer, playbooks, reporting support	B7, B8
SEBI cloud framework: governance, shared responsibility, exit readiness	Cloud framework assessment	B3
System audits and PCM audit framework	System audit and closure validation	B4
DPDP safeguards and breach intimation (from May 2027)	DPDPA programme and breach drills	B6

THE CODEC NETWORKS VALUE ADD

Why market participants choose Codec Networks

CERT-In empanelled

Meets CSCRF's requirement that cyber audits and VAPT be performed by CERT-In empanelled auditing organisations.

Certified and accountable

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

CSCRF-native

Every finding mapped to the CSCRF category, control and timeline that applies to your entity.

Trading-platform depth

Testing of trading apps, APIs, OMS/RMS and algo platforms, including order-flow logic.

Full stack, one partner

Audits, VAPT, SOC, forensics, cloud and privacy connected from finding to closure.

Certified experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI and CHFI professionals using NIST CSF 2.0 and MITRE ATT&CK.

How we engage

Discover & scope

SEBI registrations, CSCRF category, trading channels, critical systems 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 audit, expiry day and incident a non-event.

Tell us your registrations, CSCRF category and deadlines. We will propose a practical, CSCRF-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: CDSL press release (August 2026); SEBI CSCRF circular (20 August 2024) and extensions.