

CSCRF-ready. Market-ready. Every day.

SEBI cyber resilience, system audits, trading platform security, cloud audits and SOC for capital market entities.

Three questions every market participant should be able to answer

Which CSCRF category are we in, and are we compliant?

Requirements differ for MIs, Qualified, Mid-size, Small-size and Self-certification REs.

Are our cyber audits and VAPT done by a CERT-In empanelled auditor?

CSCRF requires CERT-In empanelled auditing organisations for cyber audits and VAPT.

Could we report an incident to SEBI within six hours?

CSCRF and CERT-In both set a 6-hour reporting window.

18.59 cr

Demat accounts at CDSL
(June 2026)

6 hours

Incident reporting to SEBI
and CERT-In

Twice a year

Cyber audits for MIs and
Qualified REs

May 2027

Most DPDP obligations
take effect

Built for every market participant

Stock exchanges · clearing corporations · depositories · stock brokers and trading platforms · depository participants · professional clearing members · custodians · KRAs · RTAs · market technology vendors.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
SEBI CSCRF (Aug 2024; clarifications 2025)	Graded controls by RE category; CERT-In empanelled cyber audits and VAPT; SOC or M-SOC; 6-hour reporting
SEBI cloud framework and system audits	Cloud governance and shared responsibility; system and PCM audits
CERT-In · DPDP	6-hour CERT-In reporting, 180-day logs, investor data safeguards

WHAT WE DO

SEBI cyber resilience, audits, platform security, cloud and SOC

SEBI CSCRf Compliance

Categorisation, gap assessment, CERT-In empanelled cyber audits, Cyber Capability Index support.

System & PCM Audits

System audits under SEBI circulars, PCM audits, findings closure and revalidation.

Trading Platform Security

Trading app, web, API, OMS/RMS and algo platform testing; VAPT with retest.

Cloud Audits

Assessment against SEBI's cloud framework, posture and IAM reviews, exit readiness.

24/7 SOC & Response

Managed SOC, M-SOC readiness, SOC efficacy, threat hunting, 6-hour reporting support.

Investor Data & Privacy

KYC data mapping, DPDPA readiness, DLP and vendor data-sharing reviews.

Choose your starting point

Foundation

CSCRf categorisation and gap review, annual VAPT and cyber audit, M-SOC readiness, policy pack. For Small-size and Self-certification REs.

Assurance

Annual or half-yearly cyber audit, trading app and API testing, 24x7 managed SOC, cloud framework assessment. For Mid-size REs.

Continuous Resilience

Half-yearly audits and VAPT, red teaming, SOC efficacy and Cyber Capability Index, Board reporting. For MIIIs and Qualified REs.

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 the CSCRf category, control and timeline that applies to your entity, plus CERT-In and DPDP.

One connected partner

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

Book a scoping session

Share your SEBI registrations, CSCRf category and audit deadlines. We will propose a CSCRf-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: CDSL press release (August 2026); SEBI CSCRf circular (20 August 2024) and extensions.