

Codec Networks

Coding Threats. Decoding Solutions.

CAPITAL MARKETS & SECURITIES

Protect the Market. Prove Your Resilience.

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

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

SEBI CSCRF, cloud framework and system audits



How Codec Networks helps

Services, bundles and packages built for the sector



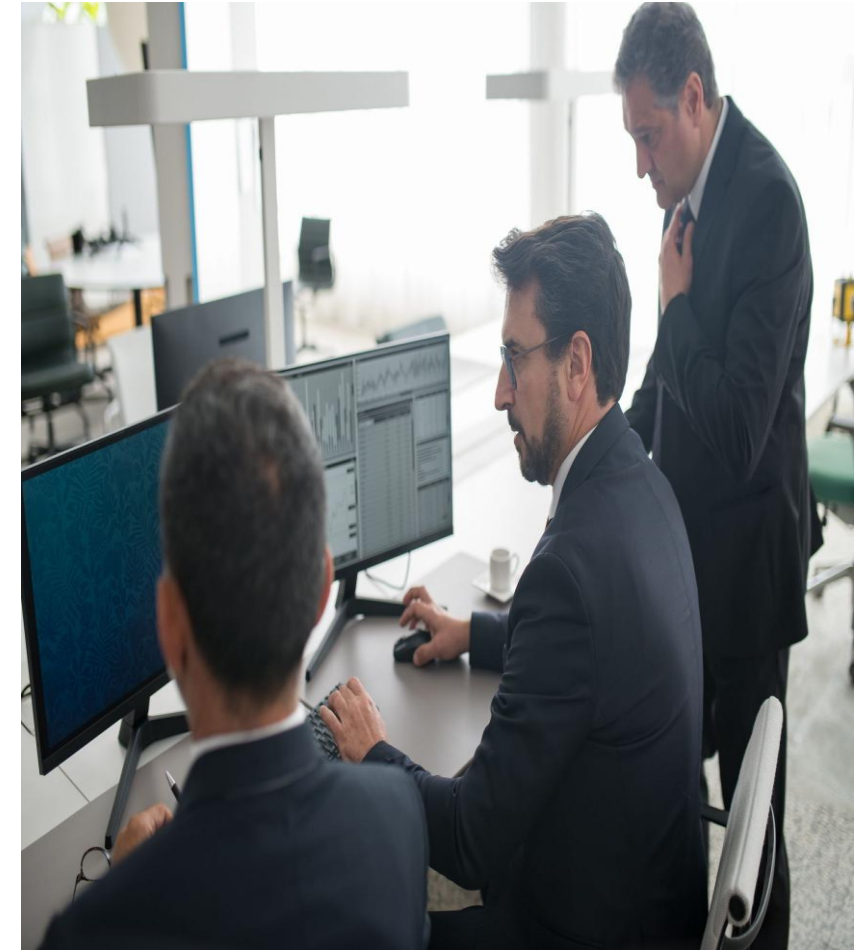
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



A digital market at investor scale

Crores of investors, millisecond trading, one supervisory framework

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

What this means: every SEBI regulated entity must now know its CSCRF category, run CERT-In empanelled audits and VAPT on the prescribed cycle, and be able to detect and report incidents within six hours.

Sources: CDSL press release (August 2026); SEBI CSCRF circular (20 August 2024) and 2025 extensions and clarifications.

Who we serve across capital markets



Stock exchanges

Trading venues and Market SOC operators



Clearing corporations

Clearing, risk and settlement



Depositories

Securities held in demat form



Stock brokers

Trading apps, APIs and algo platforms



Depository participants

Demat account servicing



Professional clearing members

Clearing for trading members



Custodians & KRAs

Custody and KYC registration



RTAs

Investor records and corporate actions

The threats that cost market participants the most

Six priorities from our 18-threat capital markets assessment



Trading account takeover

Phished credentials used to trade and launder money



DDoS & outages

Platforms unavailable during market hours



Algo & API abuse

Faulty or malicious order flows



Ransomware

Brokers, DPs and RTAs encrypted and extorted



Unauthorised transfers

Back-office misuse of demat accounts and pledges



Slow detection & reporting

Missing the 6-hour SEBI and CERT-In window

Attacks target every stage of the trade lifecycle

Where Cyber Risk Sits in the Trade Lifecycle

Each stage of a securities transaction has its own attack surface



Market integrity depends on every link—an intermediary's breach can become a market-wide event.

Source: Codec Networks analysis

What regulators now expect

SEBI's CSCRF applies to most regulated entities from 31 August 2025

The CSCRf rulebook—and the calendar it sets

Requirement	Frequency / deadline	Source
CSCRf compliance date: MIIs, KRAs, QRTAs	1 January 2025	SEBI CSCRf and extensions
CSCRf compliance date: all other REs	31 August 2025	SEBI circular CIR/2025/96
Cyber audit by CERT-In empanelled auditor	Twice a year (MII, QRE); annual (most others)	SEBI CSCRf
VAPT by CERT-In empanelled auditor	Per category; time-bound closure	SEBI CSCRf
24x7 SOC / Market SOC onboarding	Ongoing, by category	SEBI CSCRf
Cyber incident reporting	Within 6 hours	SEBI CSCRf; CERT-In
Cloud governance and shared responsibility	Ongoing	SEBI cloud framework (Mar 2023)
DPDP safeguards and breach intimation	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for Capital Markets Cybersecurity

Key SEBI and cross-sector instruments shaping cybersecurity in the securities market

● In force ● Upcoming (from Oct 2026)

Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Mar 2023	● SEBI framework for adoption of cloud services by regulated entities
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Jun 2024	● SEBI system audit framework for professional clearing members
Aug 2024	● SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) issued
Jan 2025	● CSCRF compliance date for MIs, KRAs and QRTAs
Apr 2025	● SEBI revises CSCRF categorisation thresholds
Aug 2025	● CSCRF compliance date for all other REs; technical clarifications issued
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: SEBI circulars, CERT-In, MeitY. Applicability depends on RE category.

How Codec Networks helps

CSCRF · System audits · Platform security · Cloud audits · SOC

One partner across the trade lifecycle



SEBI CSCR Compliance

Categorisation, gap assessment, CERT-In empanelled cyber audits



System & PCM Audits

System audits, PCM audits, closure and revalidation



Trading Platform Security

Trading apps, APIs, OMS/RMS and algo platforms



Cloud Audits

SEBI cloud framework, posture and IAM



24/7 SOC & Response

Managed SOC, M-SOC readiness, threat hunting



Investor Data & Privacy

KYC data, DPDPA readiness, DLP

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Small-size and self-certification REs

- CSCRF gap review (B4)
- Annual VAPT and cyber audit (B1, B4)
- M-SOC onboarding readiness (B7)
- Policy pack and roadmap (B5)

Assurance

Mid-size REs and growing brokers

- Cyber audit (B4)
- Trading app and API testing (B2)
- 24x7 managed SOC (B7)
- Cloud framework assessment (B3)

Continuous Resilience

MIIs and Qualified REs

- Half-yearly audits and VAPT (B1, B4)
- Red teaming and threat hunting (B10, B7)
- SOC efficacy and CCI support (B5)
- Board and IT committee reporting

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
CSCRF: cyber audit by a CERT-In empanelled auditor—twice a year for MIIIs 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 MIIIs, 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

Five new case studies, five broken chains

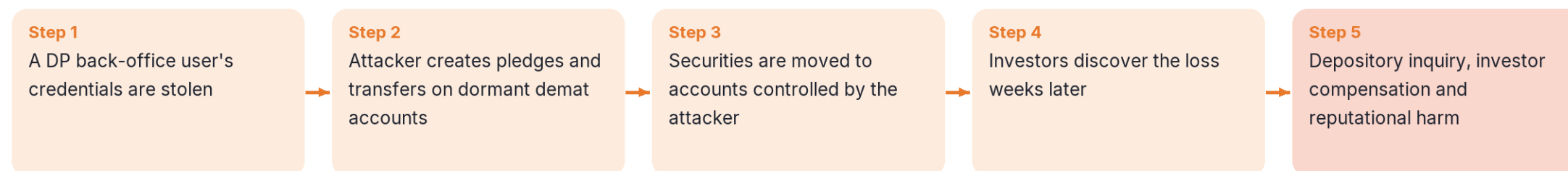
Illustrative composite scenarios written for 2026—not client engagements

1	The Trading Account That Traded Itself	Phished investor accounts move money through illiquid trades; device binding and surveillance stop it	B2 · B7 · B10
2	The Algo That Went Rogue	A faulty vendor algo floods the exchange; SDLC, risk limits and kill-switch tests prevent it	B2 · B9 · B7
3	Ransomware at the RTA	Investor records stolen before a record date; segmentation, backups and playbooks limit the damage	B7 · B10 · B8
4	The Pledge That Was Never Authorised	Stolen DP back-office credentials move securities; MFA, maker-checker and alerts break the chain	B3 · B7 · B4
5	The Cloud Bucket of KYC Records	A public bucket exposes KYC files; cloud framework reviews and posture monitoring prevent it	B3 · B6 · B8

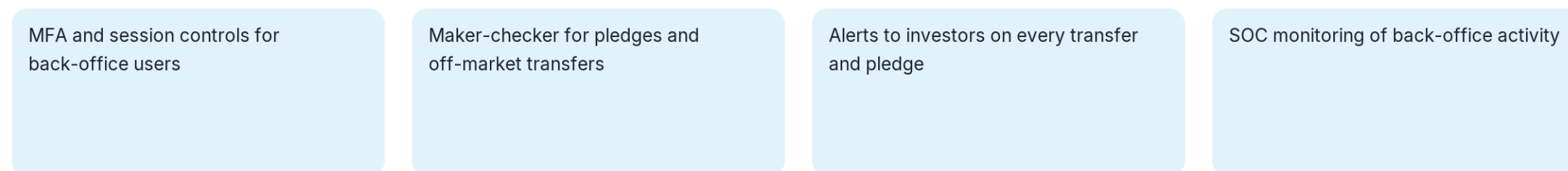
Example: breaking an unauthorised-pledge chain

Case 4: The Pledge That Was Never Authorised

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: MFA and session controls for DP back-office users, maker-checker for pledges and off-market transfers, investor alerts on every movement and SOC monitoring of back-office activity.

Why market participants choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

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



Regulation-mapped

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



Tests the whole chain

Technical, process and monitoring tests together



Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected



Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

SEBI registrations, CSCRF category, trading channels and your audit calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

 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

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

 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.