Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · ASSET & INVESTMENT MANAGEMENT

Protect Investor Trust. Prove Cyber Resilience.

System audits, SEBI cyber resilience, investor data protection, application security and BCP/DR for mutual funds, AMCs, portfolio managers, AIFs, investment advisers and wealth platforms.

System Audits | SEBI CSCRF Cyber Resilience | Investor Data Protection | Application Security | BCP/DR

THE CHALLENGE

Investors trust you with their savings. Attackers want them too.

India's mutual fund industry manages over ₹82 lakh crore across nearly 28 crore folios—and SEBI's CSCRF now applies graded cybersecurity requirements to AMCs, portfolio managers and AIF managers.

What keeps leadership teams awake

- Redemption fraud and bank-detail changes
- Front-running and leakage of order information
- Investor data leaking through RTAs, distributors and apps
- Ransomware at the AMC, RTA or fund accountant
- Deepfake fund managers and fake investment groups
- CSCRF audits, VAPT and 6-hour incident reporting

₹82 lakh cr+
Mutual fund industry AUM (AMFI, June 2026)

27.86 cr
Mutual fund folios (June 2026)

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

31 Aug 2025
CSCRF compliance date for AMCs and other REs

The rulebook has changed

Instrument	What it means for you
SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) (20 Aug 2024)	Graded by category (AMCs by AUM; PMs and AIF managers by size); CERT-In empanelled cyber audits and VAPT; SOC or Market SOC; 6-hour reporting
SEBI system audit framework for mutual funds (2019)	Periodic system audits of AMC systems and processes, interfaces and controls
SEBI cloud framework (Mar 2023)	Cloud governance, shared responsibility, data security and exit readiness
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 investment lifecycle

Built around our primary proposition for the sector: **system audits, cyber resilience, investor data protection, application security and BCP/DR.**

System Audits & CSCRF

- MF and AMC system audits
- CSCRF categorisation and gap assessment
- CERT-In empanelled cyber audits
- Trustee and Board reporting

Investor Data Protection

- Investor data mapping across RTA and distributors
- DPDPA readiness and consent review
- DLP and access controls
- Breach response workflow

Application Security

- Investor app and portal testing
- Distributor and platform API testing
- Redemption and bank-change flow testing
- Secure SDLC

BCP/DR & Resilience

- BCP and DR reviews and drills
- Ransomware readiness and backup testing
- Recovery objective validation
- Crisis communication exercises

24/7 SOC & Insider Monitoring

- Managed SOC or M-SOC readiness
- Dealing-room and insider monitoring
- Fraud and redemption anomaly detection
- 6-hour reporting support

Third-Party Assurance

- RTA, custodian and fund accountant reviews
- Pricing and data vendor assessments
- Distributor platform assurance
- Cloud provider assessments

Who we serve: asset management companies and mutual funds · portfolio managers · AIF managers · investment advisers and research analysts · wealth and investment platforms · RTAs, custodians and fund accountants serving the industry.

BUNDLED SERVICE MODELS

Packaged by size and CSCRF category

Eleven Codec Networks bundles apply directly to asset and investment managers:

- **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

Advisers, small PMS and AIF managers

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

Assurance

Mid-sized AMCs, PMS and wealth platforms

- CSCRF cyber audit and VAPT
- Investor app and API testing
- 24x7 managed SOC
- BCP/DR and cloud review

Continuous Resilience

Large AMCs (Qualified REs)

- Frequent cyber audits and VAPT
- Red teaming and insider monitoring
- Third-party and RTA assurance
- Board and trustee reporting

Mapped to your obligations

Requirement	How we help	Bundle
CSCRF: cyber audit and VAPT by CERT-In empanelled auditors, frequency by category	CSCRF cyber audit and VAPT with closure	B4, B1
SEBI system audit framework for mutual funds and AMCs	MF system audit and closure validation	B4
CSCRF: SOC for larger REs; Market 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 (March 2023)	Cloud framework assessment	B3
Third-party oversight of RTAs, custodians and vendors	Third-party assurance programme	B9
DPDP safeguards and breach intimation (from May 2027)	DPDPA programme and breach drills	B6

THE CODEC NETWORKS VALUE ADD

Why asset managers choose Codec Networks

CERT-In empanelled

Meets CSCRF's requirement for CERT-In empanelled auditing organisations for cyber audits and VAPT.

Certified and accountable

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

CSCRF and system-audit native

Findings mapped to CSCRF, SEBI MF system audit requirements, CERT-In and DPDP.

Investor-journey testing

Onboarding, redemption, bank-change and distributor flows tested end to end.

Full stack, one partner

Audits, VAPT, SOC, forensics, BCP/DR and privacy connected from finding to closure.

Certified experts

CISA, ISO 27001 LA/LI, CEH, OSCP and CHFI professionals.

How we engage

Discover & scope

SEBI registrations, CSCRF category, investor channels, service providers 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, NFO and incident a non-event.

Tell us your registrations, AUM band and service providers. We will propose a practical, SEBI-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: AMFI data (June 2026); SEBI CSCRF circular (20 August 2024) and extensions.