Codec Networks
Coding Threats. Decoding Solutions.

ASSET & INVESTMENT MANAGEMENT CYBERSECURITY

Investor-safe. CSCRF-ready. Every day.

System audits, SEBI cyber resilience, investor data protection, application security and BCP/DR for asset and investment managers.

Three questions every asset manager should be able to answer

Which CSCRF category are we in, and are we compliant?
AMCs are categorised by AUM; portfolio managers and AIF managers by their own thresholds.

Would we stop a fraudulent redemption after a bank-detail change?
Redemption and bank-mandate fraud is a leading risk for investor-facing platforms.

Could we report an incident to SEBI within six hours?
CSCRF and CERT-In both set a 6-hour reporting window.

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

27.86 cr
MF folios (June 2026)

6 hours
Incident reporting to SEBI and CERT-In

May 2027
Most DPDP obligations take effect

Built for every asset and investment manager

AMCs and mutual funds · portfolio managers · AIF managers · investment advisers and research analysts · wealth and investment platforms · RTAs, custodians and fund accountants.

The rules that drive your security calendar

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

WHAT WE DO

System audits, cyber resilience, data protection, AppSec and BCP/DR

System Audits & CSCRF
MF and AMC system audits, CSCRF categorisation, CERT-In empanelled cyber audits.

Investor Data Protection
Investor data mapping across RTAs and distributors, DPDPA readiness, DLP.

Application Security
Investor app, portal and distributor API testing, including redemption and bank-change flows.

BCP/DR & Resilience
BCP and DR reviews and drills, ransomware readiness, recovery objective validation.

24/7 SOC & Insider Monitoring
Managed SOC or M-SOC readiness, dealing-room monitoring, redemption anomaly detection.

Third-Party Assurance
RTA, custodian, fund accountant, pricing vendor and distributor assessments.

Choose your starting point

Foundation
CSCRF applicability and gap review, annual VAPT and audit, M-SOC readiness, policy pack. For advisers and smaller PMS and AIF managers.

Assurance
CSCRF cyber audit and VAPT, investor app and API testing, 24x7 managed SOC, BCP/DR and cloud review. For mid-sized AMCs, PMS and platforms.

Continuous Resilience
Frequent audits and VAPT, red teaming, insider monitoring, third-party and RTA assurance, Board and trustee reporting. For large AMCs.

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 CSCRF, SEBI's MF system audit requirements, CERT-In and DPDP.

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

Book a scoping session

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