Codec Networks

Coding Threats. Decoding Solutions.

ASSET & INVESTMENT MANAGEMENT

Protect Investor Trust. Prove Cyber Resilience.

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

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

SEBI CSCRF, MF system audits and cloud framework

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

Savings at national scale, served digitally

More investors, more folios, more data to protect

₹82.22 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

What this means: asset and investment managers must protect investor journeys end to end—across AMCs, RTAs, distributors and fund accountants—while meeting SEBI's CSCRF and system audit requirements.

Sources: AMFI data (June 2026); SEBI CSCRF circular (20 August 2024) and 2025 extensions.

Who we serve across asset and investment management

Mutual funds & AMCs

Scheme management and investor servicing

Portfolio managers

Discretionary and advisory PMS

AIF managers

Category I, II and III funds

Investment advisers

SEBI-registered advisers and analysts

Wealth platforms

Online investing and wealth apps

RTAs

Investor records and transactions

Custodians & fund accountants

Custody, NAV and accounting

Distribution partners

Distributors, banks and MF platforms

The threats that cost asset managers the most

Six priorities from our 18-threat asset management assessment

Redemption fraud

Bank-detail changes and account takeover

Front-running & leaks

Order information leaving the dealing desk

Investor data leakage

RTAs, distributors and apps oversharing data

Ransomware

AMC, RTA or fund accountant systems encrypted

NAV & pricing tampering

Compromised data feeds and fund accounting

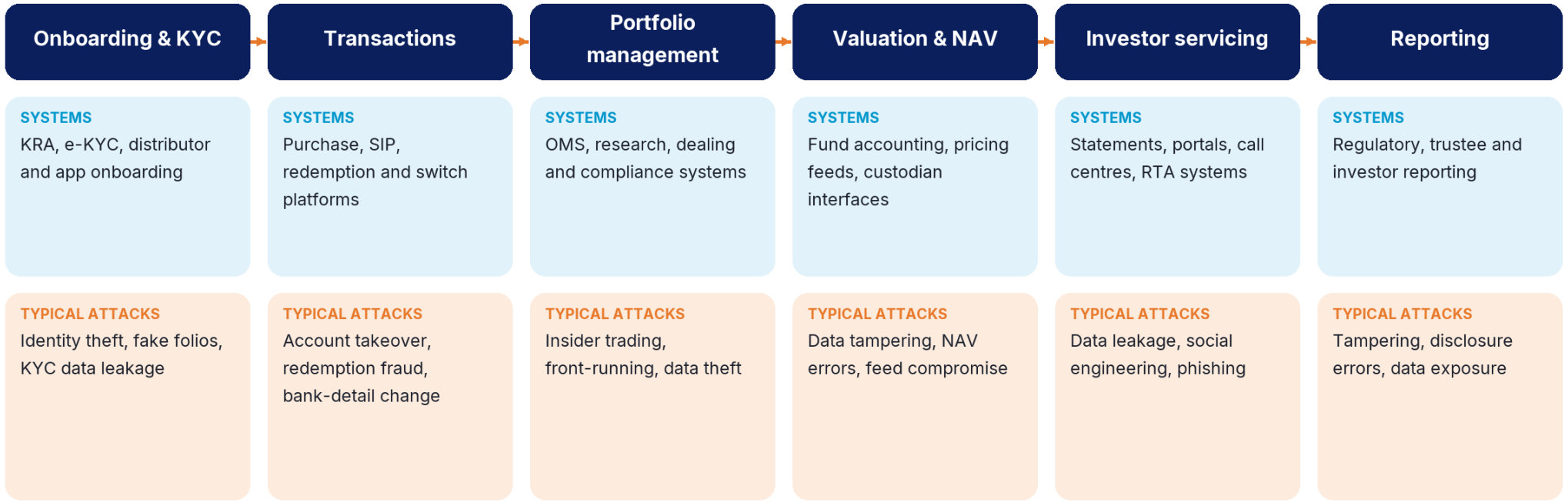
Deepfake impersonation

Fake fund managers and investment groups

Attacks target every stage of the investment lifecycle

Where Cyber Risk Sits in the Investment Lifecycle

Each stage of an investor's journey carries its own attack surface



Investor trust depends on every link—from the distributor's app to the fund accountant's NAV feed.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

SEBI's CSCRF applies to AMCs, portfolio managers and AIF managers from 31 August 2025

Codec Networks
Coding Threats. Decoding Solutions.

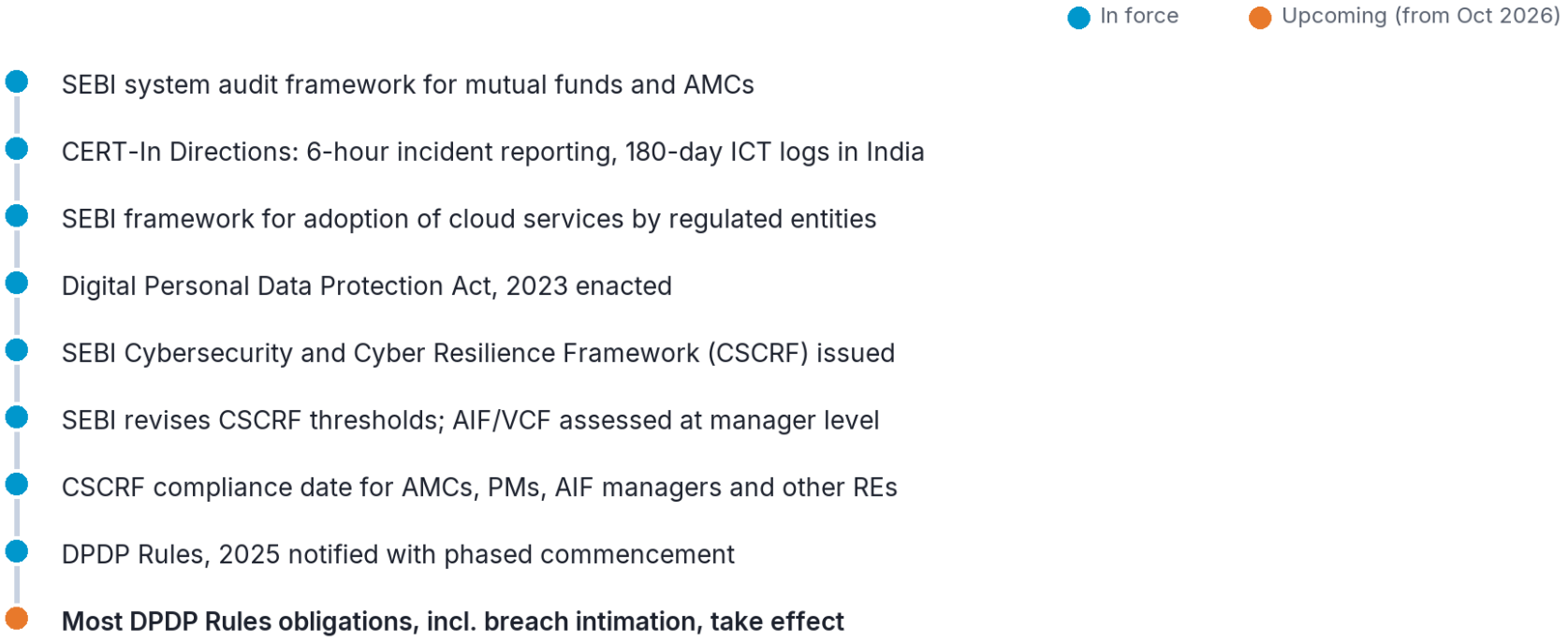
The rules that shape asset management security

Requirement	Frequency / deadline	Source
CSCRF compliance date for AMCs, PMs, AIF managers	31 August 2025	SEBI CSCRF and extensions
Cyber audit by CERT-In empanelled auditor	By category (more frequent for Qualified REs)	SEBI CSCRF
VAPT by CERT-In empanelled auditor	By category; time-bound closure	SEBI CSCRF
SOC or Market SOC onboarding	Ongoing, by category	SEBI CSCRF
Cyber incident reporting	Within 6 hours	SEBI CSCRF; CERT-In
System audit of AMC systems	Periodic	SEBI MF system audit framework (2019)
Cloud governance	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 Asset Management Cybersecurity

Key SEBI and cross-sector instruments shaping cybersecurity in asset management



Sources: SEBI circulars, CERT-In, MeitY. Applicability depends on registration and CSCRF category.

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

How Codec Networks helps

System audits · CSCRF · Data protection · AppSec · BCP/DR

Codec Networks
Coding Threats. Decoding Solutions.

One partner across the investment lifecycle

System Audits & CSCRF

MF system audits, CSCRF gap and cyber audits

Investor Data Protection

Data mapping, DPDPA readiness, DLP

Application Security

Investor apps, portals and distributor APIs

BCP/DR & Resilience

Drills, ransomware readiness, recovery validation

24/7 SOC & Insider Monitoring

SOC, M-SOC readiness, dealing-room monitoring

Third-Party Assurance

RTAs, custodians, pricing vendors, distributors

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **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

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

Advisers, small PMS and AIF managers

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

Assurance

Mid-sized AMCs, PMS and platforms

- CSCRF audit and VAPT (B4, B1)
- App and API testing (B2)
- 24x7 managed SOC (B7)
- BCP/DR and cloud review (B10, B3)

Continuous Resilience

Large AMCs (Qualified REs)

- Frequent audits and VAPT (B4, B1)
- Red teaming and insider monitoring (B10, B7)
- RTA and vendor assurance (B9)
- Board and trustee reporting

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Redemption That Went to the Wrong Account**	A SIM swap and bank-detail change divert a redemption; cooling periods and step-up checks stop it	**B2 · B7 · B6**
2	**The Dealer Who Traded Ahead**	Order information leaks from the dealing desk; DLP and surveillance catch it	**B7 · B6 · B8**
3	**The NAV Feed That Lied**	A pricing vendor's API is abused; signed feeds and tolerance checks prevent wrong NAVs	**B9 · B2 · B4**
4	**The Distributor App That Leaked Folios**	A partner API exposes folios; authorisation testing and minimisation prevent it	**B2 · B9 · B6**
5	**The Deepfake Fund Manager**	A fake video lures investors; brand monitoring and takedowns protect them	**B7 · B10 · B11**

Example: breaking a redemption-fraud chain

Case 1: The Redemption That Went to the Wrong Account

ILLUSTRATIVE ATTACK PATH

Step 1
Fraudster obtains an investor's PAN, email and phone number from a leaked database

→

Step 2
SIM swap gives control of OTPs; email is compromised

→

Step 3
Bank mandate is changed through the online portal

→

Step 4
Large redemption is paid to the fraudster's account

→

Step 5
Investor complaint, compensation and regulatory scrutiny

WHERE CONTROLS BREAK THE CHAIN

- Cooling period and alerts after bank-detail changes
- Step-up verification on high-value redemptions
- SIM-change and device signals in risk scoring
- RTA and AMC fraud-monitoring use cases

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

Codec Networks

What we test: alerts and cooling periods after bank-detail and contact changes, step-up verification for high-value redemptions, SIM-change signals in risk scoring and joint AMC–RTA fraud monitoring.

Why asset managers choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to CSCRF, SEBI MF system audits, 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 MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Registrations, AUM band, investor channels, service providers and 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.

Codec Networks
Coding Threats. Decoding Solutions.