

CREDIT INFORMATION & FINANCIAL DATA CYBERSECURITY

Every record protected. Every score trusted.

Data access controls, privacy, IT audit, API testing and data integrity and leakage assessments for credit and financial data firms.

Three questions every credit data leader should be able to answer

Who can pull or export our data today?

Member keys, analyst accounts and service identities should be least-privilege, purpose-bound and monitored.

Could a tampered file change a credit history?

Submission files need integrity checks, reconciliation and anomaly detection before they update records.

Could we report a leak within six hours?

CERT-In requires reporting within six hours of noticing an incident; RBI and partners expect prompt notice too.

Fortnightly

Credit data reporting to
CICs

31 Jul 2026

RBI cyber Directions incl.
CICs

6 hours

Incident reporting to
CERT-In

May 2027

Most DPDP obligations
take effect

Built for every credit data firm

Credit information companies · credit analytics and scoring firms · KYC utilities and KRAs · financial data processors · lenders and fintechs that report or consume credit data.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CICRA 2005 · RBI Directions (2025–26)	Security safeguards and privacy principles; CIC Directions; July 2026 cyber framework for CICs (as reported)
SEBI CSCRF · CKYCR	Cyber resilience for KRAs; KYC records management
CERT-In · DPDP	6-hour reporting, 180-day logs; consent, safeguards, breach intimation

Data access, privacy, IT audit, API testing, integrity and leakage

Data Access Controls

Privileged, analyst and member access reviews; purpose-bound access; recertification.

Privacy & DPDPA

Consent and purpose reviews, data inventory, retention and breach workflows.

IT Audit

IS audits aligned to RBI, CICRA and SEBI CSCRf; ISO 27001 readiness.

API Testing

Member and consumer report APIs, upload and dispute flows, abuse testing.

Data Integrity

Submission-file controls, pipeline reconciliation, model change control.

Leakage Assessments

DLP and egress testing, test-data exposure, cloud and data-lake reviews.

Choose your starting point

Foundation

Data access and leakage assessment, API testing, ISO 27001 pack, DPDPA quick assessment. For analytics firms and data processors.

Assurance

IS audit and gap closure, API and integrity testing, cloud review, managed SOC. For KYC utilities, KRAs and mid-sized processors.

Continuous Resilience

Continuous testing and red teaming, member and vendor assurance, SOC with insider signals, Board reporting. For bureaus and large platforms.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

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

Regulation-mapped

Every finding mapped to CICRA, RBI, SEBI, CERT-In and DPDP.

One connected partner

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

Book a scoping session

Share your data flows, integrations and audit deadlines. We will propose a regulation-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. Sources: RBI, CERT-In, MeitY. RBI 2026 Direction details as reported; confirm against the official texts.