

Resilient networks. Trusted connections.

Network and 5G security, cloud-native core assessment, IAM, SOC and telecom cyber compliance for telecom and connectivity providers.

Three questions every telecom leader should be able to answer

Are we aligned to the Telecom Cyber Security Rules?

The rules require a cyber security policy, a CTSO and incident reporting within six hours.

Who can reach our network elements?

Vendor, partner and privileged access must be brokered, time-bound and monitored.

Could we detect a quiet intrusion in the core?

Nation-state actors target routers and cores for long-term access; threat hunting finds them.

21 Nov 2024

Telecom Cyber Security Rules notified

6 hours

Incident reporting to the Government

Jun 2021

Trusted sources directive in force

May 2027

Most DPDP obligations take effect

Built for every connectivity provider

Mobile network operators · fixed-line and broadband ISPs · enterprise connectivity and managed network providers · tower, fibre and infrastructure providers · network and equipment vendors · private 5G and IoT operators.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
Telecommunications Act · Cyber Security Rules (2023, 2024)	Cyber security policy, CTSO, 6-hour incident reporting
Trusted sources · MTCTE	Trusted products; security testing against ITSAR
CERT-In · DPDP	6-hour reporting, 180-day logs; subscriber data safeguards

WHAT WE DO

Network and 5G security, core assessment, IAM, SOC and compliance

Network & 5G Security

RAN, transport, IP, DNS, BGP and signalling assessments; DDoS testing.

Cloud-Native Core

5G core API, Kubernetes, NFV and service mesh security reviews.

IAM

Privileged, vendor and dealer access controls and reviews.

24/7 SOC

Telecom-aware SOC, threat hunting and 6-hour reporting support.

Telecom Cyber Compliance

Telecom Cyber Security Rules and CTI readiness, policy and CTSO support.

Vendor & Supply Chain

Network vendor, firmware and managed partner assurance.

Choose your starting point

Foundation

Network and edge VAPT, Telecom Cyber Security Rules gap check, policy pack, router and DNS hardening. For regional ISPs and infrastructure providers.

Assurance

IT and OSS/BSS testing, vendor and privileged access review, ISO 27001 and DPDPA, managed SOC. For national ISPs and enterprise connectivity.

Continuous Resilience

5G core and signalling assessments, red teaming and hunting, SOC with network and fraud signals, Board reporting. For mobile operators and vendors.

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 the Telecommunications Act, Telecom Cyber Security Rules, CERT-In and DPDP.

One connected partner

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

Book a scoping session

Share your network, vendors and obligations. We will propose a rule-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: DoT, CERT-In, MeitY. Confirm obligations against the official notifications.