



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · TELECOMMUNICATIONS & CONNECTIVITY

Secure the Network. Protect Everything on It.

Network and 5G security, cloud-native core assessment, IAM, SOC and telecom cyber compliance for telecom operators, ISPs, enterprise connectivity providers and infrastructure and network vendors.

Network & 5G Security

Cloud-Native Core

IAM

24/7 SOC

Telecom Cyber Compliance

Vendor Access

THE CHALLENGE

Every service runs on your network. Attackers know it.

Telecom networks carry the country's banking OTPs, emergency calls and government services. The Telecommunications Act, 2023 and the Telecom Cyber Security Rules, 2024 now set specific security duties, including a Chief Telecommunication Security Officer and six-hour incident reporting.

What keeps leadership teams awake

- Nation-state intrusion into network infrastructure
- SIM-swap and subscriber fraud
- Exposed interfaces in cloud-native 5G cores
- Ransomware on OSS/BSS and billing
- Vendor remote access into network elements
- Telecom Cyber Security Rules, CERT-In and DPDP obligations



21 Nov 2024

Telecom Cyber Security Rules notified

6 hours

To report security incidents to the Central Government

Jun 2021

Trusted sources and products directive in force

May 2027

Most DPDP obligations take effect

The rulebook has changed

Instrument	What it means for you
Telecommunications Act, 2023	Framework for telecom networks and services, including security of networks and services
Telecom Cyber Security Rules, 2024 (21 Nov 2024)	Cyber security policy, Chief Telecommunication Security Officer, incident reporting within 6 hours and details within 24 hours
Trusted sources and equipment testing	National Security Directive on Telecom Sector; MTCTE security testing against ITSAR
CERT-In Directions · DPDP Act & Rules	6-hour incident reporting, 180-day logs; subscriber data safeguards and breach intimation from May 2027

One partner from SIM to core

Built around our primary proposition for the sector: **network and 5G security, cloud-native core assessment, IAM, SOC and telecom cyber compliance.**

Network & 5G Security

- RAN, transport and IP network testing
- Router, DNS and BGP security reviews
- Signalling and interconnect assessments
- DDoS resilience testing

Cloud-Native Core

- 5G core and network function API testing
- Kubernetes and NFV hardening
- Service mesh and mutual TLS reviews
- Core telemetry and logging

IAM

- Privileged access to network elements
- Vendor and partner access brokering
- Dealer and retail access controls
- Joiner-mover-leaver reviews

24/7 SOC

- Telecom-aware SOC and threat hunting
- Network infrastructure telemetry
- Fraud and SIM-change signals
- 6-hour incident reporting support

Telecom Cyber Compliance

- Telecom Cyber Security Rules gap assessment
- Cyber security policy and CTSO support
- CTI Rules readiness
- Audit and evidence tracking

Vendor & Supply Chain

- Network vendor security assessments
- Trusted-source documentation support
- Firmware and update integrity reviews
- Managed service partner assurance

Who we serve: 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 network operators.

Packaged for how telecom providers buy

Eleven Codec Networks bundles apply directly to telecom and connectivity providers:

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

Regional ISPs and infrastructure providers

- Network and edge VAPT
- Telecom Cyber Security Rules gap check
- Cyber security policy pack
- Router and DNS hardening review

Assurance

National ISPs and enterprise connectivity

- IT and OSS/BSS testing
- Vendor and privileged access review
- ISO 27001 and DPDPA readiness
- 24x7 managed SOC

Continuous Resilience

Mobile operators and network vendors

- 5G core and signalling assessments
- Red teaming and threat hunting
- SOC with network and fraud signals
- Board and regulator reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber security policy and Chief Telecommunication Security Officer (Telecom Cyber Security Rules, 2024)	Policy and governance support	B5
Security incidents reported within 6 hours, details within 24 hours (Telecom Cyber Security Rules)	SOC monitoring, IR retainer and reporting support	B7, B8
Security of critical telecommunication infrastructure (CTI Rules, 2024)	CTI readiness assessment and testing	B4, B1
Trusted sources and tested equipment (NSDTS, MTCTE)	Vendor and supply-chain assurance	B9
Cyber incidents to CERT-In within six hours; 180-day logs	Logging review and reporting support	B7
Subscriber personal data safeguards (DPDP)	DPDPA programme for subscriber data	B6
Secure cloud-native network functions	Cloud-native core assessment	B3, B1

Why telecom providers choose Codec Networks

CERT-In empanelled

Independent audits and testing recognised by regulators and enterprise customers.

Certified and accountable

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

Telecom-aware depth

Network, 5G core, OSS/BSS and SIM-fraud scenarios tested end to end.

Rule-mapped

Findings mapped to the Telecom Cyber Security Rules, CERT-In and DPDP.

Full stack, one partner

Testing, SOC, forensics and compliance connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Licence type, network architecture, 5G core and OSS/BSS, vendors and your compliance 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 MTTR/MTTD metrics.



START WITH A SCOPING SESSION

Let's make your next audit, network change and incident a non-event.

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