

Codec Networks

Coding Threats. Decoding Solutions.

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 and connectivity providers

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

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



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



A new rulebook for telecom cybersecurity

The Telecom Cyber Security Rules were notified in November 2024

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

What this means: telecom entities must adopt a cyber security policy, appoint a Chief Telecommunication Security Officer, report incidents within six hours with details within 24 hours, use trusted products and protect subscriber data.

Sources: DoT (Telecom Cyber Security Rules, 2024), CERT-In, MeitY.

Who we serve across telecom and connectivity



Mobile operators

4G and 5G networks



Broadband ISPs

Fibre and wireless access



Enterprise connectivity

MPLS, SD-WAN, leased lines



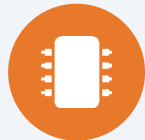
Tower and fibre providers

Passive infrastructure



Network vendors

RAN, core and transport



Private 5G and IoT

Campus and industrial networks



Managed network services

Outsourced operations



Interconnect and exchanges

Peering and roaming

The threats that cost telecom providers the most

Six priorities from our 18-threat telecom assessment



Nation-state intrusion

Long-term access to networks



SIM-swap fraud

OTPs in the wrong hands



5G core exposure

Open APIs between functions



Ransomware on OSS/BSS

Billing and provisioning stop



Vendor access abuse

Support tunnels into the network



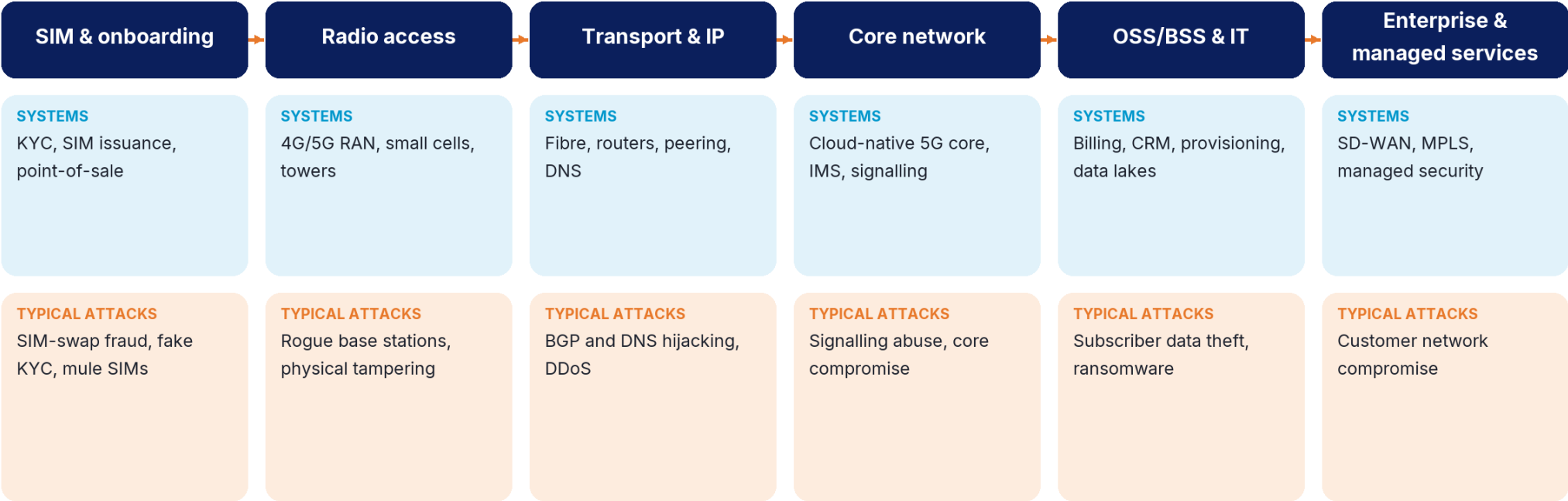
Slow detection & reporting

Missing the 6-hour window

Attacks target every layer from SIM to core

Where Cyber Risk Sits in Telecom Networks and Services

Every layer from SIM to core carries its own attack surface



Telecom security protects every service that depends on the network—banking OTPs, emergency calls and government systems.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

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

The rules that shape telecom cybersecurity

Requirement	Frequency / deadline	Source
Cyber security policy	Required	Telecom Cyber Security Rules, 2024
Chief Telecommunication Security Officer	Appointed; details to Government	Telecom Cyber Security Rules, 2024
Security incident reporting	Within 6 hours; details within 24 hours	Telecom Cyber Security Rules, 2024
Critical telecommunication infrastructure	Per notification	Telecom CTI Rules, 2024
Trusted sources and products	In force since June 2021	NSDTS
Equipment security testing	Per MTCTE schedule	MTCTE / ITSAR (NCCS)
Cyber incident reporting to CERT-In	Within 6 hours	CERT-In Directions, 2022
Subscriber personal data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for Telecom Cybersecurity

Key DoT, TRAI and cross-sector instruments shaping telecom cybersecurity

● In force ● Upcoming (from Oct 2026)

Jun 2021	● National Security Directive on Telecom Sector: trusted sources and products
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Dec 2023	● Telecommunications Act, 2023 enacted
Nov 2024	● Telecom Cyber Security Rules and Critical Telecommunication Infrastructure Rules notified
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: DoT, TRAI, CERT-In, MeitY. Confirm obligations against the official notifications.

Codec Networks

How Codec Networks helps

Network & 5G · Cloud-native core · IAM · SOC · Telecom compliance · Vendors

One partner from SIM to core



Network & 5G Security

RAN, transport, DNS, BGP, signalling



Cloud-Native Core

5G core APIs, Kubernetes, NFV



IAM

Privileged, vendor and dealer access



24/7 SOC

Telecom-aware SOC and threat hunting



Telecom Cyber Compliance

Cyber Security Rules, CTI, CTSO support



Vendor & Supply Chain

Vendors, firmware, managed partners

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



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

Regional ISPs and infrastructure providers

- Network and edge VAPT (B1)
- Cyber Security Rules gap check (B4)
- Policy pack (B5)
- Router and DNS hardening (B3)

Assurance

National ISPs and enterprise connectivity

- IT and OSS/BSS testing (B1, B2)
- Vendor and privileged access (B3, B9)
- ISO 27001 and DPDPA (B5, B6)
- 24x7 managed SOC (B7)

Continuous Resilience

Mobile operators and network vendors

- 5G core and signalling (B1, B3)
- Red teaming and hunting (B1, B10)
- SOC with network and fraud signals (B7)
- Board and regulator reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

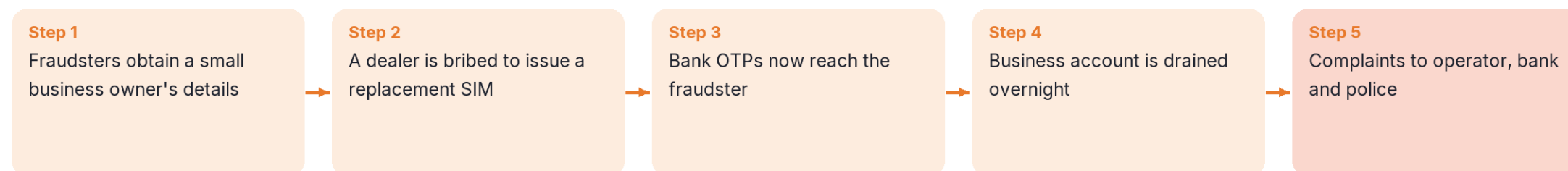
Illustrative composite scenarios written for 2026—not client engagements

1	The SIM Swap That Emptied a Business Account	A bribed dealer issues a SIM; verification and dealer monitoring stop it	B3 · B7 · B8
2	The Router Nobody Patched	A state-backed group persists in edge routers; hardening and hunting find it	B1 · B7 · B8
3	The Core Function With an Open API	An unauthenticated 5G core API leaks data; mTLS and core testing prevent it	B3 · B1 · B7
4	The Vendor Support Tunnel	A phished vendor tunnel disrupts the network; brokered access prevents it	B9 · B3 · B7
5	The Billing System Held to Ransom	Ransomware stops billing; segmentation and backups limit it	B7 · B8 · B10

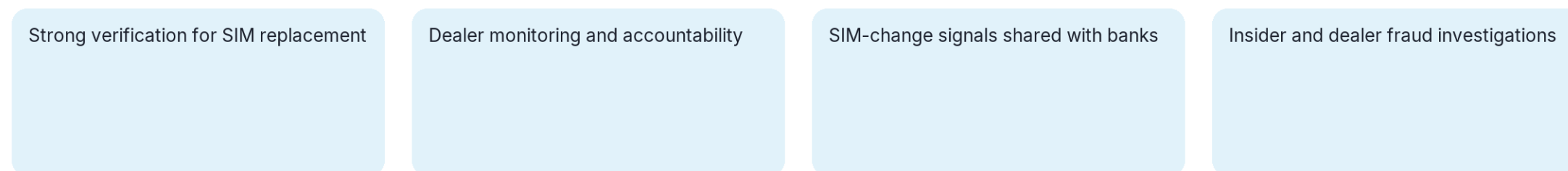
Example: breaking a SIM-swap fraud chain

Case 1: The SIM Swap That Emptied a Business Account

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: identity verification for SIM replacement, dealer access and monitoring, SIM-change signals to banks, insider and dealer fraud detection, and the 6-hour incident reporting step.

Why telecom providers choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

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



Regulation-mapped

Mapped to the Telecommunications Act, Telecom Cyber Security Rules, 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 MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Licence type, network architecture, 5G core, vendors and compliance 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.