

Codec Networks

Coding Threats. Decoding Solutions.

RAILWAYS, METRO & SURFACE TRANSPORT

Keep the Trains Moving. Keep the Passenger Safe.

Ticketing and API testing, communications and OT assessments,
SOC and incident exercises for railways, metro and surface
transport organisations

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

CERT-In, NCIIPC, railway and metro safety regimes, RBI/NPCI and DPDP



How Codec Networks helps

Services, bundles and packages built for the sector



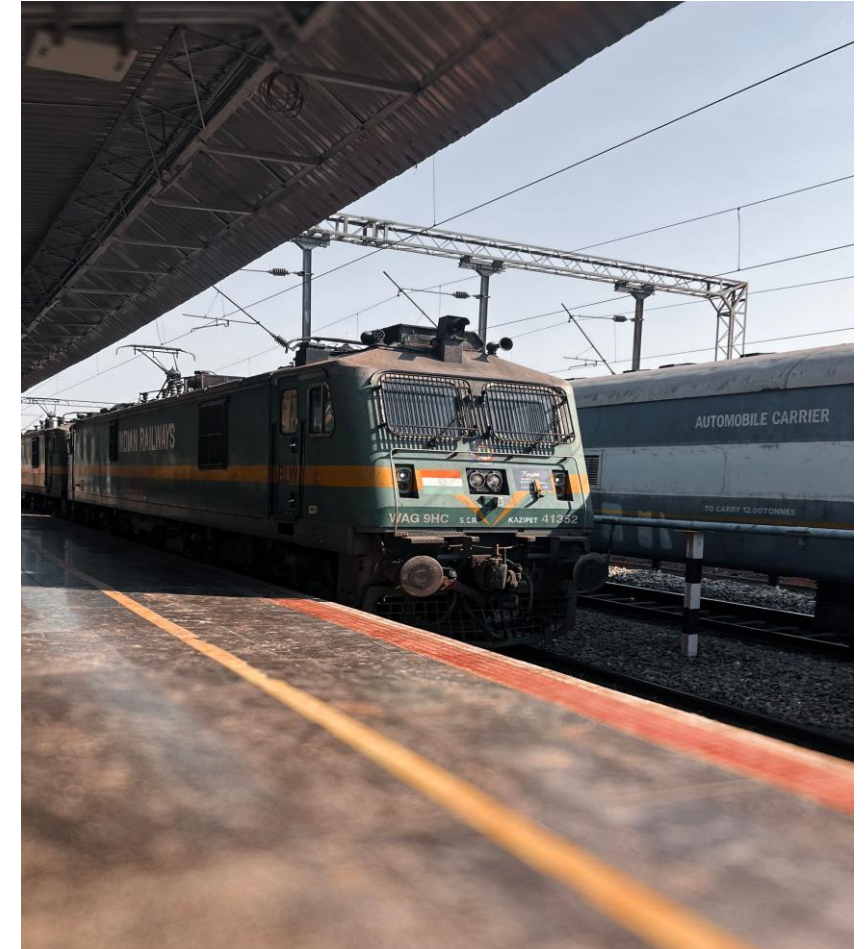
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Cyber incidents in transport stop services and shake public trust

Global incidents show the operational and reputational stakes

741 crore

Passengers carried by Indian Railways in 2025-26

~1,095 km

Operational metro network across 26 Indian cities (2026)

£29 m

Reported cost of the 2024 Transport for London cyber attack

6 hours

To report cyber incidents to CERT-In

What this means: transport operators must separate signalling and control from IT, control supplier access, harden ticketing and payment platforms against bots and fraud, protect passenger information channels, monitor IT and OT around the clock and report incidents within six hours.

Sources: Ministry of Railways, MoHUA, UK National Crime Agency reporting on TfL, CERT-In.

Who we serve across railways, metro and surface transport



Indian Railways

Zones, divisions, production units



Railway PSUs

IRCTC, CRIS, RailTel, DFCCIL, RVNL



Metro and RRTS

Metro corporations, NCRTC



State transport

STUs, city bus operators



Tolling

NHAI concessionaires, FASTag issuers



Ticketing platforms

Online rail and bus booking



Transit technology

AFC, ITS, telematics, apps



Signalling and OEMs

Signalling, rolling stock, integrators

The threats that cost transport operators the most

Six priorities from our 18-threat sector assessment



Ransomware shutdowns

Operations, ticketing and back office stopped



Signalling and control intrusion

Interlocking, Kavach, CBTC and SCADA



Supplier and OEM access

Apps and remote support that stop trains



Ticketing bots and API fraud

Scalping, scraping and payment abuse



False passenger information

Displays, PA and apps hijacked



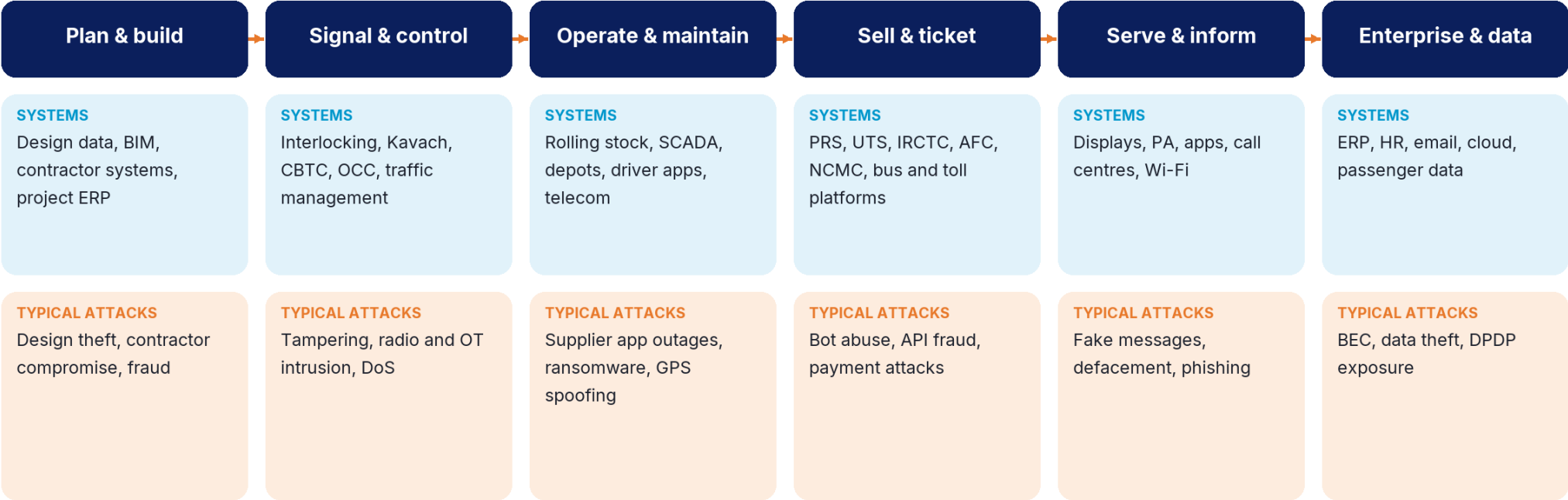
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from planning to the passenger

Where Cyber Risk Sits Across the Rail and Surface Transport Value Chain

Every stage from planning to the passenger carries its own attack surface



In transport, a cyber incident becomes a safety, crowd and public-trust event within minutes—controls must follow the train, the bus and the ticket end to end.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, NCIIPC, railway and metro safety regimes, RBI/NPCI and DPDP

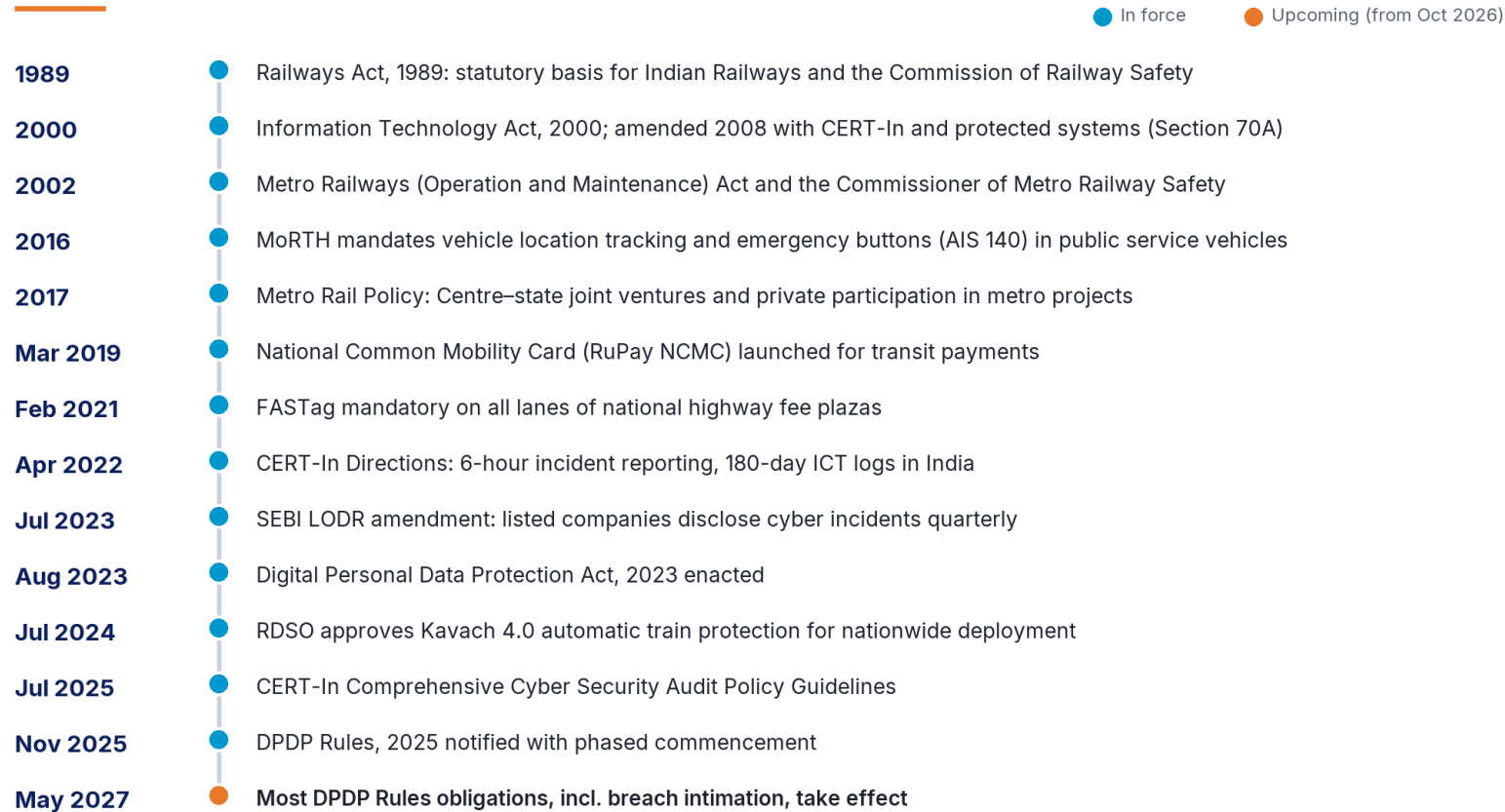
The rules and standards shaping transport cybersecurity

Requirement	Frequency / deadline	Source
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
Independent cyber audits	Risk-based, incl. OT/ICS	CERT-In audit guidelines, 2025
Protected systems and CII	Per notification	NCIIPC (IT Act Section 70A)
Safety certification of railways and metros	Before opening and on change	Railways Act 1989; Metro Railways Act 2002
Vehicle tracking and emergency buttons	Public service vehicles	MoRTH notification 2016; AIS 140
Card tokenisation, NETC and NCMC rules	Ongoing	RBI; NPCI scheme rules; PCI DSS
Cyber incident disclosure (listed PSUs)	Quarterly corporate governance report	SEBI LODR, 2023
Passenger and employee data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Rail and Surface Transport Cybersecurity

Safety, sector and cross-sector instruments and the standards that connect them



Sources: Ministry of Railways, MoHUA, MoRTH, NPCI, MeitY, CERT-In, SEBI. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Ticketing & APIs · Signalling & OT · Communications · IT/OT SOC · Exercises · Passenger data

One partner from the control room to the ticket



Ticketing & API Testing

PRS, UTS, AFC, toll and app platforms



Signalling & OT Assessment

Interlocking, Kavach, CBTC, SCADA



Communications Security

Radio, telecom, displays, station networks



24/7 IT/OT SOC

Monitoring and threat hunting



Incident Exercises

Ransomware, signalling, crowd scenarios



Passenger Data Protection

DPDP across apps, cards and CCTV

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

State transport undertakings, concessionaires and transit tech start-ups

- Ticketing and app assessment (B1, B2)
- IT and depot network review (B3)
- Backup and recovery review (B3)
- Policy, awareness and crisis plan pack (B5, B10)

Assurance

Metro corporations, railway PSUs and tolling operators

- OT and signalling assessment (B1)
- AFC and payment testing (B2, B5)
- Annual independent audit (B4)
- 24x7 IT/OT SOC (B7)

Continuous Resilience

Indian Railways units, CII owners and multi-city operators

- Testing and red teaming (B1, B10)
- Kavach, CBTC and OCC programmes (B1, B3)
- SOC with threat hunting (B7)
- Board and NCIIPC reporting (B4, B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	IT/OT SOC, IR retainer, reporting support	B7, B8
Independent cyber audits incl. OT/ICS (CERT-In guidelines, 2025)	Independent IT/OT audits	B4, B1
Protected systems and CII duties (NCIIPC, IT Act s.70A)	CII-aligned assessments and controls	B4, B3
Safety certification of signalling and control (CRS, CMRS)	Signalling and OT security reviews	B1, B5
Card tokenisation, NETC and NCMC rules; PCI DSS (RBI, NPCI)	Payment flow testing, PCI DSS readiness	B2, B5
Quarterly incident disclosure, listed PSUs (SEBI LODR)	Incident records, disclosure support	B4, B8
Passenger, commuter and employee data (DPDP)	DPDPA programme	B6

Five new case studies, five broken chains

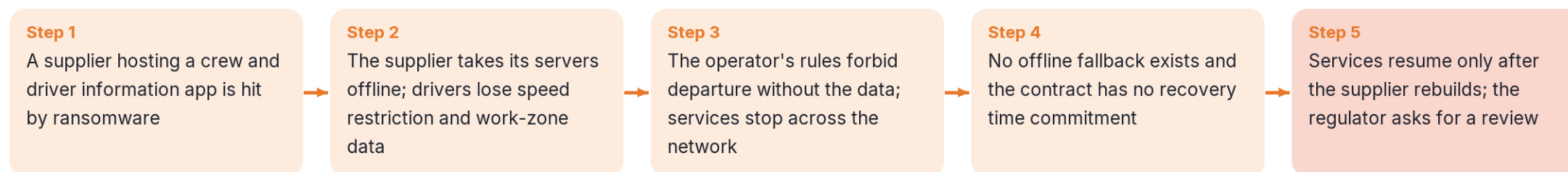
Illustrative composite scenarios written for 2026—not client engagements

1	The Driver App That Stopped the Trains	A ransomware-hit supplier takes its driver app offline and services stop; supplier mapping and fallbacks prevent it	B9 · B10 · B7
2	The Ticketing API Nobody Rate-Limited	Bots scalp seats through an unprotected API; testing, rate limits and monitoring stop it	B2 · B7 · B6
3	The Station Displays That Lied	Hacktivists push false evacuation messages; segregation and override controls contain it	B3 · B9 · B10
4	The Toll Plaza Payment Diversion	BEC diverts FASTag settlements; verification and monitoring catch it	B10 · B7 · B2
5	The Engineering Laptop on the Interlocking Network	Contractor malware reaches signalling maintenance systems; segmentation and device controls prevent it	B1 · B3 · B9

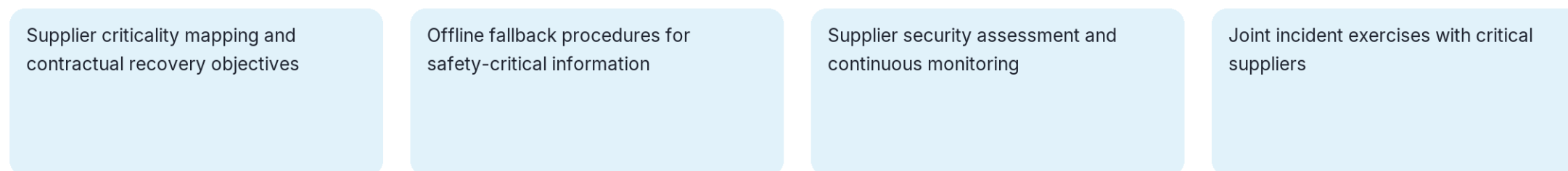
Example: breaking a supplier-outage-to-service-stoppage chain

Case 1: The Driver App That Stopped the Trains

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: which suppliers' systems operations cannot run without, whether contracts carry recovery objectives, whether offline fallbacks exist and are rehearsed, how supplier access and health are monitored, and how operations, suppliers and leadership respond in a joint exercise.

Why transport operators 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 CERT-In, NCIIPC, CRS/CMRS, RBI/NPCI and DPDP expectations, IEC 62443 and PCI DSS



Tests the whole chain

Technical, process and monitoring tests together



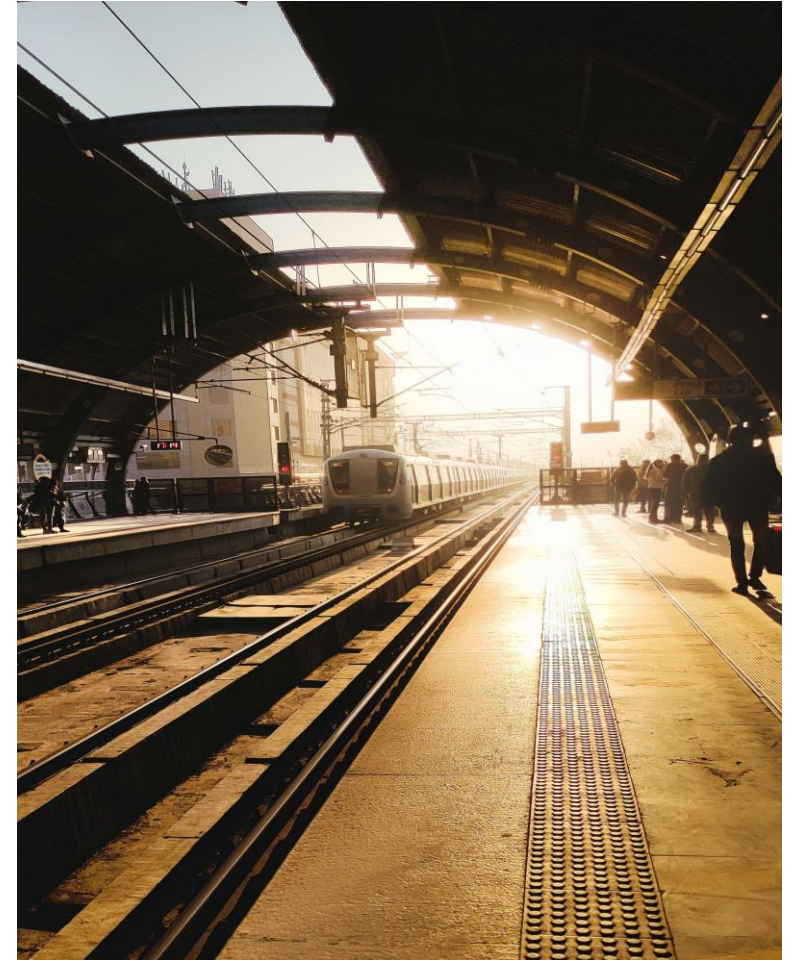
Full stack, one partner

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

Corridors, signalling and control systems, ticketing and toll platforms, suppliers with remote access, passenger data and your 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.