

Safe journeys. Secure systems.

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

Three questions every transport leader should be able to answer

Could a supplier outage stop our trains or buses?

Denmark's trains stopped in 2022 when one supplier's app went down; know your critical suppliers and your fallbacks.

Could bots or fraudsters beat our ticketing at launch?

Unprotected APIs and weak rate limits turn peak bookings into fraud, outages and public complaints.

Could someone push a false message to our displays?

Passenger information and PA systems reachable from office IT can trigger crowd and safety events.

741 crore

Rail passengers, 2025-26

~1,095 km

Metro network in 26 cities

£29 m

TfL 2024 attack cost

6 hours

Incident reporting to CERT-In

Built for every transport operator

Indian Railways zones and divisions · railway PSUs · metro and RRTS corporations · state transport undertakings · toll concessionaires and FASTag issuers · ticketing, mobility and transit technology companies.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits incl. OT
NCIIPC · CRS and CMRS · RBI and NPCI	Critical sector duties; safety certification; payment and tokenisation rules
DPDP · SEBI LODR · standards	Passenger data from May 2027; quarterly disclosure (listed PSUs); IEC 62443, PCI DSS

WHAT WE DO

Ticketing, signalling, communications, SOC, exercises and privacy

Ticketing & API Testing

PRS, UTS, AFC, toll and app platforms tested for bots, fraud and abuse.

Signalling & OT Assessment

Interlocking, Kavach, CBTC, OCC and SCADA reviews with safety teams.

Communications Security

Train radio, telecom, passenger information and station networks.

24/7 IT/OT SOC

Stations, OCCs, platforms and suppliers monitored; 6-hour reporting.

Incident Exercises

Ransomware, signalling and crowd scenarios rehearsed end to end.

Passenger Data Protection

DPDP programmes across apps, cards, CCTV and loyalty data.

Choose your starting point

Foundation

Ticketing and app assessment, IT and depot network review, backup and recovery review, policy and crisis plan. For state transport undertakings, concessionaires and transit tech start-ups.

Assurance

OT and signalling architecture assessment, AFC and payment testing, annual audit, IT/OT SOC. For metro corporations, railway PSUs and tolling operators.

Continuous Resilience

Continuous testing and red teaming, Kavach, CBTC and OCC programmes, SOC with hunting, Board and NCIIPC reporting. For Indian Railways units and multi-city operators.

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

One connected partner

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

Book a scoping session

Share your corridors, control systems, ticketing platforms and suppliers. We will propose a practical, safety-aware 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: Ministry of Railways, MoHUA, UK National Crime Agency reporting, CERT-In. Confirm obligations against the official instruments.