

Codec Networks

Coding Threats. Decoding Solutions.

AVIATION & AEROSPACE

Keep the Aircraft Moving. Keep the Passenger's Trust.

Airport IT/OT assessment, passenger data security, SOC, supplier assurance and resilience for airlines, airports, ground handlers, MRO and aerospace companies

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, ICAO Annex 17, BCAS, NCIIPC, DPDP, SEBI and EASA Part-IS



How Codec Networks helps

Services, bundles and packages built for the sector



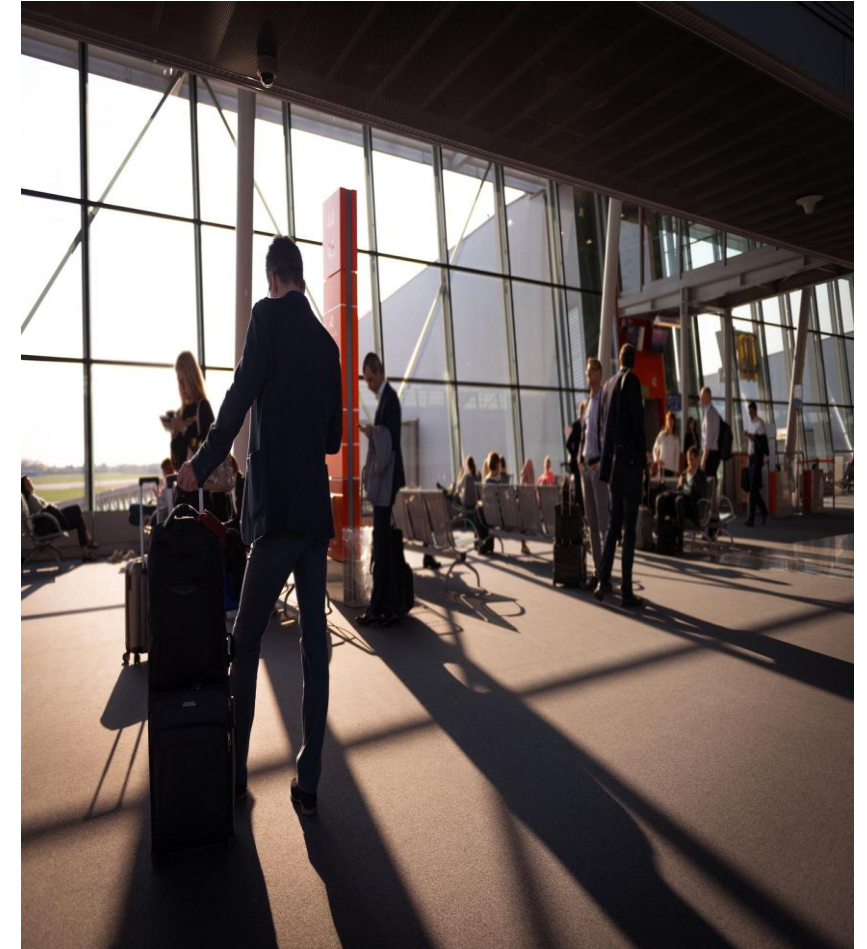
Proof in scenarios

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 aviation stop passengers and aircraft

Indian scale and global incidents show the operational stakes

16.5 crore

Domestic air passengers in India
in FY25

4.5 m

Air India passengers affected by
the 2021 SITA breach

5.7 m

Qantas customers exposed via a
contact-centre platform (2025)

6 hours

To report cyber incidents to
CERT-In

What this means: airlines and airports must assess IT and OT together, protect passenger data wherever providers hold it, assure the shared platforms and suppliers they depend on, rehearse manual fallback, monitor around the clock and report incidents within six hours.

Sources: DGCA and ICRA traffic data, Air India and Qantas statements, public reporting, CERT-In.

Who we serve across aviation and aerospace



Airlines

Scheduled, regional and cargo carriers



Airport operators

Metro hubs, PPP and AAI airports



Ground handlers

Ramp, check-in, baggage, fuelling



MRO and engineering

Line, base and engine maintenance



Aerospace manufacturers and suppliers

OEMs, tier suppliers, defence aerospace



Air cargo and express

Cargo terminals, freighters, customs



Air navigation and airport technology

ATM, CNS, common-use and airport IT providers



Business aviation and new entrants

Charter, drones, advanced air mobility

The threats that cost aviation companies the most

Six priorities from our 18-threat aviation and aerospace assessment



Ransomware shutdowns

Check-in, baggage and dispatch stopped



Passenger data breaches

Passports and loyalty data at providers



Shared platform outages

One provider, every counter



Airport OT exposure

Baggage, BMS, access control, CCTV



Supplier compromise

Handlers, MRO, IT and aerospace suppliers



Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from booking to maintenance

Where Cyber Risk Sits Across the Aviation Journey

Every stage from booking to maintenance carries its own attack surface



In aviation, an hour of check-in downtime is queues at every gate—and a leaked passenger file carries passports, not just emails.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, ICAO Annex 17, BCAS, NCIIPC, DPDP, SEBI and EASA Part-IS

The rules and standards shaping aviation 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 and cloud	CERT-In audit guidelines, 2025
Protection of critical aviation ICT systems	Per national programme	ICAO Annex 17 Standard 4.9.1; DGCA, BCAS
Protected systems in transport	Per notification	NCIIPC (IT Act Section 70A)
Passenger, crew and loyalty data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Information security management (EU-facing)	From Oct 2025 / Feb 2026	EASA Part-IS (EU 2022/1645, 2023/203)
Civil aviation law and rules	In force Jan 2025	Bharatiya Vayuyan Adhiniyam, 2024

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Aviation Cybersecurity

International aviation standards, Indian aviation law and cross-sector cyber instruments that reach airlines, airports and aerospace

● In force ● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000 enacted; CERT-In and CII provisions added by the 2008 amendment
2018	● ICAO Annex 17 Amendment 16 adds Standard 4.9.1: States protect critical aviation ICT systems and data
2019	● ICAO Aviation Cybersecurity Strategy approved at the 40th Assembly
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Jul 2023	● SEBI LODR amendment: listed companies disclose cyber incidents in the quarterly corporate governance report
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Jan 2025	● Bharatiya Vayuyan Adhiniyam, 2024 in force, replacing the Aircraft Act, 1934
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines incl. OT/ICS
Oct 2025	● EASA Part-IS applies to aerodromes, design and production organisations (EU 2022/1645)
Nov 2025	● DPDP Rules, 2025 notified with phased commencement
Feb 2026	● EASA Part-IS applies to air operators, MRO and authorities (EU 2023/203)
Nov 2026	● ICAO Annex 17 Amendment 19 tentatively applicable
May 2027	● Most DPDP Rules obligations, incl. consent and breach intimation, take effect

Sources: ICAO, Ministry of Civil Aviation, MeitY, CERT-In, SEBI, EASA. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Airport IT/OT · Passenger Data · Aviation SOC · Suppliers & Platforms · Resilience · Apps & APIs

One partner from booking to maintenance



Airport IT/OT Assessment

Baggage, BMS, access control, kiosks, platforms



Passenger Data Security

PSS, loyalty, providers, DPDP



24/7 Aviation SOC

Airline, airport and OT monitoring



Supplier & Platform Assurance

Providers, handlers, MRO, vendors



Operational Resilience

Fallbacks, backups, exercises



Airline App & API Testing

Booking, check-in, loyalty, cargo

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 airports, handlers, MROs and suppliers

- IT/OT and network assessment (B1)
- Email, BEC and payment control review (B3, B10)
- Backup and recovery review (B3)
- Policy and questionnaire pack (B5)

Assurance

Airlines and metro airports

- Annual app, API and platform VAPT (B1, B2)
- Airport OT and vendor access review (B1, B9)
- Independent audit and ISO 27001 (B4, B5)
- 24x7 SOC with provider monitoring (B7)

Continuous Resilience

Airline groups, airport groups and aerospace OEMs

- Continuous testing and red teaming (B1, B10)
- Platform and supplier assurance programme (B9, B5)
- Resilience programme with exercises (B3, B10)
- SOC with threat hunting and Board reporting (B7, B4)

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)	SOC, IR retainer and reporting support	B7, B8
Independent cyber audits incl. OT (CERT-In guidelines, 2025)	Independent IT/OT audits	B4, B1
Protection of notified aviation systems (NCIIPC, transport sector)	CII-aligned assessments and controls	B4, B3
Protect critical ICT systems and data (ICAO Annex 17, Standard 4.9.1)	Airport and airline IT/OT assessments	B1, B5
Passenger, crew, loyalty and biometric data (DPDP)	DPDPA programme	B6
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8
EU and partner requirements (EASA Part-IS, NIS2, OEM contracts)	ISMS, questionnaire and supplier readiness	B5, B9

Five new case studies, five broken chains

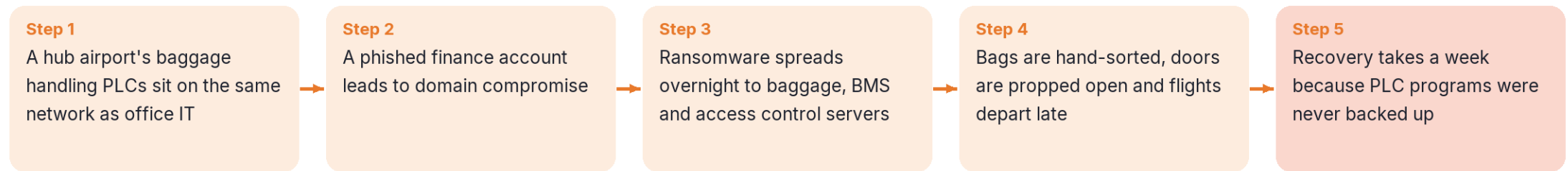
Illustrative composite scenarios written for 2026—not client engagements

1	The Check-in That Went Manual	A provider's outage stops common-use check-in; provider assurance and rehearsed fallback contain it	B9 · B10 · B3
2	The Passengers Who Were Already Gone	A processor breach exposes a decade of passport data; processor assessment and DPDP readiness prevent it	B9 · B6 · B8
3	The Baggage System on the Office Network	Ransomware reaches baggage, BMS and access control; segmentation and OT monitoring stop it	B1 · B3 · B7
4	The Miles That Flew Away	Credential stuffing drains loyalty miles; ATO testing and step-up authentication block it	B2 · B7 · B1
5	The Supplier That Stopped the Line	Ransomware at a parts supplier halts OEM deliveries; segmentation, backups and SOC prevent it	B3 · B5 · B7

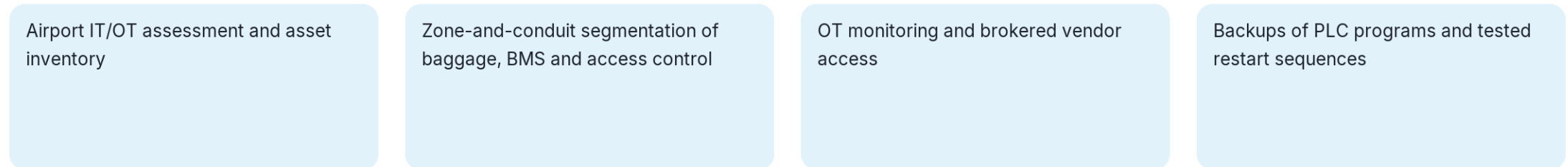
Example: breaking an airport baggage and BMS ransomware chain

Case 3: The Baggage System on the Office Network

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 airport operations depend on which systems, segmentation between office IT and baggage, BMS and access control, vendor remote access paths, PLC program backups and restart sequences, EDR and SOC detection of domain compromise, and crisis decision-making in a tabletop exercise with airport operations.

Why aviation companies 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 ICAO Annex 17, ISO/IEC 27001, IEC 62443, CERT-In expectations, DPDP and your partners' requirements



Tests the whole chain

Technical, process and monitoring tests together



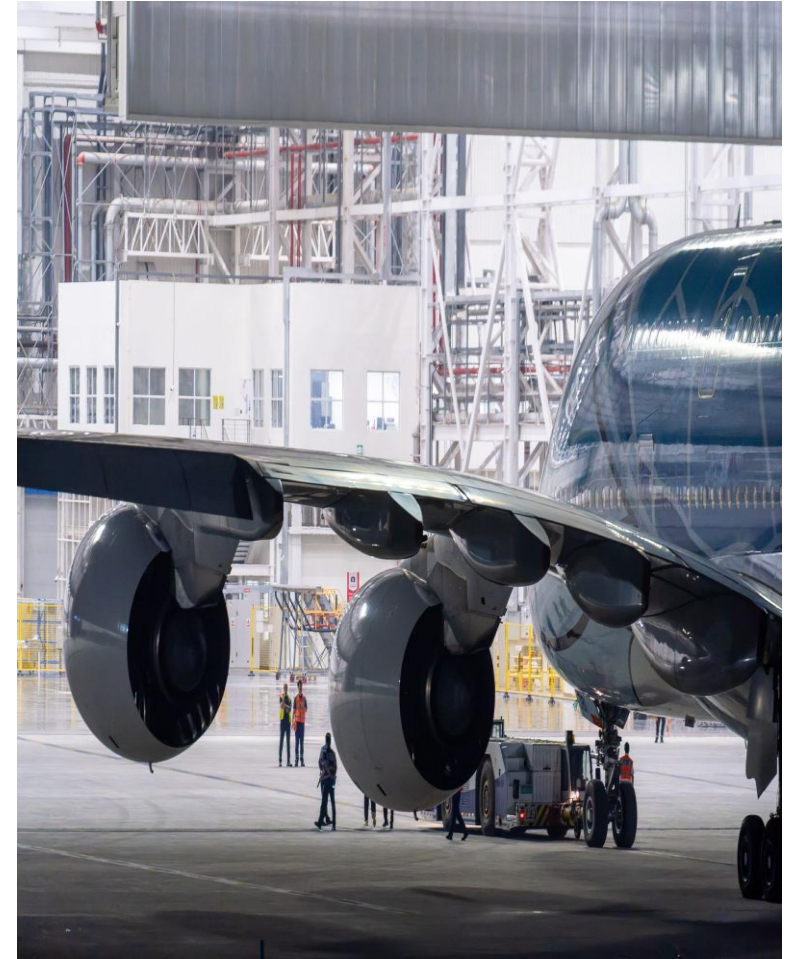
Full stack, one partner

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

Platforms and providers, apps and APIs, airport OT, loyalty and passenger data stores, critical suppliers and your audit, season and regulatory 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.