Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · AVIATION & AEROSPACE

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

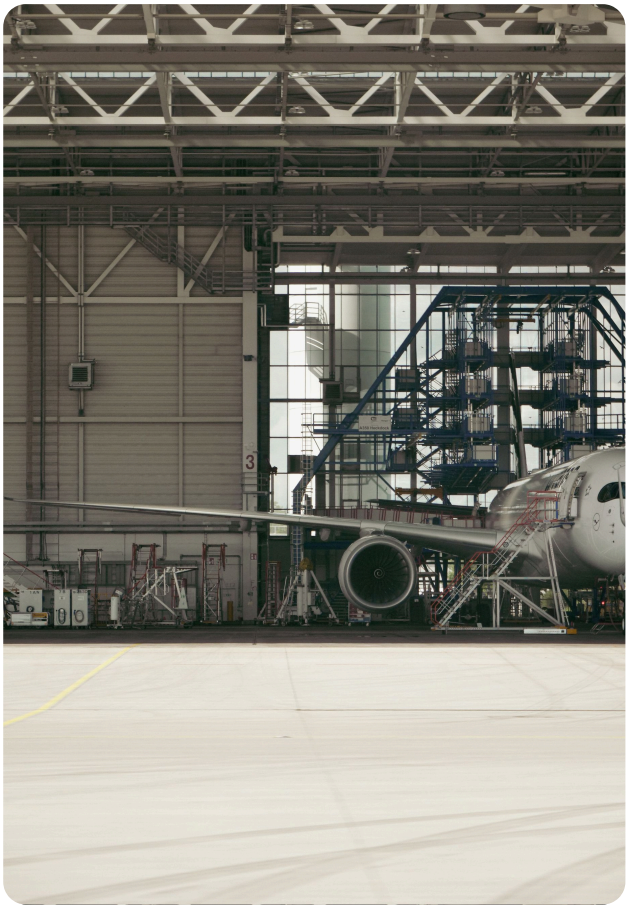
Airport IT/OT assessment, passenger data security, SOC, supplier assurance and resilience for airlines, airport operators, ground handlers, MRO firms, aerospace manufacturers and suppliers and air cargo.

- Airport IT/OT Assessment
- Passenger Data Security
- 24/7 Aviation SOC
- Supplier & Platform Assurance
- Operational Resilience
- Airline App & API Testing

THE CHALLENGE

In aviation, a cyber incident is a queue at every gate.

Indian aviation carried 16.5 crore domestic passengers in FY25 on shared platforms, airport OT and supplier networks built for efficiency, not attack. The 2021 SITA breach exposed about 4.5 million Air India passengers' data, ransomware delayed SpiceJet flights in 2022, a 2024 attack on Seattle's airport shut check-in and baggage systems, and in September 2025 one provider's outage stopped check-in at Heathrow, Brussels and Berlin.



What keeps leadership teams awake

- Ransomware stopping check-in or baggage
- Passport-grade data breached at a provider
- One shared platform's outage at every counter
- Baggage and access control on flat networks
- Loyalty account takeover and miles fraud
- CERT-In reporting, Annex 17, DPDP and SEBI

4.5 m
Air India passengers affected by the 2021 SITA breach

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

3 hubs
Heathrow, Brussels, Berlin check-in hit by one provider (2025)

6 hours
To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
CERT-In Directions and audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits incl. OT
ICAO Annex 17 · BCAS · NCIIPC	Protect critical aviation ICT systems; notified transport systems
DPDP Act and Rules (2023, 2025)	Passenger, crew and loyalty data; most duties from May 2027
SEBI LODR · EASA Part-IS	Quarterly disclosure (listed); EU information security rules

OUR SERVICE OFFERINGS

One partner from booking to maintenance

Built around our primary proposition for the sector: **Airport IT/OT assessment, passenger data security, SOC, supplier assurance and resilience.**

Airport IT/OT Assessment

- Baggage, BMS, access control, CCTV and screening system reviews
- Zone-and-conduit segmentation design
- Kiosk, Wi-Fi and common-use platform testing
- Safe, passive methods planned with airport operations

Passenger Data Security

- PSS, loyalty, contact-centre and biometric data mapping
- Processor and provider assessments
- DPDP programme and breach workflow
- Data minimisation and retention design

24/7 Aviation SOC

- Airline, airport and OT estate monitoring
- Provider and vendor access monitoring
- Loyalty fraud and account takeover signals
- 6-hour CERT-In reporting support

Supplier & Platform Assurance

- Critical platform provider risk assessments
- Ground handler, MRO and IT vendor assessments
- Contracted recovery and notification clauses
- Annex 17, Part-IS and OEM questionnaire readiness

Operational Resilience

- Dependency mapping of operations on platforms
- Manual fallback rehearsals with airlines and handlers
- Immutable backups and restore testing
- Crisis exercises with operations leadership

Airline App & API Testing

- Booking, check-in and loyalty app and API VAPT
- Payment integration and PCI DSS scoping
- Credential-stuffing and business-logic testing
- Pre-season and release retests

Who we serve: airlines · airport operators · ground handlers · MRO and engineering firms · aerospace manufacturers and suppliers · air cargo and express · air navigation and airport technology providers · business aviation and new entrants.

BUNDLED SERVICE MODELS

Packaged for how aviation companies buy

Eleven Codec Networks bundles apply directly to aviation and aerospace companies:

- **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 airports, handlers, MROs and suppliers

- IT/OT and network assessment
- Email, BEC and payment control review
- Backup and recovery review
- Policy pack and questionnaire support

Assurance

Airlines and metro airports

- Annual app, API and platform VAPT
- Airport OT and vendor access review
- Annual independent audit and ISO 27001
- 24x7 SOC with provider monitoring

Continuous Resilience

Airline groups, airport groups and aerospace OEMs

- Continuous testing and red teaming
- Platform and supplier assurance programme
- Resilience programme with exercises
- SOC with threat hunting and Board reporting

Mapped to your obligations

Requirement	How we help	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

THE CODEC NETWORKS VALUE ADD

Why aviation companies choose Codec Networks

CERT-In empanelled

Independent audits recognised by regulators, partners and insurers.

Certified and accountable

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

Operations-aware methods

Passive discovery and planned testing coordinated with airport and airline operations.

Standards-mapped

Findings mapped to ICAO Annex 17, ISO/IEC 27001, IEC 62443, CERT-In and DPDP expectations.

Full stack, one partner

IT/OT testing, SOC, forensics, supplier risk and exercises connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

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

START WITH A SCOPING SESSION

Let's make your next peak season, audit and incident a non-event.

Tell us your platforms, airports, fleets, suppliers and partners. We will propose a practical, operations-aware 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: Air India and Qantas statements, public reporting on the September 2025 Collins Aerospace MUSE disruption, CERT-In. Confirm obligations against the official instruments.