

AVIATION & AEROSPACE CYBERSECURITY

Keep the aircraft moving.

Airport IT/OT assessment, passenger data security, SOC, supplier assurance and resilience for aviation and aerospace.

Three questions every aviation leader should be able to answer

If our check-in platform went dark tonight, how would we board tomorrow?

Shared platforms fail for everyone at once; a rehearsed manual fallback with airlines and handlers decides whether it is a delay or a shutdown.

Where is every copy of our passenger data, and who processes it?

Passport-grade data sits with providers, contact centres and loyalty systems; knowing where it lives is the core of CERT-In and DPDP readiness.

Are baggage, BMS and access control separated from office IT?

Airport OT on flat networks turns a phished mailbox into stopped belts and propped doors.

4.5 m

Passengers hit by the 2021 SITA breach

5.7 m

Qantas customers exposed in 2025

3 hubs

Check-in stopped by one provider (2025)

6 hours

Incident reporting to CERT-In

Built for the whole aviation chain

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.

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
ICAO Annex 17 · NCIIPC · DPDP	Protect critical aviation ICT; notified systems; passenger data
SEBI LODR · EASA Part-IS	Quarterly disclosure (listed); EU information security rules

Airport IT/OT, passenger data, SOC, suppliers, resilience and apps

Airport IT/OT Assessment

Baggage, BMS, access control, CCTV, kiosks and common-use platforms assessed.

Passenger Data Security

PSS, loyalty, contact-centre and biometric data mapped; DPDP programme.

24/7 Aviation SOC

Airline, airport and OT monitoring with 6-hour reporting support.

Supplier & Platform Assurance

Provider, handler, MRO and vendor assessments; contract clauses.

Operational Resilience

Dependency mapping, manual fallback rehearsals, backups, exercises.

Airline App & API Testing

Booking, check-in, loyalty and cargo apps and APIs tested with retests.

Choose your starting point

Foundation

IT/OT and network assessment, BEC and payment control review, backup review, policy and questionnaire pack. For regional airports, handlers, MROs and suppliers.

Assurance

Annual app, API and platform VAPT, airport OT and vendor access review, independent audit and ISO 27001, 24x7 SOC. For airlines and metro airports.

Continuous Resilience

Continuous testing and red teaming, platform and supplier assurance, resilience programme, SOC with hunting and Board reporting. For airline groups, airport groups and aerospace OEMs.

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

One connected partner

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

Book a scoping session

Share 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 – 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: Air India and Qantas statements, public reporting on the September 2025 Collins Aerospace MUSE disruption, CERT-In. Confirm obligations against the official instruments.