INDUSTRY USE CASE

Aviation & Aerospace

Airlines, MROs, Aviation Operators & Aerospace Manufacturers

"Safety-critical systems demand compliance that never sleeps."

Aviation and aerospace organizations operate at the intersection of physical safety and cybersecurity. Regulatory bodies including the FAA, EASA, and ICAO increasingly mandate documented cybersecurity programs alongside traditional safety management systems. Auditerra brings compliance expertise and continuous monitoring to aviation organizations that cannot afford gaps — operational or regulatory.

FAA | EASA Part-IS | ICAO | SMS | NIST CSF | ISO 27001

The Challenge

- FAA and EASA cybersecurity requirements for avionics systems, ground infrastructure, and operational technology are evolving rapidly and are not yet uniformly interpreted.
- MROs handling proprietary manufacturer data and military components face CMMC and ITAR obligations on top of aviation-specific regulatory requirements.
- Safety Management Systems (SMS) increasingly require integration of cybersecurity risk into safety risk assessment processes — a gap most SMS programs have not addressed.
- Supply chain integrity is a critical concern: aerospace manufacturers must assess and monitor cyber risk across complex, multi-tier supplier networks.
- Incident reporting obligations under aviation safety regulations intersect with cybersecurity breach notification requirements in ways that create conflicting timelines.

Compliance Frameworks We Cover

FAA Cybersecurity

FAA Order 1370.121 and advisory circulars establish cybersecurity requirements for air traffic systems, avionics, and airport infrastructure. CISA coordination is increasingly expected for critical aviation systems.

EASA Part-IS

EASA's Information Security regulation (Part-IS) requires organizations to establish, implement, and maintain an Information Security Management System (ISMS) for aviation safety-relevant systems.

ICAO Cybersecurity Framework

ICAO Annex 17 and associated guidance documents establish a risk-based approach to cybersecurity for civil aviation — covering airports, air navigation service providers, and aircraft operators.

SMS Integration

Safety Management Systems (SMS) mandated by ICAO and national authorities must now incorporate cybersecurity hazard identification into safety risk management processes.

NIST CSF / ISO 27001

Aerospace manufacturers and defense suppliers commonly implement NIST CSF or ISO 27001 as the underlying security framework, mapped to aviation-specific regulatory requirements.

How Auditerra Engages — Our Process

Step 1 — Demo

A no-pressure, industry-tailored demo so you see exactly how our platform and auditors work together before any commitment.

Step 2 — Readiness Check

We conduct a gap assessment to map your current compliance posture, identify risk areas, and build a prioritized remediation roadmap.

Step 3 — Active Engagement

Our certified auditors don't hand you a to-do list. They work alongside your team — reviewing evidence, walking through controls, and personally resolving gaps in real time.

Step 4 — Continuous Monitoring

Compliance doesn't end at certification. Auditerra monitors your posture year-round, alerts you to drift, and keeps you audit-ready at all times — not just during audit season.

Why Not Big 5 or SaaS-Only?

Provider	What You Get	What's Missing
Big 5 Consulting	Deep expertise, global reach	Enterprise pricing — out of reach for most
SaaS-Only Platforms	Evidence collection platform	No human auditor — you're on your own
Auditerra	Platform + certified human auditors	Nothing. Custom pricing. Full engagement.

Integrating Cybersecurity Into Safety Management Systems

The aviation industry's safety culture is its greatest strength — and the model for how cybersecurity compliance should work. Auditerra helps aviation organizations integrate cybersecurity risk identification into existing SMS frameworks, ensuring that cyber hazards are assessed with the same rigor as physical safety risks. We map EASA Part-IS ISMS requirements to existing quality and safety management documentation, reducing duplication and accelerating regulatory acceptance. For MROs and aerospace manufacturers with ITAR or CMMC obligations, we layer those requirements into the same continuous monitoring workflow — giving you a single, unified compliance posture across all applicable frameworks.

What You Get with Auditerra

✓ EASA Part-IS ISMS gap assessment and implementation roadmap

✓ FAA and ICAO cybersecurity control documentation and evidence management

✓ SMS cybersecurity integration — hazard identification and risk assessment alignment

✓ Supply chain cyber risk assessment for aerospace manufacturer supplier networks

✓ CMMC and ITAR compliance support for MROs handling defense-related work

✓ Continuous monitoring and incident response planning aligned to aviation reporting timelines

---

Ready to See It in Action?

Book your no-obligation demo at **auditerra.com/demo** or reach out directly at **compliance@auditerra.com**. We'll tailor the conversation to your industry, your frameworks, and your timeline — no generic pitch decks.