SOFEMA AVIATION SERVICES

Safety Risk Audit (Cyber/Information Security) - EASA Part 145 - Risk

Introduction

This Safety Risk Audit is designed for EASA Part-145 organisations to identify, explore, and rate hazards in information and cyber security that may impact aviation safety.
It focuses solely on safety risk exposure and provides a structured approach consistent with Regulation (EU) 2023/203 (Part-IS).

Key integration points:

- Under-reporting of issues/events
- Manpower competence & training
- Documentation integrity
- 145–CAMO interface & data exchange risks

The safety audit process aligns with:

- IS.I.OR.205 (risk assessment, mapping)
- IS.I.OR.210 (treatment planning)
- IS.I.OR.215/230 (internal/external reporting)
- IS.I.OR.220 (detection/response)
- IS.I.OR.260 (continuous improvement)

Purpose & Scope

Purpose:
Identify and evaluate cyber/information hazards that could degrade maintenance integrity, e-records, planning systems, tooling/software, or supplier interfaces — i.e., hazards with potential to undermine airworthiness and safety.

Scope:

- Digital records & planning/MIS
- Tooling, calibration benches, OT/ICS
- Supplier and CAMO/DOA/OEM interfaces
- Cloud/SaaS, remote access, data flows
- Documentation and reporting behaviours
- Workforce competence & training

Method

Mapping - Map data flows for one recent heavy check and/or one line event: origin of data, systems, human touchpoints, supplier handovers. Anchored to IS.I.OR.205.

Scenario Interviews - Run "what-if" drills seeded by realistic EASA threat scenarios (e.g., ransomware, e-sign misuse, supplier API breach).

Weak Signal Sampling - Test detectability through evidence: backups, logs, auth trails, restores — minimal, just enough to validate realism.

Risk Scoring - Rate hazards by impact, likelihood, detectability. Propose treatments, assign ownership.

Trigger Check - Any hazard plausibly meeting "significant risk to aviation safety" → confirm reporting readiness (IS.I.OR.230).

Risk Scale

- **Impact (1–5):** Negligible → Catastrophic (airworthiness at risk).
- **Likelihood (1–5):** Rare → Likely (12–24 months).
- **Detectability (1–5):** Excellent → Poor (adjust ±1).

Risk = Impact × Likelihood (adjust detectability).

Escalation Thresholds:
≥15 OR any impact ≥4 → treatment planning + reporting trigger review.

Hazard Domains & Probing Guide

Under-Reporting of Issues

- **Hazard Q:** Are critical cyber/information events under-reported, hiding systemic risks?
- **Scenarios:** Technicians bypass IT "glitches," staff fear blame, supplier advisories not cascaded.
- **Weak signals:** Very few reports; informal workarounds; major issues found late.
- **Good practice:** Anonymous/low-friction reporting; "speak up" culture; feedback loop ("you said / we did").

Competence & Training of Manpower

- **Hazard Q:** Could competence gaps cause unsafe cyber behaviour or missed threat detection?

- **Scenarios:** Certifying staff unaware of phishing; IT delays patching during checks; untrained contractors.
- **Weak signals:** Overdue refreshers; >10% phishing failures; unclear access approval roles.
- **Good practice:** Role-specific training; CAMO/145 joint sessions; cyber-safety drills linked to RTS.

Documentation Integrity (Records & Data)

- **Hazard Q:** How could documentation be corrupted, unavailable, or misused?
- **Scenarios:** Records altered by compromised admin; backup failures; CAMO gets incomplete defect reports.
- **Weak signals:** Inconsistent timestamps; untested restores; shadow documentation.
- **Good practice:** Immutable backups; dual authorisation; CAMO cross-checks; strong e-sign audit trails.

145–CAMO Interface Risks

- **Hazard Q:** Could poor AMO–CAMO coordination create cyber blind spots?
- **Scenarios:** Defect reports lost/corrupted; CAMO compromise contaminates AD/SB data; inconsistent access policies.
- **Weak signals:** Frequent clarifications; CAMO/AMO misaligned patch cycles; no joint incident drills.
- **Good practice:** Shared hazard register; encrypted data exchange; SLA for defect reporting; joint escalation process.

Maintenance Information System (MIS)

- **Hazard Q:** How could task/RTS data be corrupted or delayed?
- **Scenarios:** Ransomware; silent DB corruption; wrong due-list.
- **Weak signals:** Backup errors; ignored alerts; DB integrity issues.
- **Good practice:** Frequent restore drills; immutable backups; quality monitors; playbooks for degraded ops.

Authorised E-Signatures

- **Hazard Q:** Where could identity misuse enable false RTS?
- **Scenarios:** Shared workstations; SSO hijack; break-glass abuse.

- **Weak signals:** Out-of-hours sign-offs; stale accounts; unusual MFA bypasses.
- **Good practice:** MFA on RTS; dual control; just-in-time elevation; monitored sessions.

Tooling, Calibration & Firmware

- **Hazard Q:** Could firmware/config changes corrupt tool readings?
- **Scenarios:** USB downgrade; vendor backdoor; unsigned updates.
- **Weak signals:** Missing hashes; vendor account reuse; off-network updates.
- **Good practice:** Signed firmware; allow-listed media; supplier attestation; baseline diffs.

Supplier & Data Exchange Interfaces

- **Hazard Q:** Where could a third-party compromise flow into production data?
- **Scenarios:** API key leakage; MSP SSO compromise; poisoned SBOM.
- **Weak signals:** Long-lived keys; broad vendor rights; no TIAs.
- **Good practice:** Time-boxed access; key rotation; joint incident drills; segmented enclaves.

Remote Access & Field Support

- **Hazard Q:** Could remote access be misused to alter RTS data/tools?
- **Scenarios:** Phished laptop; unmanaged tablet; rogue VPN.
- **Weak signals:** Stale VPN certs; BYOD drift; ticketed remote tools.
- **Good practice:** ZTNA posture checks; MFA enforced; session recording.

Change, Patch & Dependency Risk

- **Hazard Q:** Which unpatched defects could corrupt data or halt operations?
- **Scenarios:** Schema change breaks job cards; DB CVE unpatched; hijacked script.
- **Weak signals:** Deferred workarounds; untested rollbacks; >30-day CVEs.
- **Good practice:** Rollback rehearsals; bounded exceptions; exposure metrics.

Detection, Response & Recovery

- **Hazard Q:** If hazard happens at 02:00, how fast can we contain & recover?
- **Scenarios:** Encrypting MIS; insider exfiltration; supplier outage.

- **Weak signals:** Alert fatigue; unclear escalation; backups restorable only to last week.
- **Good practice:** Playbooks; measured MTTR; reporting readiness; lessons-learned cycles.

Hazard Log (Template)

- Hazard / Scenario - Asset/Interface Affected - Impact (1–5) & Rationale
- Likelihood (1–5) & Rationale - Detectability (1–5) & Rationale
- Existing Controls / Early-Warning Indicators
- Treatment Options (IS.I.OR.210) - Residual Risk & Owner
- Reporting Trigger? (IS.I.OR.230) - Improvement Action (IS.I.OR.260) & Due Date

Maturity Cues

- **Present → Suitable → Operating → Effective**
  Use to benchmark treatment/detection strength and discuss “what would make it one step better.”

Reporting Triggers

If any hazard presents a plausible near-term aviation safety risk (e.g., records integrity not restorable), pivot immediately to internal/external reporting under IS.I.OR.215/230.

Quick Reference

- **Risk focus, not compliance**
- Anchored to IS.I.OR.205 → 260
- Emphasizes under-reporting, competence, documentation, CAMO link
- Supports hazard hunting, reporting, and continuous improvement