SOFEMA
AVIATION SERVICES

Key Components of an Effective Safety Management Audit under EASA Part-IS

Sofema Aviation Services (SAS) Considers a Safety Audit focused on Risk, Systemic Integration, and Organizational Resilience

Introduction - Under Commission Implementing Regulation (EU) 2023/203, the auditing of an Information Security Management System (ISMS) within EASA-compliant organizations

- Typically extends well beyond traditional compliance checks.
- A safety audit under Part-IS is not a mere verification of regulatory adherence (as in a compliance audit), but rather a holistic evaluation of how effectively ISMS identifies, mitigates, and controls risks that have the potential to impact aviation safety.

Risk-Centric Audit Focus – Beyond Prescriptive Compliance - A safety audit under Part-IS investigates the adequacy, integration, and performance of the ISMS in managing information and cybersecurity risks. It evaluates not only whether an organization has procedures in place, but whether these procedures are fit-for-purpose in a dynamic threat environment. This includes:

- Systemic Vulnerability Assessments: Is the organization actively mapping and evaluating vulnerabilities across digital infrastructure, supply chains, and operational interfaces?
- Risk Evolution Awareness: How well does the organization detect and adapt to emerging risks, including AI-driven threats and zero-day vulnerabilities?

In contrast to compliance audits, which would simply check for the existence of a risk assessment register, a safety audit interrogates whether identified risks are accurate, current, and meaningful in terms of safety exposure.

Integration with SMS – Evaluating Interoperability and Operational Impact - The audit must explore how the ISMS is strategically integrated into the existing Safety Management System. This includes evaluating:

- Shared processes for hazard identification and risk analysis (IS.I.OR.205 / ICAO Annex 19 alignment)
- Joint ownership of incident reporting and learning mechanisms
- Cross-functional roles—do cybersecurity risks influence flight ops, maintenance release, or airworthiness control?

Key Audit Question: Does the organization treat cybersecurity risks as siloed IT issues or as safety-critical threats embedded in operational risk architecture?

Performance-Based Evaluation of Safety Outcomes - Safety audits focus on whether the ISMS is achieving its stated safety performance objectives. This involves a deep dive into:

- Lagging Indicators: Past incidents, root cause findings, and mitigation effectiveness
- Leading Indicators: Training engagement, risk reclassification trends, and closure rate of identified vulnerabilities

Audit emphasis must be on how these indicators inform adaptive safety decision-making, not just on whether they exist.

Organizational Behaviour and Safety Culture around Cybersecurity - One of the most telling elements of a Part-IS safety audit is how the organization behaves under pressure, particularly in response to cyber incidents. The audit should assess:

- Management engagement: Does leadership understand the operational implications of cybersecurity risk? Is there clear accountability?
- Reporting culture: Are information security events routinely under-reported or reframed to avoid regulatory consequences?
- Cross-role collaboration: Is the ISMS truly embedded across business units, or confined to IT/security teams?

These soft indicators often reveal deep-seated systemic weaknesses long before technical vulnerabilities are formally identified.

Third-Party Risk Oversight as a Safety Concern - From a safety audit lens, supply chain and subcontractor risk management is more than a matter of compliance with IS.I.OR.235. It is about the propagation of threat exposure through integrated operational processes.

- How is cybersecurity risk evaluated during procurement?
- Are audit findings on third parties influencing broader safety performance reviews?
- Is there adequate contractual leverage and enforcement to ensure third-party resilience?

Testing Organizational Resilience and Recovery Capabilities - Resilience is not theoretical. The safety audit should evaluate:

- Realistic scenario testing of incident response (e.g., ransomware compromising aircraft maintenance data mid-inspection)
- Post-incident root cause analysis maturity
- Recovery time vs. impact on maintenance release, dispatch reliability, or continued airworthiness

Rather than asking “Is there a plan?”, the audit seeks to answer “How well does the plan work under operational stress?”

Ensuring Safety Performance through SPI-Driven Evaluation

To ensure EASA Part-IS obligations translate into operational safety assurance, organizations must develop risk-based Safety Performance Indicators (SPIs). These SPIs must be measurable, dynamic, and relevant to aviation safety objectives.

Characteristics of Effective ISMS SPIs:

- Risk-linked: Directly tied to high-consequence information security threats (e.g., system integrity of technical logbooks)
- Predictive: Focus on detection time, false-positive rate in monitoring, and rate of successful phishing simulations
- Actionable: Used to calibrate controls, resource allocation, and training programs

ISMS Safety Audit Considerations:

- Are SPIs based on operational exposure and threat intelligence?
- Do they trigger safety board-level review or remain buried in technical reports?
- Are they used to recalibrate risk posture, or simply archived for audit readiness?

A true safety audit under Part-IS is a strategic activity. It moves past checkbox auditing to challenge whether the ISMS protects aviation safety under real-world conditions. It evaluates risk ownership, control effectiveness, and the organization's ability to learn and evolve in a complex, adversarial environment.

- For subject matter experts we are demonstrating safety assurance through cybersecurity maturity.

- Our ISMS Safety Audit must answer not whether risks are documented, but whether they are controlled, and whether that control is meaningful in preserving aviation system safety.