SOFEMA
AVIATION SERVICES

Is Your Information Security Management System Audit Ready?

Sofema Aviation Services provides a quick check to prepare for the Competent Authority Oversight

Check the following key areas to prepare for regulatory oversight (EASA Part-IS Focus)

The following checklist is designed to help organizations verify their compliance and maturity in key areas of their Information Security Management System (ISMS) prior to a regulatory audit.

1. ISMS Scope and Context

Audit Point	Key Verification Checks
Scope Definition & Preliminary Assessment	Verify that the scope definition explicitly lists all activities, systems, and data that have a potential impact on aviation safety. Check for a preliminary high-level risk/impact assessment used to define this scope.
Functional Chains & External Agreements	Review documentation of functional chains and external agreements. Verify that information is shared with interfacing partners (upstream and downstream) to enable informed shared risk management.

2. Risk Management Methodology

Audit Point	Key Verification Checks
Risk Assessment Methodology	Examine the risk assessment methodology. Ensure the risk matrix clearly links IT security factors (threat, vulnerability) with ICAO Annex 13 safety outcomes (Negligible, Incident, Accident/Unsafe Condition).
Risk Treatment Plan & Effectiveness	Review the Risk Treatment Plan. Confirm that implemented controls address the entire risk lifecycle and that a process exists to check the continued effectiveness of the controls (e.g., testing, continuous monitoring).

3. Monitoring, Incident Response, and Reporting

Audit Point	Key Verification Checks
Continuous Monitoring	Verify the monitoring system actively looks for deviations that indicate a compromise of a safety-critical function. Check internal procedures for collecting and evaluating reports from personnel and contracted organizations.
Incident Response & Disaster Recovery	Assess the incident response and disaster recovery plans. Confirm that RTOs (Recovery Time Objectives) are set based on the safety criticality of the affected assets. Evaluate exercises/drills to confirm the ability to transition to a safe state.
External Reporting Procedure	Verify the documented external reporting procedure meets the 72-hour deadline and mandates reporting to all relevant bodies (CA, DAH, system designer). Scrutinize incident records for evidence of timely reporting.

4. Personnel Competence and Third-Party Management

Audit Point	Key Verification Checks
Personnel Screening and Training	Verify the documented process for screening and training personnel, ensuring the competence program addresses the combined safety/security knowledge needed under Part-IS.
Third-Party Contracts	Review contracts with third parties (e.g., SOC, vulnerability management). Verify that the contract explicitly grants the organization (and the CA) the necessary access and audit rights.

5. ✓ ISMS Governance and Oversight

Audit Point	Key Verification Checks
Internal Audit Program	Verify the internal audit program reviews the ISMS. Check the feedback mechanism, ensuring audit findings related to Part-IS reach the accountable manager for timely and effective closure.
Record Management	Verify the procedures for managing records, ensuring controls guarantee the integrity, authenticity, and authorized access of key documentation and data logs.
Continuous Improvement Program (CIP)	Review the CIP results. Check that maturity assessments are conducted and that corrective actions derived from deficiencies are implemented, followed by a reassessment of the affected ISMS elements.
Change Management Procedure	Verify that the organization has an approved change procedure. Check records of changes made to the ISMS (e.g., risk methodology, scope) to ensure the appropriate approval level (internal procedure or CA prior approval) was used.