EASA ISMS for Part 21 J & Part 21 G_R1

Sofema Aviation Services (SAS) Considers Information Security Management System (ISMS) requirements specifically for Initial Airworthiness Subpart G and J organizations under European Union Aviation Safety Agency (EASA) regulations.

Introduction Delegated Regulation (EU) 2022/1645

(EU) 2022/1645 is a key piece of European aviation legislation that primarily focuses on enhancing information security within the aviation industry's design and production domains.

- The regulation specifically amends Commission Regulation (EU) No 748/2012, which lays down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts, and appliances, as well as for the certification of design and production organisations (EASA Part 21) (European Union, 2022).
- The core impact of Delegated Regulation (EU) 2022/1645 is the introduction of a mandatory requirement for certified organisations to implement an Information Security Management System (ISMS) to mitigate cyber risks that could potentially affect aviation safety.

Key Focus Areas and Impact on EASA Part 21

The regulation introduces new requirements that directly impact both Design Organisation Approvals (DOA, Part 21J) and Production Organisation Approvals (POA, Part 21G).

EASA Part 21J – Design Organisation Approval (DOA)

The amendments to Part 21J place a significant obligation on Design Organisation Approval holders to address information security in the design phase.

- **Mandatory Information Security Management System (ISMS):** Design organisations must establish, implement, and maintain an ISMS.
- **Policy and Risk Management:** The ISMS must include a policy on information security, particularly concerning its potential impact on aviation safety. It mandates a process to systematically identify, assess, and mitigate risks related to information security that could affect the airworthiness and environmental characteristics of the product, part, or appliance (Meissner et al., 2025).

This requirement ensures that security considerations are integrated into the initial design of aeronautical products, making them resilient to cyber threats from the outset.

EASA Part 21G – Production Organisation Approval (POA)

Similarly, the regulation imposes corresponding requirements on Production Organisation Approval holders.

- **ISMS Requirement:** Production organisations are also required to implement and maintain an ISMS.
- **Production System Integration:** The ISMS must be integrated into the organisation's overall management system, ensuring that production processes, which include data handling and system interaction, are secure against information security threats (Meissner et al., 2025).
- **Safeguarding Product Conformity:** The primary goal is to ensure that information security risks do not compromise the conformity of the produced parts and appliances with the approved design data.

ISMS Applicability and Deadline - 16 October 2025

The ISMS requirements, as per EASA Part-IS, are applicable to both Part 21 Subpart J (Design Organisation Approval - DOA) and Part 21 Subpart G (Production Organisation Approval - POA) holders.

These organizations must establish, implement, and maintain an ISMS to manage risks related to the security of information and information and communication technology (ICT) systems that support their operations.

ISMS Requirements in Part 21 Subpart J (DOA) and Subpart G (POA)

Part-IS mandates that the ISMS be a structured system designed to manage information security risks, ensuring the confidentiality, integrity, and availability of critical information and ICT systems.

The ISMS, in the context of both Design and Production organizations, must be integrated into the organization's overall Management System (which, following recent amendments to Regulation (EU) No 748/2012, already includes a Safety Management System - SMS).

Core ISMS Elements (Part-IS)

The ISMS, which aligns closely with international standards like ISO/IEC 27001 but with an aviation-specific focus, generally requires the organization to address the following areas:

- **Information Security Policy:** A formal statement from the accountable manager demonstrating commitment to information security.
- **Information Security Risk Management:** A documented process to identify, analyze, assess, and treat information security risks, particularly those that could affect airworthiness and aviation safety.
- **Information Security Governance:** Defining roles, responsibilities, and accountability for the ISMS, including top management's commitment.
- **Incident Management:** Establishing processes for detecting, responding to, and recovering from information security incidents.

- **Personnel Security:** Ensuring personnel are appropriately vetted, trained, and aware of their information security responsibilities.
- **Supply Chain Security:** Managing information security risks at the interfaces with external suppliers, partners, and subcontractors, which is critical for both design data (Subpart J) and production processes (Subpart G).

Integration with Part 21 Management Systems

For both DOAs and POAs, the ISMS must become a component of the wider management system required by Part 21.

- **For Subpart J (DOA):** The organization's Design Management System must incorporate the information security elements. This is crucial as a DOA is responsible for initial airworthiness, which involves managing and protecting highly sensitive design, modification, and certification data (e.g., Type Design, STCs, repair designs).
- **For Subpart G (POA):** The organization's Production Management System must incorporate the ISMS. This ensures the protection of the information and systems used for manufacturing, quality control, conformity assessment, and the issuance of authorized release certificates (EASA Form 1), all of which are vital for initial airworthiness.

The underlying objective is to manage the cyber risks that could compromise the airworthiness, environmental protection, or safe operation of an aircraft product, part, or appliance designed or produced by the organization.

Major Regulatory References for Part-IS

The requirement for an ISMS in initial airworthiness organizations is mandated by recent amendments to the core EASA regulation.

Regulation	Scope	Relevance to ISMS
Regulation (EU) No 748/2012	Initial Airworthiness and Environmental Protection (The core "Part 21" regulation)	The regulation that contains the Annex I **(Part 21)** rules. It was amended to mandate the Management System requirements, including ISMS.
Commission Delegated Regulation (EU) 2022/1645	Information Security Requirements for Design Organisations and Production Organisations.	This is the primary legal text introducing **Part-IS.D.OR** (Design Organisation Requirements) and **Part-IS.P.OR** (Production Organisation

Regulation	Scope	Relevance to ISMS
		Requirements), mandating the establishment of the ISMS for DOA and POA holders.
Acceptable Means of Compliance (AMC) & Guidance Material (GM) to Part-IS	Provides detailed, non-binding means and guidance for complying with the Part-IS regulations.	Crucial for understanding *how* to implement the ISMS, including acceptable risk assessment methodologies and scope definition.

Key Challenges and Issues for ISMS Implementation

The main hurdles for both Design (Subpart J) and Production (Subpart G) organizations revolve around integration, scope definition, and resource allocation.

Integration with Existing Management Systems

The biggest challenge is successfully integrating the new ISMS into the existing organizational framework, which already includes a Quality Management System (QMS) and the recently mandated Safety Management System (SMS).

- **Philosophical Shift:** Organizations must bridge the gap between Safety Risk Management (SRM), which traditionally focuses on human factors, operational failure, and physical hazards, and Information Security Risk Management (ISRM), which focuses on cyber threats, technological vulnerabilities, and data integrity.
- **Harmonisation:** The risk assessment and risk acceptance methodologies of the ISMS must be harmonized with the existing SMS framework to create a single, cohesive Management System. For instance, a cyber-attack that corrupts the design data (Subpart J) or the conformity statement data (Subpart G) must be treated as a major safety risk in the management system.

Defining the Scope of Critical Assets

Determining which systems and data fall under the "aviation safety" scope of the ISMS is a critical and complex task.

- **Subpart J (DOA):** The core critical assets are the systems that manage the Type Design data, Supplemental Type Certificates (STCs), repair design approvals, and the Design Assurance

System processes. An ISMS failure could lead to unauthorized design changes or loss of technical documentation, directly compromising initial airworthiness.

- **Subpart G (POA):** Critical assets include the systems managing the manufacturing data, quality control records, conformity assessments, and the electronic issuance of the EASA Form 1 (Authorized Release Certificate). A breach here could result in the production of non-conforming or unairworthy parts being released into service.
- **IT vs. OT:** Organizations must identify and protect not just their corporate IT systems (email, finance) but also their Operational Technology (OT) systems, such as manufacturing execution systems, testing equipment control systems, and data links with the Design Organization.

Resource, Competency, and Organisational Gaps

A lack of internal expertise and resources is a widespread issue, particularly for Small and Medium Enterprises (SMEs).

- **Skill Shortage:** Traditional Part 21 quality and compliance personnel often lack deep cybersecurity and IT governance expertise required to build and maintain an ISMS. This necessitates hiring new personnel or relying heavily on external consultants.
- **Accountability:** Establishing clear roles for the ISMS, including who serves as the Information Security Responsible Person, and defining their relationship to the Accountable Manager (as defined in 21.A.145(c) for POA and 21.A.245(c) for DOA) is a major organisational step.
- **Cost of Compliance:** The initial investment in security tools, training, gap analysis, and external audits to meet the October 2025 deadline can be substantial, placing a financial strain on organizations.

Supply Chain Security

The initial airworthiness supply chain is highly complex, involving multiple vendors for parts, design inputs, and specialized manufacturing processes.

- Interdependence: Both DOA and POA holders rely on the secure exchange of sensitive data with their suppliers and subcontractors. Part-IS requires organizations to address risks arising from these external interfaces.
- Vulnerability: A weakness in a third-party IT system used by a part supplier (Subpart G) or a design partner (Subpart J) could introduce a vulnerability into the organization's own airworthiness processes, making secure contractual agreements and oversight of subcontractors a major point of focus.

ISMS Impact: Subpart J (Design) vs. Subpart G (Production)

The distinction in ISMS focus is rooted in each organization's primary contribution to the aircraft's initial airworthiness: Design Data Integrity versus Conformity of Manufacturing.

Feature	Subpart J (DOA) - Design Organisation	Subpart G (POA) - Production Organisation
Primary Focus of ISMS	**Confidentiality and Integrity of Intellectual Property** and approved design data.	**Integrity and Availability of Manufacturing Data** and release authorization.
Most Critical Assets	**Type Certificate (TC) Data:** Drawings, specifications, stress analysis, test reports, and Instructions for Continued Airworthiness (ICA).	**Production Data:** Manufacturing plans, work instructions, quality inspection records, non-conformity data, and material traceability logs.
Core Airworthiness Risk	Unauthorized Modification or Corruption of the Type Design leading to an unairworthy design being certified.	Unauthorized Release of a non-conforming product, part, or appliance (e.g., fraudulent EASA Form 1).
Key Threat Scenarios	Data Exfiltration/Theft of proprietary design secrets (IP). 2. Integrity Breach allowing unauthorized changes to stress models or compliance documents.	Availability Loss of manufacturing systems (e.g., ransomware halting the production line). Integrity Breach of electronic quality gates or conformity statements.
Integration Point	Integrated into the Design Assurance System and documented in the Design Organisation Handbook (DOH).	Integrated into the Production Management System and documented in the Production Organisation Exposition (POE).
Supply Chain Focus	Secure data exchange with Risk-Sharing Partners (RSP) and major design subcontractors.	Secure control of manufacturing data provided to External Production Suppliers and secure storage of receiving/inspection records.

Key Takeaways

1. **DOA (Subpart J)** holders must prioritize the Confidentiality and Integrity of their proprietary design data. Their ISMS is fundamentally a tool to protect the "blueprint" of initial airworthiness.
2. **POA (Subpart G)** holders must prioritize the Integrity and Availability of the systems that manage the manufacturing process and certify conformity. Their ISMS protects the "execution" of the design and the reliability of the EASA Form 1.
3. Both organizations face a common challenge: ensuring that their ISMS effectively manages the cyber risks that could ultimately compromise the safety and airworthiness of the final product, part, or appliance.

Would you like to explore the specific requirements within the Part-IS AMC/GM for either the Design Organisation (Subpart J) or the Production Organisation (Subpart G)?

Focus on the manpower implications to ensure compliance

The introduction of the Information Security Management System (ISMS) via EASA Part-IS creates substantial manpower implications for both Part 21 Subpart J (DOA) and Subpart G (POA) holders, fundamentally requiring new roles, competencies, and a significant organization-wide training effort.

Manpower Implications: New Roles and Competencies

The most critical manpower addition is the establishment of a person or group responsible for the ISMS, often referred to in the guidance material as the Information Security Responsible Person (ISRP).

- **Responsibility:** The ISRP is delegated the day-to-day duties of establishing, implementing, and maintaining the ISMS. This includes overseeing risk assessments, implementing controls, managing incident response, and ensuring continuous monitoring.
- **Accountability:** Crucially, while responsibilities can be delegated, accountability cannot be transferred from the Accountable Manager (as defined in 21.A.245(c) for DOA and 21.A.145(c) for POA). The ISRP must report directly to the Accountable Manager.
- **Competency Gap:** This role demands a hybrid skillset combining deep cybersecurity knowledge (e.g., risk assessment frameworks, network security, and incident response) with a fundamental understanding of aviation safety and the organization's core Part 21 processes (design assurance or production conformity). Most organizations will face a challenge in recruiting or training personnel who possess this unique combination.

Dedicated ISMS Team and Subject Matter Experts (SMEs)

Beyond the ISRP, organizations must dedicate resources to run the ISMS functions:

- **Risk Assessors:** Personnel capable of conducting Information Security Risk Assessments (ISRA), which must be integrated with the Safety Risk Management (SRM) process. This requires training existing safety/compliance personnel in cybersecurity principles or incorporating dedicated IT security personnel into the management team.
- **Incident Response Team:** A defined team with documented procedures to detect, respond to, and recover from information security incidents. This team must include representation from IT, Quality/Compliance, and relevant operational departments (e.g., Design Office or Production Floor).
- **Compliance Monitoring:** The existing compliance monitoring function (Quality Assurance/Internal Audit) must expand its scope to include scheduled audits of the ISMS and information security controls. Auditors will require specialized training in ISO/IEC 27001 or equivalent security standards to perform these duties effectively.

Organisational and Training Commitments

Manpower compliance extends beyond management roles to the entire workforce.

Organisation-Wide Training and Awareness

Part-IS mandates a pervasive security culture, meaning every employee is a component of the ISMS's defensive capability.

- **General Awareness Training:** All personnel, from the shop floor in Subpart G to design engineers in Subpart J, must receive mandatory and periodic training on information security policy, procedures, and basic threat recognition (e.g., phishing, unauthorized data handling).
- **Role-Specific Training:** Technical staff must receive specialized training on secure system operation, secure coding practices (for design organizations), and the secure handling of sensitive data (e.g., digital work orders, EASA Form 1 certificates).

Documentation and Procedure Development Effort

A significant short-term manpower investment is required to create the foundational ISMS documentation:

- **DOA Focus (Subpart J):** Dedicated time from Subject Matter Experts (SMEs) is needed to update the **Design Organisation Handbook (DOH)** to include the ISMS policy, risk processes, and procedures for protecting design data integrity (e.g., change control systems).
- **POA Focus (Subpart G):** SMEs must update the **Production Organisation Exposition (POE)** to cover ISMS integration, focusing on controls for critical manufacturing systems, electronic conformity statements, and the security requirements for external production vendors.

Generic Overview of the ISMS Risk Assessment Process

The ISRA process generally follows six steps, aligning with established standards like ISO/IEC 27001 but tailored for the aviation safety context.

1. Define Scope and Assets (Boundary)

The process begins by clearly establishing the boundaries of the ISMS, focusing only on systems and data that, if compromised, could impact the safety function of the organization.

- **Scope Definition:** Identify the entire set of organizational activities, physical locations, and interfaces (especially with suppliers) relevant to the organization's approval (DOA or POA).
- **Asset Identification:** Inventory all critical **Information Assets** and **ICT Systems** within that scope.
    - **Subpart J (DOA):** Design software, Type Design documentation, simulation models, and airworthiness data servers.
    - **Subpart G (POA):** Manufacturing execution systems, electronic test stations, quality control databases, and the system issuing the EASA Form 1.
- **Asset Valuation:** Classify these assets based on the required levels of **Confidentiality, Integrity, and Availability (CIA)**. Integrity is often the most critical factor for airworthiness data.

Identify Threats and Vulnerabilities

This step focuses on identifying what could happen and the weaknesses that would allow it to happen.

- **Threat Identification:** Identify potential malicious (cyberattacks, insider misuse, tampering) and non-malicious (human error, system failure, environmental events) sources of harm.
- **Vulnerability Assessment:** Identify weaknesses in people, processes, and technology that could be exploited by those threats (e.g., unpatched software, weak access controls, lack of security awareness).

Risk Analysis and Safety Impact Evaluation (The Integration Point)

This is the critical step where cybersecurity meets safety management.

- **Risk Analysis (Likelihood):** Determine the probability or frequency of a threat successfully exploiting a vulnerability.
- **Safety Impact Assessment (Severity):** Evaluate the potential consequence of the security incident on airworthiness and safe operation. This must be categorized using the organization's existing SMS Safety Risk Classification (e.g., Catastrophic, Hazardous, Major, Minor).

- **Risk Evaluation:** Calculate the Inherent Risk (Likelihood x Severity) and compare it against the organization's established Risk Acceptance Criteria.

Risk Treatment and Control Selection

For all risks deemed unacceptable or intolerable, the organization must select and implement appropriate security controls.

- **Risk Treatment Options:** Choose a strategy to manage the risk:
    - **Mitigation (most common):** Implement technical (e.g., Multi-Factor Authentication, encryption) or organizational (e.g., updated policies, training) controls to reduce the likelihood or impact.
    - **Avoidance:** Cease the risky activity (e.g., stop using a vulnerable system).
    - **Acceptance:** Formally accept a low or tolerable level of risk, documenting the justification with the Accountable Manager's approval.
- **Residual Risk:** Re-evaluate the risk level after the controls are implemented. This Residual Risk must fall within the organization's acceptable threshold.

Documentation and Communication

The entire process must be formally documented to demonstrate compliance to the competent authority.

- **Risk Register:** Maintain a structured log detailing every identified risk, its analysis, the implemented controls, and the final residual risk level.
- **Management System Updates:** Incorporate the ISMS policies, procedures, and controls into the primary organizational manuals (DOH for Subpart J, POE for Subpart G).
- **Policy Endorsement:** The information security policy and the Risk Acceptance Criteria must be approved by the **Accountable Manager**.

Monitoring and Continuous Improvement

The ISMS is a continuous lifecycle, not a one-time project.

- **Monitoring:** Regularly check the effectiveness of the implemented controls and processes through internal audits and vulnerability scanning.
- **Review:** The ISMS performance must be reviewed periodically by senior management (Management Review) to ensure it remains suitable for the evolving cyber threat landscape.

- **Learning:** The detection, investigation, and reporting of security incidents and identified vulnerabilities must feed back into the ISRA process, triggering new assessments and control updates.

Sofema Aviation Services and Sofema Online provide EASA Part 21 Classroom, Webinar & Online Training please see the websites or email team@sassofia.com