

PART-IS

European Regulatory Framework for Safer Aviation

References : Regulation (EU) 748/2012 as amended – Part-21 ; AMC/GM Part-IS ; ISO/IEC 27001:2022.

Information security represents a new and critical challenge for aviation safety. Since 2022, the European Union Aviation Safety Agency (EASA) has introduced a dedicated compliance framework, adding information security requirements to Part-21. The objective is to protect critical data and prevent any potential impact on aviation safety.

***Part-IS** aims to ensure that aviation organisations implement robust information security measures to safeguard systems and data.*

WHO IS AFFECTED BY PART-IS ?

This regulation applies to **all stakeholders involved in aviation safety**, including manufacturers and OEMs, airlines, airports, air traffic management (ATM) service providers, maintenance organisations (MROs), as well as the entire supply chain of approval holders.

In summary: **organisations approved by EASA under Delegated Regulation (EU) 2022/1645 must comply with Part-IS, which will become mandatory from 16 October 2025**, and by February 2026 for other organisations.

WHAT ARE THE PART-IS REQUIREMENTS ?

WHAT NEEDS TO BE IMPLEMENTED TO ENSURE COMPLIANCE ?

Applicability : all DOA and POA, regardless of their size

Compliance with Part-IS requires the establishment of a clear framework to reduce risks related to cybersecurity and information security.

Organisations must therefore:

- implement a proportionate **Information Security Management System (ISMS)** covering risks that impact aviation safety
- ensure the ISMS covers confidentiality, integrity and availability of data and is integrated with the existing SMS/Quality system (process alignment)
- cascade the requirement to suppliers and partners (flow-down)
- define **governance policy, roles and responsibilities** within the organisation (management commitment, IS committee, ISMS manager...)
- establish an information security policy approved by top management, consistent with the organisation's quality and safety policy, as well as its procedures referenced in the **organisation manual**

PART-IS

European Regulatory Framework for Safer Aviation

References : Regulation (EU) 748/2012 as amended – Part-21 ; AMC/GM Part-IS ; ISO/IEC 27001:2022.

- define an incident management process (detection, handling, response and mitigation of cybersecurity and information security risks)
- develop a risk analysis and management framework addressing information risks and their potential impacts on safety (threats, vulnerabilities, scenarios...)
- ensure monitoring and improvement through an internal audit and reporting programme
- establish a corrective actions and continuous improvement process
- train and raise staff awareness on cybersecurity applied to aeronautical design
- be able to present evidence and documentation during authority audits (EASA or CAA)
- foster a security culture: raise awareness and train teams and stakeholders on the importance of cybersecurity and their role in maintaining compliance.

R&R CONSULTING'S APPROACH

Organisations may encounter several challenges in achieving compliance, notably regarding:

- the complexity of aeronautical systems
- interpretation of the regulation (as it is new)
- the complexity of implementing the required actions to meet the requirements
- change management (resistance, concerns...)

As Part-21 experts, R&R; Consulting can support you at each stage of this compliance process: gap assessment, roadmap, audit preparation, communication with the authority, and team training.

For more information on how we can support you in this area, or for any other certification needs, please contact us at: contact@rr-consulting.aero