Aero Compliance Solutions

Guide To EASA Part-IS

EASA Part-IS Cheatsheet for Small Organisations

Navigating Compliance and Operational Impact

What is EASA Part-IS?

EASA Part-IS establishes regulatory requirements for managing information security risks in aviation, aiming to protect safety-critical systems and operations from cyber threats.

It mandates that organisations implement an Information Security Management System (ISMS) integrated with existing Safety Management Systems (SMS).

FAQs

1. Does Part-IS apply to my organisation?

Yes, if you are an approved aviation organisation (AOC, CAMO, ATO, Part-145 organisation, design & production organisation and many more), compliance is required. Exceptions apply to operations with small aircraft (ELA2) or specific VFR-only activities.

2. What does compliance involve?

You need to:

- Establish and maintain an ISMS tailored to the organisation's aviation safety risks.
- Perform information security risk assessments and develop risk treatment measures.
- Document policies and procedures in an Information Security Management Manual (ISMM).
- Train personnel in information security roles and responsibilities.
- Establish a reporting system to report significant information security incidents to regulators.
- Implement measures to detect information security incidents.
- Conduct independent audits on information security.

EASA European Union Aviation Safety Agency

ISO 27001 Certified

Aero Compliance Solutions

3. How does Part-IS align with ISO 27001?

If you have an ISO 27001-certified ISMS, you're well-prepared. However, Part-IS introduces aviation-specific elements like:

- Focus on risks impacting aviation safety.
- Integration with SMS and regulatory requirements.
- Functional chain risk assessments, including operational interfaces.

4. What is the compliance deadline?

- 16 October 2025 for airports, production, and design organisations.
- 22 February 2026 for AOCs, CAMOs, training organisations, and others.

5. How are subcontracted activities affected?

You must ensure subcontracted CAMOs and third parties align with Part-IS by including security clauses in contracts and conducting interface risk assessments.

How EASA Part-IS Affects Small Organisations

1. Risk Assessment:

Operators must identify risks to operations, systems, and interfaces with third parties. Use a risk matrix incorporating aviation safety impacts.

2. Functional Chains:

Part-IS requires securing operational information flows (e.g., between airports, AOCs, and navigation services). Collaborate with linked organisations to manage shared risks.

3. Incident Reporting:

Implement internal mechanisms to detect, assess, and report security events. External reporting to regulators (e.g., EASA via ECCAIRS) is mandatory for significant incidents.

4. Personnel and Training:

Ensure personnel are trained to manage security responsibilities and report vulnerabilities. Screening and ongoing competence checks are required.

5. Documentation:

Develop an ISMM that includes:

- Risk management processes.
- Incident response plans.
- Functional chain security procedures.

Integration with ISO 27001

- Mapping ISO 27001 Controls: Many controls in ISO 27001 align with Part-IS, especially those related to risk assessment, incident management, and supplier relationships.

- Gap Analysis: Use tools like the EASA Checklist to identify gaps between existing ISMS and Part-IS requirements.

- Enhancements: Incorporate aviation-specific safety considerations into your ISMS.

Aero Compliance Solutions

Next Steps for Small Operators

1. Perform a Gap Analysis:

Evaluate your current ISMS or SMS against Part-IS requirements using tools like EASA's gap analysis checklist.

2. Develop an ISMM:

Align your manual with regulatory requirements, ensuring it addresses safety-critical risks and interfaces.

3. Train Your Team:

Conduct targeted training for personnel on new policies, reporting mechanisms, and functional chain risks.

4. Engage Subcontractors:

Update contracts to include security obligations and assess risks at operational interfaces

.

5. Act Early:

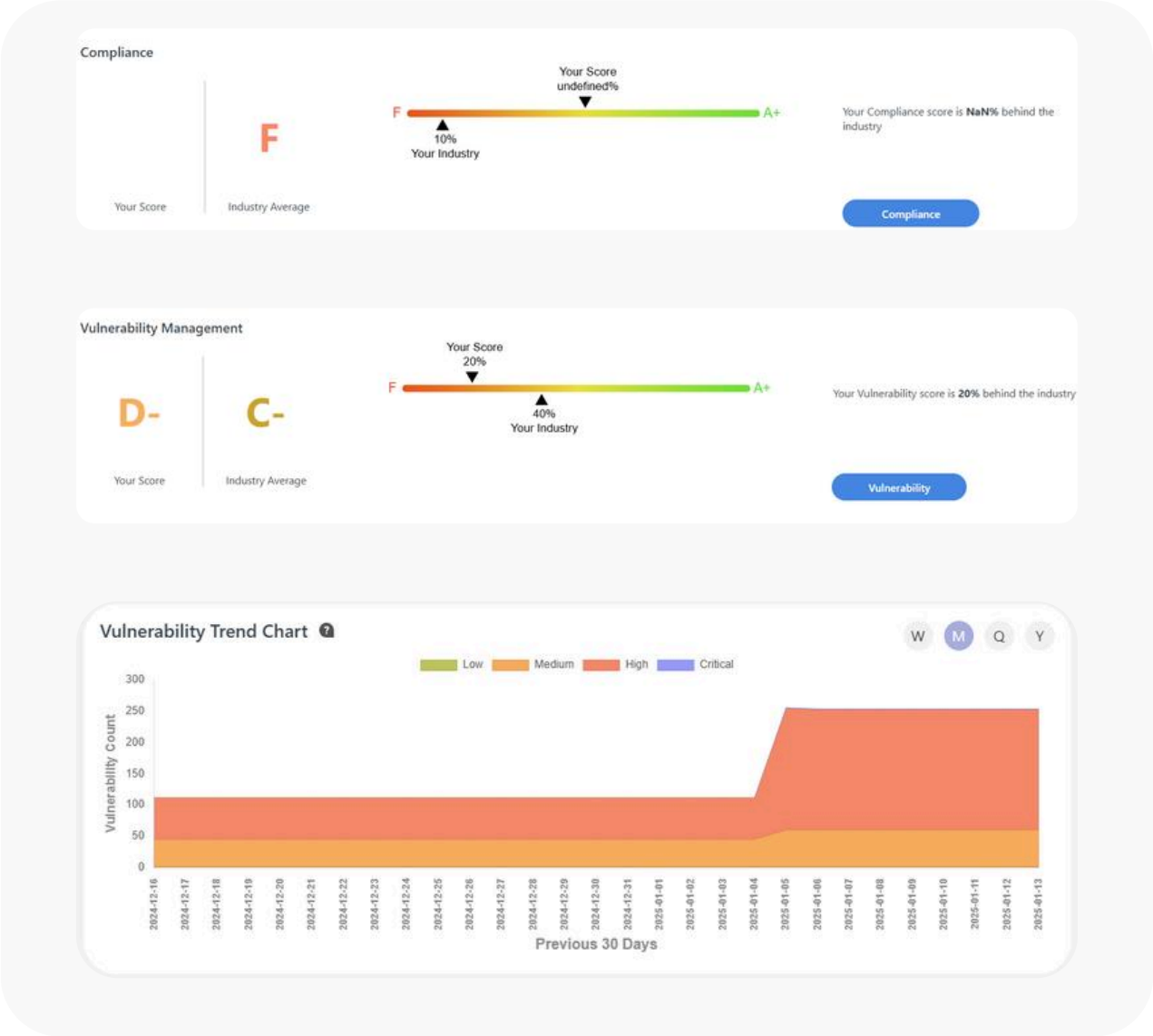
Begin implementing changes now to avoid resource bottlenecks closer to the compliance deadlines.

Aero Compliance Solutions

How We Can Help

- Templates:
  - Information Security templates provided based on the latest Part-IS requirements.

- Comprehensive Scans & Detailed Finding Reports:
  - Scans of your system, including an overall grade, statistics on target machines, and a count of vulnerabilities per target.
  - Breakdown of vulnerabilities by severity (Critical, High, Medium, Low), including specific vulnerabilities and affected targets.



EASA European Union Aviation Safety Agency

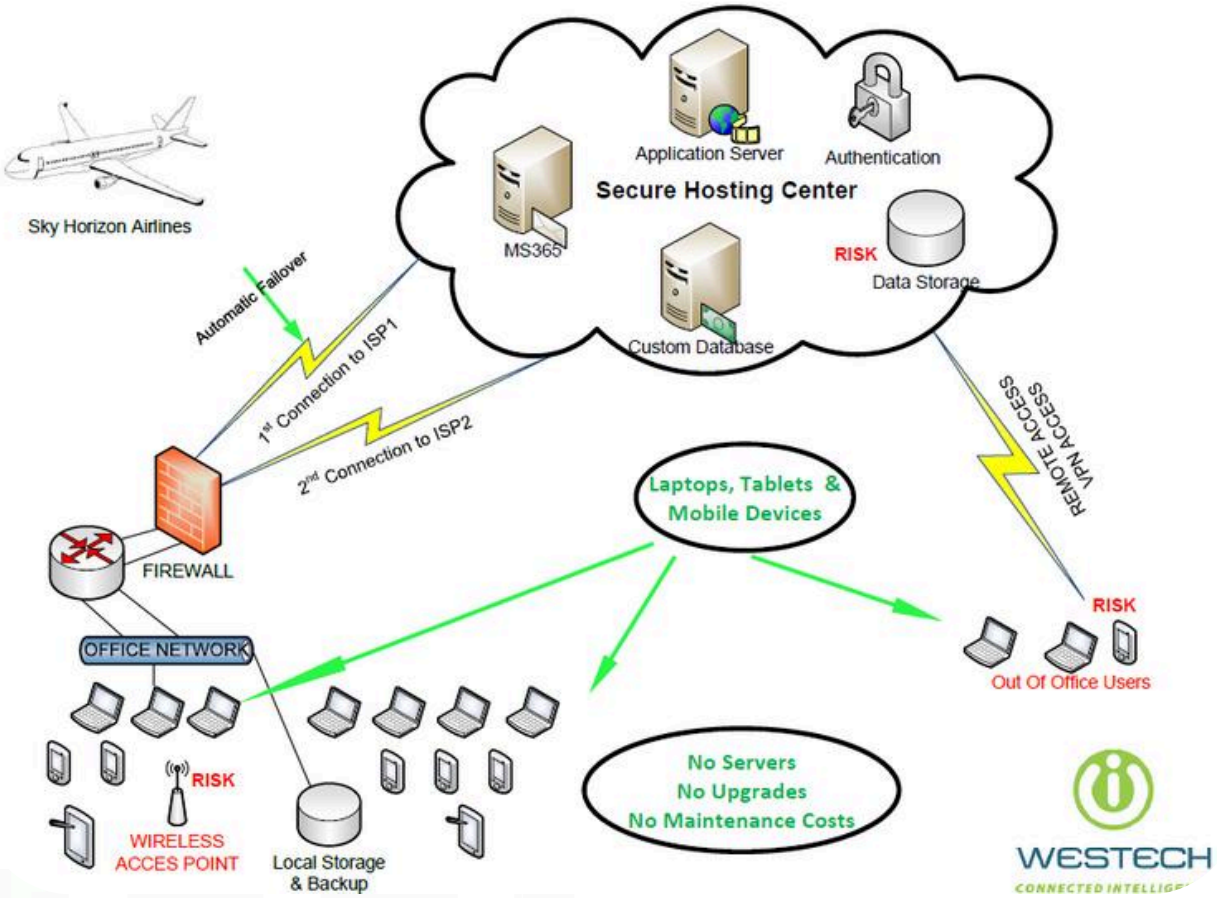
ISO 27001 Certified

Aero Compliance Solutions

- Root Cause Analysis:
  - Identification of the root causes of vulnerabilities.

- Mitigation Plans:
  - Recommended actions to address each vulnerability.

- Charts and Graphs:
  - Visual representations of vulnerability distribution and risk levels.



Key Benefits of Compliance

- Enhanced safety through robust risk management.
- Streamlined regulatory approval processes.
- Improved stakeholder confidence (regulators, partners, and passengers).
- Future-proofed operations against evolving cyber threats.

For tailored support and practical tools to simplify compliance, engage with an EASA Part-IS consultant or certified software solution.

What We Provide

- Consultation
- Templates
- Smart Software
- ISMM (Part-IS manual)
- Independent Audits
- Compliance Checks
- Risk Assessments

ACS
Aero Compliance Solutions

Book a Free Demo

sales@redifly.com

+353 (01) 582 4299

Schedule a Call

Jack Clancy
Head of Sales & Marketing

Just copy & paste the link below into your browser and pick a time

https://calendly.com/redifly/discoverycall

Find Us on Social

REDiFly

REDiFly

EASA European Union Aviation Safety Agency

ISO 27001 Certified