Integrating Cybersecurity into EASA-Compliant SMS for Part-145, Part-OPS, and Part-CAMO

Sofema Aviation Services (SAS) www.sassofia.com Considers Key Steps to Take to ensure your organisation is Cyber Compliant by February 2026

Overview of EASA Part-IS

EASA Part-IS marks a significant advancement in aviation safety and security by addressing the critical need for protection against information security threats such as cyberattacks, human errors, and systemic vulnerabilities. Anchored by **Commission Implementing Regulation (EU) 2023/203** and **Delegated Regulation (EU) 2022/1645**, it requires the integration of **Information Security Management Systems (ISMS)** into existing **Safety Management Systems (SMS)** for a unified approach to risk management.

Compliance is mandatory by **February 22, 2026**, aiming to enhance aviation organizations' resilience, safeguard operational integrity, and maintain public confidence in aviation safety.

Key Drivers of EASA Part-IS

Legal Foundations

- Regulations:
  - Commission Implementing Regulation (EU) 2023/203
  - Delegated Regulation (EU) 2022/1645
- Supporting Decisions:
  - EASA ED Decisions 2023/008/R, 2023/009/R, 2023/010/R

Applicability

- Part-145: Maintenance Organizations
- Part-OPS: Operators
- Part-CAMO: Continuing Airworthiness Management Organizations

Domain-Specific Challenges in Cybersecurity Integration

Part-145: Maintenance Organizations

- **Data Integrity Risks**
  - Susceptibility of maintenance records and diagnostic tools to tampering.
- **Third-Party Dependencies**

- Vulnerabilities at interfaces with external service providers.

- **Incident Recovery**
  - Disruption of maintenance schedules due to cybersecurity incidents.

Part-OPS: Operators

Operational Threats

- Risks to real-time systems such as flight planning and communication.

Data Breaches

- Exposure of sensitive passenger, cargo, or operational data.

System Vulnerabilities

- Interconnected systems as high-value targets for cyberattacks.

Part-CAMO: Continuing Airworthiness Management Organizations

- **Record Integrity and Availability**
  - Security of airworthiness data critical for compliance and operations.
- **Interfacing Risks**
  - Collaboration with operators and maintenance providers increases vulnerabilities.
- **Resource Allocation**
  - Balancing cybersecurity compliance with operational resources.

Best Practices for Cybersecurity Implementation

Common Best Practices

- **Develop an ISMS**
  - Tailored to aviation risks as per Annex II (Part-IS.I.OR).
  - Include risk assessment, incident detection, response, and recovery.
- **Perform Regular Risk Assessments**
  - Use frameworks like ISO 27001 or NIST to evaluate vulnerabilities.

- **Incident Management and Reporting**
  - Establish detection systems and coordinate timely responses.
- **Personnel Training and Competence**
  - Ensure tailored cybersecurity training for all roles, emphasizing proactive threat mitigation.
- **Integration with SMS**
  - Embed ISMS processes within SMS frameworks for efficiency.

Domain-Specific Best Practices

- **Part-145**:
  - Secure digital tools and enforce access controls.
  - Audit third-party service providers for compliance.
- **Part-OPS**:
  - Implement secure communication systems for flight operations.
  - Protect operational data integrity.
- **Part-CAMO**:
  - Safeguard airworthiness records and monitor system interfaces.

Oversight Considerations

For Competent Authorities

- **Regulatory Compliance**
  - Verify ISMS implementation.
- **Auditing and Monitoring**
  - Conduct periodic audits to evaluate cybersecurity measures.
- **Incident Coordination**
  - Ensure prompt reporting and coordinated responses.

For Organizations

- **Part-145**: Maintain secure backups and audit external providers.
- **Part-OPS**: Safeguard real-time operations and maintain operational data integrity.
- **Part-CAMO**: Protect airworthiness data and enforce interface security.

Building Resilience: A Call to Action

EASA Part-IS compliance is both a regulatory mandate and an opportunity to enhance cybersecurity and operational resilience. Early adoption of ISMS practices demonstrates a commitment to aviation safety, fosters stakeholder trust, and positions organizations as leaders in cybersecurity.

Partner with SAS

Sofema Aviation Services (SAS) provides comprehensive support, including assessments, training, and implementation workshops, ensuring seamless integration of ISMS into your operations.

Explore training programs and advisory services at **www.sassofia.com**, and safeguard your operations for a secure aviation future.

Next Steps

See the following course available online with Sofema
Online https://sofemaonline.com/lms/all-courses/458-easa-compliant-organization-cyber-security-responsibilities/preview