Aviation Regulatory Experts

SOFEMA
AVIATION SERVICES

Part 145 Cyber Security Implementation – 2 Days

A Practical Approach to Complying with Regulation (EU) 2023/203 – Information Security Risks

Introduction

As the aviation industry becomes increasingly digitalized, cybersecurity and information security have emerged as critical regulatory priorities. Regulation (EU) 2023/203 mandates that EASA Part 145 organizations establish an Information Security Management System (ISMS) to ensure compliance by February 2026.

This 2-day intensive training focuses on the implementation of cybersecurity measures, covering risk assessment, compliance strategies, structured risk mitigation, and cyber incident response. Participants will gain practical skills to integrate cybersecurity within their EASA Part 145 maintenance organizations, ensuring regulatory compliance and operational resilience.

Who is the course for?

This training is suitable for Accountable Managers & Nominated Post Holders, Safety, Compliance & Quality Managers, IT & Cybersecurity Specialists in MROs, Maintenance, Repair & Overhaul (MRO) Engineers & Managers, Procurement, Supply Chain & Vendor Management Professionals, and Regulatory Compliance Officers & Auditors.

What is the Benefit of this Training – What will I learn?

a) Understand EASA Cybersecurity Regulations – including Regulation (EU) 2023/203, NIS2 Directive (EU) 2022/2555, and relevant aviation cybersecurity requirements.

b) Identify & Assess Cyber Risks – Recognize threats, vulnerabilities, and compliance challenges within Part 145 maintenance environments.

c) Implement Cybersecurity Risk Management – Conduct structured risk assessments aligned with EASA IS.I.OR requirements.

d) Develop an Information Security Management System (ISMS) – Establish an effective security framework in compliance with EASA Part 145.

e) Understand External & Internal Cyber Incident Reporting – Ensure compliance with EASA-mandated reporting requirements (IS.I.OR.230).

f) Navigate Cultural & Operational Challenges – Manage staff awareness and resistance to cybersecurity implementation.

g) Work Through Practical Scenarios & Gap Analysis – Identify compliance shortfalls and corrective actions through real-world case studies.

tel + 359 2 821 08 06
email team@sassofia.com

Date	On Demand
Category	Personal Development
Venue	On Demand
Level	Basic
Price	On Demand

www.sassofia.com

Detailed Content / Topics - The following Subjects will be addressed

Why Are We Seeing EASA Mandated Regulations Related to Information Security and Cyber Security?

What Will This Mean for European Aviation?

General Introduction – Part 145 Information Security

Regulatory Drivers for Information Security – EASA Part 145

Summary of Directive (EU) 2022/2555 (NIS2 Directive)

Reference Listing of Relevant Documentation – EASA Aviation Cyber Security

EASA Part 145 Information Security Duties, Accountabilities, Responsibilities (IS.I.OR.240)

Part 145 - Gap Analysis – Information Security & Cybersecurity

The Potential for Information Security / Cyber Exposure in Aircraft Maintenance

Identifying and Assessing Cyber Risks within EASA Part 145 Organizations

Information Security Reporting Criteria – External & Internal (IS.I.OR.230)

Information & Cyber Security – Structured Risk Assessment Considerations

Guidance for EASA Part 145 Compliant Information Security Manual

Considering Cultural Resistance & Staff Awareness in EASA Part 145 Cybersecurity Implementation

Cyber Security & Information Security Training for EASA Part 145 Organizations

Debrief & Close

Pre-requisites

The pre-requisites for this training include a basic understanding of EASA Part 145 regulations, foundational cybersecurity concepts, and experience in aviation maintenance or regulatory compliance.

Target Groups

The target groups for this training include Accountable Managers, Safety and Compliance Managers, IT and Cybersecurity Specialists in MROs, MRO Engineers and Managers, Procurement and Vendor Management Professionals, and Regulatory Compliance Officers.

Date	On Demand
Category	Personal Development
Venue	On Demand
Level	Basic
Price	On Demand

Learning Objectives

a) Understand EASA cybersecurity regulations, including Regulation (EU) 2023/203 and the NIS2 Directive.
b) Identify and assess cyber risks within EASA Part 145 maintenance environments.
c) Develop and implement an Information Security Management System (ISMS) in compliance with EASA requirements.
d) Gain practical skills in cyber incident response, reporting, and managing compliance challenges.

What do People Say about Sofema Aviation Services Training?

"I found satisfying answers to all my questions."
"The instructor demonstrated a very deep knowledge of the subject."
"The length of the course fits my needs and expectations."
"The content was really effective, I gained a lot of new knowledge."
"The practical examples were perfectly delivered."

Duration

Delivery Mode: Available onsite or virtual via Sofema Online
Duration: 2 Days – 09:00 to 17:00 (with refreshment breaks)

✉ Register Now: team@sassofia.com
☎ Call: +359 28210806

Ensure Compliance Before the February 2026 EASA Deadline – Secure Your Spot Today!

Date	On Demand
Category	Personal Development
Venue	On Demand
Level	Basic
Price	On Demand