Aviation Regulatory Experts

SOFEMA AVIATION SERVICES

Cybersecurity in Aviation – EASA - Compliant Training Program – 3 Days

Introduction

As aviation continues to embrace technological advancements, the need for robust cybersecurity measures has never been more critical. The Cybersecurity in Aviation – EASA-Compliant Training Program is designed to provide professionals in the aviation industry with a comprehensive understanding of cybersecurity regulations and practices, specifically aligned with the European Union Aviation Safety Agency (EASA) requirements. This program will equip participants with the tools to assess and mitigate cyber risks in aviation systems, integrate cybersecurity into organizational safety management systems, and respond effectively to cyber incidents. By the end of the training, participants will be prepared to implement a cybersecurity culture and ensure regulatory compliance within their organizations.

Who is the course for?

This course is designed for professionals in the aviation industry, including safety managers, compliance and quality managers, and personnel from maintenance, design, and production organizations. It is also ideal for IT and cybersecurity specialists in aviation, as well as operational and senior managers responsible for ensuring compliance with EASA regulations.

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

a) Understand the regulatory framework for cybersecurity under EASA requirements.
b) Assess cybersecurity risks, identify threats, and implement mitigation strategies.
c) Integrate cybersecurity into the Safety Management System (SMS)
d) Develop incident response and reporting capabilities compliant with EASA AMC/GM.
e) Establish a cybersecurity culture and develop internal audit processes for compliance.

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

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

Detailed Content / Topics - The following Subjects will be addressed

Day 1: Introduction to Cybersecurity in Aviation

- Definition of Cybersecurity and Cyber Resilience
- Key Terminology: Threats, Vulnerabilities, Risk, Mitigation
- Overview of Aviation-Specific Cyber Threats: Aircraft, Ground Systems, Communications
- EASA Cybersecurity Regulations:
- EU Regulation 2019/1583
- ED Decision 2020/006/R
- AMC/GM for Safety Management Systems
- International Requirements: ICAO Annex 17 & Annex 19 (Security and SMS)
- Role of Cybersecurity in EASA Part 21J, Part 21G, CAMO, and Part 145 Organizations
- Integration of Cybersecurity into the Safety Management System (SMS)
- Hazard Identification and Risk Management for Cyber Threats
- Organizational Roles and Responsibilities for Cybersecurity

Day 2: Cyber Risk Assessment and Threat Management

- Introduction to Cyber Risk Assessment Methodology
- Identifying Threats and Vulnerabilities in Aviation Systems
- Risk Evaluation and Ranking
- Conducting Cyber Risk Assessments for:
- Aircraft Systems (e.g., Avionics, Fly-by-Wire)
- Ground Infrastructure and IT Systems
- Communication Networks
- Case Study: Risk Assessment of Aircraft System Vulnerability
- Implementation of Risk Controls and Mitigation Measures
- Cybersecurity Tools and Best Practices (Monitoring, Firewalls, Access Control)
- Threat Detection and Prevention Strategies

Day 3: Incident Management and Response

- Incident Management Framework
- EASA Requirements for Cyber Incident Reporting
- Developing Incident Response Plans (IRPs)
- Identifying Causes, Response Actions, and Recovery Procedures
- Reporting Cyber Incidents under EASA Guidelines
- Root Cause Analysis and Corrective Actions
- Lessons Learned and Continuous Improvement
- Aligning Cybersecurity with Safety Risk Assessments

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

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

Aviation Regulatory Experts

SOFEMA AVIATION SERVICES

Learning Objectives

- Understand the key cybersecurity regulations and frameworks applicable to aviation, particularly those outlined by EASA.
- Identify and assess cybersecurity risks in aviation systems, including aircraft, ground infrastructure, and communication networks.
- Develop and implement cybersecurity strategies that align with Safety Management Systems (SMS) and EASA guidelines.
- Create and manage incident response plans to address cybersecurity threats, ensuring compliance with EASA's reporting and corrective action requirements.

Target Groups

- Safety Managers
- Compliance & Quality Managers
- Maintenance, Design, and Production Organization Personnel (EASA Part 21J, 21G, Part 145, and CAMO)
- IT and Cybersecurity Specialists in Aviation
- Operational and Senior Managers

Pre-requisites

The pre-requisites for this training include role-specific knowledge within an EASA organization, and familiarity with regulatory requirements and internal security procedures.

What do People Say about Sofema Aviation Services Training?

"The course content was highly relevant and well-presented."
"Interactive sessions helped clarify key concepts."
"The instructor's practical examples brought the material to life."

Duration

3 days – Start at 09.00 and finish at 17.00, with appropriate refreshment breaks.
To register for this training, please email team@sassofia.com or Call +359 28210806

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

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