Consider Aviation Industry Learning Objectives for Cybersecurity Training Compliant with EASA Requirements

Sofema Aviation Services (SAS) www.sassofia.com considers fundamental issues related to the challenge to address cyber security threats within EASA regulated Organisation

Learning Objectives for Cybersecurity in Aviation compliant with **EASA requirements**, shall align with **EASA regulations**.

- EASA emphasizes cybersecurity compliance focusing on protecting aviation systems, processes, and organizations from cyber threats.

Consider the following for further discussion:

Knowledge-Based Objectives - Students will gain foundational understanding of cybersecurity concepts within the aviation domain.

- Identify key cybersecurity regulations under EASA (e.g., EU Regulation 2019/1583, NIS Directive, AMC/GM guidance).
  - ***COMMISSION IMPLEMENTING REGULATION (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures***
  - ***EU's NIS Directive (Directive on security of network and information systems)***
- Explain the importance of cyber resilience in aviation (aircraft systems, ground infrastructure, communications).
- Define critical terms: cyber threats, vulnerabilities, mitigation, and risk assessment.
- Understand the cybersecurity roles and responsibilities of EASA-regulated entities (e.g., operators, CAMOs, Part 21J, 21G organizations).

Application-Based Objectives
Learners will be able to analyze and apply cybersecurity practices in aviation contexts.

- Perform cybersecurity risk assessments for aviation systems (aligned with EASA AMC/GM guidance).
- Identify cyber vulnerabilities in aircraft systems (e.g., avionics, fly-by-wire), IT systems, and operational networks.
- Describe how cybersecurity fits into Safety Management Systems (SMS) as required under ICAO Annex 19 and EASA SMS frameworks.

- Develop mitigation plans to address detected vulnerabilities.

Skill-Based Objectives

The focus is on developing hands-on competencies for cybersecurity professionals in aviation.

- Analyze **cybersecurity incidents** using case studies in aviation to understand root causes and lessons learned.
- Demonstrate the implementation of cybersecurity **best practices** across operational systems, focusing on risk controls and reporting mechanisms.
- Utilize cybersecurity **monitoring tools** and **threat intelligence platforms** in aviation systems.
- Prepare a **cybersecurity audit checklist** in line with EASA AMC guidelines for Part-145 maintenance and design organizations.

Compliance Objectives
Ensure alignment with EASA's specific cybersecurity requirements.

- Describe EASA's cybersecurity framework for the following domains:
  - Design Organizations (Part 21J)
  - Production Organizations (Part 21G)
  - Maintenance Organizations (Part 145)
- Discuss how organizations comply with EASA mandates regarding:
  - Reporting cybersecurity incidents (Part 21 and Safety Reporting).
  - Incorporating cybersecurity into continuing airworthiness processes under CAMO requirements.
- Develop awareness and culture-building strategies for promoting cybersecurity competence and accountability among aviation personnel.

Alignment with EASA Requirements

- **Integration into SMS**
  - Cybersecurity must be integrated into the SMS framework, requiring safety hazard identification, risk management, and continuous improvement.
- **Training Focus**

  - EASA mandates cybersecurity competence for personnel, emphasizing tailored training for specific roles:
    - Operational Personnel: Understanding basic cyber hygiene and secure communication practices.
    - Managers/Engineers: Identifying threats, applying risk controls, and ensuring compliance.
- **Compliance Culture -** Training must cultivate a compliance-driven approach to incident reporting, system monitoring, and proactive risk management.

Sample Learning Objective Statement

- By the end of the training, participants will be able to:
  - Identify and mitigate cyber risks in aviation systems, ensuring compliance with EASA requirements.
  - Apply cybersecurity measures within SMS frameworks for aviation safety and resilience.
  - Analyze and respond to cybersecurity threats effectively while maintaining operational continuity.

Next Steps

See the following 2 day course https://sassofia.com/course/implementing-information-cyber-security-program-easa-part-145-organization-2-days/ for comments or questions please email team@sassofia.com