

PRODUCT SHEET

Part-IS Foundation Training for Cybersecurity

EASA-approved eLearning for civil aviation organisations under the European Part-IS framework

EASA	REGULATORY	DELIVERY
Art. 92 - approved Part-IS Foundation Training for Cybersecurity	EU 2022/1645 · EU 2023/203	Self-paced eLearning · 8 hours

01 COURSE OVERVIEW

This EASA-approved course delivers structured foundation training on the information security risks that may affect aviation safety under the European Part-IS framework. It is designed for aviation organisations and the personnel required to understand, recognise and respond to these risks.

Content is aligned with Commission Delegated Regulation (EU) 2022/1645 and Commission Implementing Regulation (EU) 2023/203, and is structured to support documented training evidence and competent-authority oversight readiness.

02 WHO SHOULD ATTEND

▪ Air operators	▪ ANSP / ATM providers
▪ Aerodromes & airport operators	▪ CAMO organisations
▪ MRO / Part-145 organisations	▪ Technical staff
▪ Management & accountable managers	▪ Compliance, safety, security & IT personnel
▪ Operational & support personnel under Part-IS	

03 BENEFITS OF THE COURSE

▪ EASA-approved Part-IS Foundation Training for Cybersecurity	▪ Supports audit & competent-authority oversight readiness
▪ Aligned to EU 2022/1645 & EU 2023/203	▪ Self-paced eLearning for efficient organisation-wide rollout
▪ Practical aviation scenarios, plain-language delivery	▪ Suitable for technical and non-technical roles

04 COURSE AIMS

- Introduce the cybersecurity risk landscape in civil aviation and the increasing digital dependencies of aviation operations.
- Explain how cybersecurity and information security are connected to aviation safety and organisational resilience.
- Present the EASA Part-IS regulatory framework, including its purpose, scope, applicability and affected stakeholders.
- Explain the role of an Information Security Management System (ISMS) under Part-IS and its coordination with the Safety Management System (SMS).
- Introduce key concepts related to safety-relevant assets, threat identification, risk assessment, unacceptable risk and security controls.
- Clarify the basic principles of cybersecurity event and incident reporting, escalation and competent authority involvement.
- Raise awareness of third-party risks, personnel trustworthiness, competence and human factors in aviation cybersecurity.
- Support aviation organisations in building personnel-awareness evidence for audits, oversight activities and Part-IS compliance preparation.

05 COURSE AT A GLANCE

FORMAT	eLearning · self-paced
DURATION	8 hours
LEVEL	Foundation
LANGUAGE	English
CERTIFICATE	For completion of the EASA Approved training

06 CURRICULUM

Preface – Purpose, regulatory basis, scope, foundation level, eLearning methodology, abbreviations and definitions.

MODULE 1 Cybersecurity in Civil Aviation – Operational Context

- Digital Transformation of Aviation Systems
- Cyber Threat Landscape in Aviation
- Interdependency Between Cybersecurity and Aviation Safety
- Safety Impact vs. Operational Impact
- Stakeholders Subject to Part-IS
- Case Study: Ransomware Impacting Airport Operations

MODULE 2 Regulatory Framework of Part-IS

- Commission Delegated Regulation (EU) 2022/1645
- Commission Implementing Regulation (EU) 2023/203
- Scope and Applicability of Part-IS
- International Cybersecurity Frameworks
- Competent Authority Oversight

MODULE 3 Information Security Management System (ISMS) under Part-IS

- Definition and Purpose of ISMS in Aviation
- ISMS Structure and Governance
- Management Accountability and Personnel Roles
- Relationship and Coordination Between ISMS and Safety Management System (SMS)
- Identification of Aviation Safety-Relevant Assets
- Threat Identification and Risk Assessment Principles
- Concept of "Unacceptable Risk"
- Risk Prioritization at Foundation Level

MODULE 4 Security Controls and Incident Management

- Risk Treatment and Security Controls
- Monitoring and Continuous Improvement
- Information Security Incident Reporting
- Difference Between Event and Incident
- Reporting Flow and Escalation Principles
- External Providers Supporting Information Security Management Activities
- Personnel Trustworthiness and Competence

MODULE 5 Practical Application and Terminology

- Key Part-IS terminology explained in plain language
- Communicating cyber risk to non-technical management
- Practical aviation scenario: compromised flight planning system
- Lessons learned and organisational resilience
- Summary of key takeaways
- Practical consolidation of Part-IS concepts for professional communication

07 LEARNING OUTCOMES

On completion, learners will be able to:

- Describe the objective, scope and practical relevance of EASA Part-IS for aviation organisations.
- Explain how cybersecurity requirements support aviation safety and organisational resilience.
- Identify the key stakeholders, responsibilities and types of aviation assets affected by Part-IS.
- Recognise common cyber threat scenarios that may impact aviation systems, operations and safety-relevant processes.
- Explain the purpose, structure and governance role of an Information Security Management System (ISMS) in aviation.
- Understand the concept of unacceptable risk and the role of basic risk assessment in supporting compliance decisions.
- Distinguish between preventive, detective and corrective security controls, and understand how they contribute to reducing cyber risk.
- Outline the basic steps for reporting information security events and incidents under Part-IS.
- Use core Part-IS terminology accurately in professional communication with management, operational teams and compliance stakeholders.
- Communicate cyber risk in clear, non-technical language to support awareness, decision-making and organisational compliance.

08 AUDIT READINESS & CERTIFICATION

The course supports audit readiness through structured personnel foundation and documented training evidence.

Organisations may use completion records, certificates and the course outline to demonstrate that relevant personnel have received Part-IS foundation training.

09 DELIVERED BY

INFOSEC CENTER S.R.L. is a Romanian cybersecurity, audit and digital resilience company based in Iași, ISO/IEC 27001:2023 certified by TÜV AUSTRIA ROMANIA and attested by the Romanian National Cyber Security Directorate (DNSC) as a cybersecurity auditor for NIS2-related compliance. The company supports organisations in assessing cyber risks, strengthening digital infrastructure and implementing practical security measures for regulated and operational environments. INFOSEC CENTER is also connected to **FACTORY X.0 Global Forum**, a European initiative founded in Brussels by the company's team to support secure industrial digital transformation, innovation and collaboration across advanced technology ecosystems.

EDKORE is INFOSEC CENTER's eLearning platform for organisations, designed to support professional training and awareness programmes for employees across cybersecurity, data protection, digital transformation, artificial intelligence, emerging technologies and regulatory compliance. The Part-IS Foundation Training for Cybersecurity is an EASA-approved course, delivered through **EDKORE** as a specialised aviation course, supporting structured learning, learner completion tracking and documented training evidence.

Ensure full alignment with EASA Part-IS requirements.

Enroll your organisation today.

contact@edkore.com · www.edkore.com

+40 770 584 044