EASA
European Union Aviation Safety Agency

“Sharing of risks across different organisations”

Juan Anton
Cybersecurity in Aviation & Emerging Risks Section Manager

4th / 5th March 2020
2020 High Level Cybersecurity Conference
Madrid (Spain)

Your safety is our mission.

An Agency of the European Union

Key elements of the ISMS

Key elements of the ISMS

- **Establish, implement, maintain and continuously improve an ISMS. This ISMS shall (among other aspects):**
  - **Identify the organisation activities, facilities and resources, and the equipment, systems and services it provides, maintains and operates, which could be exposed to cyber risks.**
  - **Identify the interfaces with other organisations with which it shares cyber risks.**
  - Identify their **critical information and communication technology systems.**
  - **Perform information security risk assessments (initially and when changes occur).**
  - Develop and implement measures to **protect critical systems, data and processes.**
  - **Identify vulnerabilities and mitigate any unacceptable risks and vulnerabilities.**
  - Ensure that **personnel have the competences and skills** to perform their tasks.

Shared Trans-Organisational Risk Management (STORM):

Identification of interfaces with other organisations and standardisation of risk assessments

Shared Trans-Organisational Risk Assessments

- An essential part of the discussions within the ESCP.

- Two Sub-Groups:
  - Sub-Group 1: Standardisation of Risk Assessments
  - Sub-Group 2: Identification of interfaces and functional chains

- The outcome will be used in order to develop:
  - Acceptable Means of Compliance (AMC) and Guidance Material (GM) to complement the future Part-AISS rules.
  - Industry Standards which will be referred to in the AMC/GM.

EUROCAE Standards

Organisation level

- ED-201 - **Aeronautical Information System Security Framework Guidance, 2015**
- ED-2xx - **Guidance on Security Event Management, 2020**

Product (Aircrafts/STCs)

- ED-202A/DO-326A - **Airworthiness Security Process Specification, 2014**
- ED-203A/DO-356 - **Airworthiness Security Methods and Considerations, 2018**
- ED-204/DO-355 - **Information Security Guidance For Continuing Airworthiness, 2014**

ATM/ANS

- ED205 - **Security Certification and Declaration of ATM ANS Ground Sys., 2020**

EUROCAE ED201 expected evolutions

ED-201 is under revision to provide compliancy support to future EASA regulation. **Sub-Group 1 of the ESCP is contributing to this work.**

ED-201A expected to be published by the end of 2020. Will include guidance on:

EXTERNAL AGREEMENTS

An External Agreement addresses the fundamental information security problems caused by using 3rd party products, linking networks and sharing data.

RECOMMENDED CLAUSES for External Agreements

External Agreements are documented expressions of trust comprising an **auditable set of clauses** (mutual agreements) to ensure that external dependencies on partners have adequate controls for safe and secure air transport operation.

Shared Trans-Organisational Risk Assessments

- **Sub-Group 1: Standardisation of Risk Assessments**
  - Development of material for the standardisation of risks assessments, including common terms and definitions and contractual provisions between interfacing organisations in order to be able to assess and compare their shared risks.
  - This material will be used in AMC/GM material and Industry Standards (ED-201).
- **Sub-Group 2: Identification of interfaces and functional chains**
  - Identification of examples of chains of organisations and products/systems which are interconnected (end-to-end perspective). Risks are flowing along theses functional chains.
    - A particular organisation could be in several functional chains.
  - Development of maps (per aviation domain) showing examples of functional chains, in order to help organisations to identify their interfaces.
  - This material will be used for the development of AMC/GM material

Next steps

- **<u>5/6 March 2020:</u> Table-Top Exercise in Madrid (Spain)**
  - Test the methodology developed by the Sub-Group 1 on a number of example organisations, in order to assess the risks coming from their interfacing organisations/systems in the corresponding functional chain (developed by Sub-Group 2).
  - This will include participation of members from ESCP STORM Sub-Groups 1 and 2.
  - It will help fine-tune the amendments to ED-201.
- **<u>June 2020:</u> Submission of ED-201 changes for formal consultation.**
- **<u>End 2020:</u> Adoption of amendments to ED-201.**
- **<u>Not before beginning 2022:</u> Once the future Part-AISS rule is adopted by the European Commission, adoption by EASA of the associated AMC/GM material, with reference to the applicable standards.**

EASA
European Union Aviation Safety Agency

Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union