EASA
European Union Aviation Safety Agency

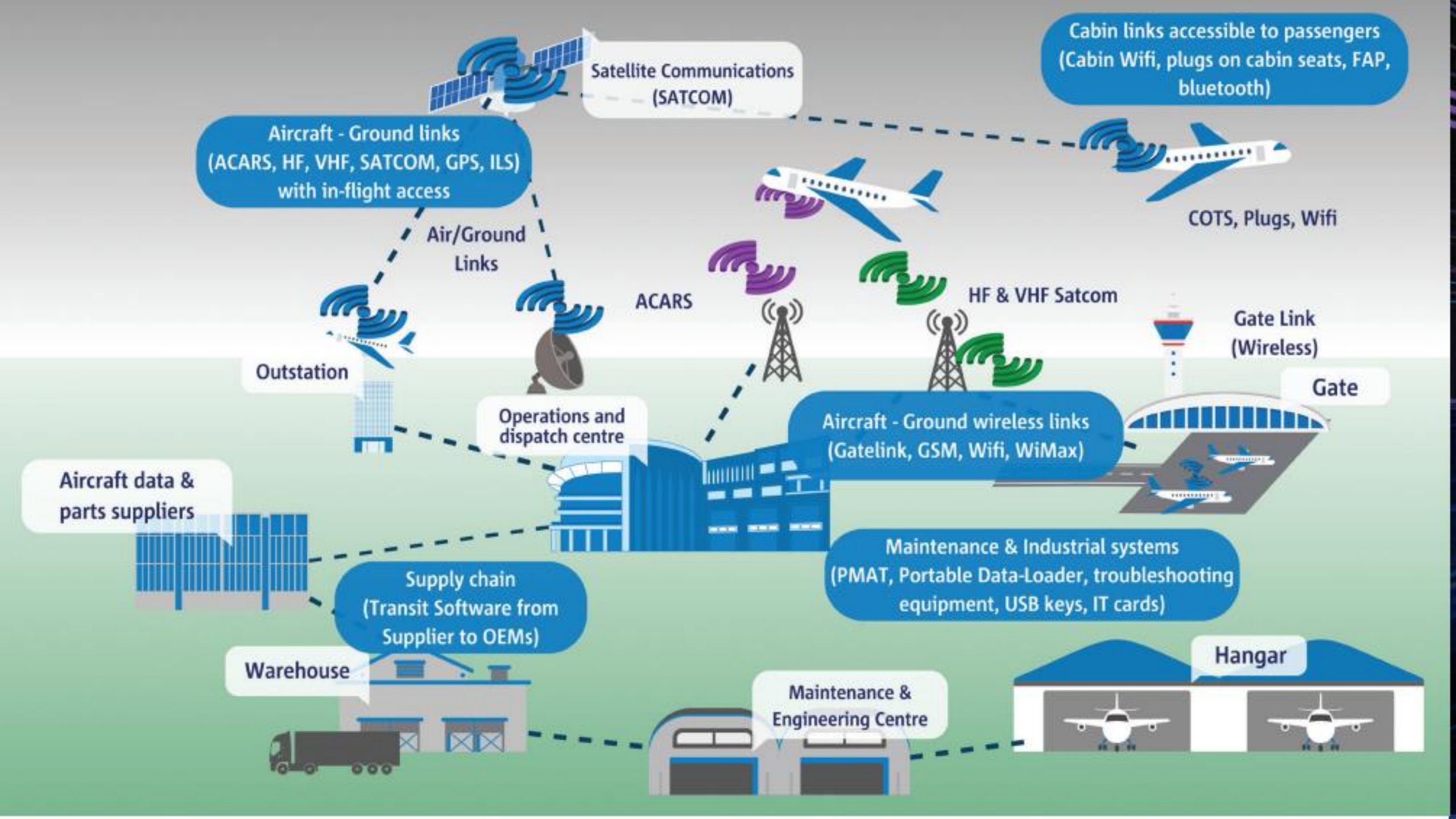
Introduction to Part-IS
EBAA Webinar

6 November 2025

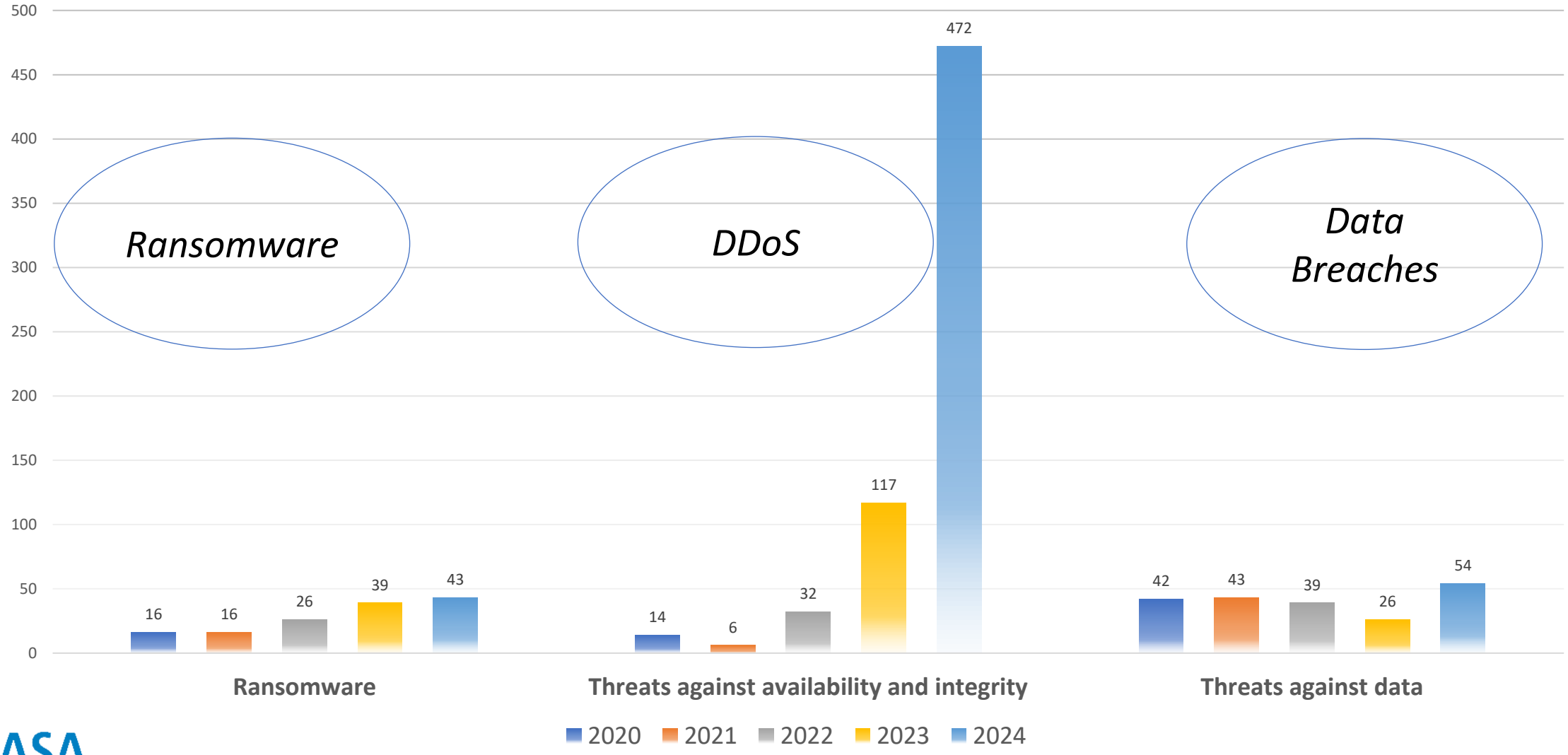
Gian Andrea Bandieri, *Section Manager Cybersecurity in Aviation and Conflict Zones*
Davide Martini, *Senior Expert Cybersecurity in Aviation*

Your safety is our mission.

An Agency of the European Union


Satellite Communications (SATCOM)
Cabin links accessible to passengers (Cabin Wifi, plugs on cabin seats, FAP, bluetooth)
Aircraft - Ground links (ACARS, HF, VHF, SATCOM, GPS, ILS) with in-flight access
Air/Ground Links
COTS, Plugs, Wifi
ACARS
HF & VHF Satcom
Gate Link (Wireless)
Outstation
Gate
Operations and dispatch centre
Aircraft - Ground wireless links (Gatelink, GSM, Wifi, WiMax)
Aircraft data & parts suppliers
Maintenance & Industrial systems (PMAT, Portable Data-Loader, troubleshooting equipment, USB keys, IT cards)
Supply chain (Transit Software from Supplier to OEMs)
Warehouse
Hangar
Maintenance & Engineering Centre

The (sad) reality - Statistics from EASA CTI team



Part-IS stands for Information Security

protection of *information* and *information systems* from unauthorised access, use, disclosure, disruption, modification, destruction to provide:

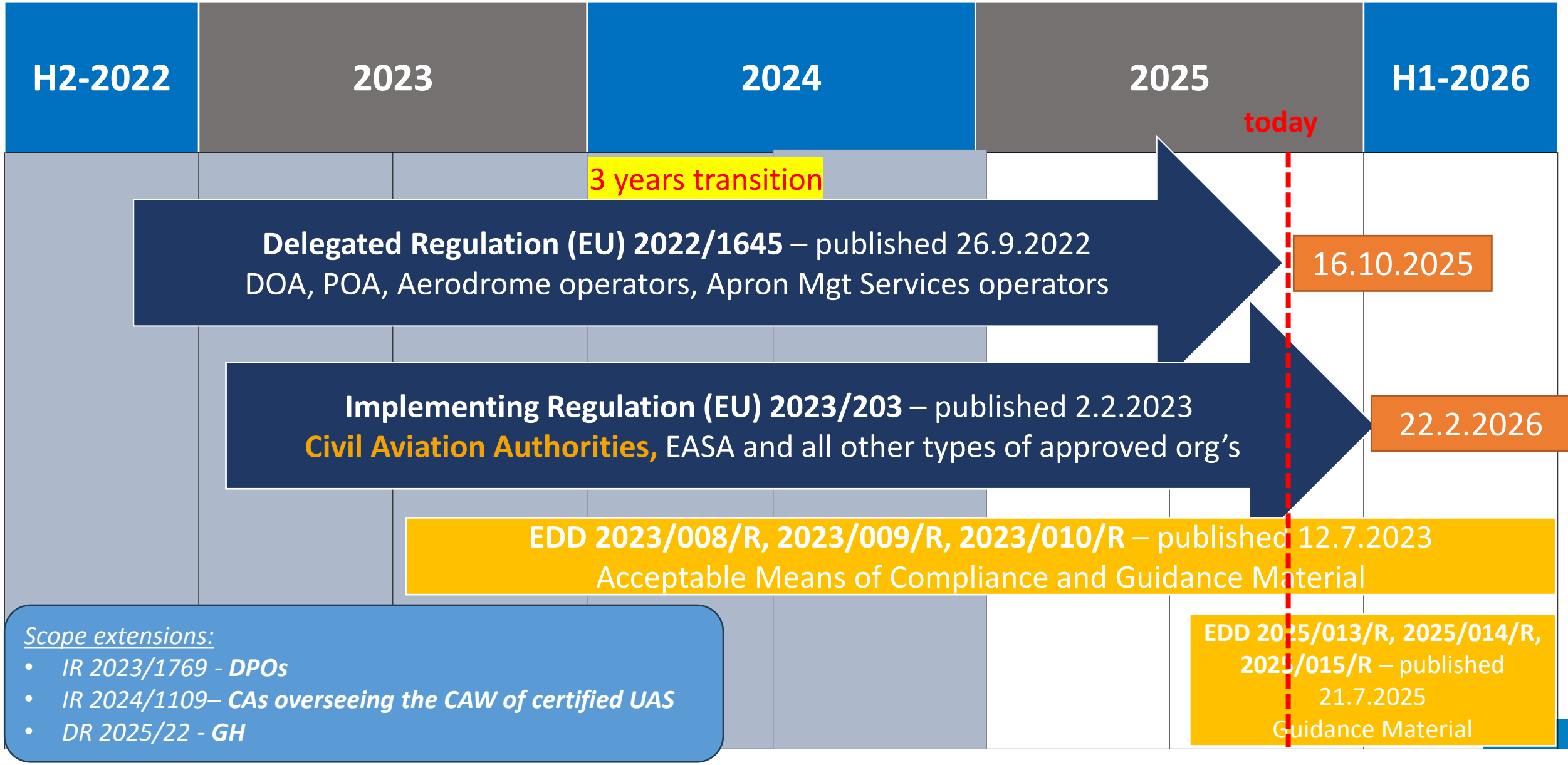
- Confidentiality
- Integrity
- Availability

What we want to achieve with Part-IS

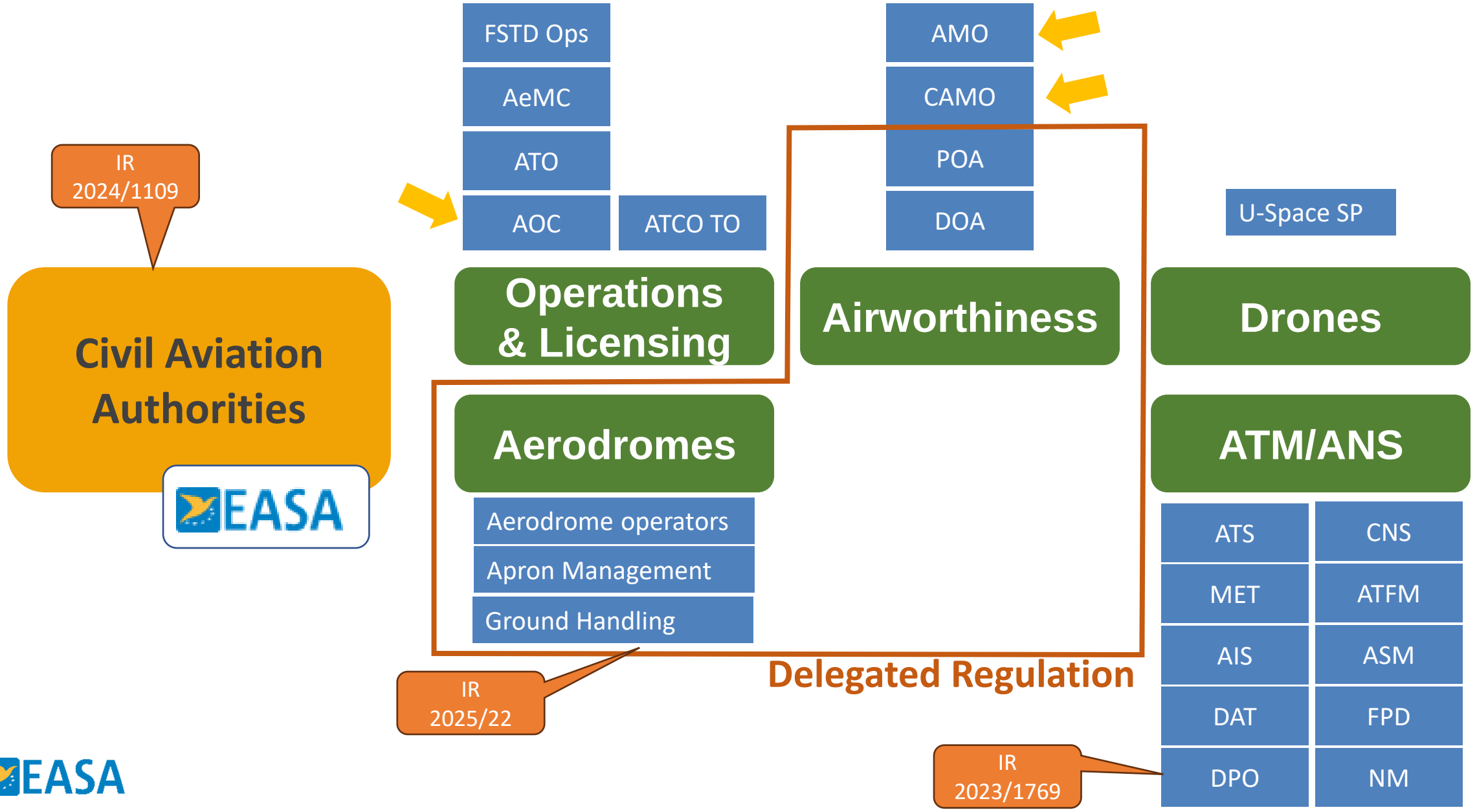
Objective	Protect the aviation system from information security risks **with potential impact on aviation safety**
Scope	Information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes
Activity	- **identify and manage** information security risks related to information and communication technology systems and data used for civil aviation purposes; - **detect** information security events, identifying those which are considered information security incidents; and - **respond** to, and **recover** from, those information security incidents

Proportionate to the impact on aviation safety

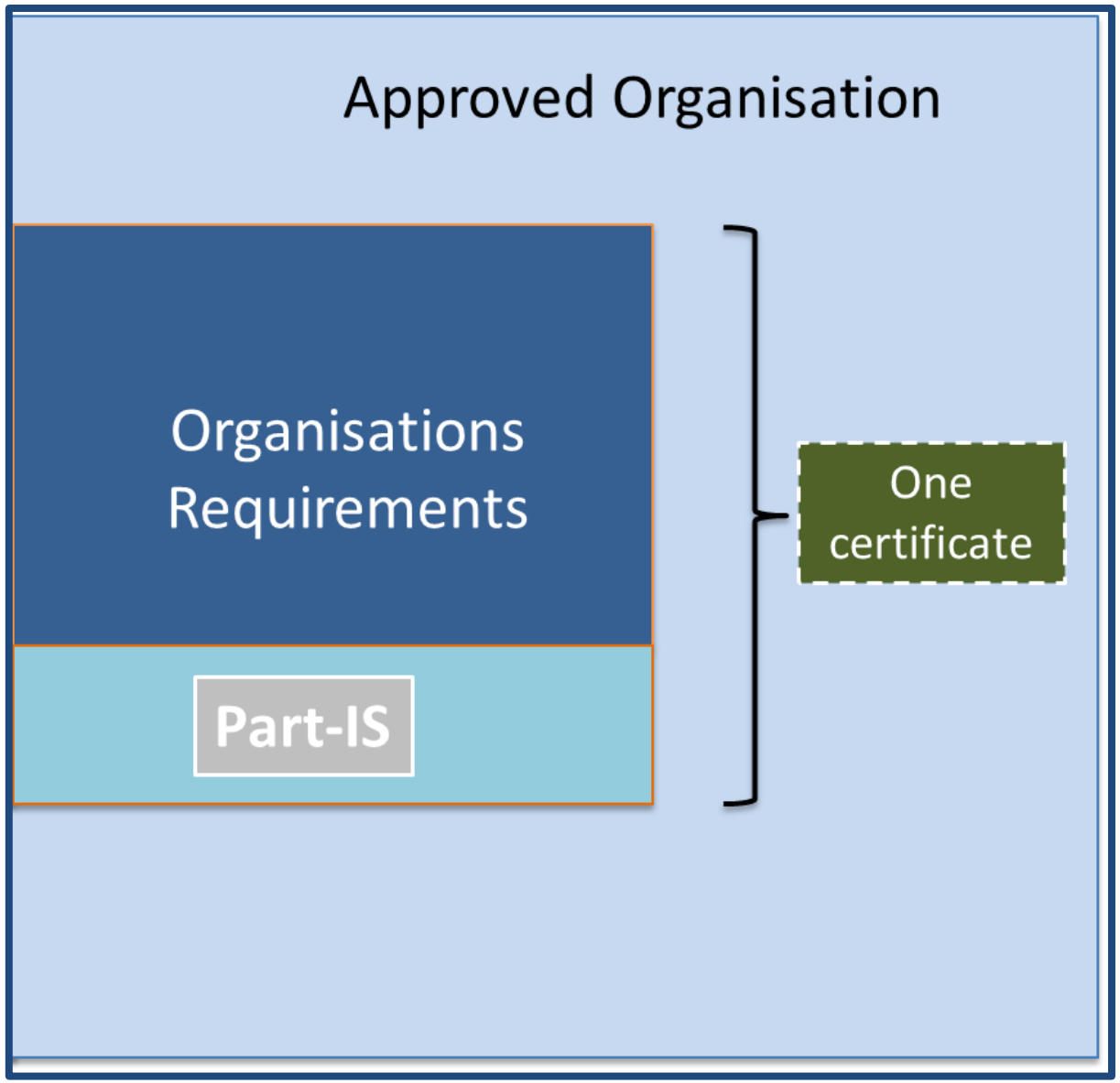
Part-IS implementation journey



Applicability of Part-IS

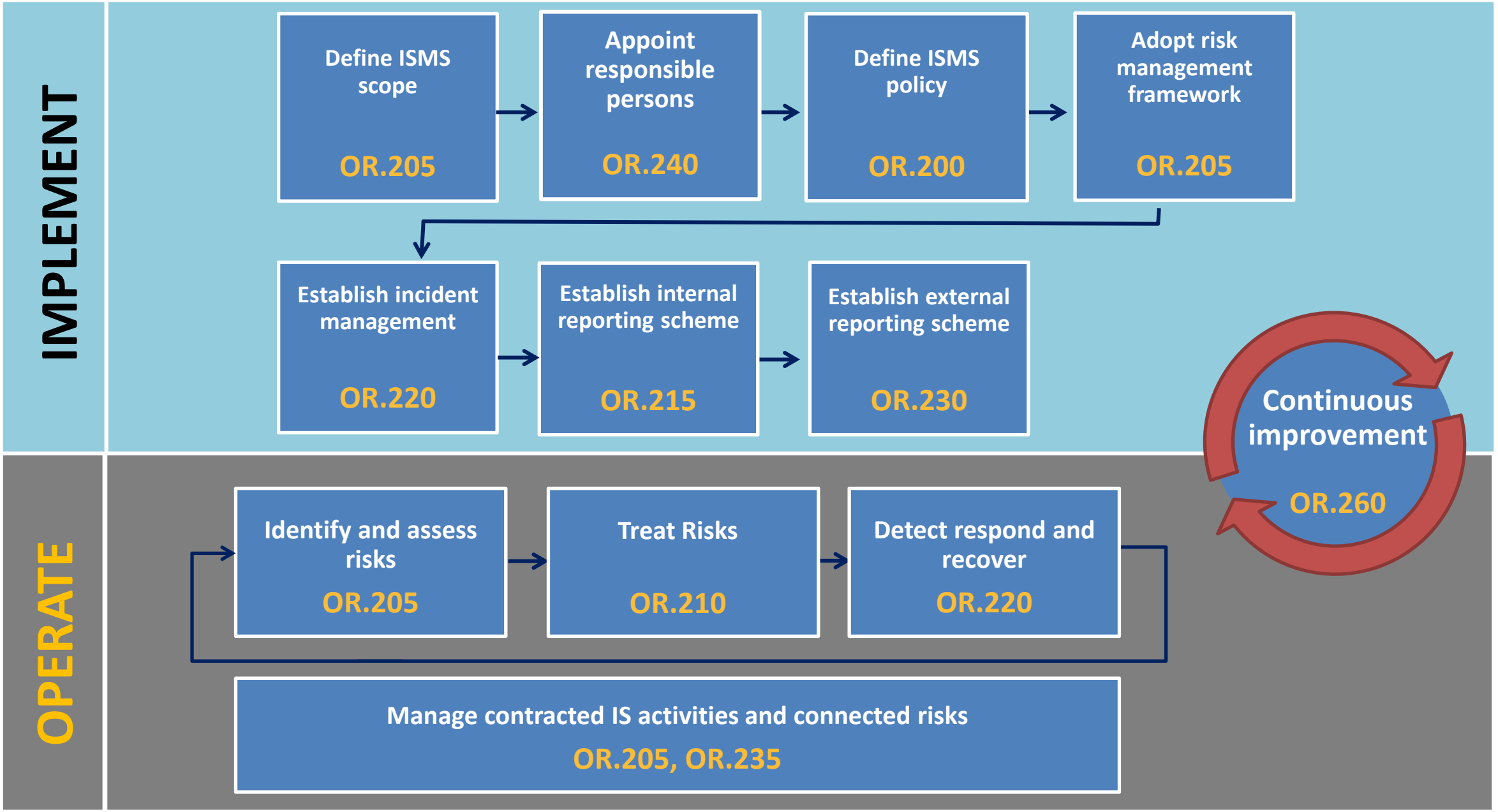


Part-IS and existing approvals/regulations

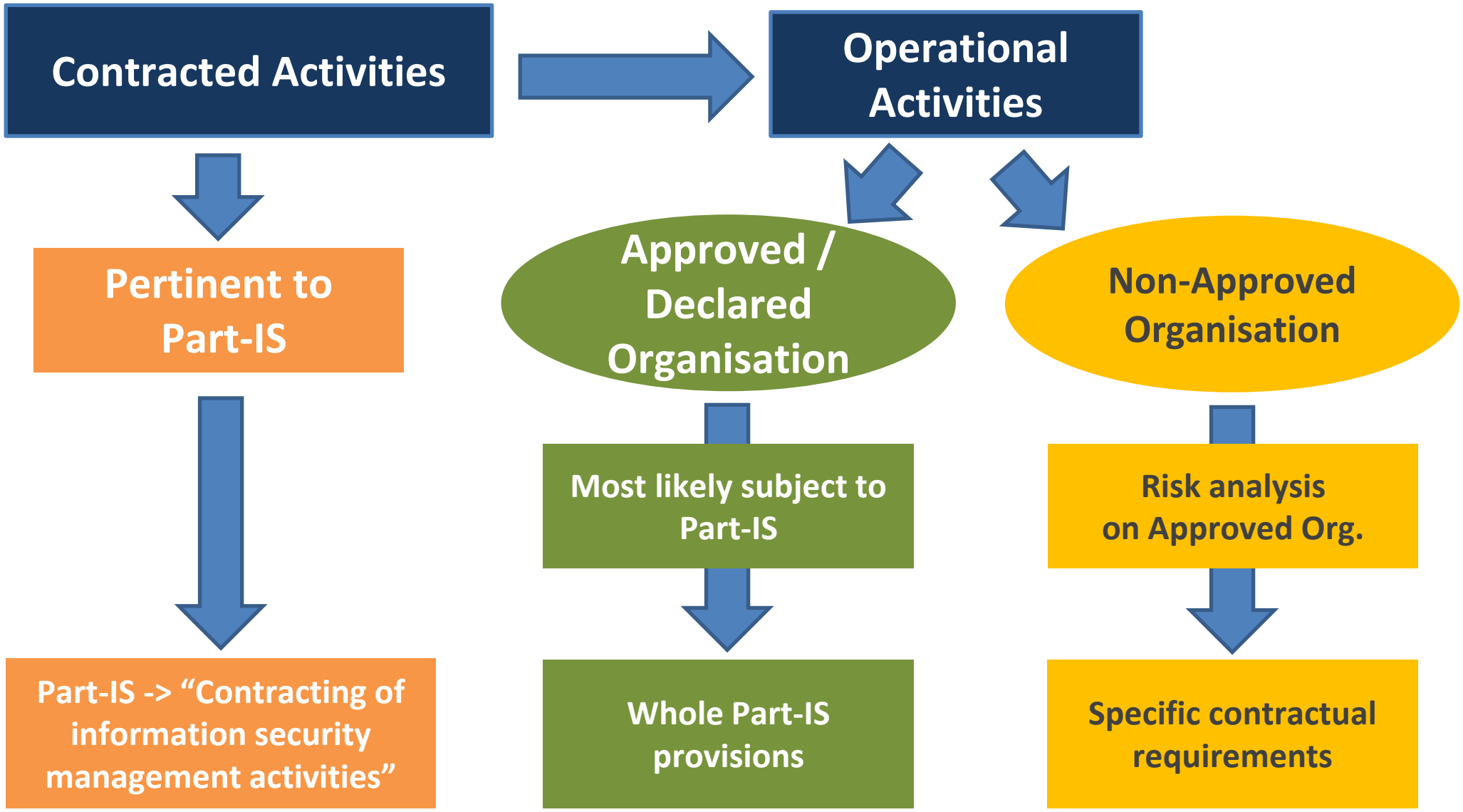


How to protect an organisation?

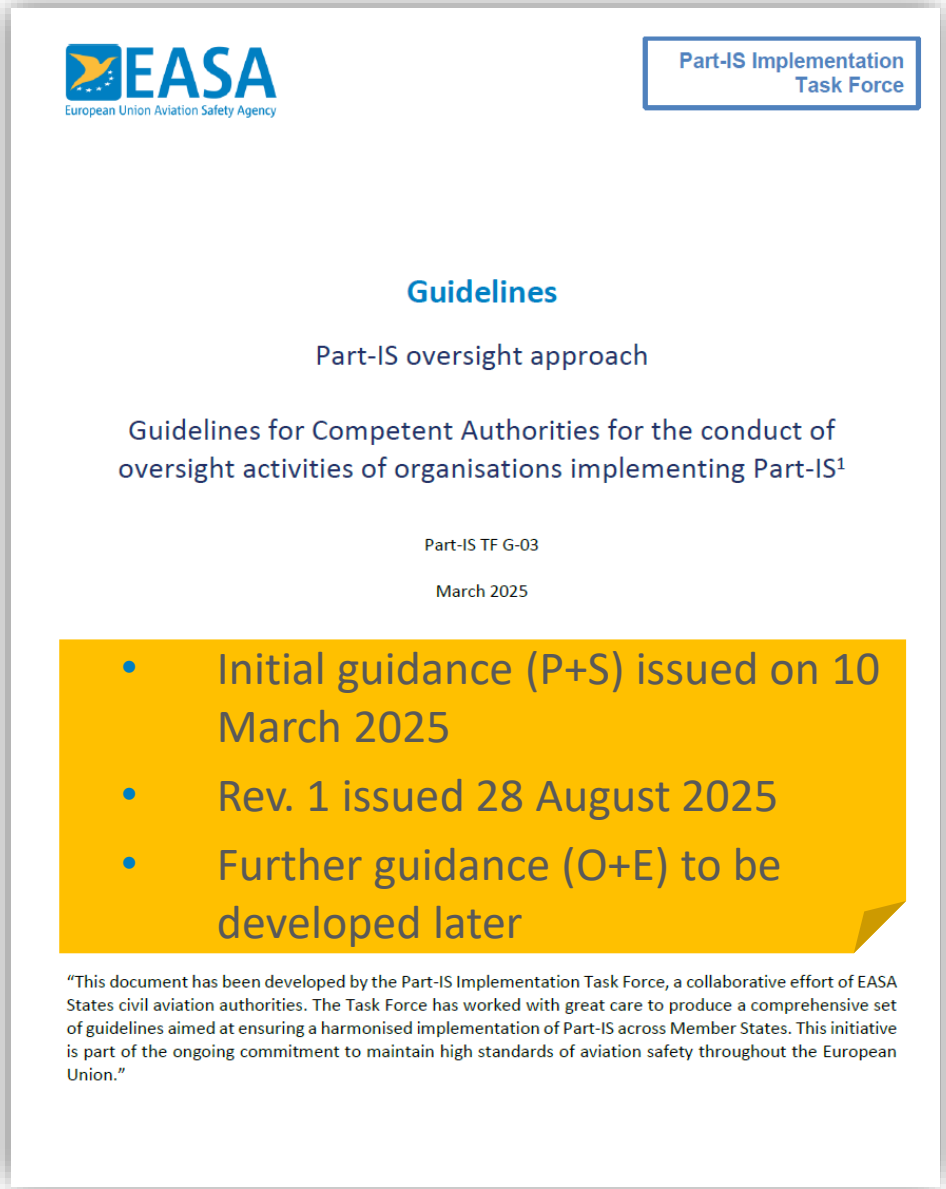
→ Each organisation shall set up, implement and maintain an **information security management system** (ISMS)


IMPLEMENT
Define ISMS scope
OR.205
Appoint responsible persons
OR.240
Define ISMS policy
OR.200
Adopt risk management framework
OR.205
Establish incident management
OR.220
Establish internal reporting scheme
OR.215
Establish external reporting scheme
OR.230
Continuous improvement
OR.260
OPERATE
Identify and assess risks
OR.205
Treat Risks
OR.210
Detect respond and recover
OR.220
Manage contracted IS activities and connected risks
OR.205, OR.235

How to handle the supply chain



Guidelines on oversight approach



EASA
European Union Aviation Safety Agency

Part-IS Implementation Task Force

Guidelines

Part-IS oversight approach

Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS[1]

Part-IS TF G-03

March 2025

- Initial guidance (P+S) issued on 10 March 2025
- Rev. 1 issued 28 August 2025
- Further guidance (O+E) to be developed later

"This document has been developed by the Part-IS Implementation Task Force, a collaborative effort of EASA States civil aviation authorities. The Task Force has worked with great care to produce a comprehensive set of guidelines aimed at ensuring a harmonised implementation of Part-IS across Member States. This initiative is part of the ongoing commitment to maintain high standards of aviation safety throughout the European Union."

- → Objective: harmonised and uniform implementation of oversight
- → Non-binding guidelines
- → Jointly drafted and agreed by all NAAs in the Part-IS Task Force
- → EASA adopts these guidelines in its capacity as Competent Authority
- → National adaptation possible, but not desirable (level playing field impacted)

Oversight approach

After applicability date

Effective

Optimized systems/processes that are resilient and sustain high performance under diverse scenarios

Operational

Fully functional systems demonstrating consistent and efficient performance under typical conditions

Initial compliance threshold

Suitable

Systems/processes meet baseline suitability criteria and are validated for fit-for-purpose use

Present

Basic awareness and establishment of foundational systems and minimal operational capabilities

At applicability date

Part-IS Regulations

Delegated Regulation No 2022/1645

- Cover Regulation
- Annex I D.OR

Implementing Regulation No 2023/203

- Cover Regulation
- Annex II I.OR
- Annex I AR
- Amendments to domain specific ARs

ED Decisions 2023/008 and 2025/013

AMC/GM to Cover Regulations

ED Decisions 2023/009 and 2025/014

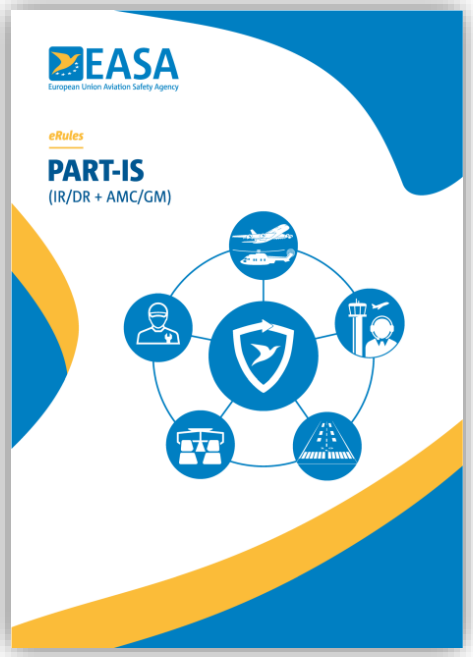
AMC/GM to Organisation Requirements

ED Decision 2023/010 and 2025/015

AMC/GM to Authority Requirements

Amdts to existing AMC/GM for ARs

6 ED Decisions



Easy Access Rules available here

Available guidance

Part-IS task force

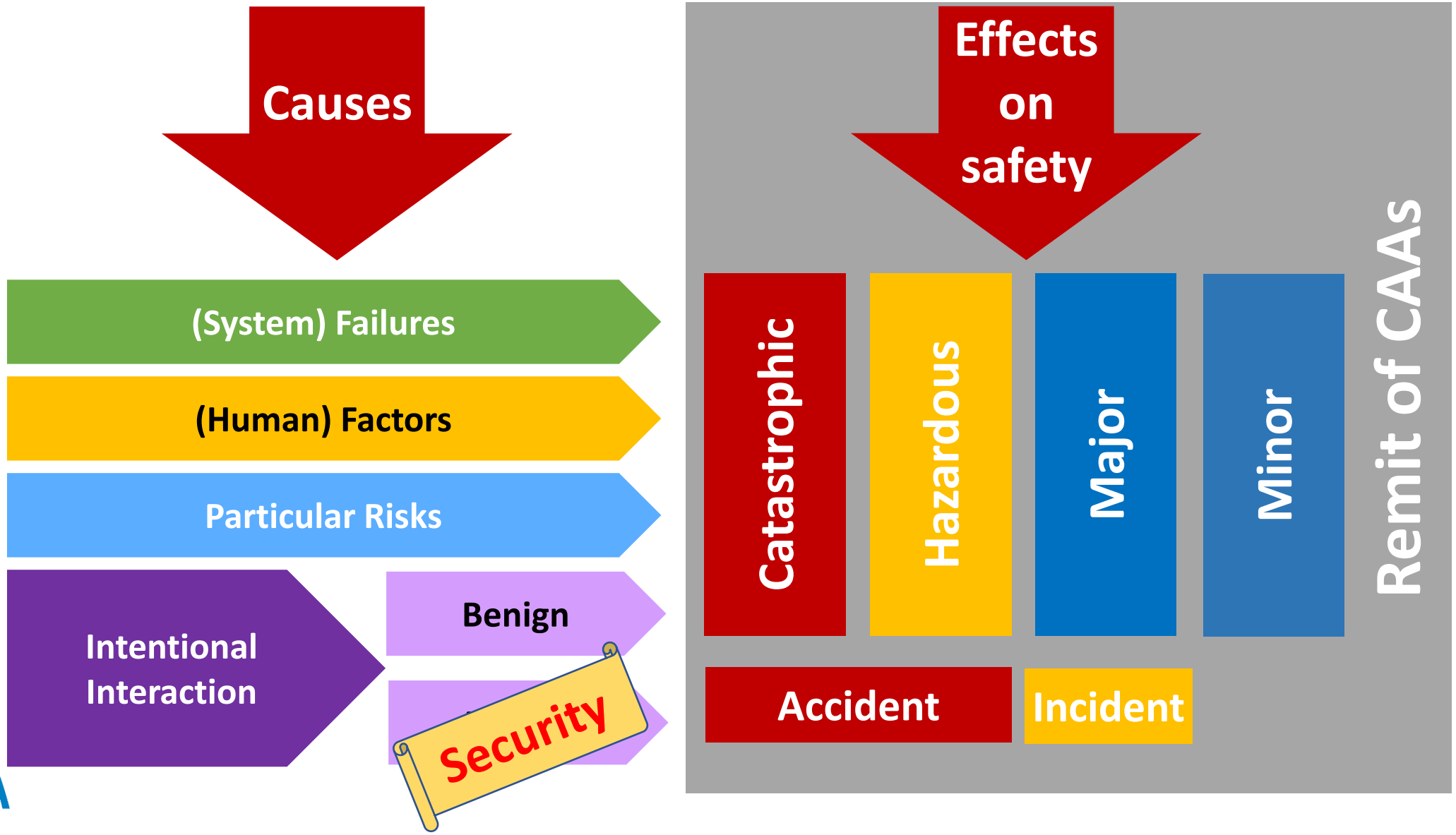
- → Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS
- → Implementation guidelines for Part-IS - IS.I/D.OR.200 (e)
- → Part-IS Oversight Approach Guidelines

EASA + others

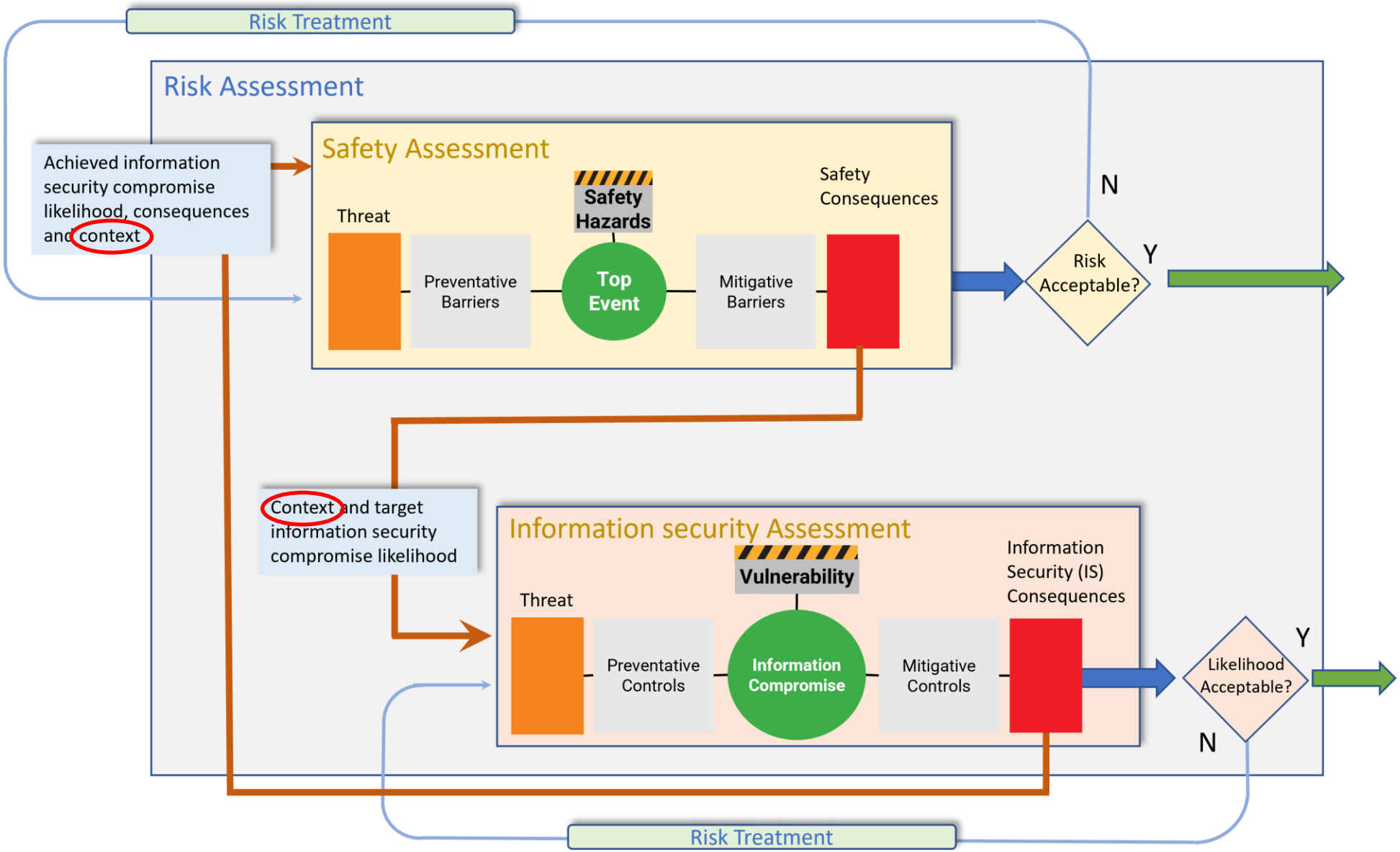
- → Frequently asked questions
- → Part-IS self assessment tool (beta version)

IS RISK MANAGEMENT THROUGH A SAFETY LENS

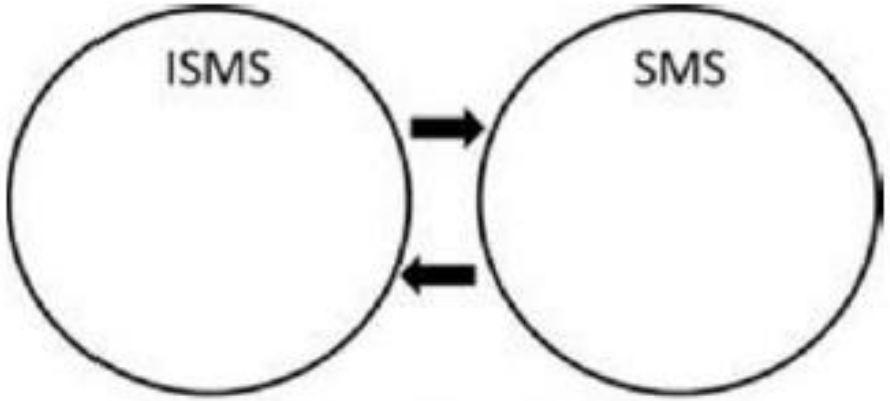
Relation between Causes and Effects



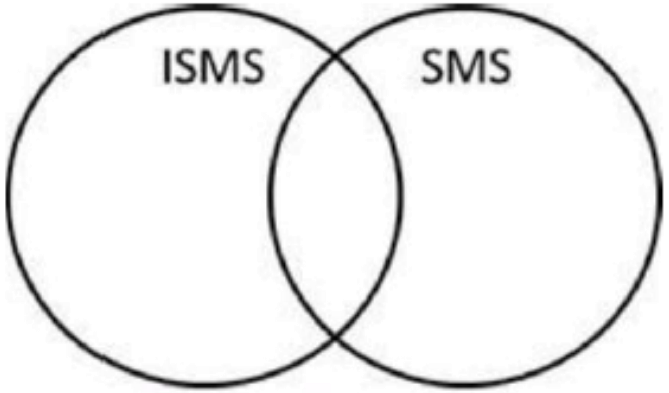
Interacting Safety & Info Sec Risk Assessment



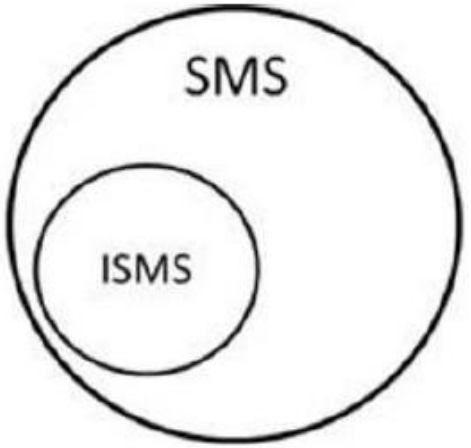
ISMS and SMS interaction



ISMS and SMS are inter-connected siblings



ISMS partially overlapping with SMS



ISMS embedded in SMS

Safety Reminder

→ All requirements related to **Safety** are applicable to any Information Security measure, as they are part of the same context:

Architecture, Perimeter, Environment

→ The level of (**Safety**) severity determines, how "badly" an organisation has to avoid them happening

Acceptable Risks, Assurance Level

Part-IS: main takeaways

WHAT:
A set of rules laying down requirements for the management of information security risks with a potential impact on aviation safety for aviation organisations and authorities across the entire aviation domain.

WHY:
To protect information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes from information security risks with potential impact on aviation safety

WHEN:
16 OCT 2025 for DOA, POA, Aerodrome operators, Apron Mgt Services operators

22 FEB 2026 for Civil Aviation Authorities, EASA and all other types of approved organisations

WHO:
In Europe: all approved organisations – some exemptions apply, derogations are possible

Outside Europe: all organisations holding an EASA approval, MOA, ATO, ANSP

Not applicable to TCO operators

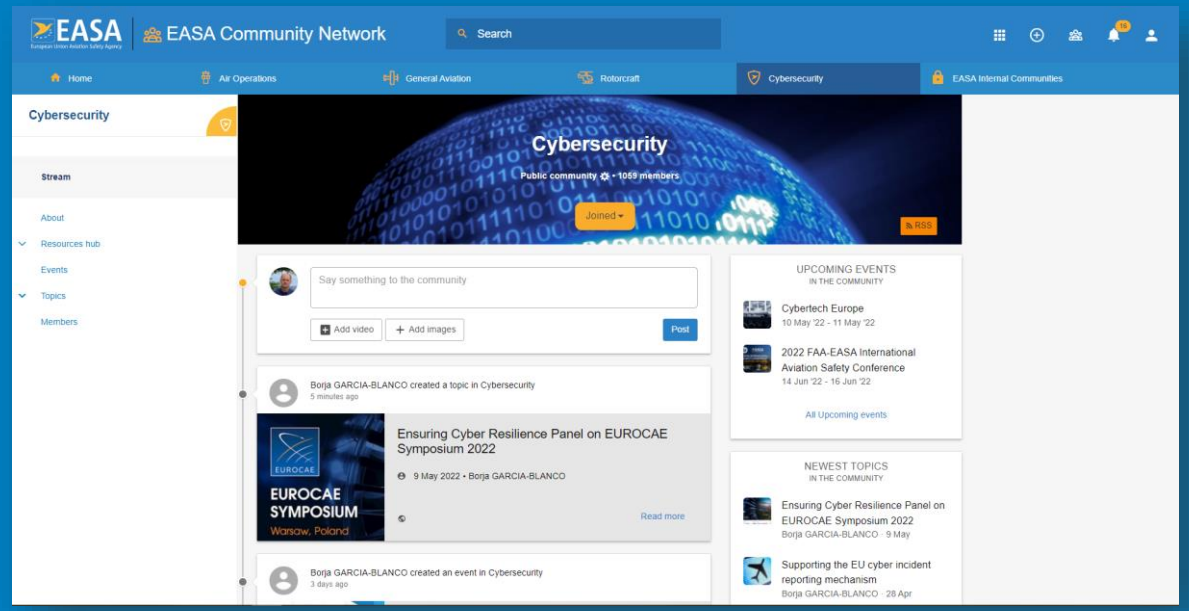
HOW:
Implement an ISMS:

- Know your risk
- Manage your risks
- Report incidents
- Adapt and improve

EASA
European Union Aviation Safety Agency

Thank you!

Join our Community:
https://www.easa.europa.eu/community/cybersecurity



Contact us at:
cybersec@easa.europa.eu

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union