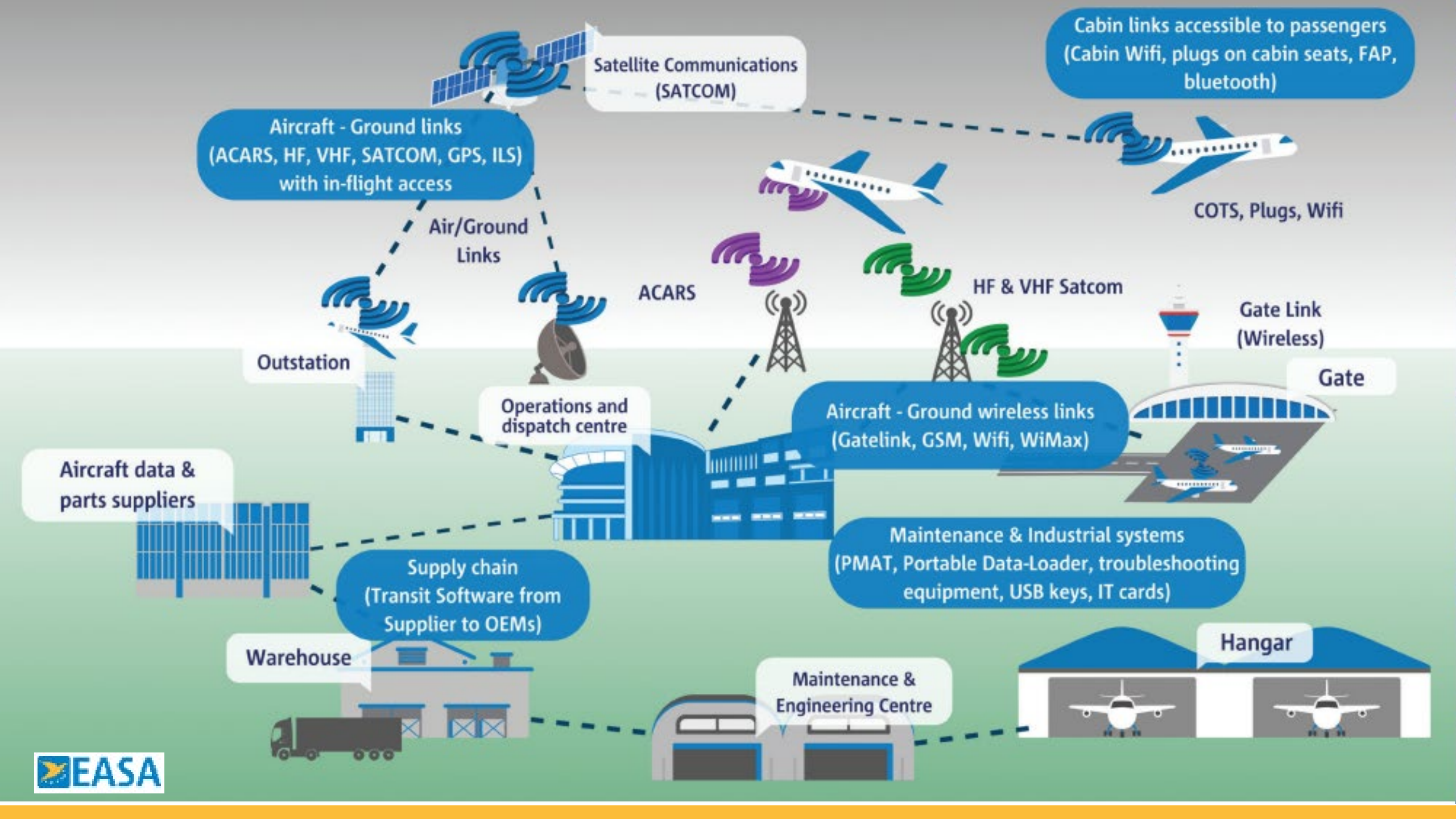
EASA
European Union Aviation Safety Agency

EASA Workshop

Electronic Flight Bag (EFB) ETSO

Part-IS Presentation

Davide Martini
Senior Expert – Cybersecurity in Aviation
Cybersecurity in Aviation & Emerging Risks


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
EASA

Making EU aviation cyber resilient

Products (Aircrafts, Engines, …)

- Transition from case by case approach to mandatory on all products now done.
- Positive change of mind set in industry: From defiance to full engagement.

Organisations (People, Processes)

- **Part-IS** Regulations published in October 2022 and February 2023
- AMC/GM published on 12 July 2023

Information Sharing

- Create a community to
  - Share knowledge
  - Perform Analysis
  - Collaborate
  - Reinforce the system

Capacity building & Research

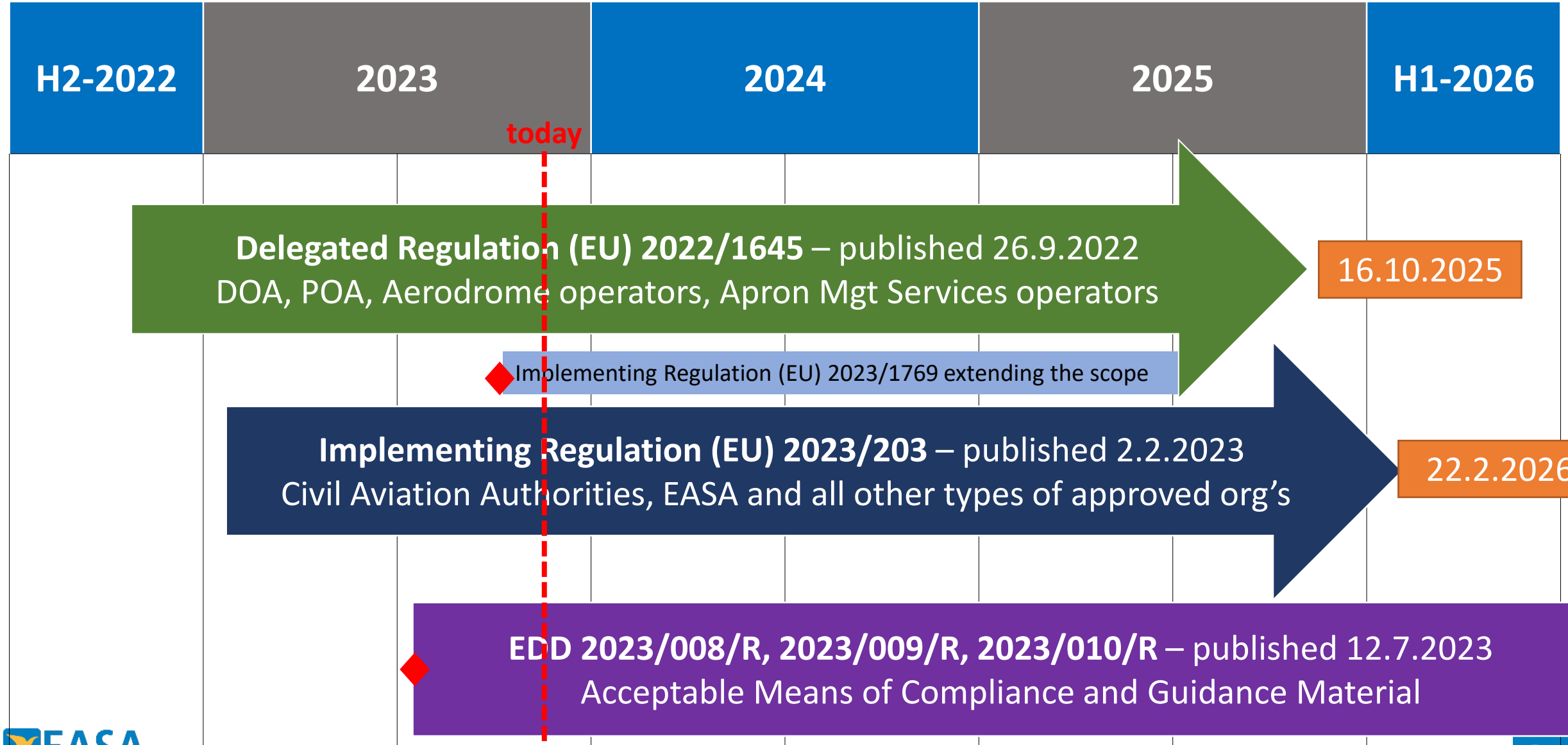
- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape

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



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 Decision 2023/208

AMC/GM to Cover Regulations

ED Decision 2023/209

AMC/GM to Organisation Requirements

ED Decision 2023/210

AMC/GM to Authority Requirements

Amdts to existing AMC/GM for ARs

3 ED Decisions

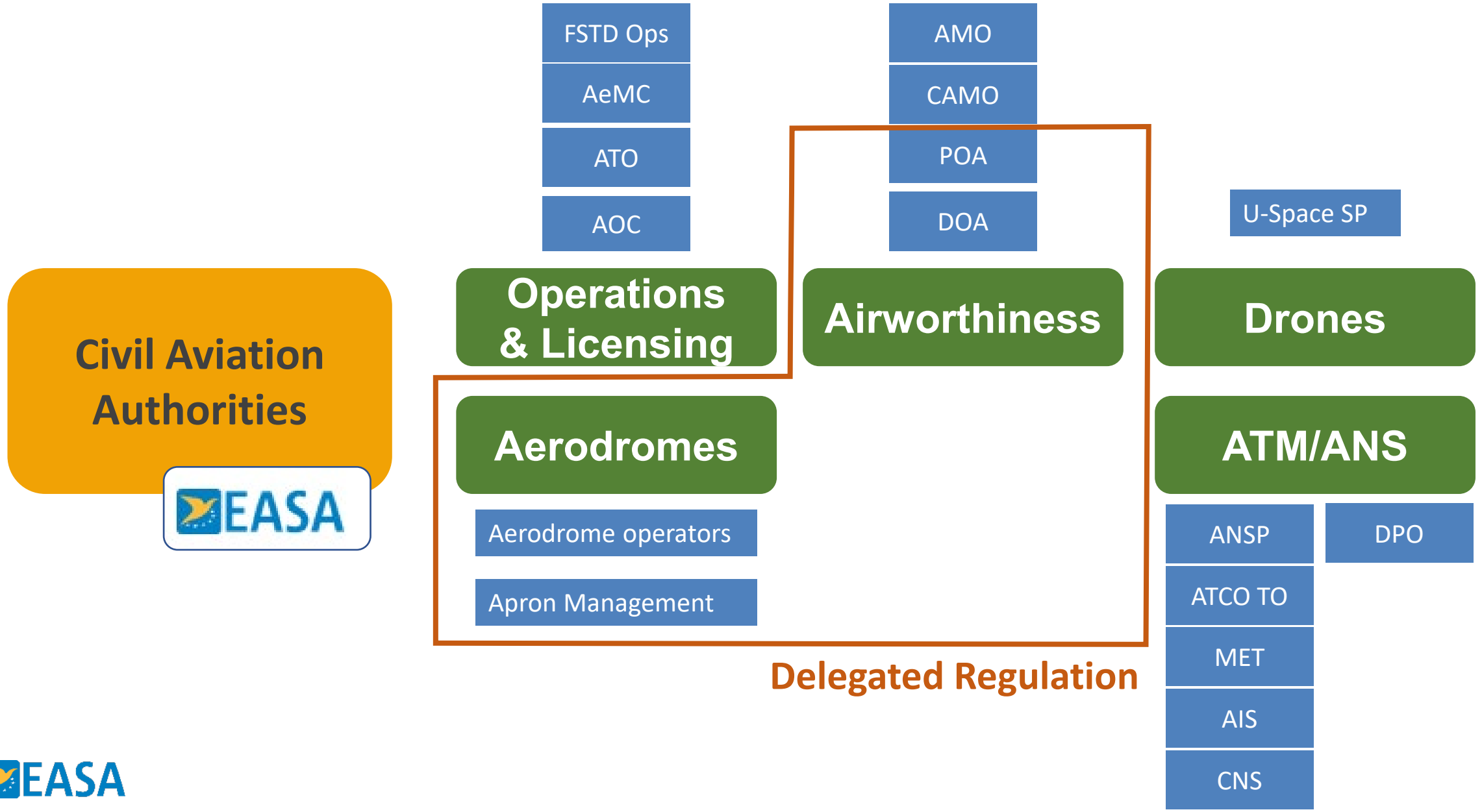
Easy Access Rules available here

AMC & GM what's in it

- → **Non-binding by definition**
- → **To facilitate timely and harmonised application of Part-IS**
- → **No additional requirements. Everything is in the Regulations**

Acceptable Means of Compliance	Guidance Material
• To address identified rule's objectives and processes • Possible ways to comply with the requirements	• To address elements in the rule that would require explanation • To integrate means of compliance by providing guidance on practical or operational aspects • Background information helping to understand the requirements

Applicability of Part-IS



Part IS is not applicable to:

Production organisations not holding an approval

Part-147 maintenance training organisations.

ATOs providing only theoretical training.

Private operators of other than complex motor-powered aircraft.

Organisations dealing only with light aircraft:

- e.g. airplanes below 2000 kg MTOM, very light rotorcraft, sailplanes, balloons and airships.

Operators of UAS in the “open” and “specific” categories.

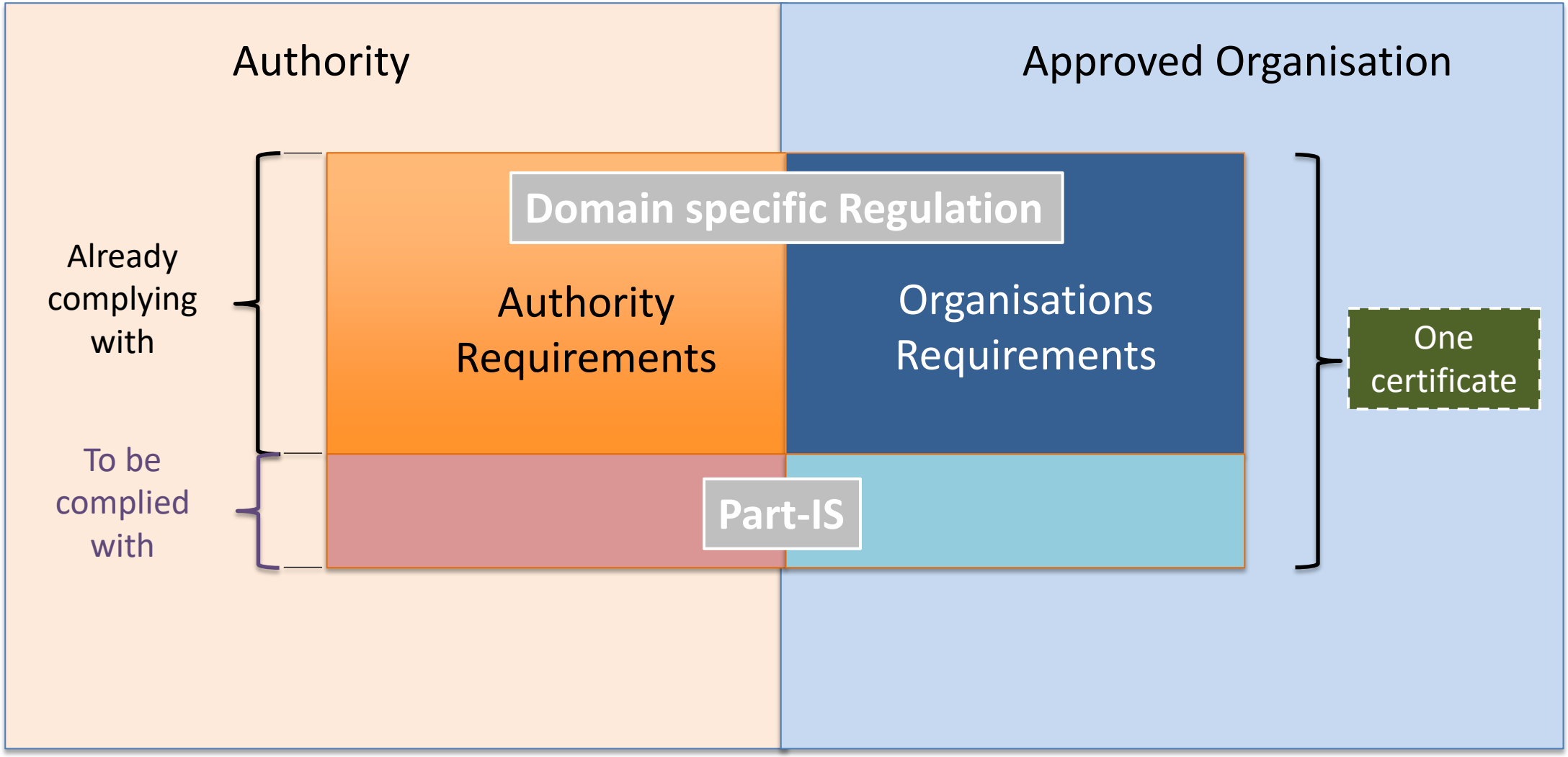
Organisation designing UAS in the “specific” category when not required to hold a DOA approval.

TCO operators

Regulated by ICAO Annex 6

Organisations approved under bilateral agreements

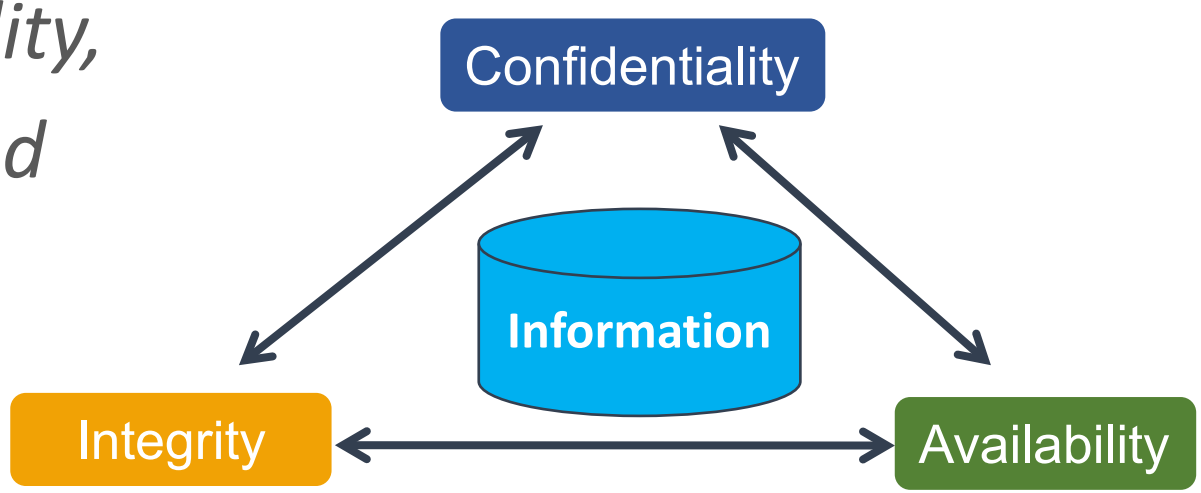
Part-IS and existing approvals/regulations



What is an ISMS?

What is Information Security Management?

- ISO 27000 states that ***Information Security Management*** *is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their*
  - *Confidentiality,*
  - *Integrity, and*
  - *Availability.*



What is an ISMS?

ISO 27001

An ISMS is the means by which management monitors and controls information security, minimizing the residual **business risk** and ensuring that information security continues to fulfill corporate, customer and legal requirements.

business risk

Part-IS

An ISMS is the means by which management monitors and controls information security, minimizing the residual business **safety risk** and ensuring that information security continues to fulfill ~~corporate, customer and~~ legal requirements and societal expectations.

safety risk

What are the Key Ingredients for Part-IS?

Basic Regulation

- Acceptable Safety Risks
- Record-keeping
- Personnel Requirements

ISO 2700x

- Information Security Management System (ISMS)
- Information Security Risk Assessment
- Continuous Improvement

NIST Cyber Security Framework

- Information Security Risk Treatment
- Information Security Incidents — Detection, Response, and Recovery

Reporting Regulation

- Information Security External Reporting Scheme

Part-IS vs existing Framework and Regulations

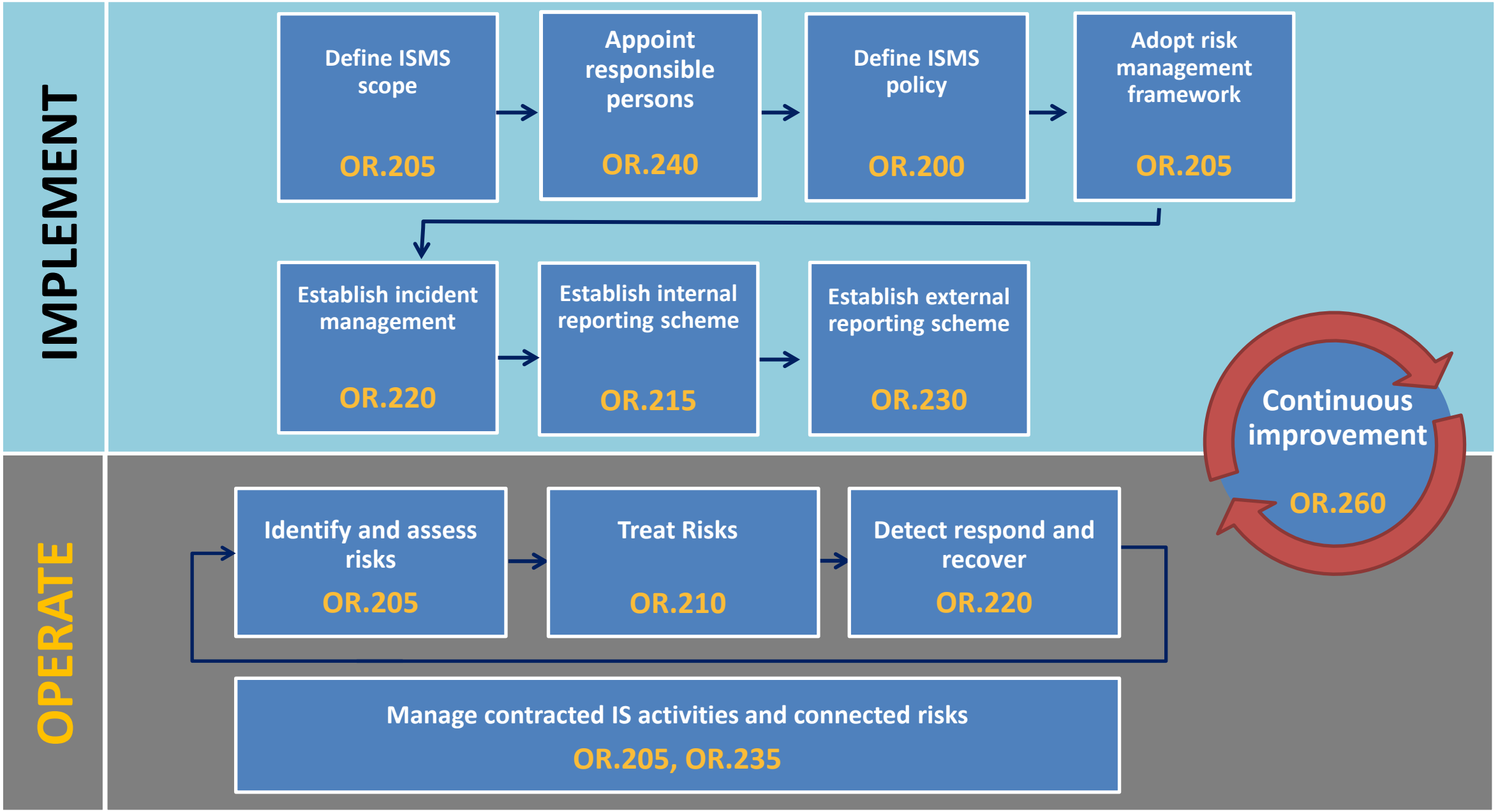
IS.OR.200 Policy on information security	IS.OR.205 IS Risk Assessment	IS.OR.210 Information Security Risk Treatment	IS.OR.220 Detection, Response, Recovery of Incidents
IS.OR.215 IS Internal Reporting Scheme	IS.OR.230 IS external reporting scheme	Implement authority measures as immediate reaction to Incidents or Vulnerabilities	IS.OR.225 Response to findings by the authority
IS.OR.235 Contracting of IS management activities	IS.OR.240 Personnel requirements	IS.OR.245 Record-keeping	IS.OR.200 Compliance monitoring

IS.OR.250 Information security management manual (ISMM)

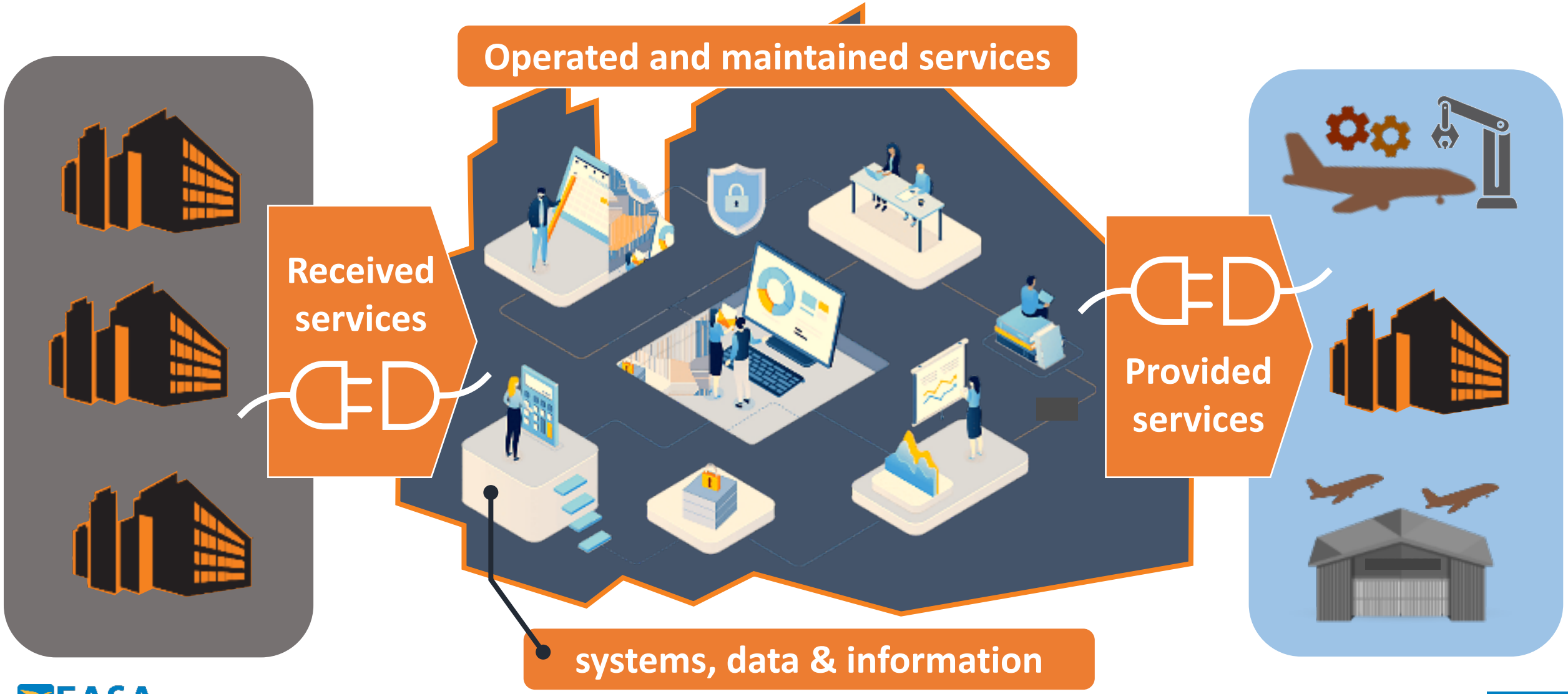
IS.OR.255 Changes to the information security management system

IS.OR.260 Continuous improvement

Colour code: NIST Framework | ISO 2700x | Basic Reg. | Reporting Reg.


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

Risk assessment - scope identification



EASA
European Union Aviation Safety Agency

Thank you for your attention!

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union