PANEL:
EU REGULATION AGENDA AND ITS IMPACT ON THE CYBERSECURITY MARKET

MODERATOR:

Sofia-Roxana BANICA

Market, Certification and Standardisation Unit - ENISA

Cybersecurity Officer

Christin Hartung-Kuemmerling

Federal Office for Information Security, Germany

Head of Division

Volkmar Lotz

SAP

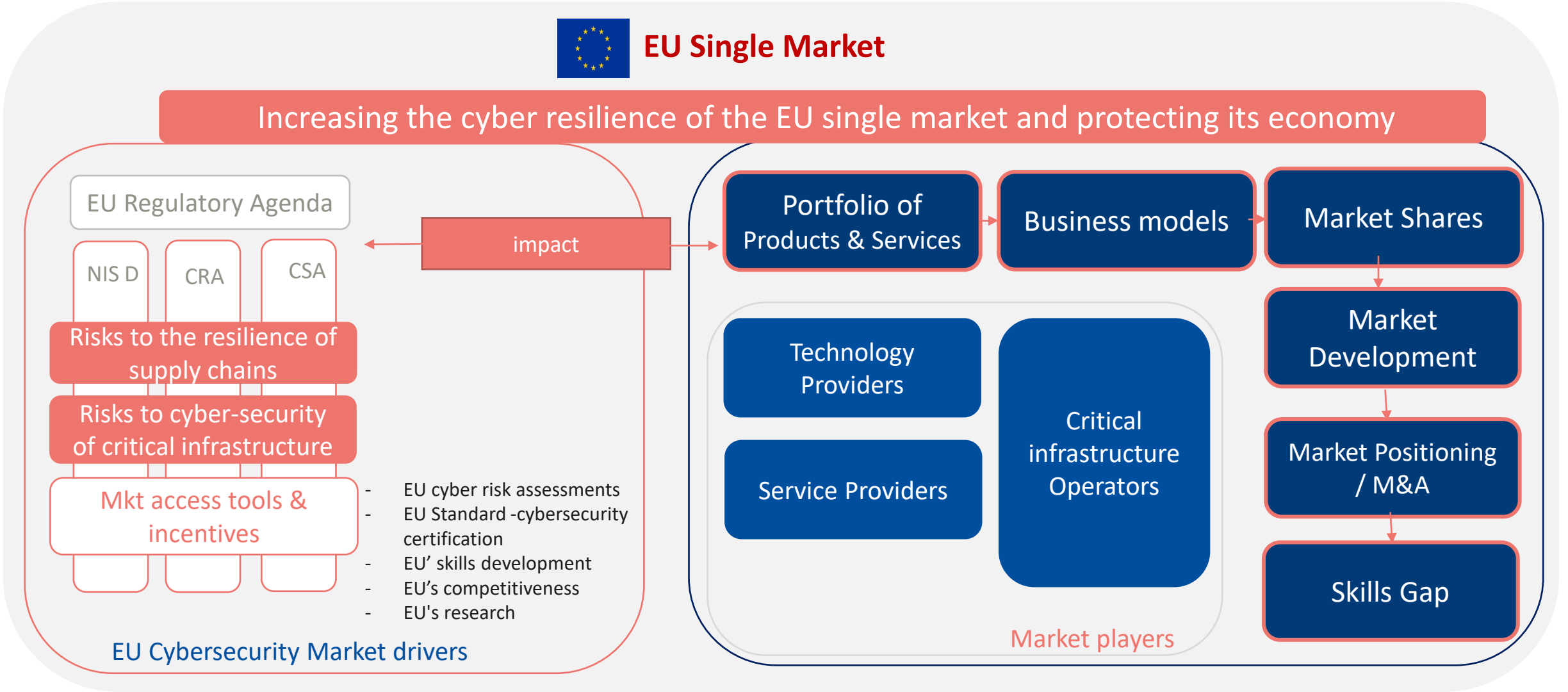
Head SAP Security Research

Davide Martini

Senior Expert - Cybersecurity in Aviation

EU Agency for Aviation Safety (EASA)

THE PANEL OVERVIEW :
EU REGULATION AGENDA and its **IMPACT on THE CYBERSECURITY MARKET**



THE PANEL OBJECTIVE

Bringing value

This panel will contribute to the analysis of regulatory initiatives vis-a-vis perception and impact they may have on the EU Single Market and the ability of EU economic actors to develop the internal market.

Disclaimer:

All speakers will speak in their own capacity and from their experience accumulated in existing roles, not generating opinions on behalf of the institution they represent.

I. RISKS TO THE RESILIENCE OF SUPPLY CHAINS

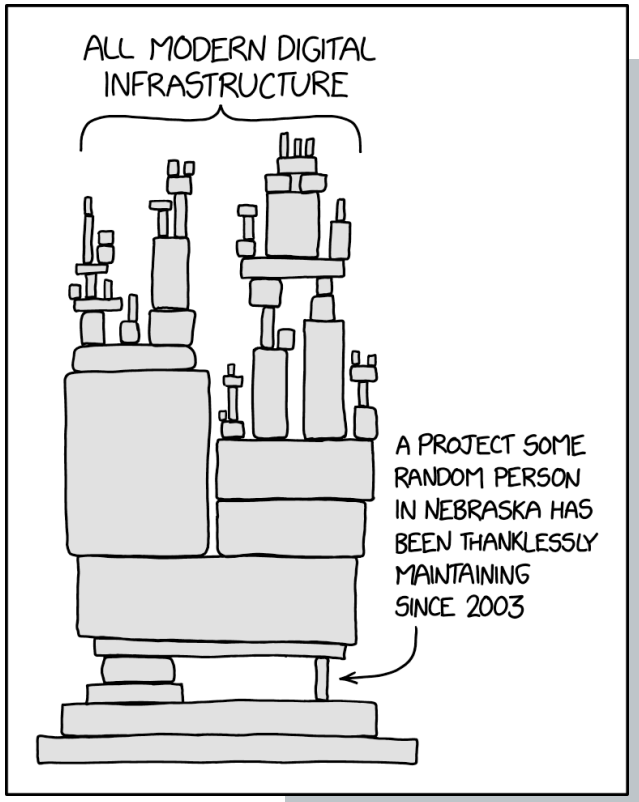
Supply Chain Security is a topic in multiple different regulations

- New vulnerabilities are discovered every day and have to be patched
- Continuous monitoring is necessary
- A digital product that is deemed secure when entering the market is not necessarily secure at a later stage during its life cycle
- Without knowing the contents of the product, no statement can be made about the security of it

* Cyber Resilience Act
** European Union's directive on security of network and information systems

SBOM as a CRA requirement

- Software Bill Of Materials (SBOM)
  Information about software components contained in a product
- Draw up SBOM in a *commonly used and machine-readable format* to track known newly emerged vulnerabilities and risks
  → SBOM should cover at the very least the top-level dependencies of the product
- The Commission may specify format and elements of the SBOM
- The market surveillance authority may request the SBOM, provided that it is necessary in order for this authority to be able to check compliance with the essential requirements



https://imgs.xkcd.com/comics/dependency_2x.png

RISKS TO THE RESILIENCE OF SUPPLY CHAINS

handing over the microphone

2 minutes

The software industry depends on Open Source

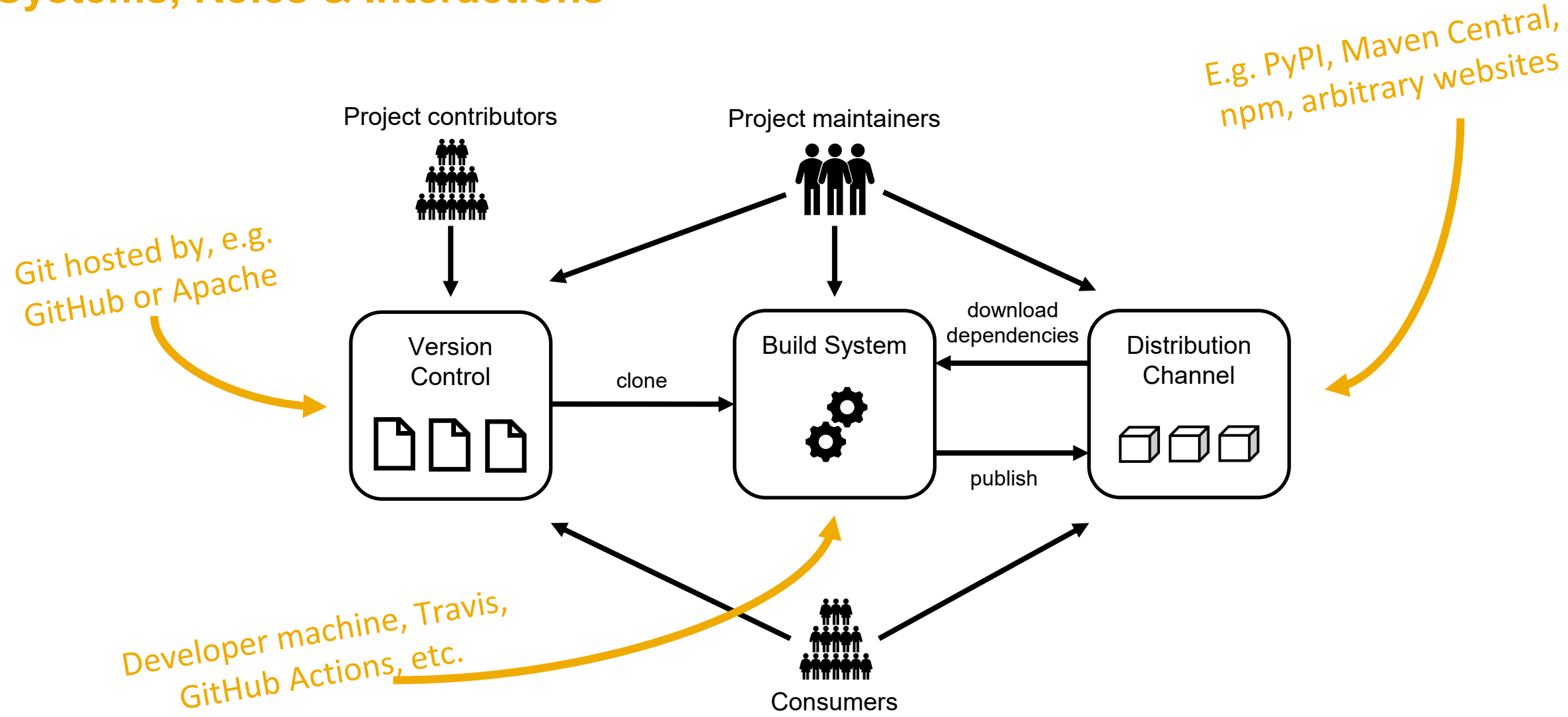
Wide-spread use of open source [1], 75-95% of code base of typical SAP apps is open source

Example: Steady has > 10 + 23722 contributors

[1] https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2022.pdf

Open-Source Supply Chain Model

Systems, Roles & Interactions



Volkmar: 1 min

Taxonomy of Open-Source Software Supply Chain Attacks

- Attacker's perspective
- Language agnostic
- From the review of ~370 scientific papers as well as grey literature
- 17 experts assessed its correctness and completeness
- Available online and open-source: Risk Explorer for Software Supply Chains

118

Unique attack vectors

33

Unique high-level safeguards

370

Scientific and grey literature references

https://sap.github.io/risk-explorer-for-software-supply-chains/

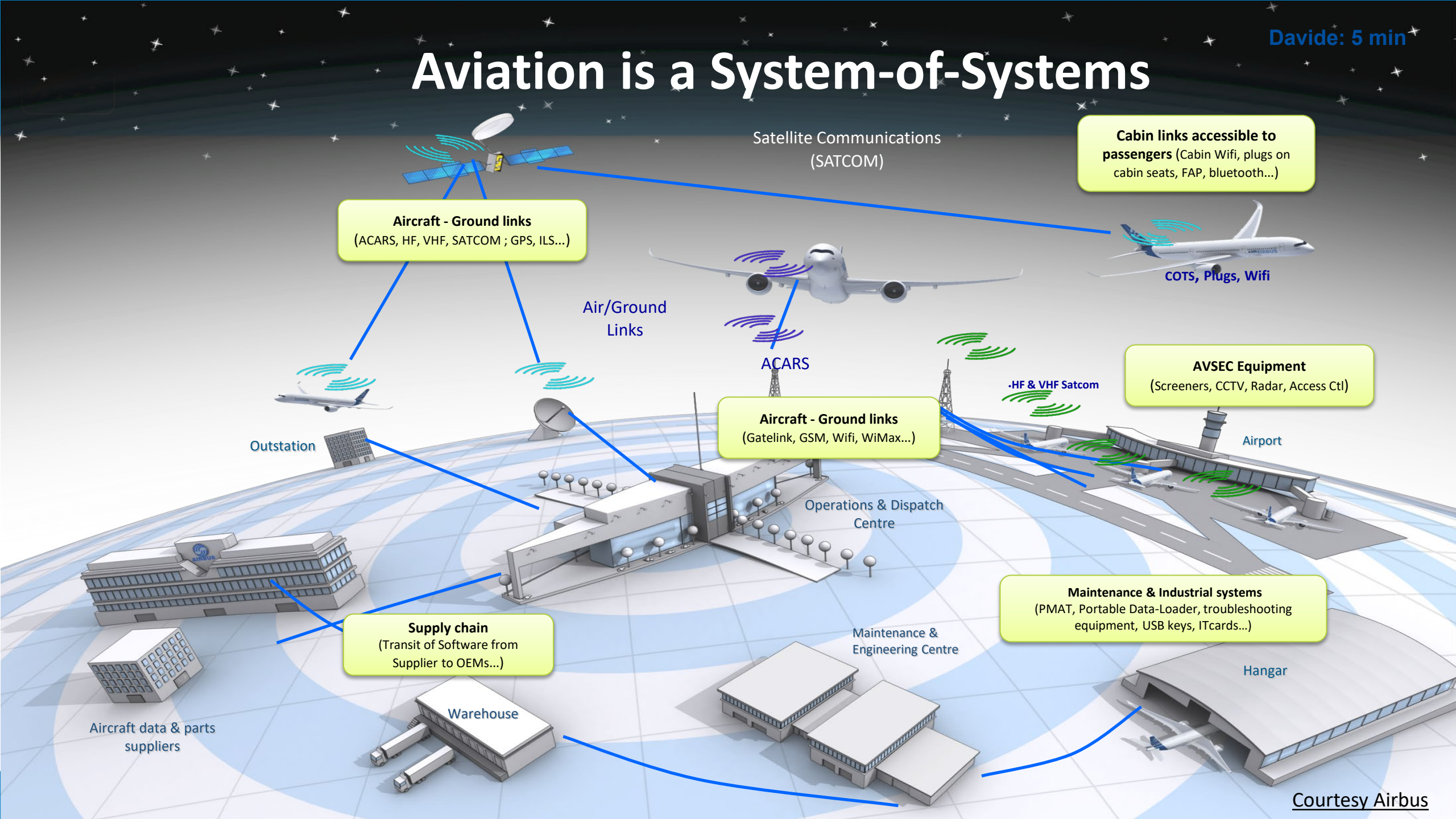
RISKS TO THE RESILIENCE OF SUPPLY CHAINS

handing over the microphone

2 minutes

Davide: 5 min

Aviation is a System-of-Systems



Courtesy Airbus

Key elements

Davide: 4 min

Resilience of aviation products (Aircrafts, Engines, …)

Certification specifications

Resilience of aviation organisations

Part-IS regulation

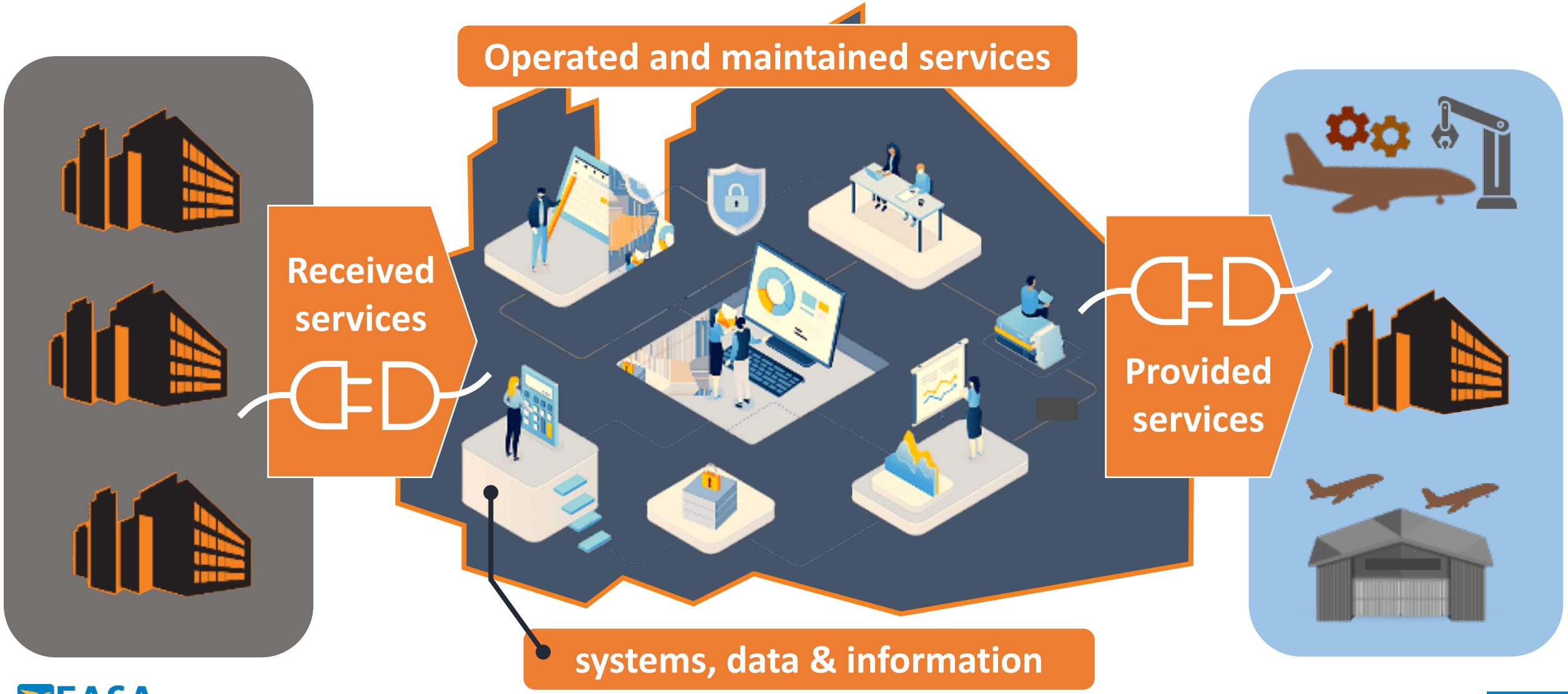
Technologies

Processes

People

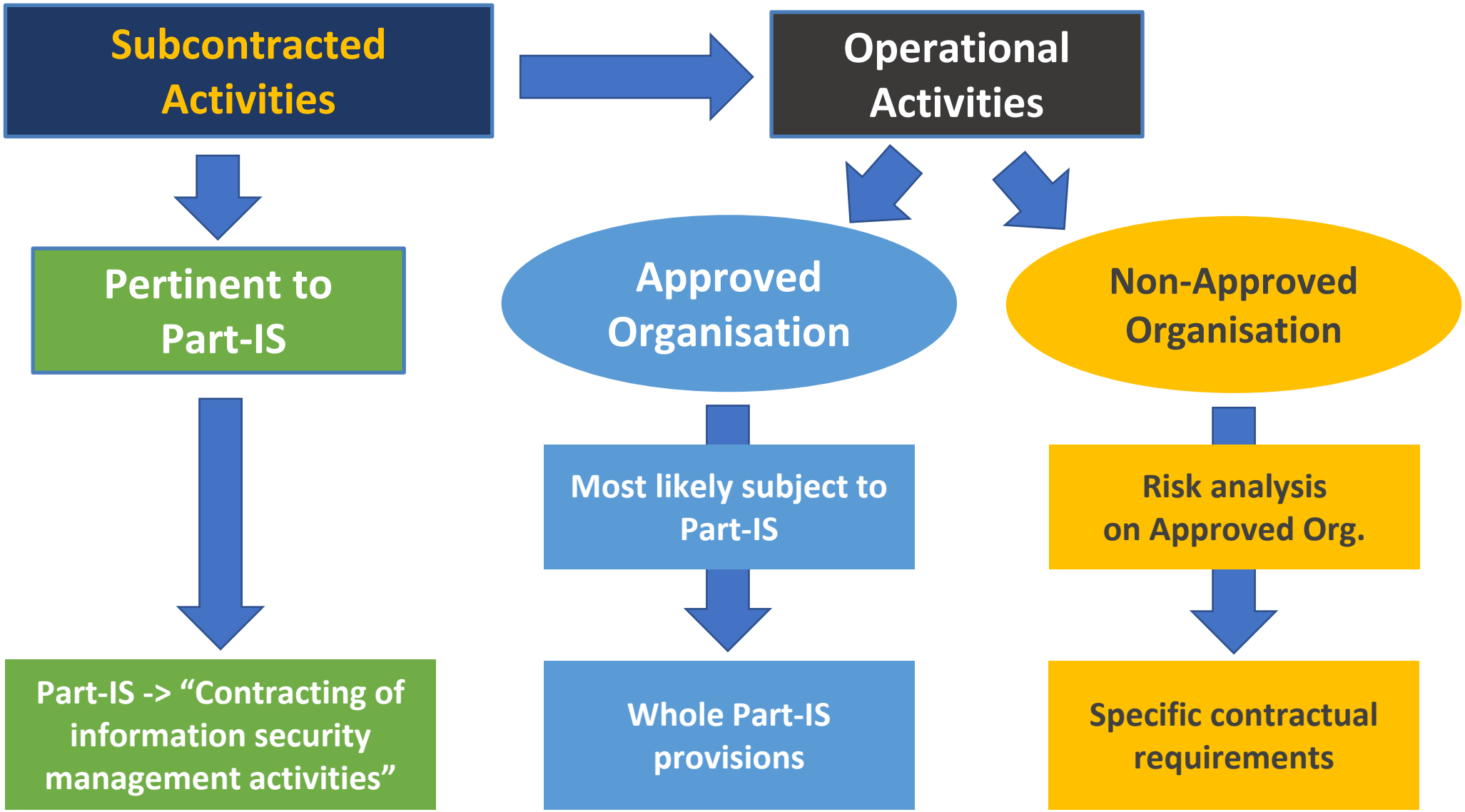
Risk assessment - scope identification

Davide: 3 min



How the supply chain is affected

Davide: 2 min



RISKS TO THE RESILIENCE OF SUPPLY CHAINS

Q & A

5 minutes

(only the participants present in the conference room)

II. MARKET IMPACT (CURRENT REGULATORY FRAMEWORK) + LESSON LEARNED FROM AVIATION

EASA: the European Union Aviation Safety Agency

Davide: 6 min

Mission is to provide safe air travel for EU citizens in Europe and worldwide

We regulate:

- Operations & Licensing
- Airworthiness
- Drones
- Aerodromes
- Environment
- Air Traffic Management

Established **2002** — **20 years+** in operation

735

31 EASA member states = 27 + 4

EU + Switzerland, Norway Iceland, Liechtenstein

Headquarters in **Cologne**

Office in **Brussels**

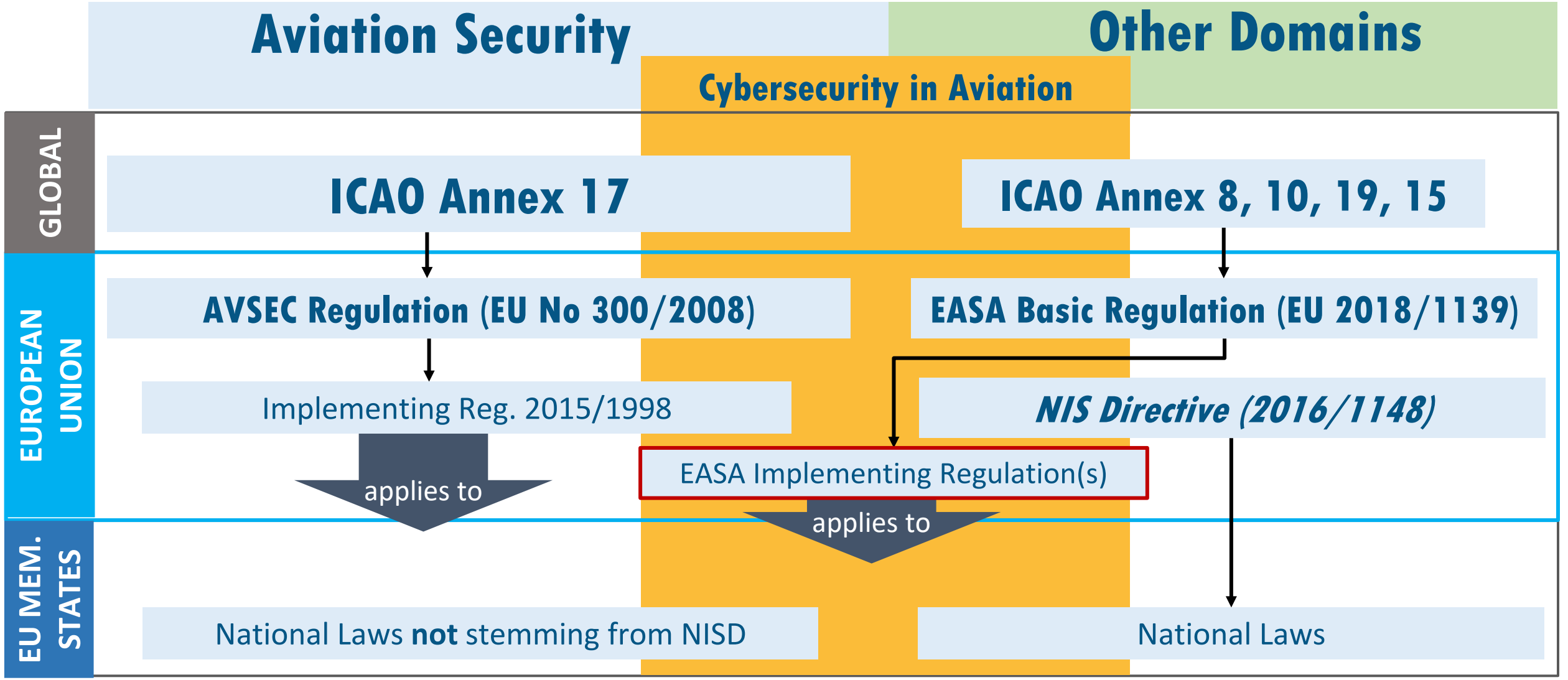
TASKS

- Draft the aviation safety regulations
- Certify & approve products and organisations
- Provide oversight and support to Member States
- Promote the use of European standards worldwide
- Cooperate with international actors to achieve the highest safety level for EU citizens globally

EASA

Overview of the EU regulatory framework

Davide: 4 min



EASA

Product certification

Davide: 3 min

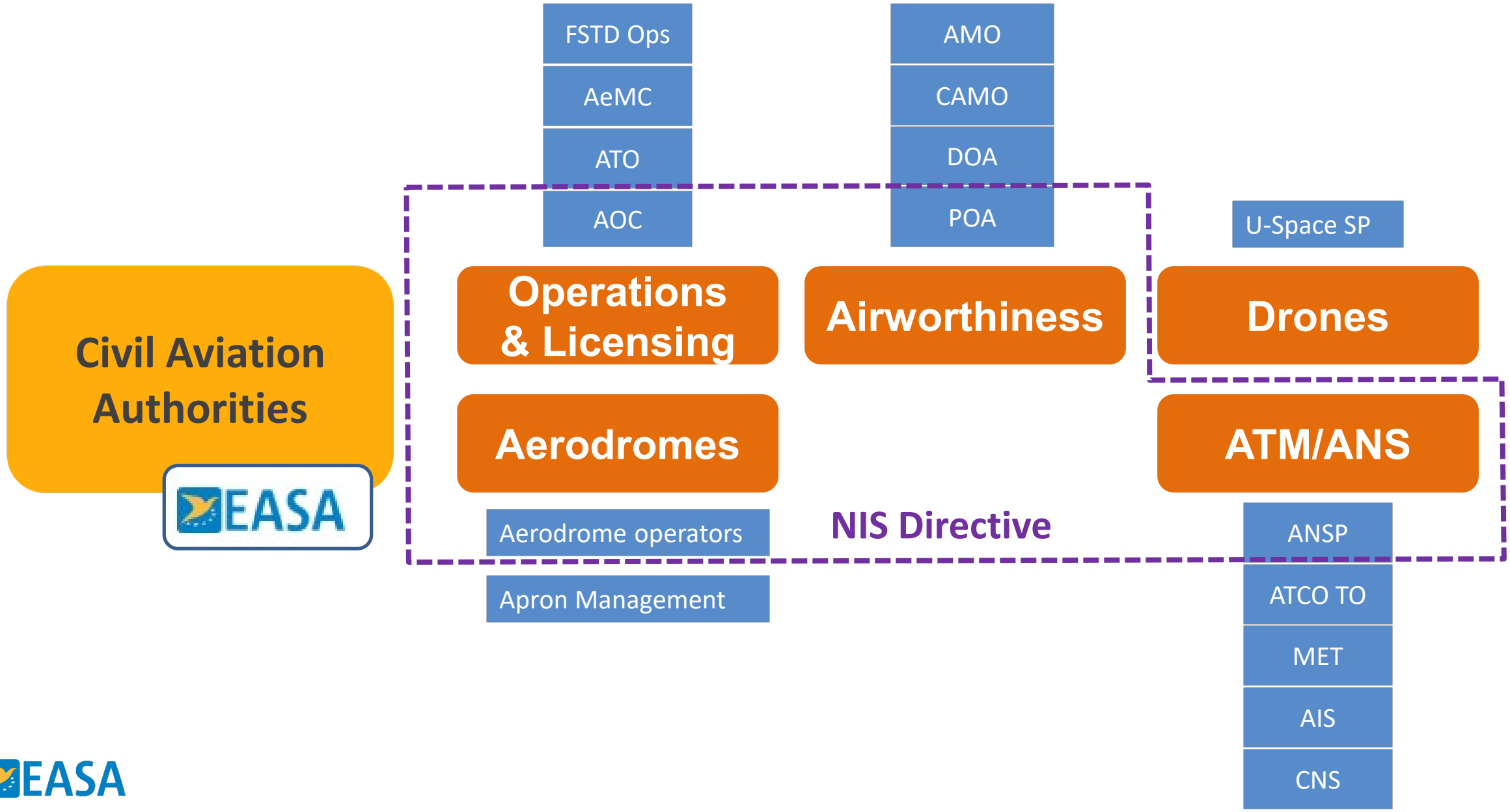
Since EASA was created (2003), it certifies products covering information security aspects.

These requirements were amended and incorporated into Certification Specifications and Acceptable Means of Compliance (Decision 2020/006/R of 01 July 2020)

In the near future, it will also certify UAS.

Aviation Organisations Part-IS

Davide: 1 min



RISKS TO THE RESILIENCE OF SUPPLY CHAINS

handing over the microphone

2 minutes

Excerpt from the current regulatory framework for Cybersecurity

Cybersecurity Act (Juni 2019)

- Contains European framewok for the certification of ICT products, services and processes
- Target – Manufacturers and providers of ICT products, services and processes

Radio Equipment Directive - Delegated Act (October 2022)

- Integration of considerations in regard to privacy and personal data, network security and fraud prevention into the design of radio equipment
- Target – manufacturers, importers and distributors

NIS 2 Directive (January 2023)

- Businesses identified by the Member States as operators of essential services in vital sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents.
- Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive.
- Target – operators of essential services & digital service providers

Cyber Resilience Act (proposal)

- horizontal European cyber security requiremens for a broad range of digital products and services enableling consumers & organizations to use secure products & services
- Introduces obligations for manufacturers during whole product lifecycle (design & development phase, maintenance phase)
- mandates manufacurers to establish vulnerability management & provide useful information for users
- Target – manufacturers, importers and distributors

RISKS TO THE RESILIENCE OF SUPPLY CHAINS

handing over the microphone

2 minutes

Volkmar: 5 min

Some European Legislation related to security and privacy

Legislations targeting security

- **Cybersecurity Act,**
  - Regulation (EU) 2019/881
- **Network and Information Security Directive** (NIS2),
  - Directive (EU) 2022/2555
- **Cyber Resilience Act** (CRA)
  - COM(2022) 454 final
- **European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centre** (ECCC),
  - Regulation (EU) 2021/887
- **Cyber Solidarity Act**
  - COM(2023) 209 final

Legislations including security requirements

- **AI Act**
  - COM(2021) 206 final
- **AI Liability Directive**
  - COM(2022) 496 final
- **Data Act**
  - COM(2022) 68 final
- **Digital Services Act**
  - COM(2020) 825 final
- **Digital Markets Act**
  - Regulation (EU) 2022/1925

Legislations targeting privacy

- **GDPR**
  - Regulation (EU) 2016/679
- **E-privacy**
  - COM(2017) 10 final
- **E-IDAS**
  - Regulation (EU) 2014/910, COM(2021) 281 final

Sector-focused legislations

- **DORA**
  - Regulation (EU) 2022/2554
- **RED**
  - Directive (EU) 2014/53
- **Chips Act**
  - COM(2022) 46 final
- **Critical Entities Resilience Directive**
  - Directive (EU) 2022/2557
- **Machinery Directive**
  - COM(2021) 281 final

Volkmar: 5 min

Observations

The market impact goes far beyond the cybersecurity market: Let’s talk about a market for secure products and services

- for instance, consider the scope of the CRA

There are challenges …

- Harmonization of requirements and processes across the legislative landscape
- Clear definition of scope
- Global perspective

… and opportunities

- Increase the level of cybersecurity across the EU
- Security and privacy as unique selling points for market players

Blocker or enabler for new technologies like Generative AI?

RISKS TO THE RESILIENCE OF SUPPLY CHAINS

handing over the microphone

2 minutes

Roxana: 5 min

Attendees [Voting session]: PERCEPTION AND IMPACT

Questions:

1. Do you perceive the impact of the regulations, beneficial?
2. Do you perceive the impact of the regulations burdensome?
3. Have you developed new products (increased your product portfolio) to support your customers to comply with a new regulation?
4. Has the demand for cybersecurity products and services increased?
5. Did you need to develop new skills, employees with new skills?

Answers:

YES	NO

MARKET IMPACT (CURRENT REGULATORY FRAMEWORK) + LESSON LEARNED FROM AVIATION

Q & A

5 minutes

(only the participants present in the conference room)

III. ARE YOU READY FOR CRA?

Are you ready for the Cyber Resilience Act?

- CRA is still in the draft stage
- BSI published the technical guideline **TR 03183-2** in August 2023 as a stepping stone towards CRA
  - Part 1 - **General requirements for all products with digital elements** (tbd) will contain requirements for manufacturers and products on the basis of CRA articles and annexes
  - Part 2 – establishes **SBOM** requirements (published) and is aiming to strengthen software supply chain security by containing
    - specifications for data fields
    - information regarding the level of detail
    - Format suggestions: SPDX or CycloneDX
  - Part 3 = **provisions for software products** (tbd)

RISKS TO THE RESILIENCE OF SUPPLY CHAINS

handing over the microphone

2 minutes

Volkmar: 5 min

CRA readiness from software vendor's and SaaS providers perspective

We expect that a number of SaaS offers will be in the scope of the CRA rather than of the NIS2 directive

- For instance, SAP offers SaaS services likely in both of the scopes

Security requirements ↗

Reporting and notification requirements →

- single points of contact
- rules follow the state of the art (e.g., balancing transparency and risk

Assurance requirements →

- Precise scope,
- Familiarity of the software industry with NLF

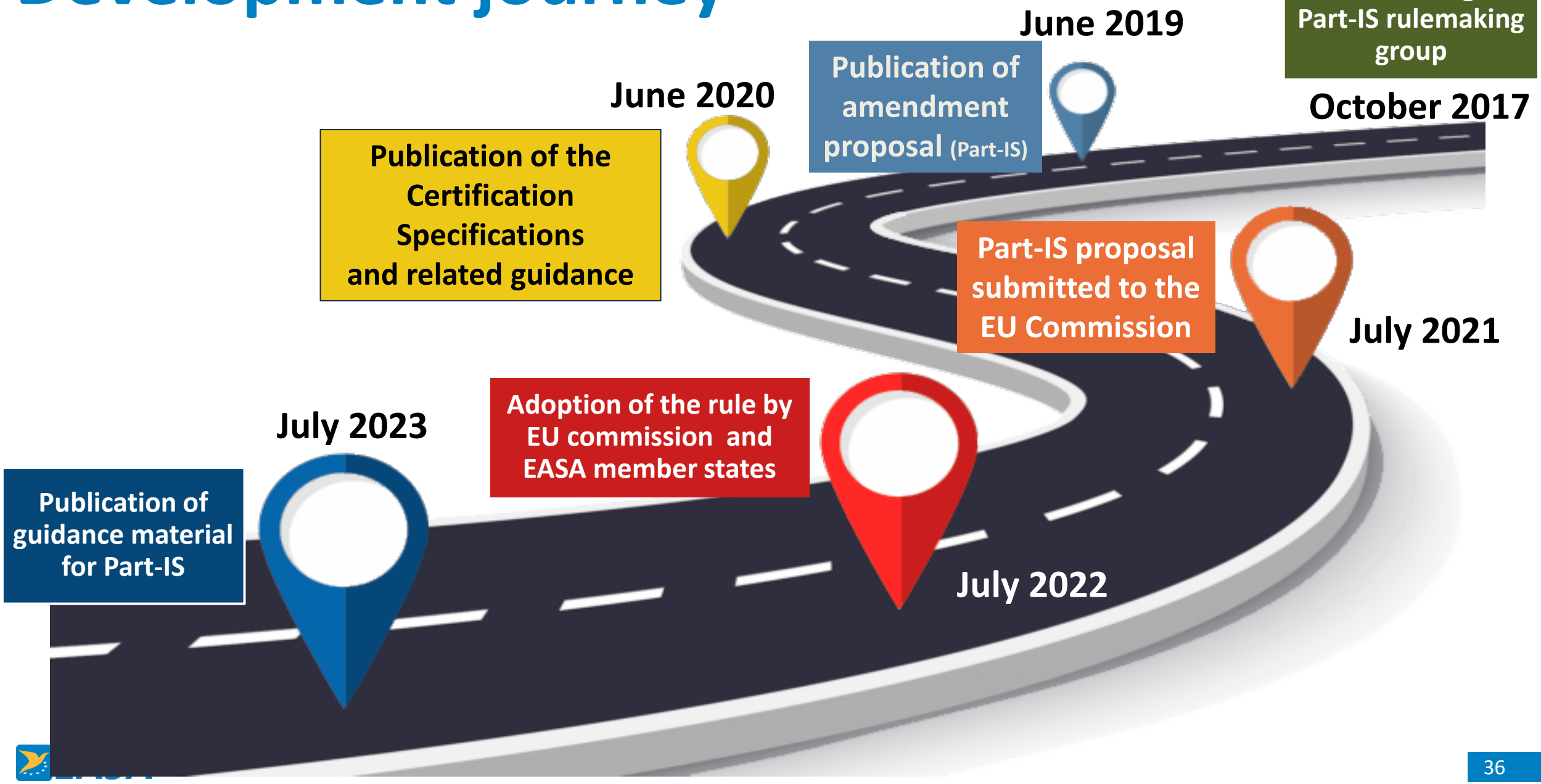
RISKS TO THE RESILIENCE OF SUPPLY CHAINS

handing over the microphone

2 minutes

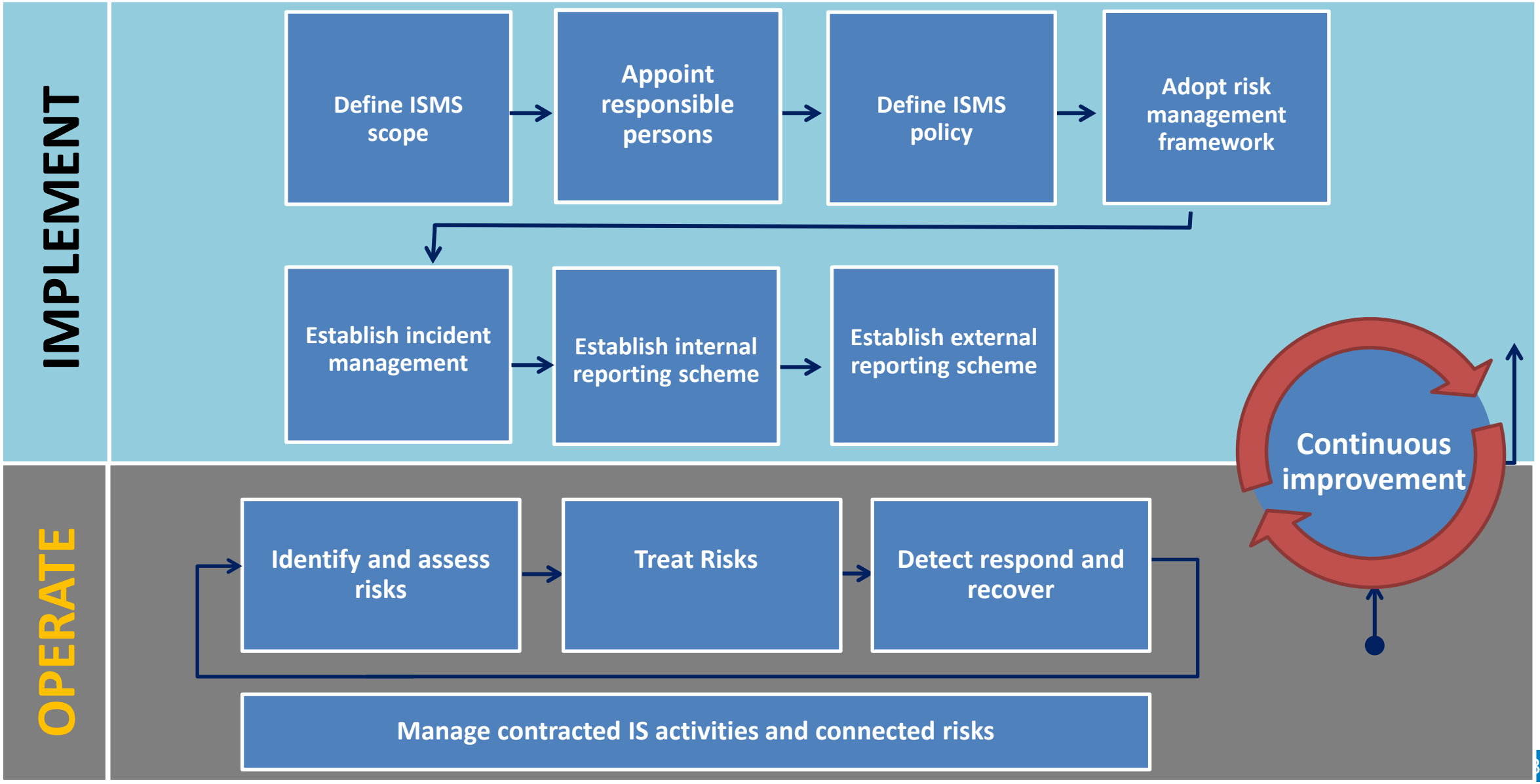
Davide: 5 min

Development journey



Davide: 3 min

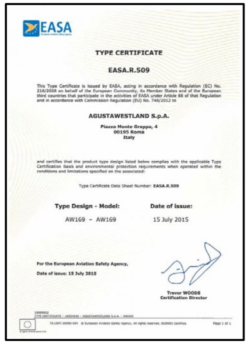
Processes under Part-IS



Davide: 2 min

Market Surveillance

Products



EASA

TYPE CERTIFICATE

EASA.R.509

AGUSTAWESTLAND S.p.A.

Type Design - Model: AW169 - AW169

Date of issue: 15 July 2015

Airworthiness of Type Design

Certification / approval

Organisations

EASA

APPROVAL CERTIFICATE

EASA.21J.713

Cobalt Aerospace Limited

as a DESIGN ORGANISATION

CERTIFICAT DE TRANSPORTEUR AÉRIEN

Air Operator Certificate

Organisation Approval

EASA or National Aviation Authority

In service / operational phase

- Monitoring of operational performance
- Systematic collection and review of data
- Airworthiness reviews with design organisation
- EASA's design organisation surveillance team

Corrective Actions if necessary

- Airworthiness Directives (ADs)
- Safety Information Bulletins (SIBs)

- Oversight of approved organisations (EASA/NAA)
- Standardisation across EU
- Audits and findings with follow-up to resolve non-conformities

ARE YOU READY FOR CRA?

Q & A

5 minutes

(only the participants present in the conference room)

All: 3 min

TAKEAWAY:

[Member State Representative]

“Like a safety net, cybersecurity regulation will give us much needed security by closing gaps and addressing current challenges. Nobody can solve the issues in the field of cybersecurity alone. We all need to work together in order to deal with current and future challenges. Let´s join forces in the standardisation processes to make sure we are all set for the future. ” Christin Hartung-Kuemmerling

[Technology Provider]

Cybersecurity regulation offers the great opportunity to increase the level of cybersecurity in Europe, from critical services to consumer products. Security can become a unique selling point. It needs to be economically viable, meaning consistent across the legislative landscape and cost effective. Given that, cybersecurity regulation can even become a driver for new technologies like AI, which otherwise might be considered as too risky. Volkmar Lotz

[Regulator]

Like a well-crafted flight plan, regulations navigate us through turbulence and shapes the course of the industry. They bring challenges that test our resilience and opportunities that propel us to new heights. Embrace the evolution, because in regulations lies the roadmap to a more secure, fairer, and innovative digital landscape... and safer skies. Davide Martini