TRAFICOM
Liikenne- ja viestintävirasto

Ilmailun Kyberturvallisuus

Ilmailun säädösinfo 14.2.2024

Tomi Salmenpää

Aiheet

- Kybersääntelyn tilanne EUssa
- Kybersääntelyn soveltaminen
- Tavoite
- Keinot

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

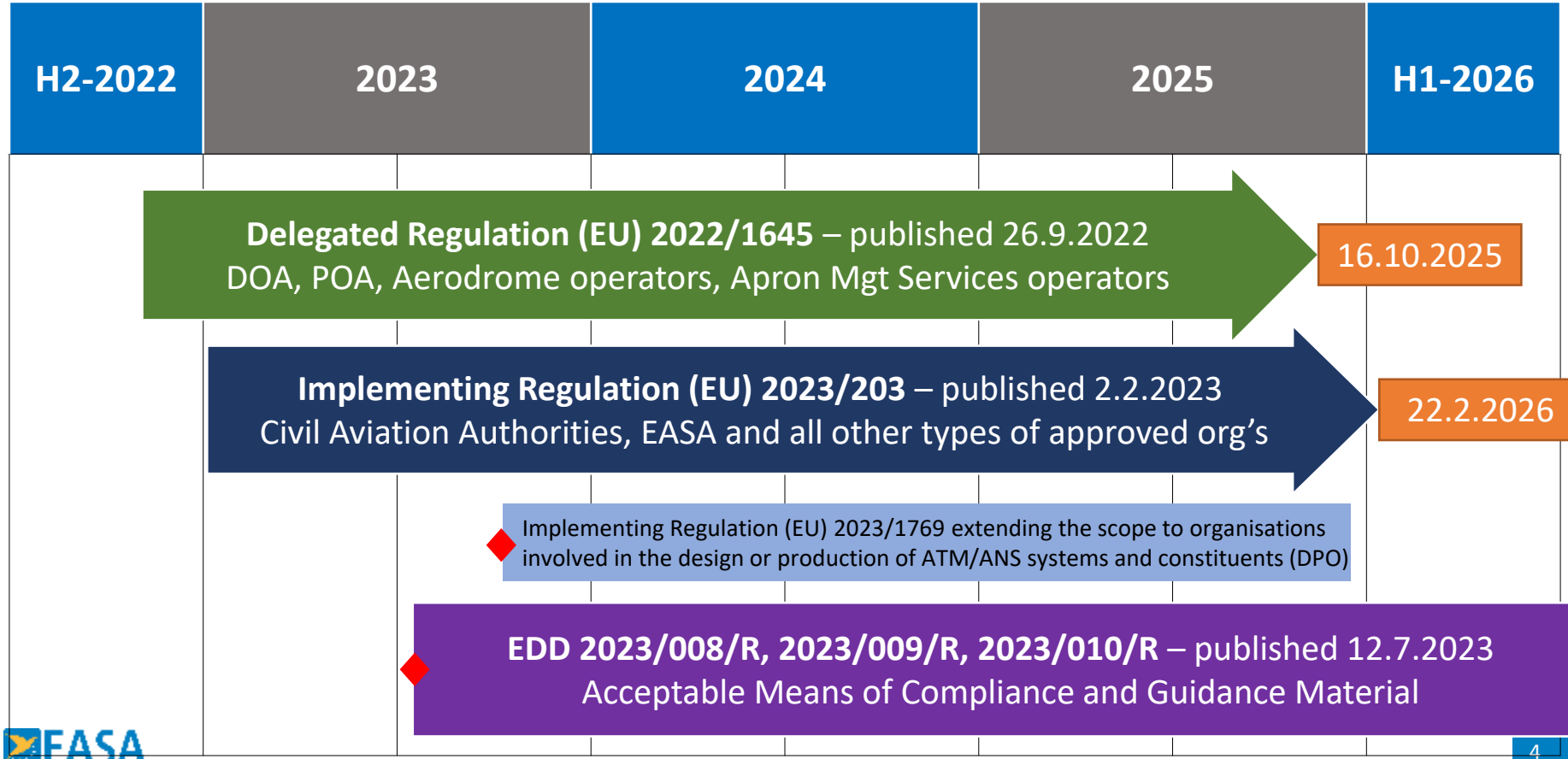
- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape

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

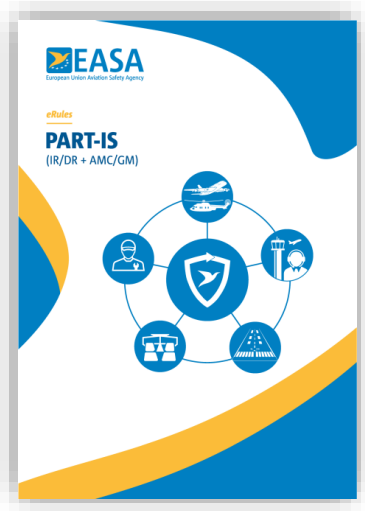
AMC/GM to Organisation Requirements

ED Decision 2023/210

AMC/GM to Authority Requirements

Amdts to existing AMC/GM for ARs

3 ED Decisions



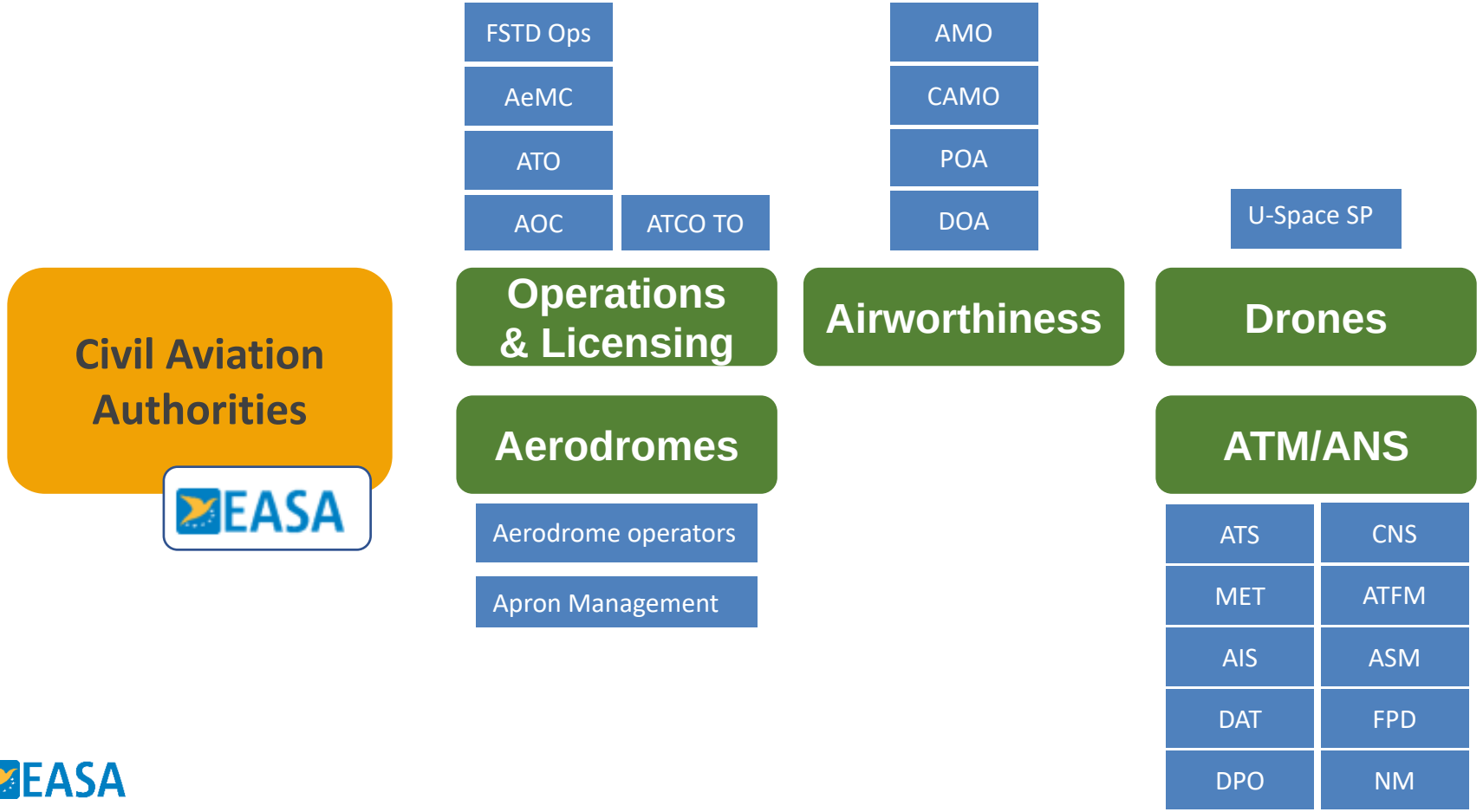
Easy Access Rules available here

AMC & GM what's in it

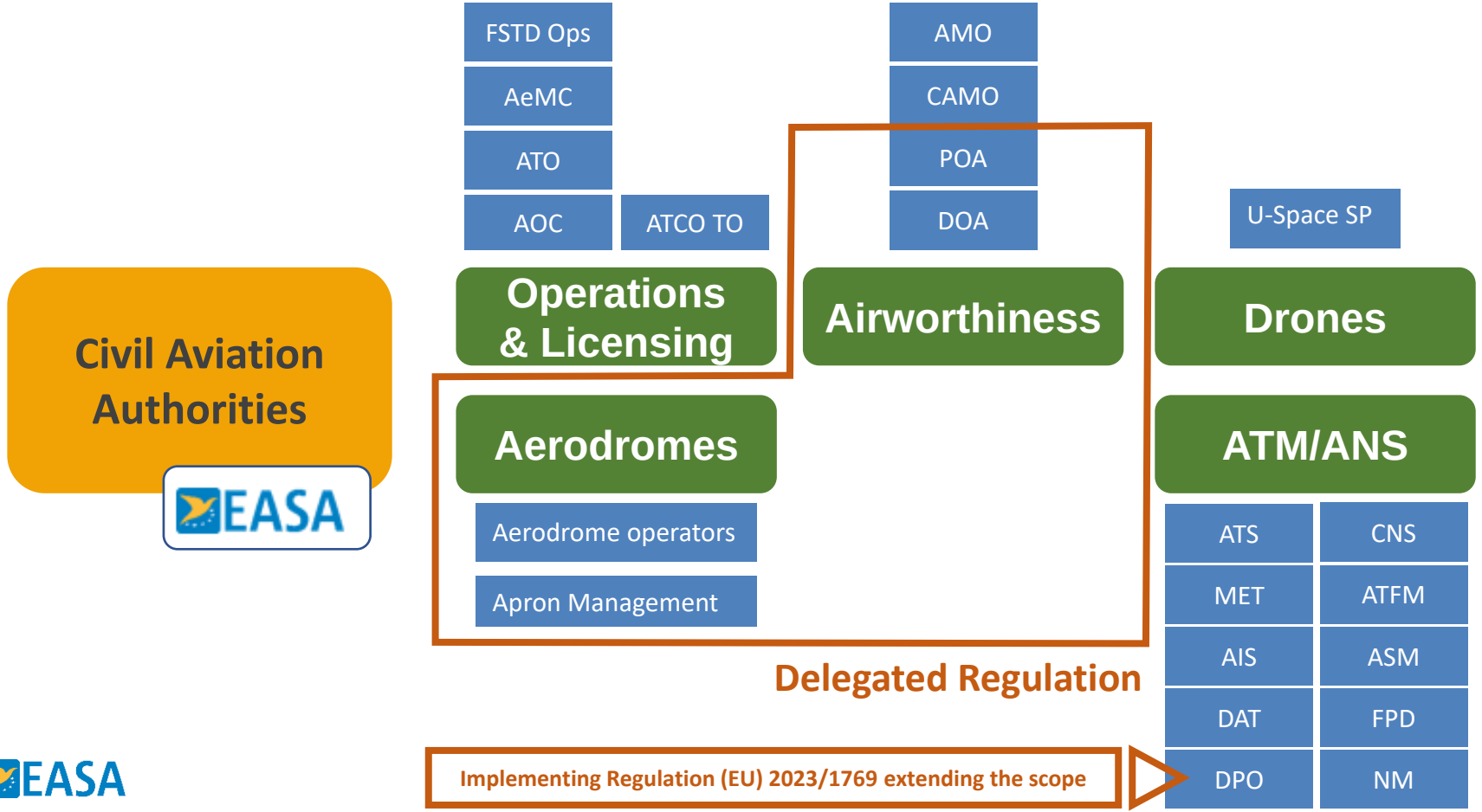
- → Non-binding by definition
- → To facilitate timely and harmonised application of Part-IS
- → No additional requirements. Everything is in the Regulations

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



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

Amendments in existing domain regulations 1/2

Organisation Requirements

1. **Provisions** to establish, implement and maintain an **ISMS** as per **IS.OR requirements**.

Authority Requirements

1. **Provisions** to establish, implement and maintain an **ISMS** as per **IS.AR requirements**.
2. **Provisions** to manage and **immediately react** to information security reports received by Organisation under IS.D/I.OR.230.
3. **Provisions** to **oversee Part-IS** implementation and **derogations** granted to Organisations as well as **changes** to the ISMS during the oversight audit cycle.
4. **Possibility** to **allocate oversight tasks** to qualified entities or relevant authority responsible for information security in the Member State.

Amendments in existing domain regulations 1/2

Organisation Requirements

1. **Provisions** to establish, implement and maintain an **ISMS** as per **IS.OR requirements**.

Hooking points to Part-IS requirements

Authority Requirements

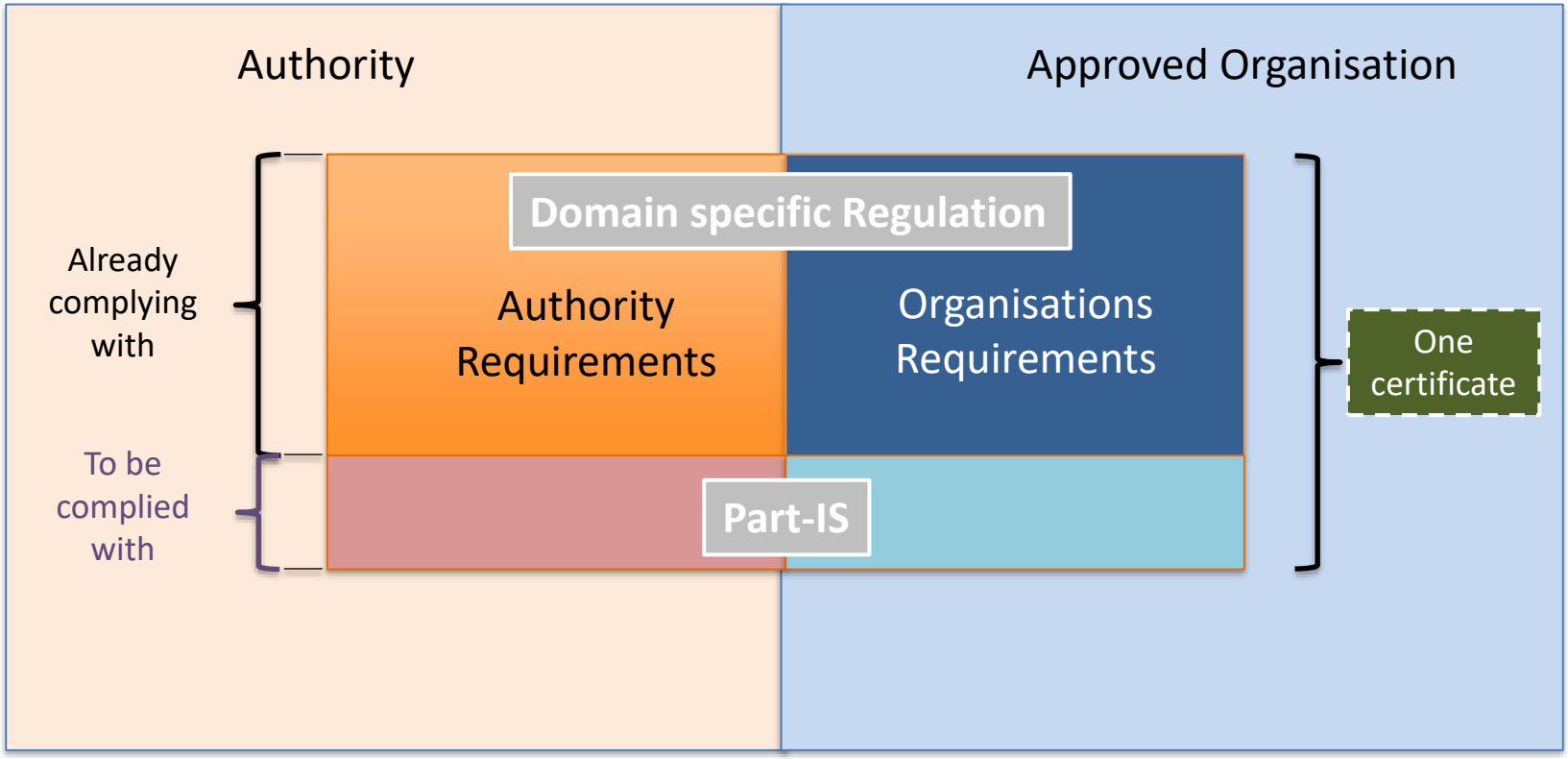
1. **Provisions** to establish, implement and maintain an **ISMS** as per **IS.AR requirements**.
2. **Provisions** to manage and **immediately react** to information security reports received by Organisation under IS.D/I.OR.230.
3. **Provisions** to **oversee Part-IS** implementation and **derogations** granted to Organisations as well as **changes** to the ISMS during the oversight audit cycle.
4. **Possibility** to **allocate oversight tasks** to qualified entities or relevant authority responsible for information security in the Member State.

Amendments in existing domain regulations 2/2

Part / Area	ORA	21	ORO	ADR	ATCO	ATM/ANS	CAMO	145
ISMS	.GEN.200A	.A.139A .A.239A	.GEN.135A	.OR.D.005A .OR.D.007 .OR.F.045A	.OR.C.001A	.OR.B.005A .OR.D.010	.A.200A	.A.200A

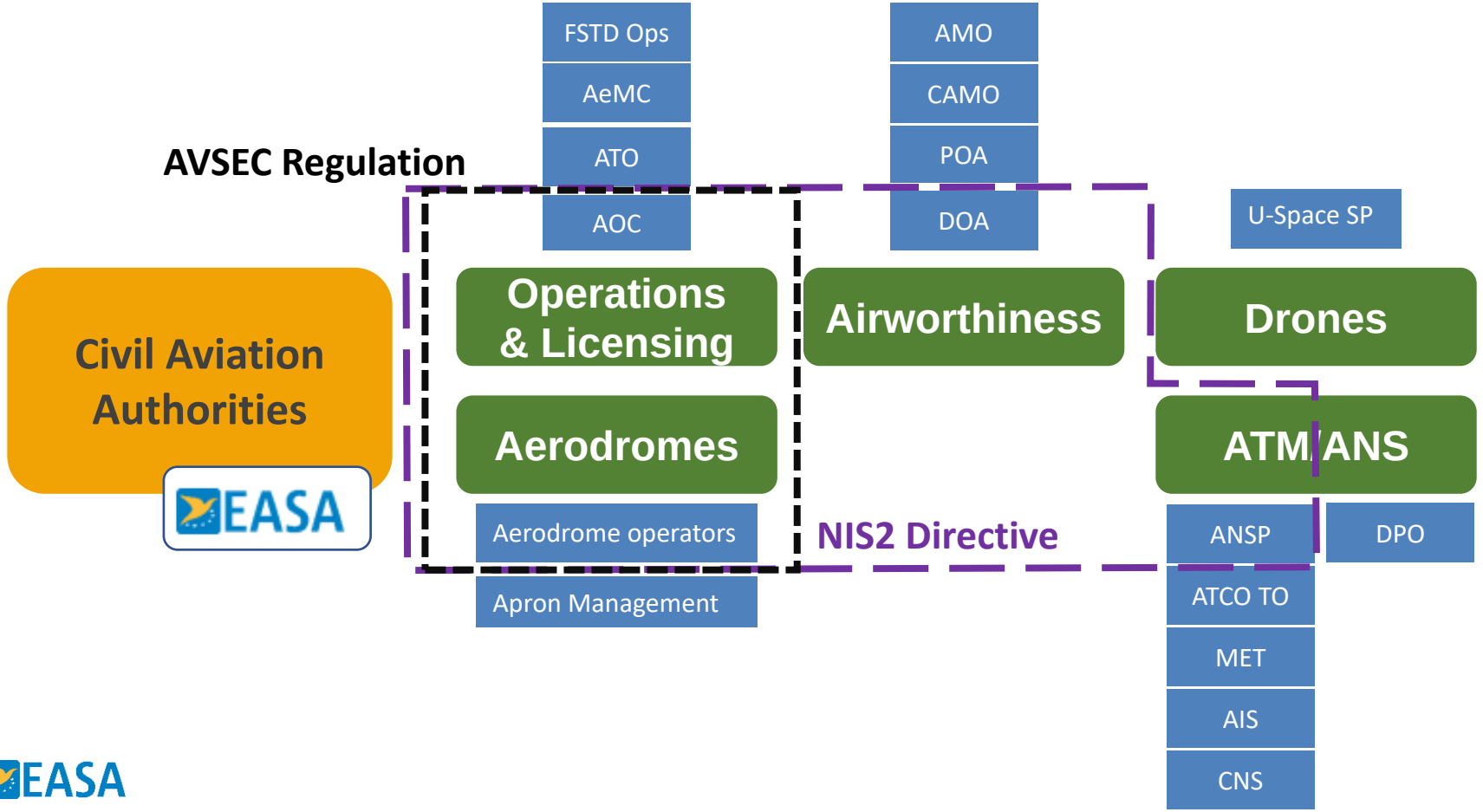
Part / Area	ARA	21	ARO	ADR	ATCO	ATM/ANS	CAMO	145	66
ISMS	.GEN.200	.B.25	.GEN.200	.AR.B.005	.AR.B.001	.AR.B.001	.B.200	.B.200	.B.15
IS Reports	.GEN.125 .GEN.135A	.B.15 .B.20A	.GEN.125 .GEN.135.A	.AR.A.025 .AR.A.030A	.AR.A.020 .AR.A.025A	.AR.A.020 .AR.A.025A	.B.125 .B.135A	.B.125 .B.135A	N/A
Oversight	.GEN.300 .GEN.330A	.B.221 .B.240A .B.431 .B.435A	.GEN.300 .GEN.330A	.AR.C.005 .C.040A	.AR.C.001 .AR.E.010A	.AR.C.010 .AR.C.025A	.B.300 .B.330A	.B.300 .B.330A	N/A
Tasks	.GEN.205	.B.30	.GEN.205	.AR.B.010	.AR.B.005	.AR.B.005	.B.205	.B.205	N/A

Part-IS and existing approvals/regulations



Part-IS and other EU legislation

Applicability of Part-IS



If I am already compliant with AVSEC Regulation?

Reg. 2022/1645, article 4.2

Where an organisation referred to in Article 2 is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 of the European Parliament and of the Council, the cybersecurity requirements contained in point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998 shall be considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.D.OR.230 of the Annex to this Regulation that shall be complied with.

IS.D.OR.230 Information security external reporting scheme

Reg. 2023/203, article 5.2

Where an organisation referred to in Article 2(1) is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 of the European Parliament and of the Council, the cybersecurity requirements contained in point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998 shall be considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.I.OR.230 of Annex II to this Regulation that shall be complied with as such.

IS.I.OR.230 Information security external reporting scheme

IS.D.OR.230 Information security external reporting scheme

IR	- Implement an IS reporting system complying with the Regulation (EU) No 376/2014 - Report incidents and vulnerabilities to the authority, to the DA holder (aircraft) or to the design organisation (system or constituent)
AMC	- Competent authorities responsible to ensure compliance with Article 7 - Competent authority notified ASAP and report within 72 hours - Reporting security-sensitive information, necessary confidentiality ensured
GM	- Reporting, analysis and follow-up of occurrences - Reg (EU) 376/2014 and IS.I.OR.230(b) should be seen as complementary - Two-Step mechanism to report occurrences (public & sensitive) - TLP & PAP - Agree on taxonomy

If I prefer to switch from AVSEC regulation to Part-IS?

Point 1.7 of the Annex to Reg. 2015/1998, as amended by Reg. 2019/1583

1.7.5 Where airport operators, air carriers and entities as defined in the national civil aviation security programme are subjected to separate cybersecurity requirements arising from other EU or national legislation, the appropriate authority may replace compliance with the requirements of this regulation by compliance with the elements contained in the other EU or national legislation. The appropriate authority shall coordinate with any other relevant competent authorities to ensure coordinated or compatible oversight regimes.

If I am already compliant with NIS Directive?

Reg. 2022/1645, article 4.1

Where an organisation referred to in Article 2 complies with security requirements laid down in accordance with Article 14 of Directive (EU) 2016/1148 that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation.

Reg. 2023/203, article 5.1

Where an organisation referred to in Article 2(1) complies with security requirements laid down in accordance with Article 14 of Directive (EU) 2016/1148 that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation.

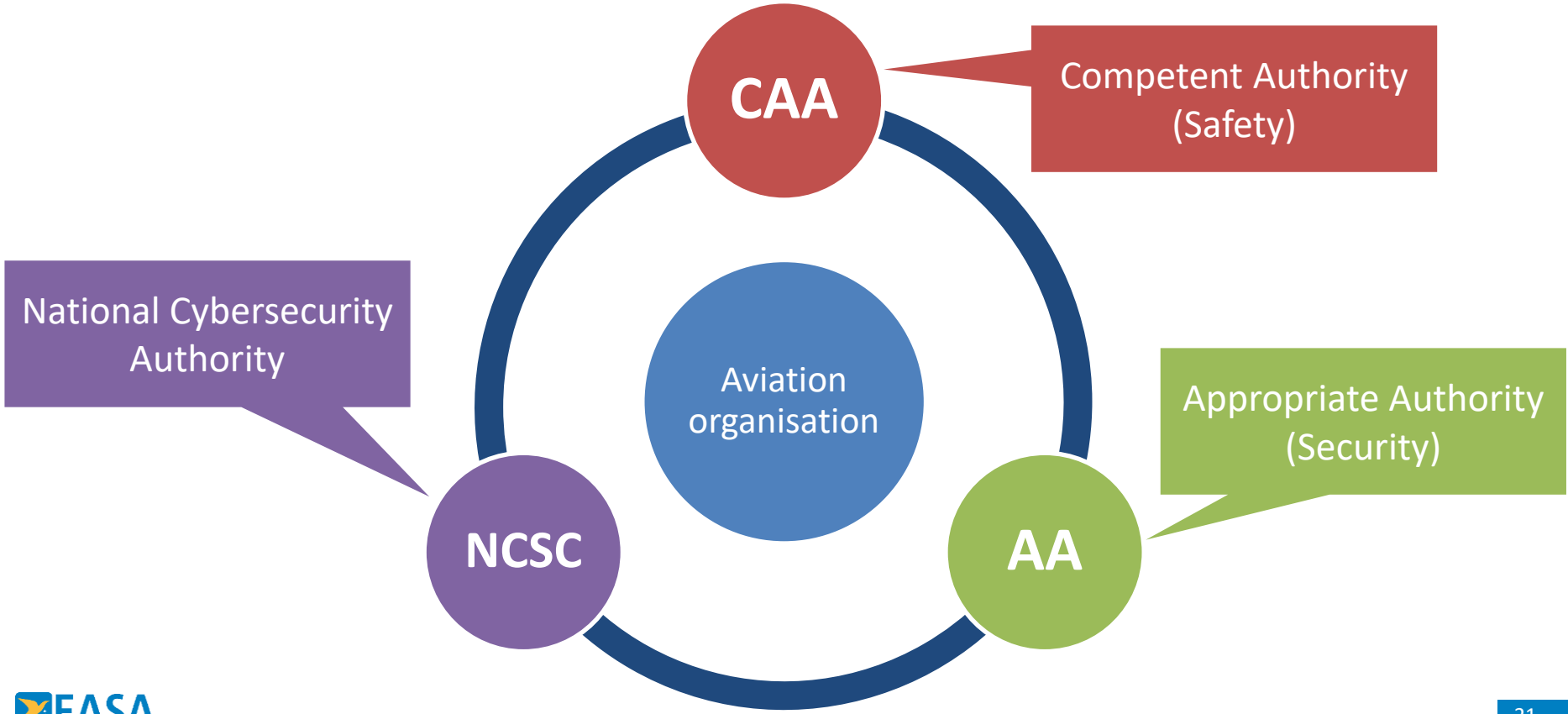
Detailed analysis of NIS Directive vs. Part-IS will be needed

If I prefer to comply with Part-IS?

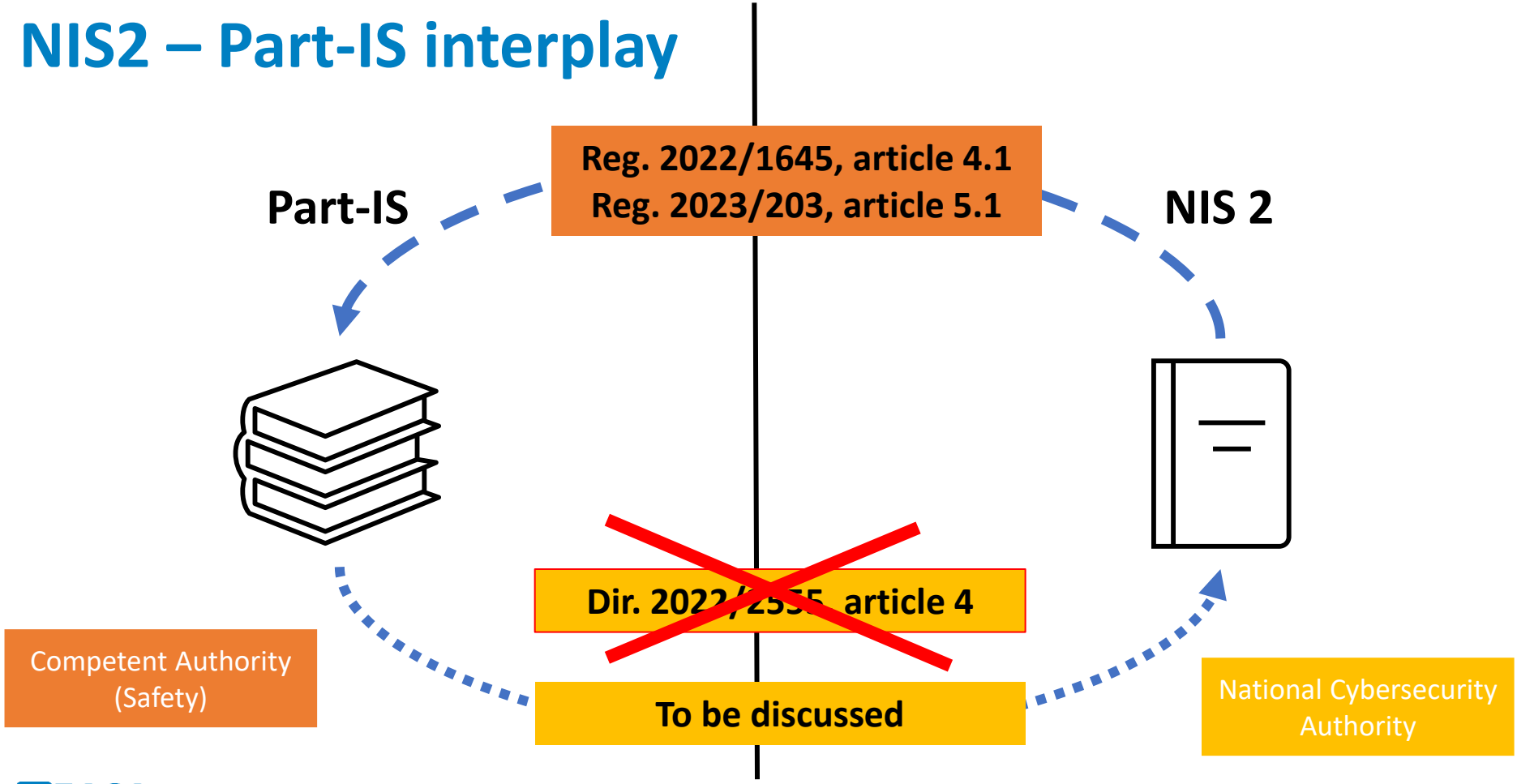
Directive 2022/2555, article 4

1. Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.
2. The requirements referred to in paragraph 1 of this Article shall be considered to be equivalent in effect to the obligations laid down in this Directive where:
   (a) cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2); or
   (b) the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive.
3. The Commission shall, by 17 July 2023, provide guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review those guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account any observations of the Cooperation Group and ENISA

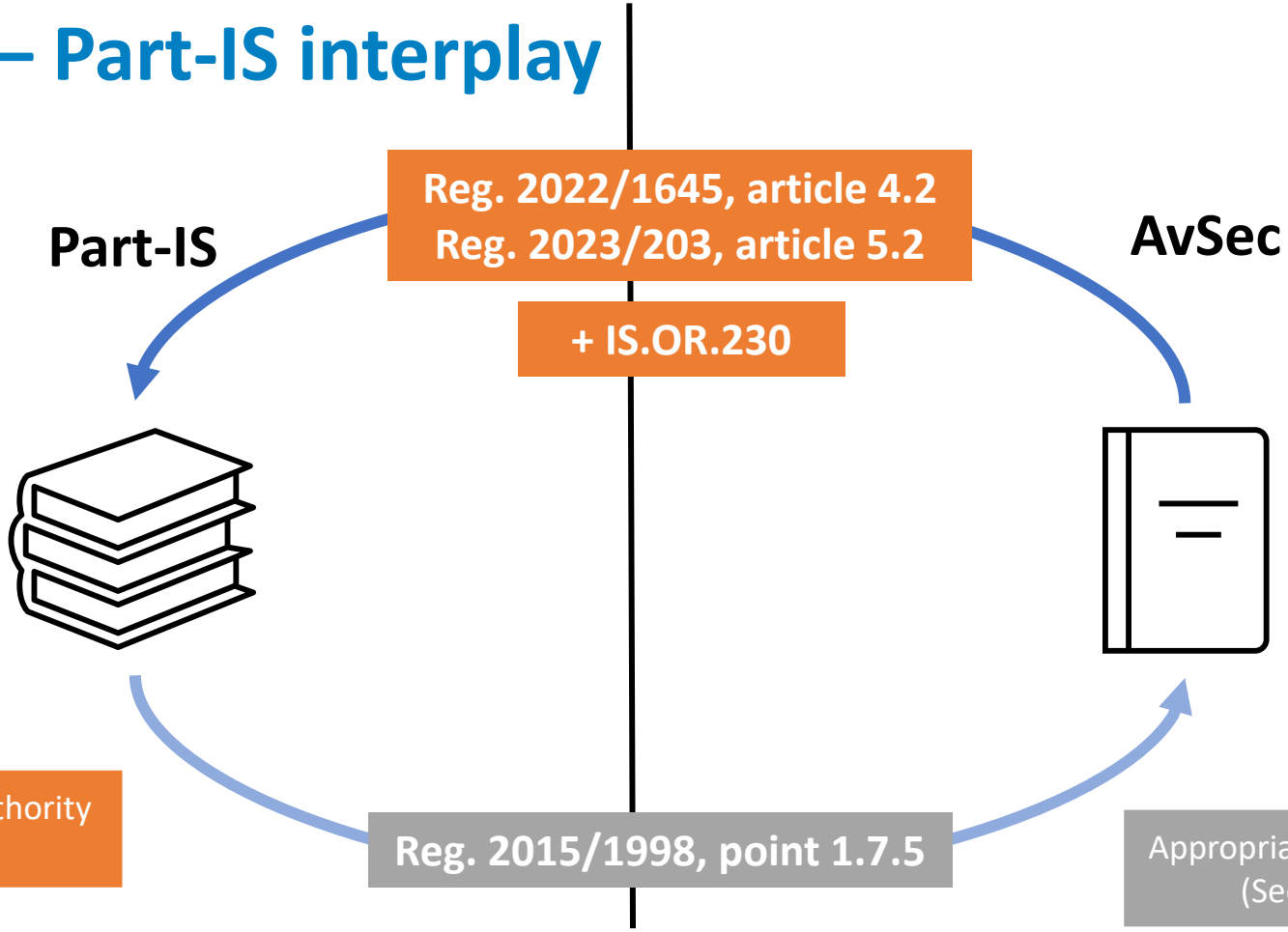
Needed: cooperation between Authorities



NIS2 – Part-IS interplay



AvSec – Part-IS interplay

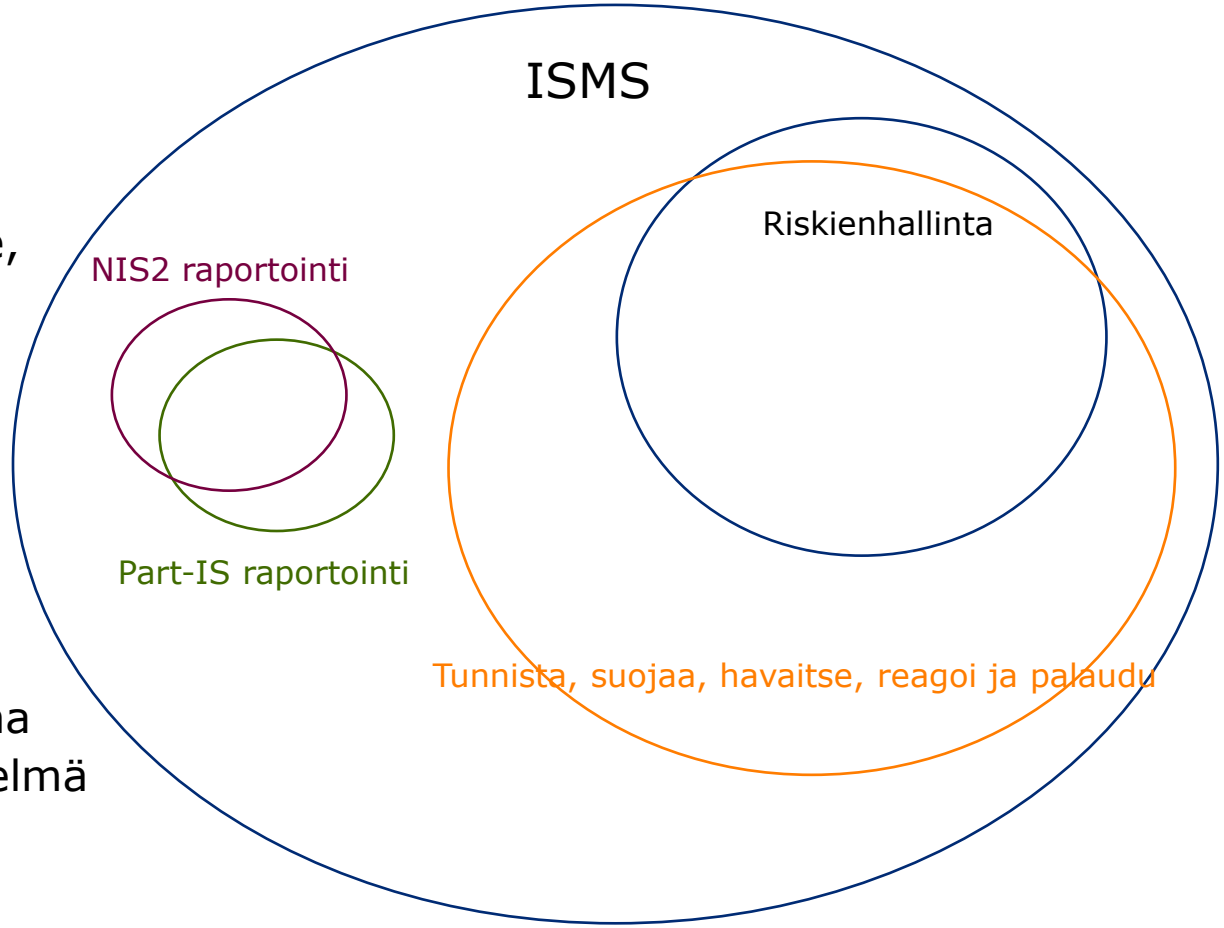


Sääntelyn tavoite?

- NIS2 -> HE 7 § Kyberturvallisuuden riskienhallinnalla tulee estää tai minimoida poikkeamien *vaikutus toimintaan, toiminnan jatkuvuuteen,* palvelujen vastaanottajiin ja muihin palveluihin
- Part-IS -> *Lentoturvallisuus*
- Avsec -> *Ilmailun turvaaminen*

Keinot?

- Part-IS ja AMC&GM: ISMS ja raportointi
- NIS2: Riskienhallinta ja raportointi
- Avsec: Tunnista, suojaa (riskienhallinta), havaitse, reagoi ja palaudu



Part-IS tarjoaa keinot myös muun sääntelyn toteuttamiseksi. Organisaatioiden kannalta ajateltuna heillä on vain yksi tietoturvallisuuden hallintajärjestelmä (ISMS)

Tilanne 14.2.2024

- EU-tasoista koordinaatiota tavoitellaan Komission fasilitoimassa ”Aviation Cybersecurity Sub-Group” ryhmässä. Työ käynnistyi ke 7.2.2024
- Suomen kansallinen lainsäädännön toteutus ja koordinaatio hyvässä tilassa. Traficom valvova viranomainen (Avsec, NIS2, Part-IS) ja voimme kehittää tehokkaan ratkaisun viranomaistyöhön ja valvontaan
- Sidosryhmätyön merkitys on suuri

Q&A