Cybersäkerhetsregler för luftfarten ”Part-IS”

Johan Harter, *inspektör cybersäkerhet*

Ordf. Part-IS Task force

Sektionen för säkerhetsskydd

sjö och luftfart

TRANSPORT STYRELSEN

Definitioner

Cybersäkerhet

Konfidentialitet

Tillgänglighet

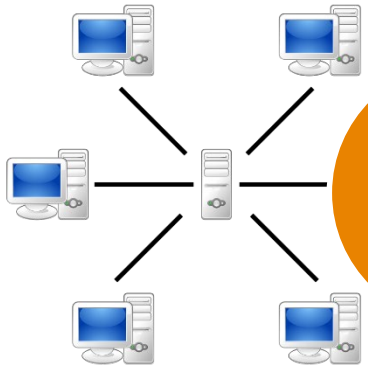
Riktighet

Informations-
säkerhet

TRANSPORT STYRELSEN

Cybersäkerhet

K T R



Infos äk

IT-säk

Cyber

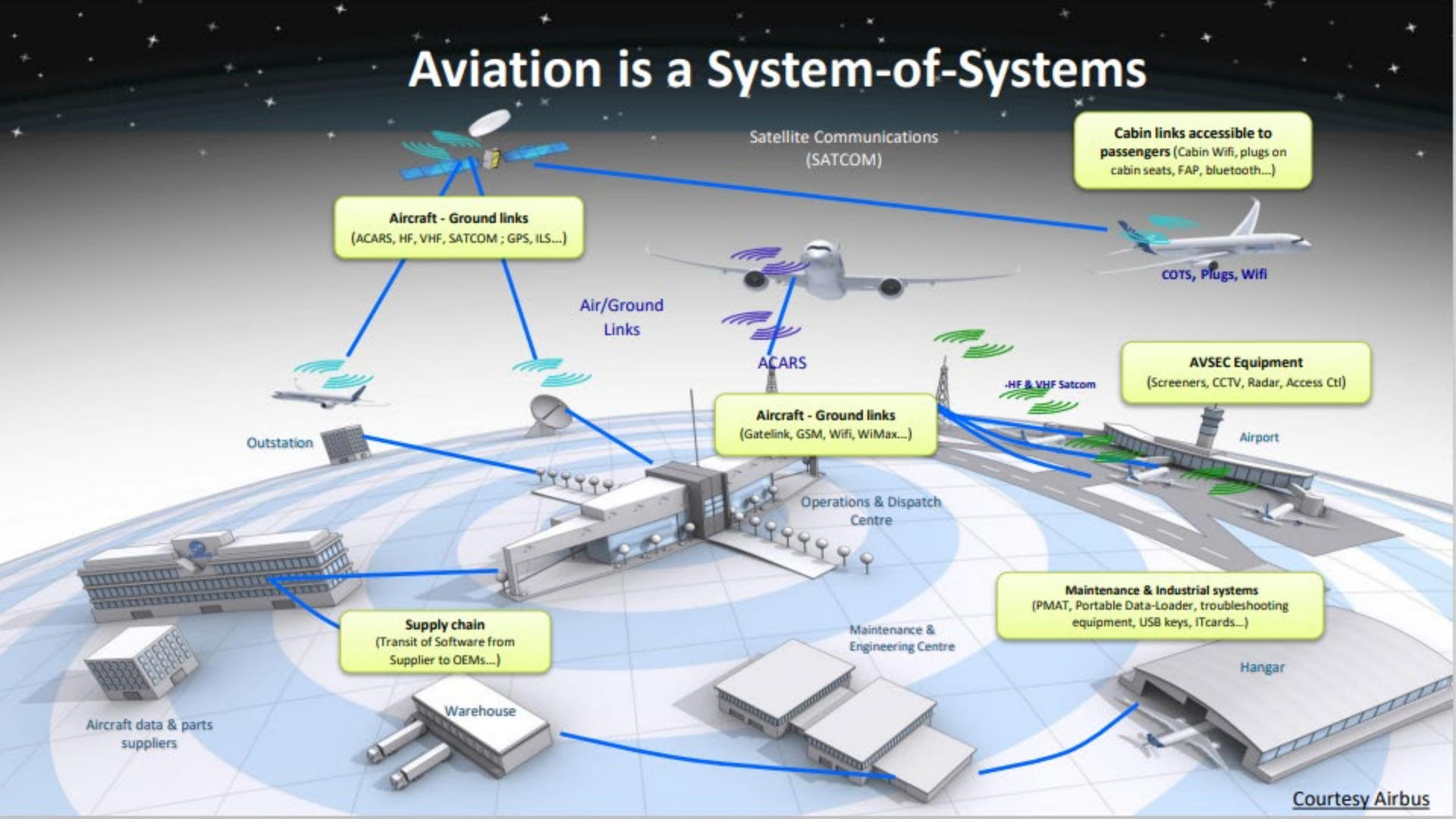
Lag krav

Part-IS
AMC & GM

Säkerhets -kultur

TRANSPORT STYRELSEN

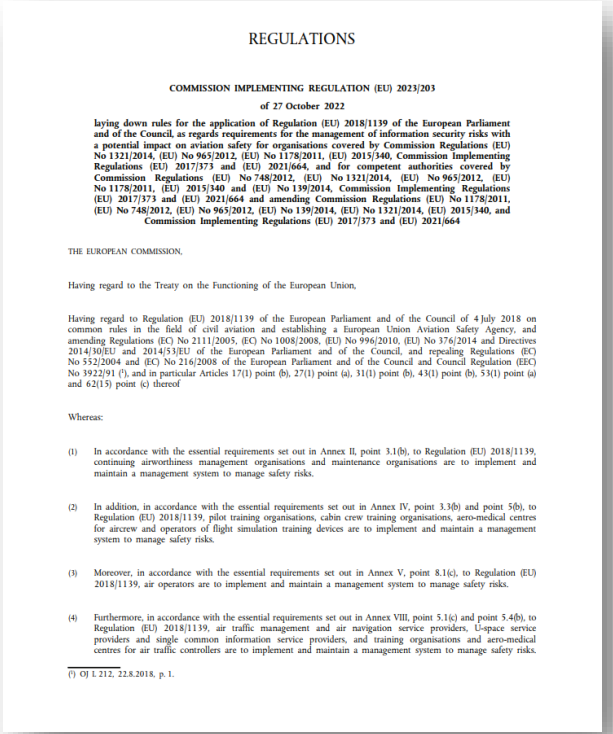
Aviation is a System-of-Systems



Courtesy Airbus

Vad är Part-IS?

- Part-IS är Safety-regulations
- ”*krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten*”
- Dels nya förordningar och dels uppdatering av befintliga



REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) 2023/203

of 27 October 2022

laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [1], and in particular Articles 17(1) point (b), 27(1) point (a), 31(1) point (b), 43(1) point (b), 53(1) point (a) and 62(15) point (c) thereof

Whereas:

(1) In accordance with the essential requirements set out in Annex II, point 3.1(b), to Regulation (EU) 2018/1139, continuing airworthiness management organisations and maintenance organisations are to implement and maintain a management system to manage safety risks.

(2) In addition, in accordance with the essential requirements set out in Annex IV, point 3.3(b) and point 5(b), to Regulation (EU) 2018/1139, pilot training organisations, cabin crew training organisations, aero-medical centres for aircrew and operators of flight simulation training devices are to implement and maintain a management system to manage safety risks.

(3) Moreover, in accordance with the essential requirements set out in Annex V, point 8.1(c), to Regulation (EU) 2018/1139, air operators are to implement and maintain a management system to manage safety risks.

(4) Furthermore, in accordance with the essential requirements set out in Annex VIII, point 5.1(c) and point 5.4(b), to Regulation (EU) 2018/1139, air traffic management and air navigation service providers, U-space service providers and single common information service providers, and training organisations and aero-medical centres for air traffic controllers are to implement and maintain a management system to manage safety risks.

[1] OJ L 212, 22.8.2018, p. 1.

TRANSPORT STYRELSEN

Vad är Part-IS?

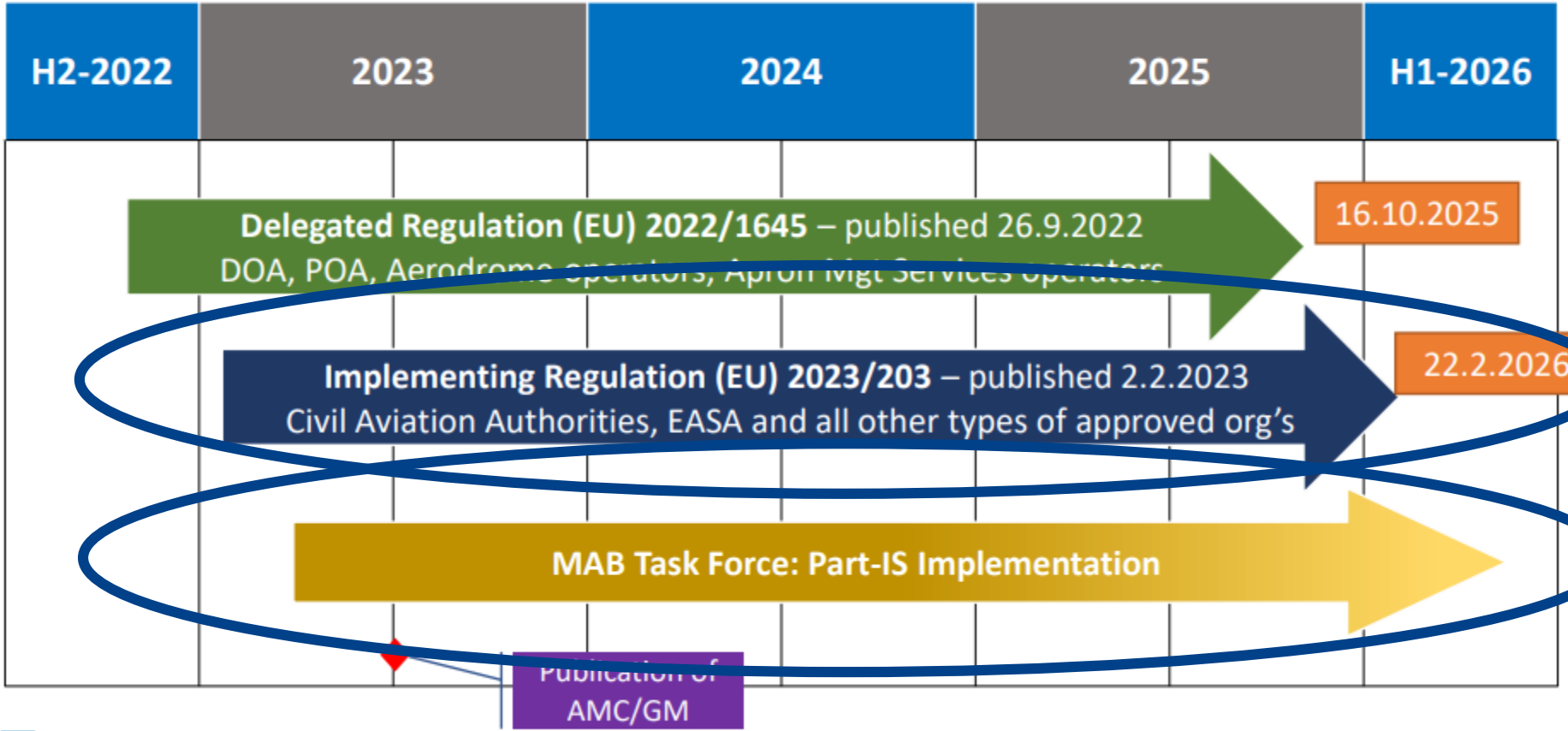
- Genomförandeförordning (EU) 2023/203;
  - Art 2, Scope 1C; air operators Annex III (Part-ORO)

- Delegerade förordning (EU) 2022/1645

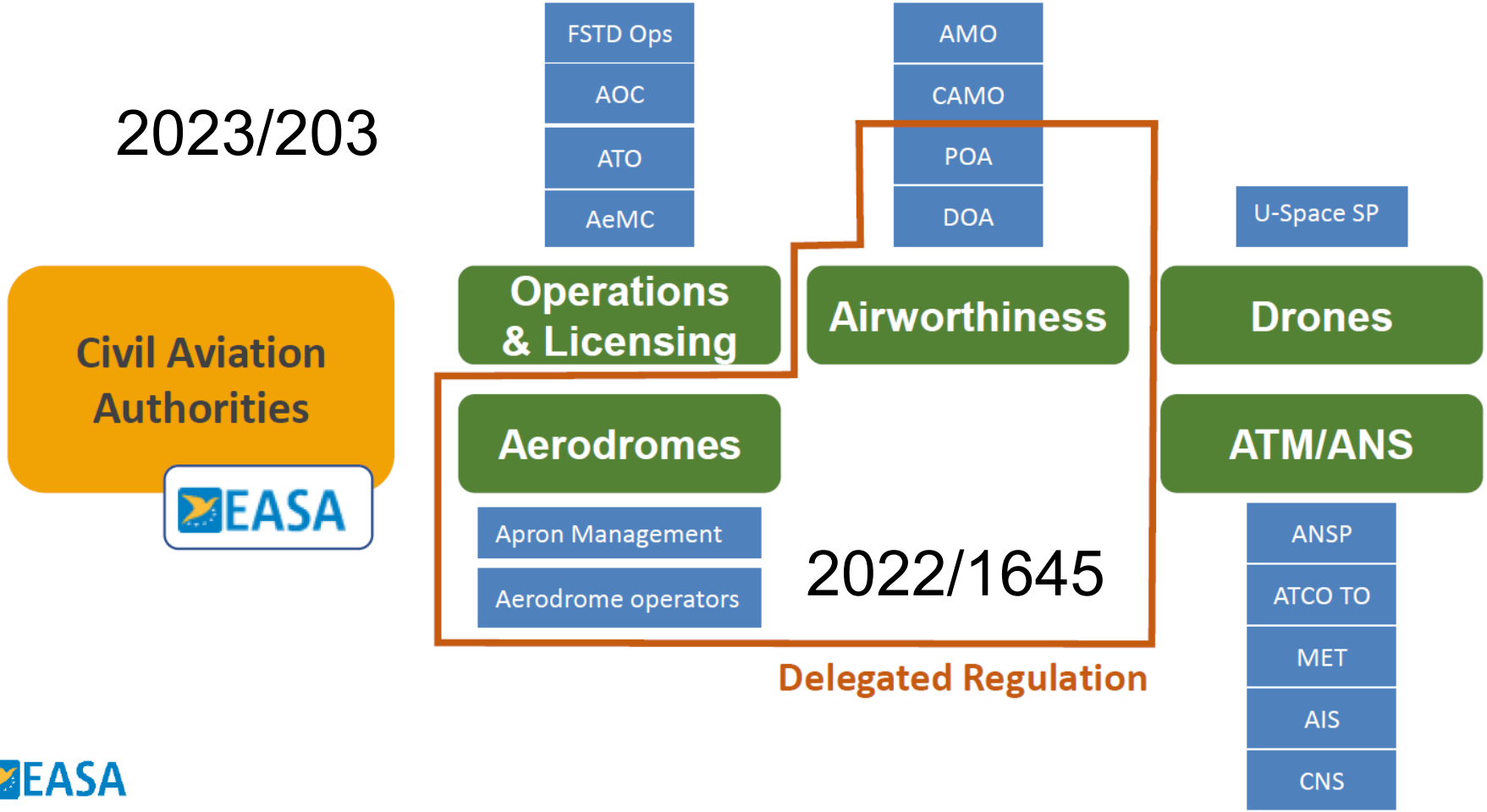
- Både för verksamhetsutövare (OR) och behörig myndighet (AR)

TRANSPORT STYRELSEN

Part-IS implementation journey



Applicability of Part-IS



EASA

AMC & GM

- Publicerades 13 juli

What we want to achieve with Part-IS

Objective	Protect the aviation system from information security risks **with potential impact on aviation safety**

Proportionate to the impact on aviation safety

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

Proportionate to the impact on aviation safety

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

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

The ISMS in Part-IS

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 | Basic Reg. | Reporting Reg. | ISO 2700x

The ISMS in Part-IS

Utmaningar

- Kompetens inom cyber
- Proportionalitet *”Vi är en liten aktör – vi har inte resurser för allt detta!”*
- ISMS (Information security management system)
- Hur kommer tillsynen att se ut

TRANSPORT STYRELSEN

Compliance vs skydd

- Det kan finnas en skillnad mellan att vara ”compliant” och att vara skyddad mot cyberrisker

- Datum för ikraftträdande är då man måste ha infört kraven – ni får börja redan nu!

TRANSPORT STYRELSEN

Kommunikationsinsatser

- Under våren 2024 har vi för avsikt att ha webbinarium om Part-IS
- Uppdatera vår hemsida med specifik information
  - https://www.transportstyrelsen.se/sv/luftfart/

- Pilotprojekt

- Vi vill ha frågor från er!

TRANSPORT STYRELSEN

Information och källor

- EASA
  - First Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645) - October 2023 — Available in pdf, online & xml format | EASA (europa.eu)
  - Ingång till all kravställan
- Cybersecurity | EASA Community (europa.eu)
- Vår hemsida kommer att uppdateras löpande

TRANSPORT STYRELSEN

”NIS2” - Nytt EU direktiv 2022/2555

- *”…åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen”*
- 18 oktober 2024 träder NIS2 ikraft
- I ”NIS1” var flygbolag (och rederier) undantagna
- Sannolikt kommer flygbolag att omfattas
- Utpekande genom omsättning eller antal anställda
  - Mer än 50 anställda *eller*
  - 10 miljoner euro i årsomsättning,
  - Utpekning kan även ske av behörig myndighet
- För frågor om NIS-lagen: nis@transportstyrelsen.se

TRANSPORT STYRELSEN

Frågor?

Principal Inspector (PI)

TRANSPORT STYRELSEN