TRAFICOM
Liikenne- ja viestintävirasto

Ilmailun kyberturvallisuuden jalkauttaminen

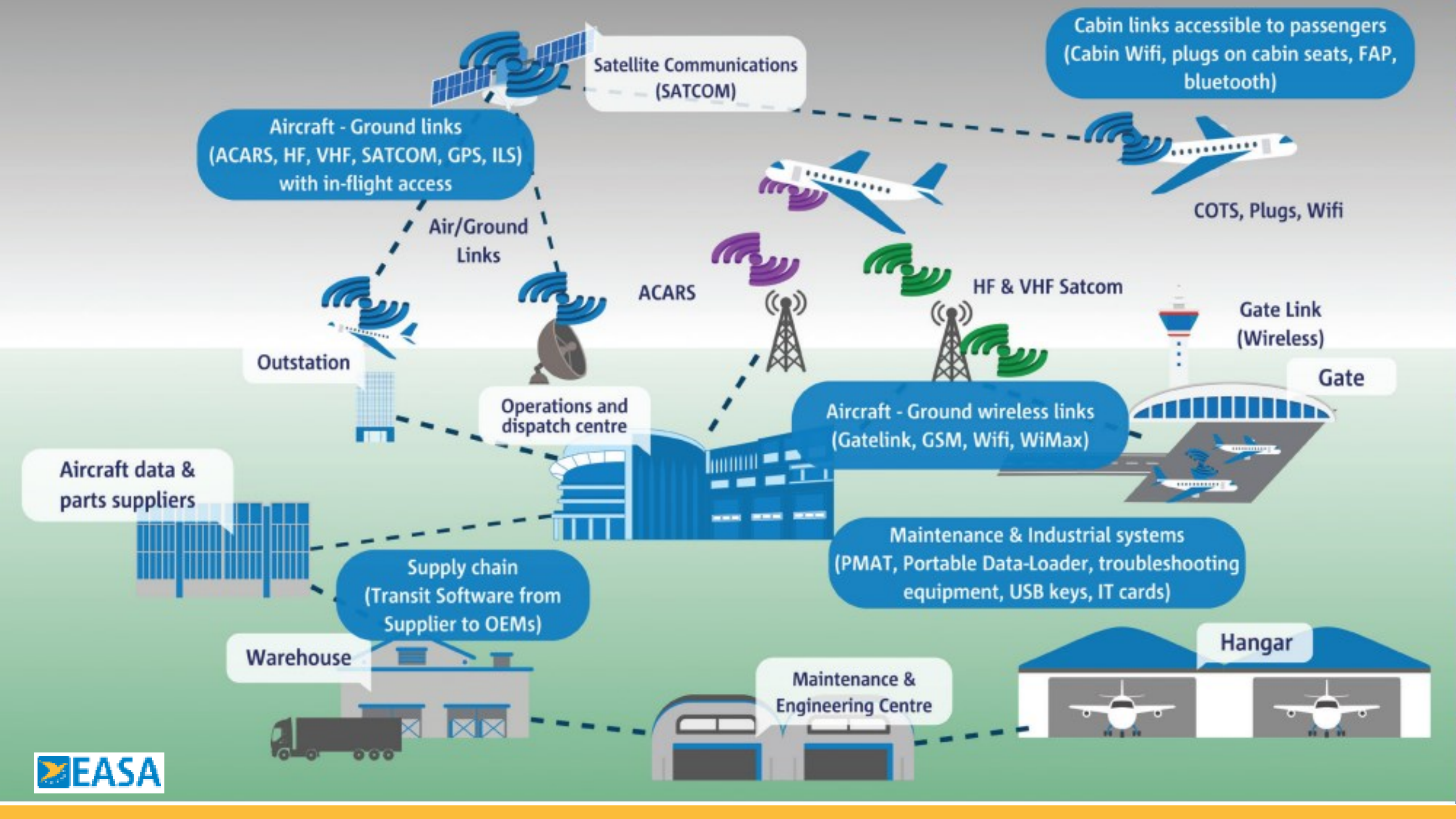
16.9.2024

Tomi Salmenpää

Agenda

- Esittely ja alustus
- Sääntely: Part-IS ja Kyberturvallisuuslaki (NIS2) lyhyesti
- Seuraavat askeleet
- Mistä lisätietoa
- Keskustelua

Päivän tavoite: Antaa organisaatioille konkreettista tietoa sääntelystä ja sen toteuttamisesta


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

Suomen ilmailun turvallisuuspolitiikka - kybernäkökulma

(Suomen ilmailun turvallisuusohjelma (FASP), luku 1.1

Kansainvälisessä siviili-ilmailussa on yhteisin sopimuksin ja säädöksin asetettu turvallisuus ja ilmailun turvaaminen korkeimmaksi päämääräksi. Suomen siviili-ilmailuviranomainen Traficom sitoutuu ylläpitämään ja kehittämään ilmailun kansallista turvallisuusohjelmaa. Erityisen tärkeänä Traficom pitää sitä, että lentoturvallisuus ja kansalaisten luottamus lentoliikennejärjestelmään säilyvät hyvänä. Luottamuksen peruspilareita ilmailujärjestelmässä ovat turvallisuus, ilmailun turvaaminen, kyberturvallisuus, terveysturvallisuus ja ympäristöystävällisyys. Osapuolten on myös huolehdittava taloudellisuudesta, luotettavuudesta ja täsmällisyydestä osana sujuvia matkaketjuja sekä tukemassa Suomen saavutettavuutta. Lisäksi on varmistettava uusien teknologioiden ja toimintamallien turvallinen integrointi ilmailujärjestelmään inhimillisten tekijöiden vahvuudet ja rajoitukset sekä teknologia huomioon ottaen. Osapuolten on varmistettava toiminnan turvallisuus myös toimintaympäristön voimakkaissa muutostilanteissa ja huolehdittava tehokkaasta muutoksen- ja riskienhallinnasta.

Suomen ilmailussa noudatetaan ICAOn ja EU:n vaatimuksia. Traficom määrittelee Suomen ilmailulle strategiset turvallisuustavoitteet ja hyväksyttävän turvallisuustason, joka ottaa huomioon EU-tason turvallisuustavoitteet sekä paikalliset olosuhteet ja Suomen ilmailun riskienhallinnan kautta nousseet turvallisuusteemat. Traficomin ja ilmailun toimijoiden on pyrittävä saavuttamaan määritellyt tavoitteet ja turvallisuustaso käytännön toiminnassaan.

Turvallisuudenhallinnan ja hyvän turvallisuuskulttuurin jatkuva kehittäminen, riski- ja suorituskykyperusteinen lähestymistapa sekä toimijoiden vastuu oman toimintansa turvallisuudesta ovat Suomen ilmailuturvallisuuden kulmakiviä. Traficom valvoo ja edistää edellä mainittujen toteutumista.

Traficom varmistaa ja edistää just culture-ilmapiirin toteutumista. Suomen ilmailujärjestelmässä just culture-ilmapiiri pitää sisällään kaikkien osapuolten osalta hyväksyttävien ja ei-hyväksyttävien toimintatapojen määrittelyn ja viestimisen, luottamuksellisen ja oikeudenmukaisen ilmapiirin edistämisen sekä just culture-periaatteiden noudattamisen käytännössä. Tämä kattaa myös ei-hyväksyttävään toimintaan puuttumisen poikkeama-asetuksen artiklan 16 kohdan 10 mukaisissa tapauksissa. Traficom edistää hyvää raportointikulttuuria ja varmistaa poikkeamatietojen luottamuksellisuuden ja asianmukaisen käytön sekä tietolähteen suojelun poikkeama-asetuksen artiklojen 15 ja 16 mukaisesti.

Traficom ylläpitää ilmailun viranomaistehtäviin tarvittavan asiantuntemuksen tehtävien edellyttämällä tasolla. Tätä tuetaan jatkuvan koulutuksen ja kansainvälisen yhteistyön avulla.

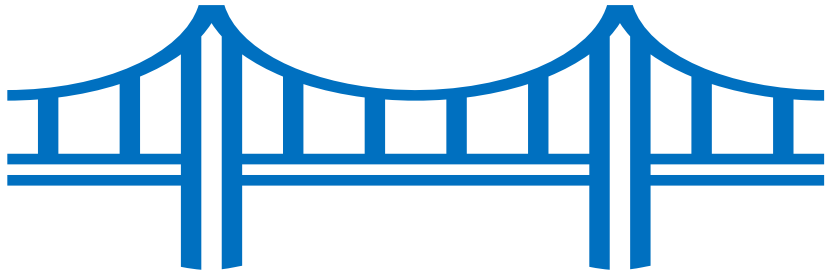
Suomen ilmailun strategiset turvallisuustavoitteet- kybernäkökulma

(Suomen ilmailun turvallisuusohjelma (FASP), luku 1.2

- Suomen ilmailun turvallisuus pysyy korkealla tasolla. Ilmailussa ei tapahdu onnettomuuksia, joiden taustalla olevat syyt johtuvat Suomen ilmailujärjestelmästä.
- Turvallisuussuorituskyvyn (safety performance) jatkuva kehitys Suomen ilmailun toimijoilla kaikilla osa-alueilla
- Suomen ilmailun keskeiset uhat (turvallisuus, ilmailun turvaaminen, kyberturvallisuus, terveysturvallisuus) on tunnistettu ja käsitellään toimijoiden turvallisuudenhallinnassa. Työssä huomioidaan myös Suomen erityisolosuhteet, kuten talvi.
- Suomen ilmailun riskienhallinta (turvallisuus, ilmailun turvaaminen, kyberturvallisuus, terveysturvallisuus) on systemaattista, vaikuttavaa ja jatkuvasti kehittyvää.
- Kyberriskienhallinta on osa ilmailun turvallisuusriskien hallintaa Traficomissa ja toimijoilla.
- Miehittämätön ilmailu on integroitu turvallisesti Suomen ilmailujärjestelmään. Miehittämättömän ilmailun toimijat tuntevat heitä koskevat säännöt ja vastaavat toimintansa turvallisuudesta. Määräystenvastaiseen toimintaan puututaan.
- Suomen ilmailun kiitotieturvallisuus pysyy korkealla tasolla.
- Reaktiivisuus: Traficom ja ilmailun toimijat reagoivat aktiivisesti havaittuihin puutteisiin ja toteuttavat korjaavat toimenpiteet jatkuvan parantamisen hengessä.
- Suomen ilmailun turvallisuusnormit ja toimintatavat täyttävät ICAOn standardit ja EU:n vaatimukset.
- Suomen ilmailun turvallisuuskulttuuri on hyvällä tasolla. Hyvää ja oikeudenmukaista turvallisuuskulttuuria sekä hyvää raportointikulttuuria ylläpidetään ja kehitetään.
- Uusien teknologioiden edistäminen ja turvallinen integrointi ilmailujärjestelmään tehdään tasapainoisesti inhimillisten tekijöiden vahvuudet ja rajoitukset huomioon ottaen.
- Suomi on aktiivinen yhteistyökumppani ilmailun kansainvälisillä foorumeilla ja osaltaan varmistaa hyvän turvallisuustason säilymisen sekä edistää turvallisuutta vahvistavia toimenpiteitä.

InfoSec Threats → **Materialisation InfoSec Hazard** → **Materialisation Safety Hazard** → **Consequence**

Tampering with InfoSec Property	Information Security Incident	Unsafe Condition	Aviation Accident or Incident



Bow-tie representation of management of aviation safety risks posed by information security treats

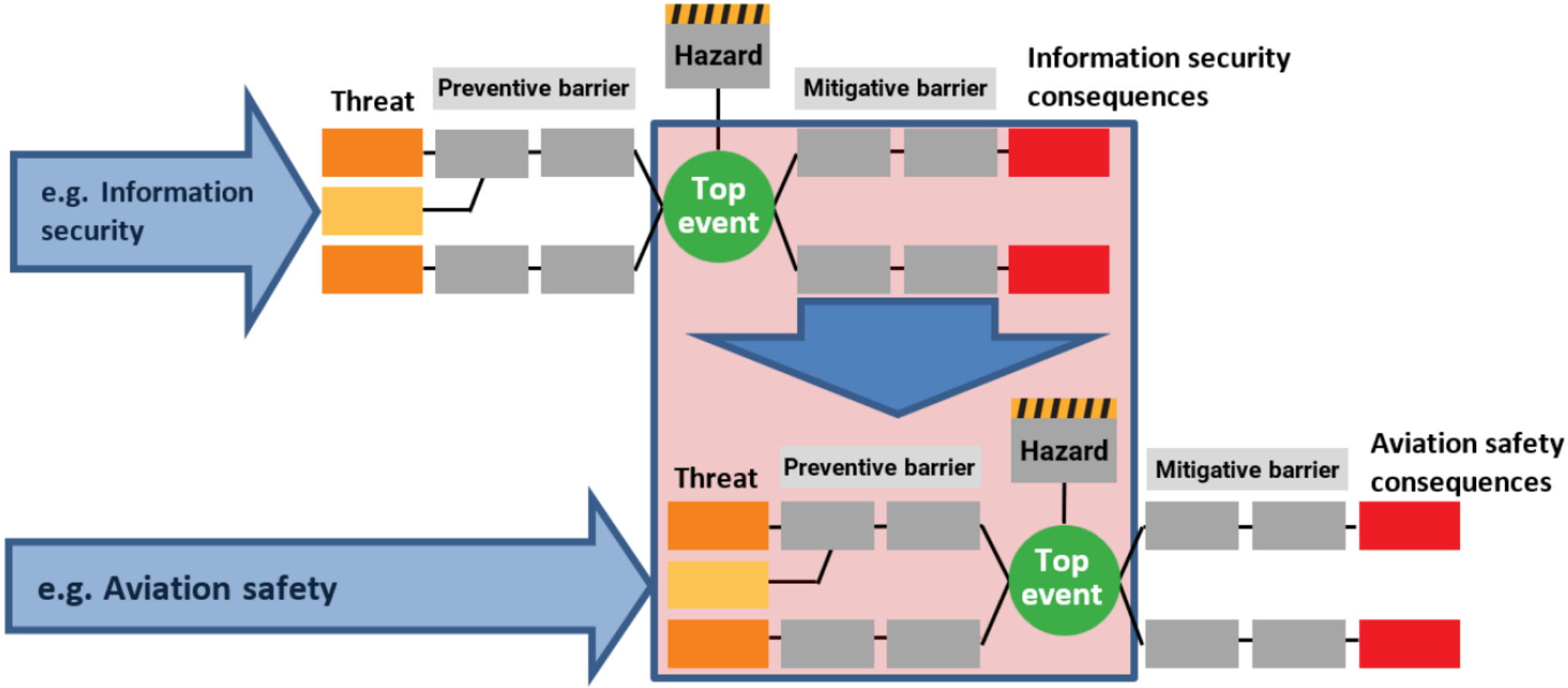


Fig. EASA Part-IS AMC&GM

SMS

SeMS

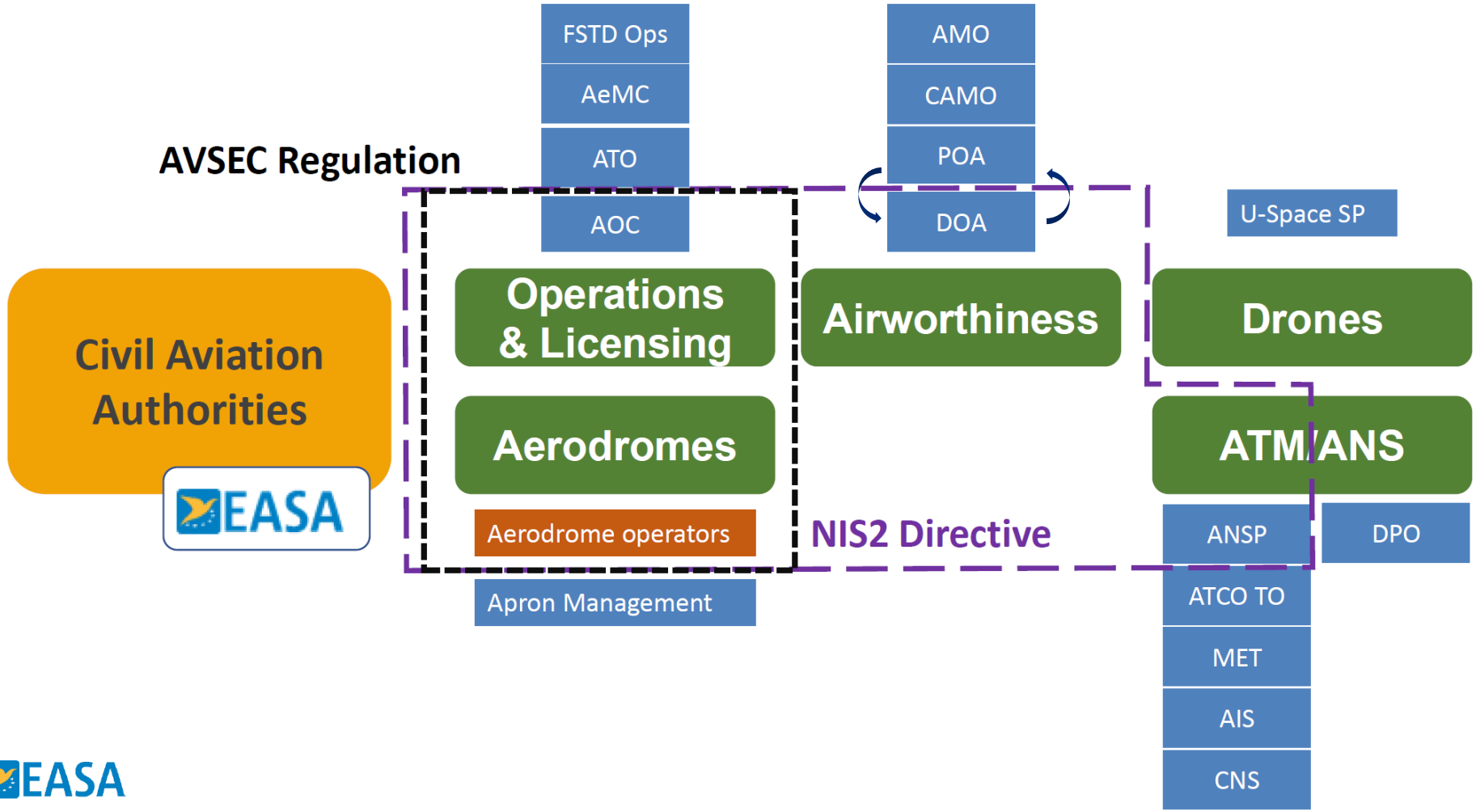
ISMS

.. Miten rakennetaan ISMS oikeassa mittasuhteessa (tasapaino)? Miten kytketään riskienhallinta yhteen?

Sama nimittäjä

- Part-IS: Safety / Tietoturva
- NIS2: Operatiivisen toiminnan jatkuvuus / Tietoturva
- Avsec: Ilmailun turvaaminen / Tietoturva

Applicability of Part-IS



EASA

Part-IS / Kyberturvallisuuslaki (NIS2) / Avsec

- Koskevuus ja vaatimukset
- Sovittaminen olemassa olevaan viranomaistyöhön kaikilla ilmailun osa-alueilla
  - Eroavaisuuksia toimintamalleissa ja kulttuurissa, sekä miten vaatimukset koskettavat juuri teidän ilmailun osa-alueella
- Mitä tarvitaan toimijoilla ja viranomaisella
  - **Toimintatapa, prosessit, työohjeet, resurssit (HTV ja osaaminen)-> koulutus, työkalut**
  - *(NIS2/Kyberturvallisuuslaki)*
    - *Valvovan viranomaisen on ylläpidettävä toimijaluetteloa – Traficomissa työn alla toimijarekisteri. Tavoitteena on julkaista ilmoittautumislomake yhdessä lain kanssa. Ilmoittautumisen määräaika 31.12.2024 mennessä. Tiedotusta & ohjeistusta tulossa.*
    - *Tulossa myös NIS2/Kyberturvallisuuslain mukainen ilmoituslomake palveluun kohdistuvasta merkittävästä poikkeamasta valvovalle viranomaiselle – korvaa nykyisen NIS1-mukaisen lomakkeen*
    - *(Nk. CER-laki (Kriittisen infrastruktuurin tunnistaminen ja kriisinkestävyyden parantaminen): viimeisimmät kommentit lakiluonnokseen kerätty elokuun alussa, odotetaan esitettäväksi Eduskunnalle (toimijoiden osalta soveltaminen alkaa 2027) – mahdolliset vaikutukset NIS2-soveltamisalaan.*

Making EU aviation cyber resilient

Products (Aircrafts, Engines, …)

- Transition from case by case approach to mandatory on all products now done.
- Requirements incorporated into CS and AMC in July 2020

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

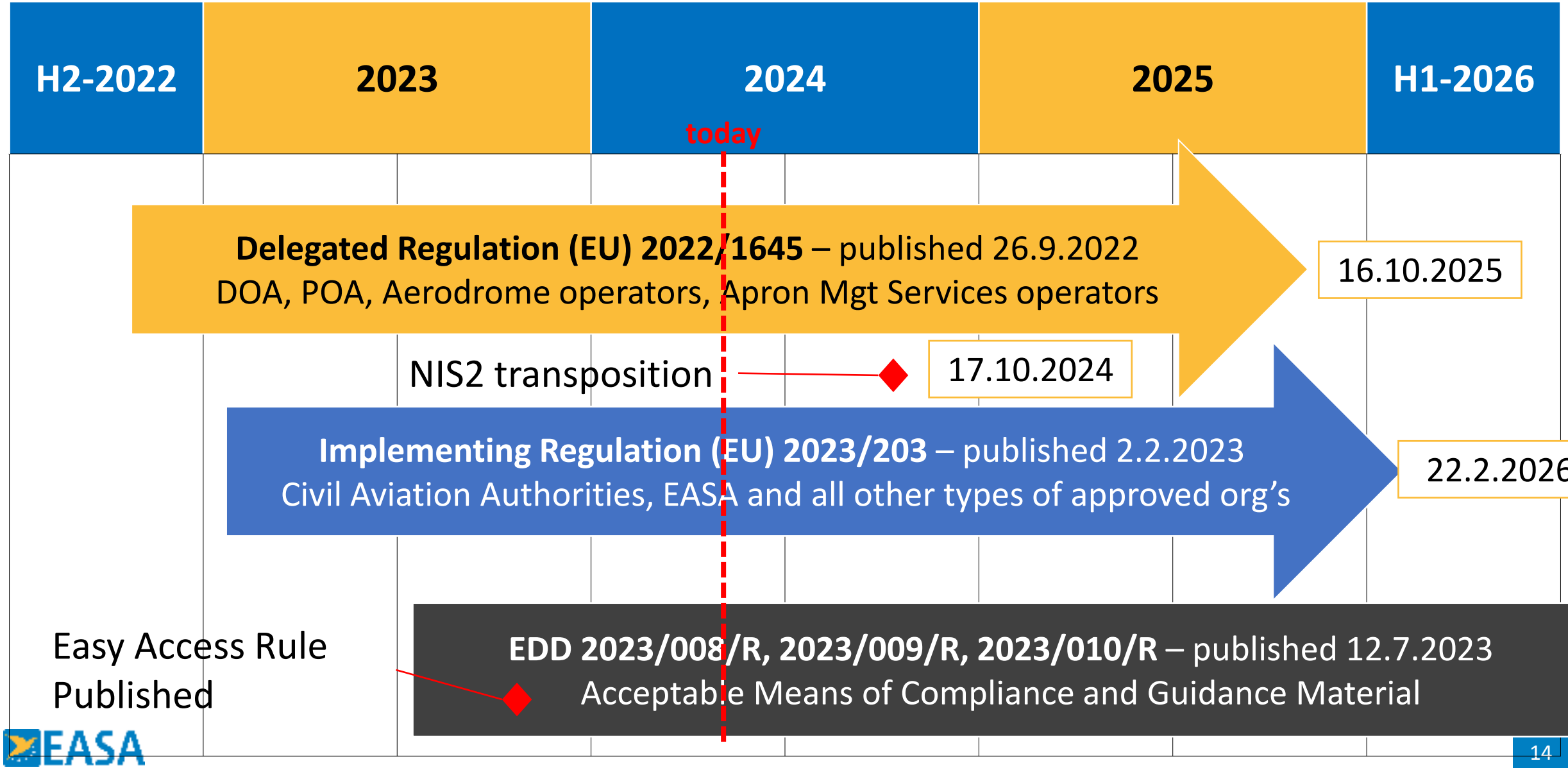
- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape

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

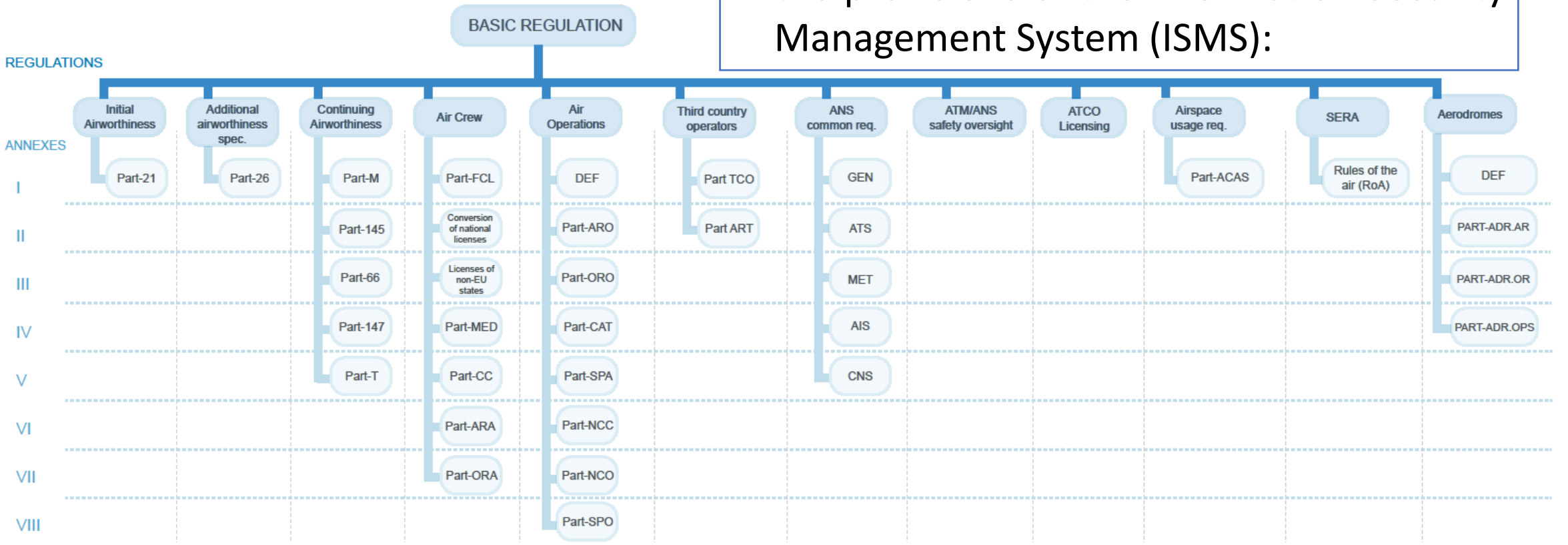
Amdts to existing AMC/GM for ARs

3 ED Decisions

Easy Access Rules available here

Part-IS cross domain applicability

Two "horizontal" regulations containing the provisions of the Information Security Management System (ISMS):



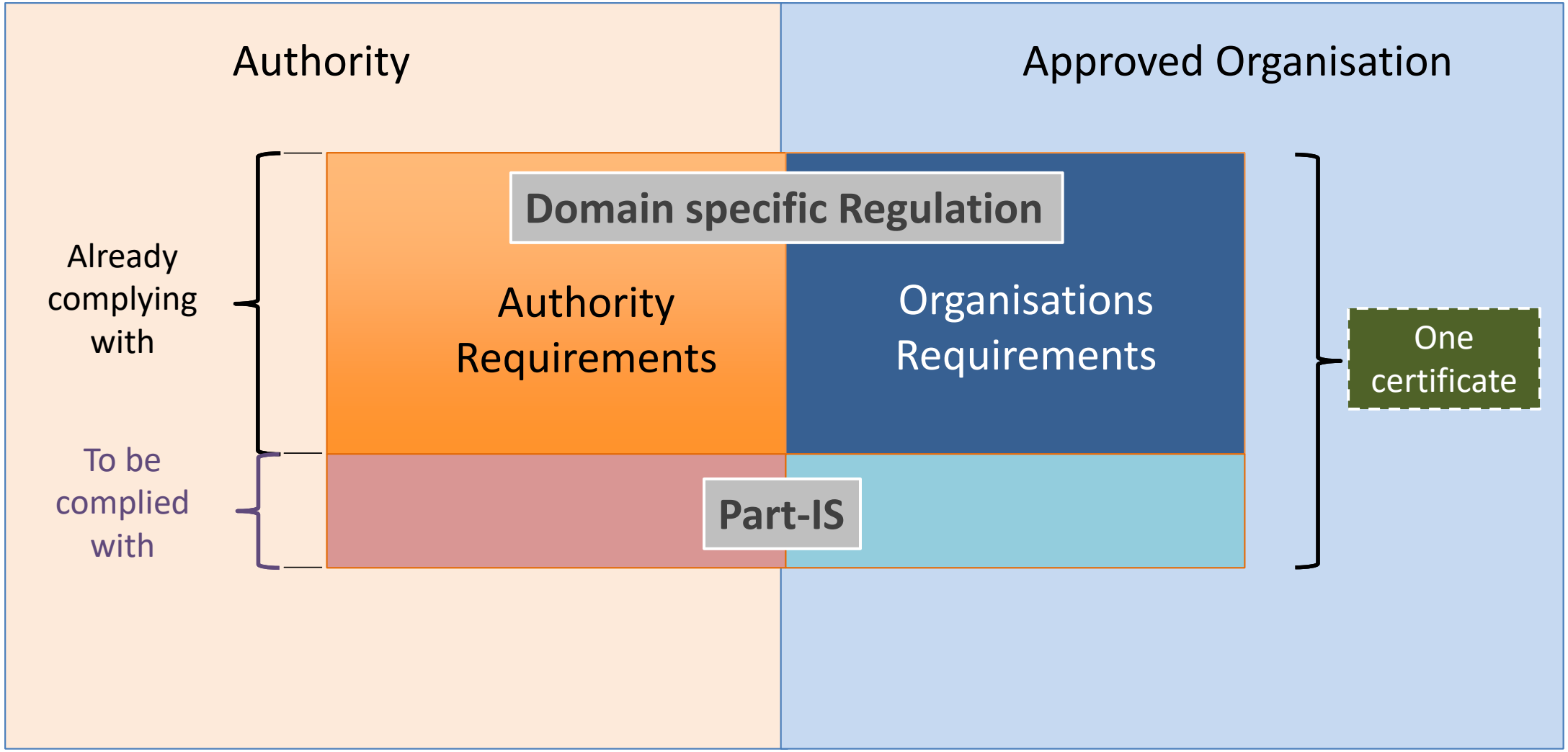
Authority Requirements: Part-IS.AR

Organisation Requirements: Part-IS.OR

Overview of Part IS requirements: Organisation vs Authority

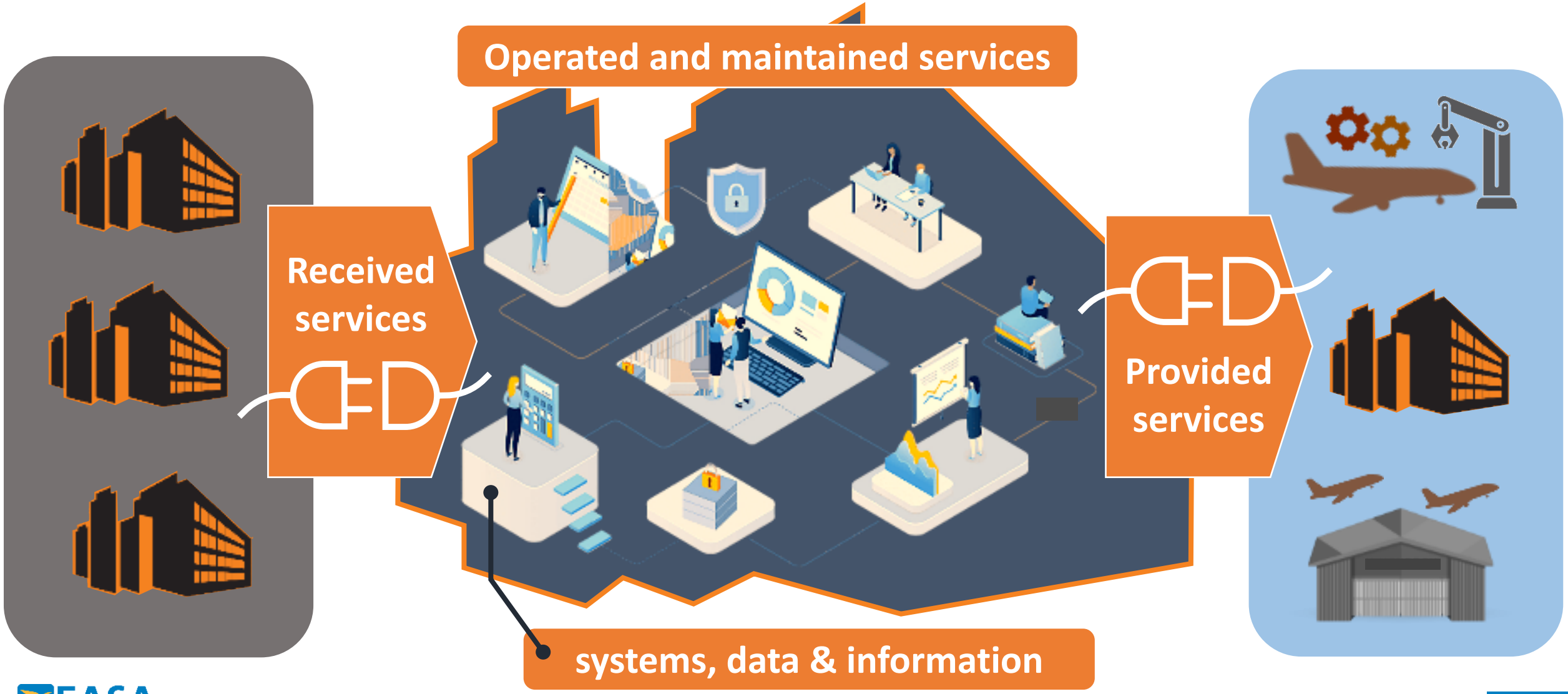
ORGANISATION	Description	AUTHORITY
IS.I.OR.100	Scope	IS.AR.100
IS.I.OR.200	Information security management system (ISMS)	IS.AR.200
IS.I.OR.205	Information security risk assessment	IS.AR.205
IS.I.OR.210	Information security risk treatment	IS.AR.210
IS.I.OR.215	Information security internal reporting scheme	
IS.I.OR.220	Information security incidents — detection, response, and recovery	IS.AR.215
IS.I.OR.225	Response to findings notified by the competent authority	
IS.I.OR.230	Information security external reporting scheme	✓
IS.I.OR.235	Contracting of information security management activities	IS.AR.220
IS.I.OR.240	Personnel requirements	IS.AR.225
IS.I.OR.245	Record-keeping	IS.AR.230
IS.I.OR.250	Information security management manual (ISMM)	
IS.I.OR.255	Changes to the information security management system	
IS.I.OR.260	Continuous improvement	IS.AR.235

Part-IS and existing approvals/regulations



NIS2		Part-IS
Policies on risk analysis and information system security	✓	OR.200(a)(1)
Incident handling	✓	OR.200(a)(5) and OR.220
Business continuity measures	✓	OR.210
Supply chain security	✓	OR.205, OR.210, OR.235
Security in systems acquisition, development and maintenance, including vulnerability handling and disclosure	✓	OR.205, OR.210, OR.230
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	✓	IS.OR.260 Cont. Imp.
Basic cyber hygiene and training	✓	IS.OR.240 Personnel Req.s
Policies on appropriate use of cryptography and encryption		Implementation dependent
Human resources security, access control policies and asset management	✓	IS.OR.240 Personnel Req.s
Use of multi-factor authentication, secured voice/video/text communications and secured emergency communication		Implementation dependent
Incident Reporting	✓	OR.230

Risk assessment - scope identification



Traficom - oma valmistautuminen

- Mitä valvomme ja mitä viranomaisen työhön kuuluu ilmailun kyberturvallisuudessa?
  - Toimintatapa, prosessit, työohjeet

- Ilmailuviranomaisen rooli kyberturvallisuudessa
  - Part-IS, NIS2, Avsec, varautuminen
  - Suomen ilmailun turvallisuussuunnitelma ja ohjelma sekä turvaohjelma
    - Turvallisuuspolitiikka ja strategiset turvallisuustavoitteet (FASP)
    - Riskienhallinta (ml. yhteistyö ilmailun kansallisen kyberriskikuvan ylläpitämiseksi)
  - Käytössämme olevat resurssit
  - Tarvittava osaaminen/pätevyys
  - Koulutustarve
  - Työkalut työn tekemiseen

Mistä löydät lisätietoa

- Traficomin nettisivut: www.traficom.fi
  - Ilmailun kyberturvallisuuden sivut: https://www.traficom.fi/fi/liikenne/ilmailu/ilmailun-kyberturvallisuus
  - Ilmailun pääsivu: https://www.traficom.fi/fi/liikenne/ilmailu
- Traficomin Kyberturvallisuuskeskuksen sivut: https://www.kyberturvallisuuskeskus.fi/fi
  - Kybermittari: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari
  - NIS2 - Euroopan unionin kyberturvallisuusdirektiivi: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi
  - ISAC-tiedonvaihtoryhmät: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat
- EASAn sivustoja kyberturvallisuudesta
  - EASA Community Network – Cybersecurity: https://www.easa.europa.eu/community/cybersecurity
  - Part-IS Implementation workshop: https://www.easa.europa.eu/community/events/part-implementation-workshop-2024
  - EASAn Cybersecurity-sivut: https://www.easa.europa.eu/en/domains/cyber-security
  - EASAn Part-IS-kysymykset ja vastaukset-sivusto: https://www.easa.europa.eu/en/the-agency/faqs/information-security-part
  - Part-IS & AMC/GM Easy Access Rule (June 2024 update): https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-information-security-regulations-eu-2023203

Seuraavat askeleet

- Sidosryhmätilaisuuksia?
  - Tulossa jatkoa jo vuoden loppuun mennessä, alussa keskitytään ISMS:ään ja riskienhallintaan
  - ”Säännölliset ilmailun kyberkahvit Teamsillä”?

Keskustelua