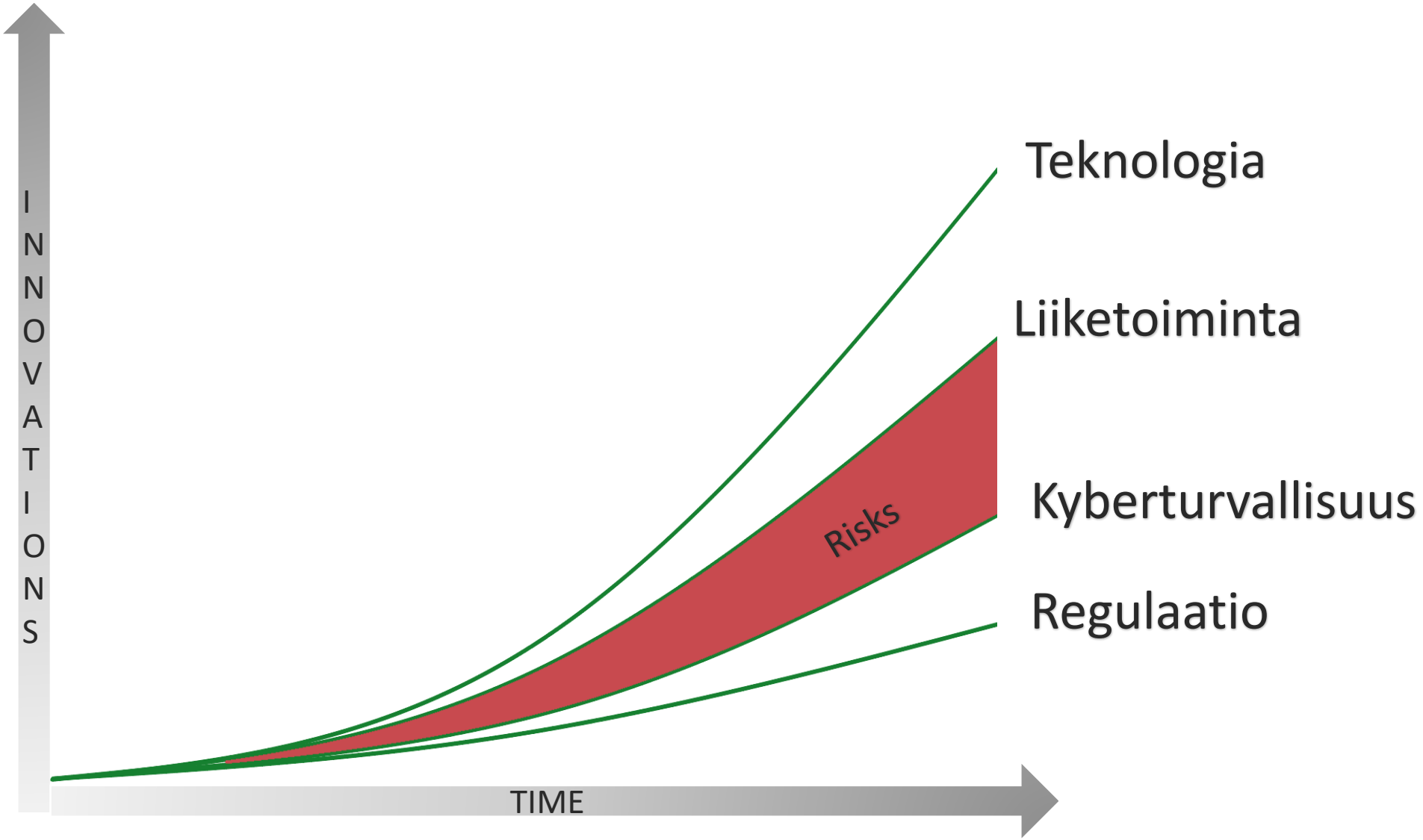
TRAFICOM
Finnish Transport and Communications Agency

Ilmailun kyberturvallisuus

11.12.2019 Säädösinfo
Traficom Kumpulantie

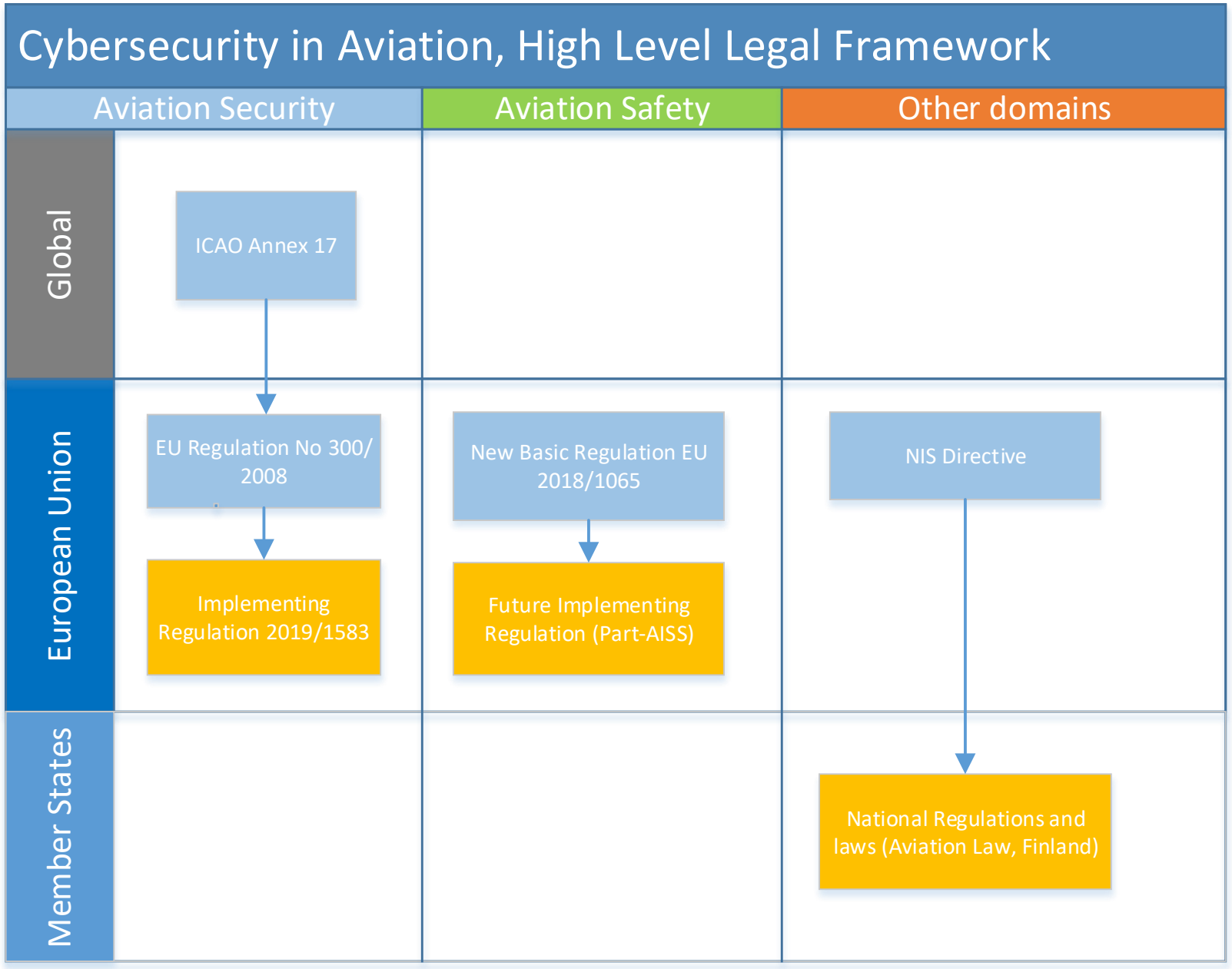
Trendi


INNOVATIONS
TIME
Risks
Teknologia
Liiketoiminta
Kyberturvallisuus
Regulaatio

Terminologia

- Kyberturvallisuus (Cybersecurity) vs. tietoturvallisuus (Information security)
- Tietoturvallisuus
  - järjestelyt, joilla pyritään varmistamaan tiedon saatavuus (Confidentiality), eheys (Integrity) ja luottamuksellisuus (Availability)
- Samoilla termeillä on eri merkitys eri foorumeilla (kontekstisidonnaisuus)

TRAFICOM


Cybersecurity in Aviation, High Level Legal Framework
Aviation Security
Aviation Safety
Other domains
Global
European Union
Member States
ICAO Annex 17
EU Regulation No 300/ 2008
Implementing Regulation 2019/1583
New Basic Regulation EU 2018/1065
Future Implementing Regulation (Part-AISS)
NIS Directive
National Regulations and laws (Aviation Law, Finland)

TRAFICOM

Other domains

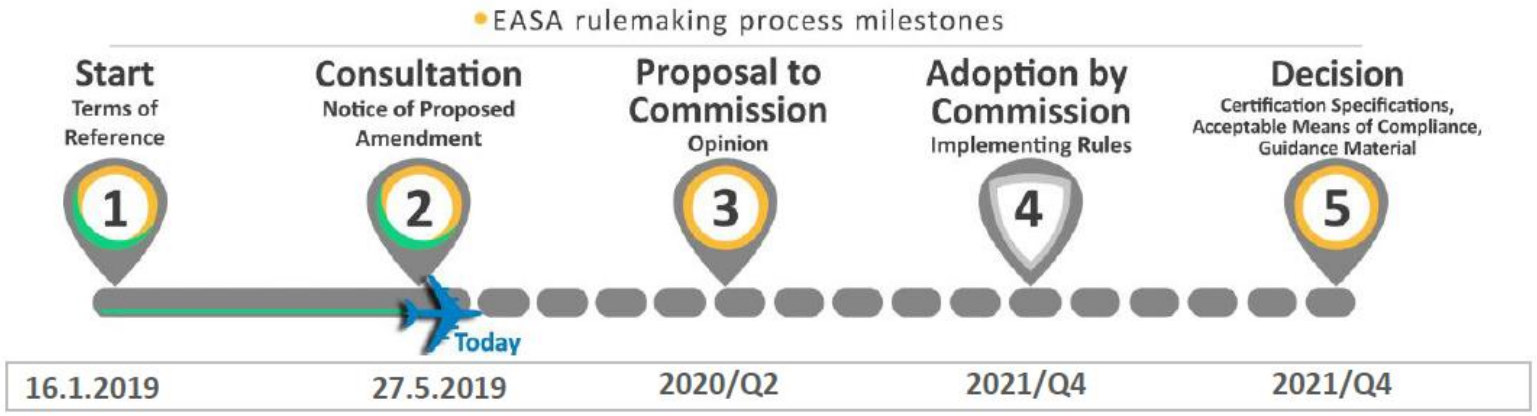
- NIS direktiivi ja ilmailulaki
  - 128 a §
    - Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta
  - 128 b §
    - Tietoturvapoikkeamista ilmoittaminen

Aviation security

- ICAO Annex 17 muutokset (Regulation 2019/1583)
  - The appropriate authority shall ensure that airport operators, air carriers and entities as defined in the national civil aviation security programme identify and protect their critical information and communications technology systems and data from **cyber-attacks which could affect the security of civil aviation**

Aviation safety

- NPAssa (2019-07) on kuvattu selkeästi sen taustat
- Kehitystyössä vahva ESCP (European Strategic Coordination Platform) osallistuminen, myös jatkossa
- Kommentointiaika 27.9.2019 mennessä
- Prosessi noudattaa normaalia EASA NPA prosessia

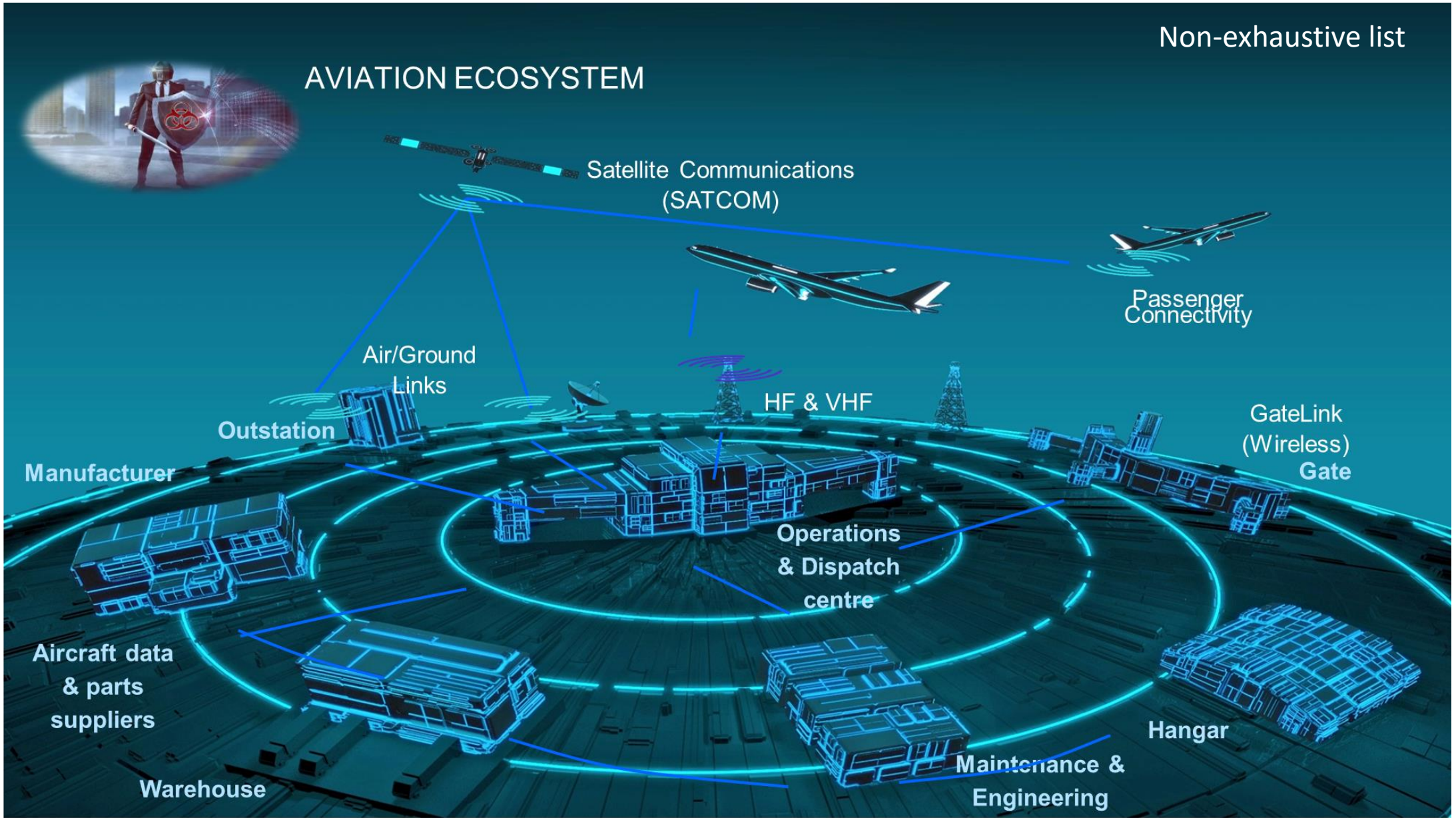


NPA Lyhyesti: mitä ja miksi

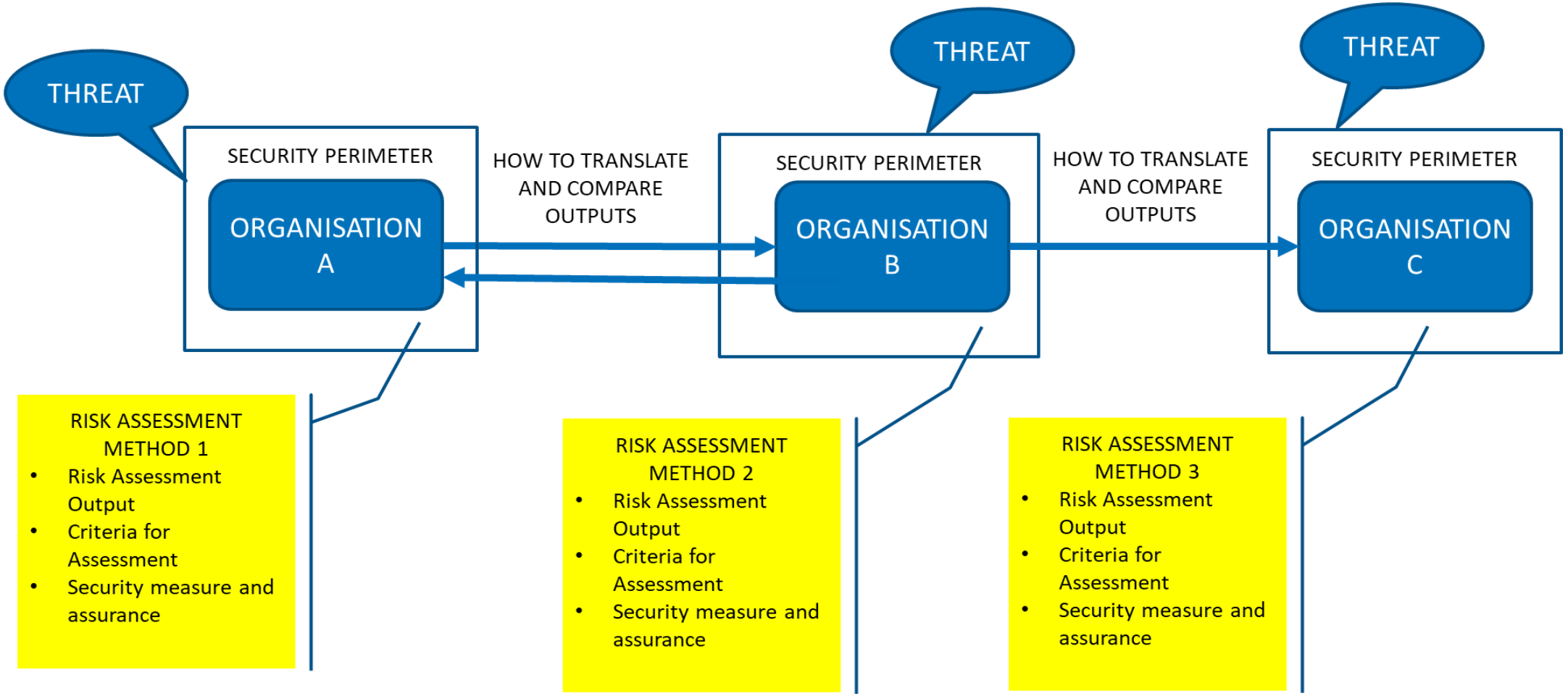
- Nykyinen lentoturvallisuussääntely tähtää onnettomuuksien todennäköisyyden pienentämiseen
- Riski on kasvanut (ja kasvaa) merkittävästi tapahtumille, joissa järjestelmän heikkouksia eri alueilla käytetään tahallisesti väärin
- Tässä NPAssa tietoturvariskit ovat riskejä, jotka voivat vaarantaa ilmailujärjestelmässä käsiteltävän, siirrettävän tai varastoitavan tiedon luottamuksellisuuden, eheyden ja saatavuuden

NPA Lyhyesti: mitä ja miksi

- Part-AISS keskittyy tietoturvariskien lentoturvallisuusvaikutuksiin kokonaisvaltaisella ja standardoidulla tavalla


Non-exhaustive list
AVIATION ECOSYSTEM
Satellite Communications (SATCOM)
Passenger Connectivity
Air/Ground Links
HF & VHF
Outstation
Manufacturer
GateLink (Wireless) Gate
Operations & Dispatch centre
Aircraft data & parts suppliers
Warehouse
Hangar
Maintenance & Engineering Centre

Tiedon jakaminen, riskienhallinta

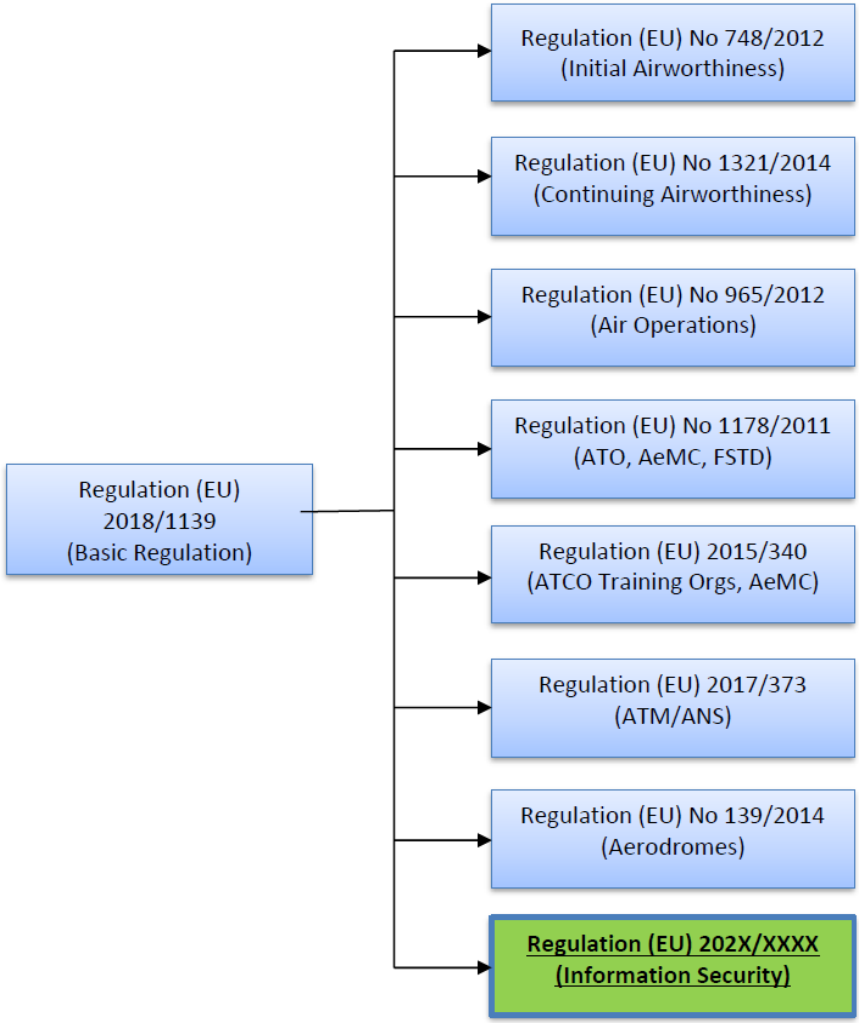


NPA: Mitä halutaan saavuttaa - tavoite

- Varmistaa, että siviili-ilmailun toimintaan osallistuvat organisaatiot ja viranomaiset kykenevät tunnistamaan, suojaamaan, havaitsemaan, vastaamaan ja palautumaan lentoturvallisuuteen vaikuttavista tietoturvatapahtumista

NPA: Miten saavutamme tavoitteen

- Painopisteenä tietoturva tapahtumien vaikutus lentoturvallisuuteen
- Laajuus: viranomaiset ja toimijat
  - i.e. design, production, management of continuing airworthiness, maintenance, air operations, aircrew, air traffic management/air navigation services (ATM/ANS) and aerodromes
  - Poislukien ELA2 toiminta
- Toimivaltainen viranomainen
- Part-AISS yhdenmukaisuus ja suhde muuhun regulaatioon
- Tämä sääntö täydentää olemassa olevia sääntöjä, eikä vaadi erillistä hyväksyntää / deklaraatiota



NPA: Miten saavutamme tavoitteen

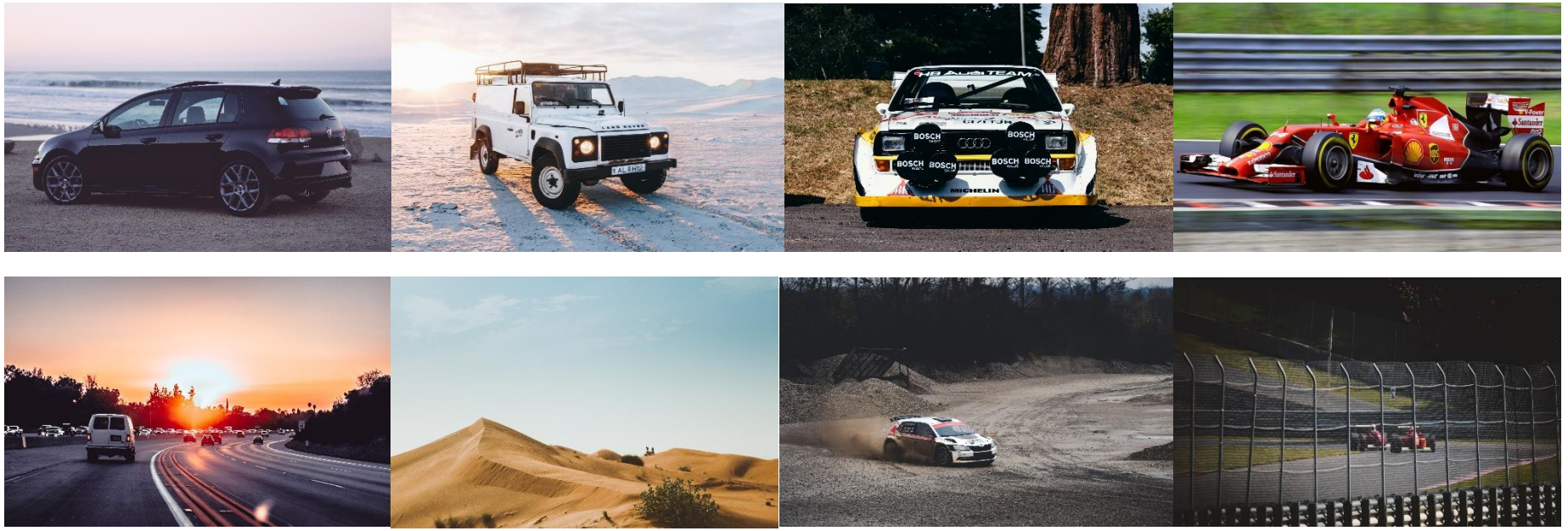
- Riski- ja suorituskykyperusteisuus
  - Yleisen tason regulaatio +
  - AMC/GM ja teollisuusstandardit
- Hallintojärjestelmien integrointi (SMS, SeMS ja ISMS)
- Siirtymäjaksot mahdollisia esim. valmiuksien mukaisesti -> toimijoiden näkemykset arvokkaita

Information Security Management System (ISMS)

- ICAO Annex 17 -> Aviation security
- NIS Directive -> Economies and societies
- Part-AISS -> Safety and the flow of traffic (EATMN)

Picture by UK CAA

Turvallisuus on ympäristösidonnaista



TRAFICOM
Finnish Transport and Communications Agency

tomi.salmenpaa@traficom.fi
www.traficom.fi
@TraficomFinland

AMC / GM työ käynnissä

- Mitkä Part-AISS osat tarvitsevat AMC:tä, mitkä sidosryhmät ja minkälaista AMC:tä
- Teollisuusstandardit
- Koordinaatio muuhun regulaatioon
- Koordinaatio viranomaisten välillä
- Riskienhallintayhteistyö
- ISMS ja pienet organisaatiot
- Maturiteettimallit
- Henkilöstön osaaminen ja koulutus
- Raportointi: mitä raportoidaan ja miten?
- Hankinta ja alihankinta
- ISMS integrointi olemassa olevien hallintajärjestelmien kanssa

Part-AISS sisältö

ANNEX I

AERONAUTICAL INFORMATION SYSTEM SECURITY — AUTHORITY REQUIREMENTS

[PART-AISS.AR]

AISS.AR.005 Objective

AISS.AR.100 Personnel requirements

AISS.AR.200 Information security management system (ISMS)

AISS.AR.400 Allocation of tasks to qualified entities

AISS.AR.500 Record keeping

AISS.AR.600 Oversight

AISS.AR.610 Oversight programme

AISS.AR.620 Information to the Agency

AISS.AR.630 Immediate reaction to an information security problem with safety impact

AISS.AR.800 Assessment of changes to organisations

AISS.AR.900 Findings and corrective actions

Part-AISS sisältö

ANNEX II

AERONAUTICAL INFORMATION SYSTEM SECURITY — ORGANISATION REQUIREMENTS

[PART-AISS.OR]

AISS.OR.005 Scope

AISS.OR.100 Personnel requirements

AISS.OR.200 Information security management system (ISMS)

AISS.OR.300 Information security internal reporting scheme

AISS.OR.310 Information security external reporting scheme

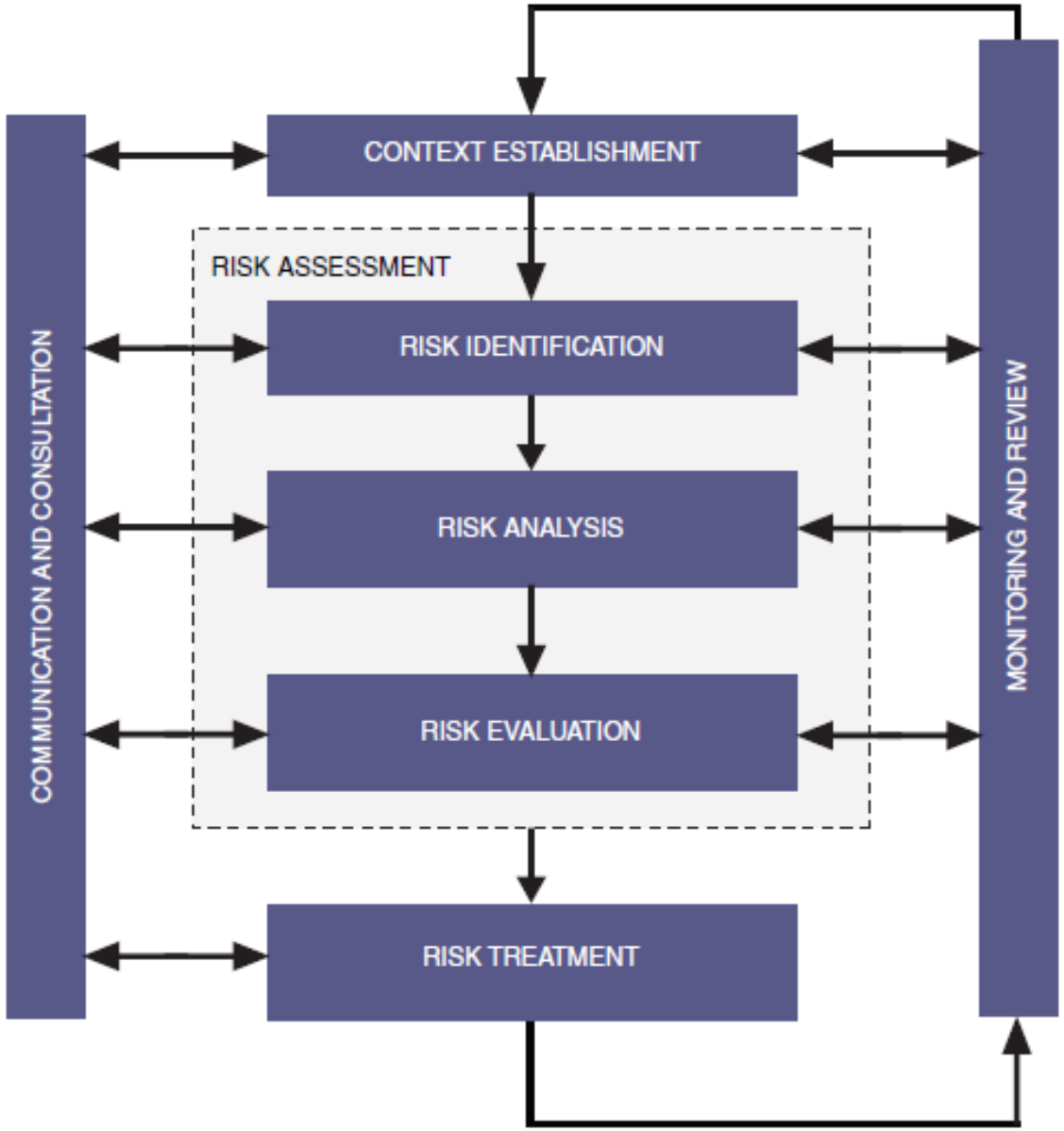
AISS.OR.400 Contracted activities

AISS.OR.500 Record keeping

AISS.OR.700 Information security management manual (ISMM)

AISS.OR.800 Changes to the organisation

AISS.OR.900 Findings



ISO 31000 / 27005

Tehokas ja kestävä kyberturvallisuus..

- Perustuu tietoturvanhallintajärjestelmään, jossa on kolme peruspilaria:
  - Ihmiset
  - Prosessit
  - Teknologia