EASA

European Union Aviation Safety Agency

Part-IS Implementation

Workshop

Cologne, November 7 - 8

Your safety is our mission.

An Agency of the European Union

Part-IS Workshop agenda – Day 1

Introduction to Part-IS & organisational impact

Scene setter on Part-IS, links with the other implementing rules for the different domains and the expected impact on the organisational structure.

EASA

Panel 1 - Part-IS early implementers' feedback

Experiences of early implementers of Part-IS, challenges and key aspects.

EASA, Airbus Commercial, Lufthansa Group, Nordic Regional Airlines AB, TRAFICOM

Q&A

Examples of functional chains and shared risks

Examples of risks at the interface between organisations.

EASA, Airbus

External Reporting under Part-IS

External reporting requirements under Part IS and the relationship with Reg. (EU) 376/2014, the reporting tools that will be available.

EASA

ISO/IEC 27000 in relation to Part-IS

Insights on the similarities and differences between ISO/IEC 27000 and Part-IS in order to leverage on existing certification.

EASA

Industry standardisation

European Cyber security for aviation Standards Coordination Group (ECSCG) activities - focus on standards that will support Part-IS implementation.

EASA

Q&A

Welcome!

Thanks for being with us virtually and in presence

Part-IS Implementation

Workshop

Introduction to Part-IS and Organisational Impact

Part-IS Implementation

Workshop

Angeliki Karakoliou is an Expert in Cybersecurity in Aviation since 2019, where she has worked in different domains including product certification and flight standards. She is currently dealing with Part-IS implementation support, Position Navigation and Time (PNT) interference and cyber threat intelligence.

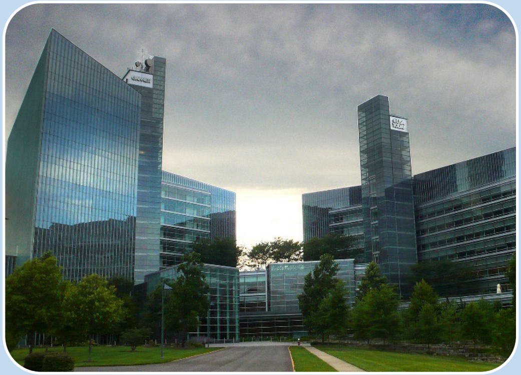
She has a background in computer science and holds a dual LLM in Law and Economics.

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

✓

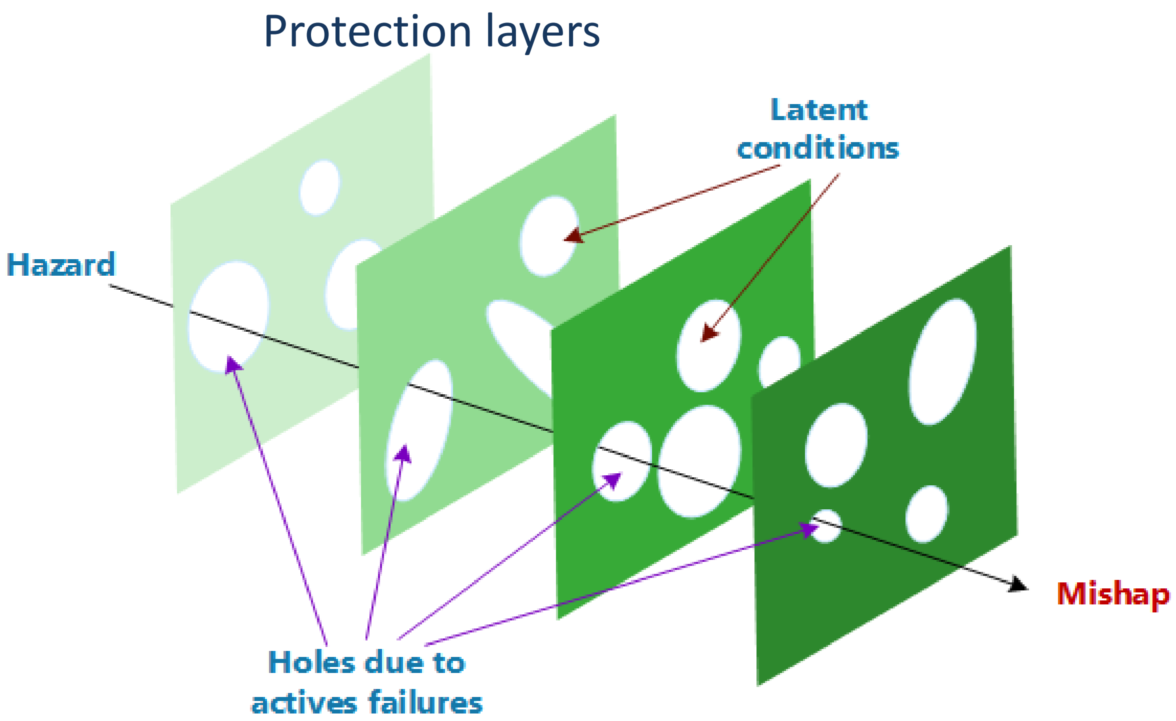
Information Sharing

- 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

The cultural bias in aviation



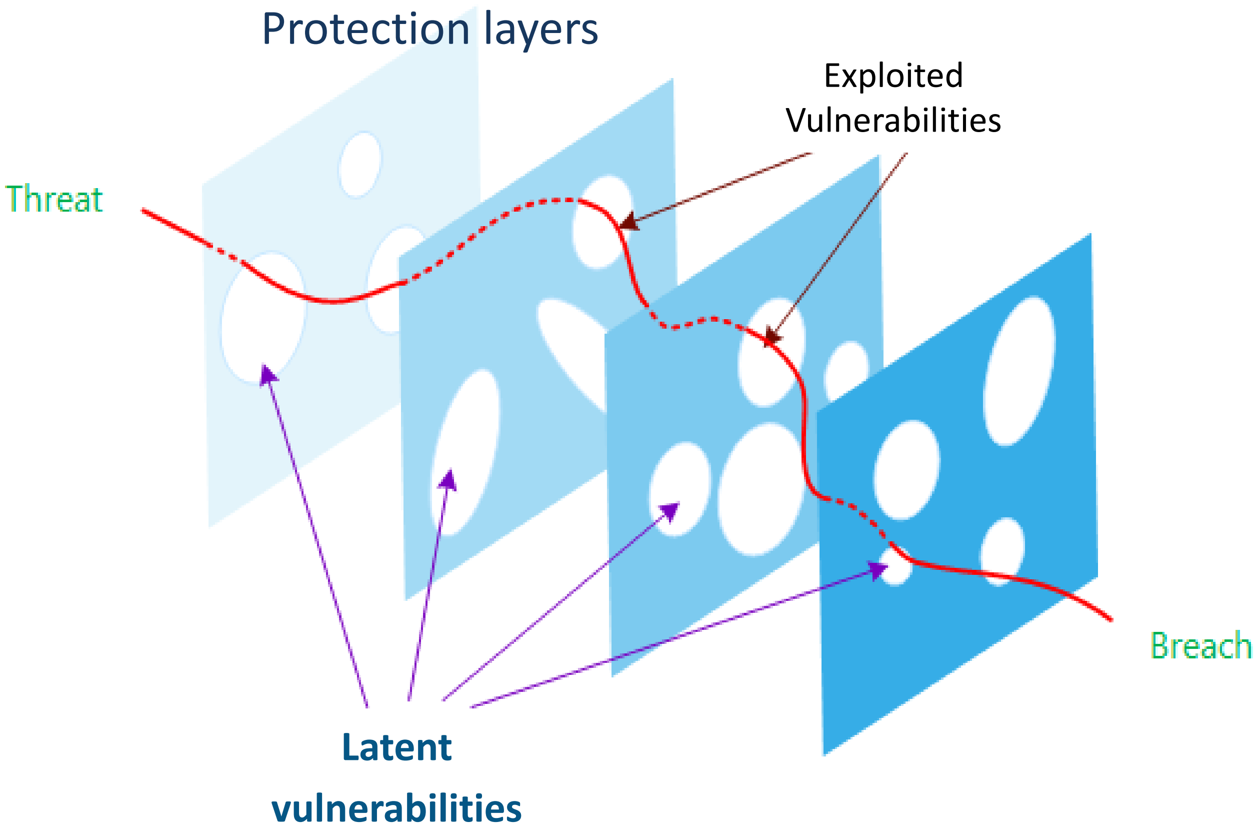
Protection layers

Latent conditions

Hazard

Mishap

Holes due to actives failures



Protection layers

Exploited Vulnerabilities

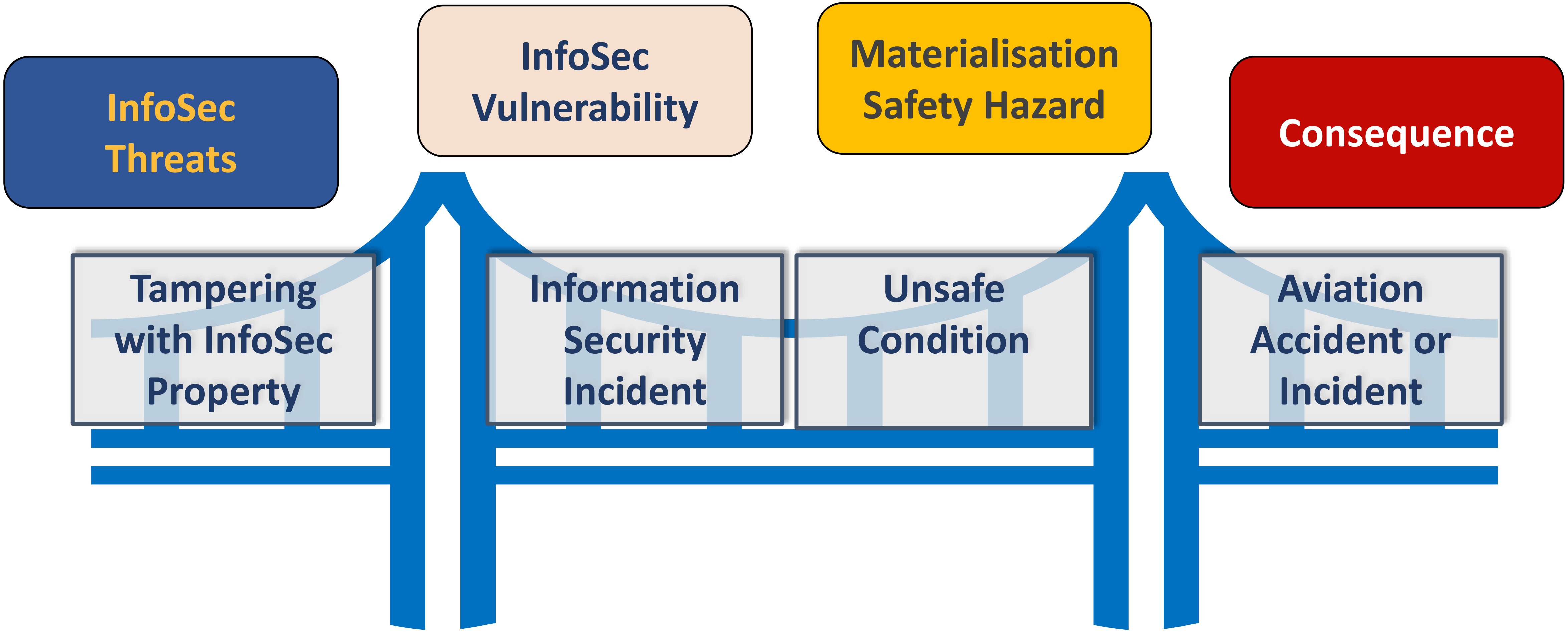
Threat

Breach

Latent vulnerabilities

Safety **vs.** **Security**

Bridging between Information Security and Safety



InfoSec Threats

InfoSec Vulnerability

Materialisation Safety Hazard

Consequence

Tampering with InfoSec Property

Information Security Incident

Unsafe Condition

Aviation Accident or Incident

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

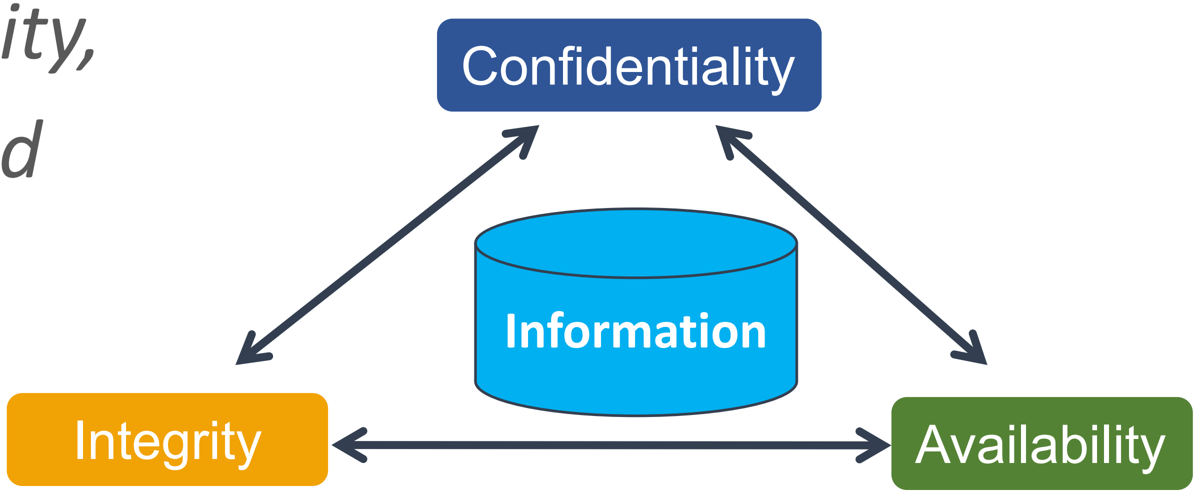
Proportionate to the impact on aviation safety

EASA

What is an ISMS?

What is Information Security Management?

- ISO 27000 states that ***Information Security Management*** *is a top-down, business driven approach to the management of an organization’s physical and electronic information assets in order to preserve their*
  - *Confidentiality,*
  - *Integrity, and*
  - *Availability.*



What is an ISMS?

ISO 27001

An ISMS is the means by which management monitors and controls information security, minimizing the residual **business risk** and ensuring that information security continues to fulfill corporate, customer and legal requirements.

business risk

Part-IS

An ISMS is the means by which management monitors and controls information security, minimizing the residual business **safety risk** and ensuring that information security continues to fulfill ~~corporate, customer and~~ legal requirements and societal expectations.

safety risk

What are the Key Ingredients for Part-IS?

Basic Regulation

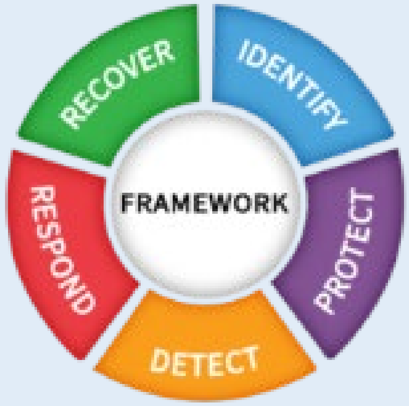
- Acceptable Safety Risks
- Record-keeping
- Personnel Requirements

ISO 2700x

- Information Security Management System (ISMS)
- Information Security Risk Assessment
- Continuous Improvement

NIST Cyber Security Framework

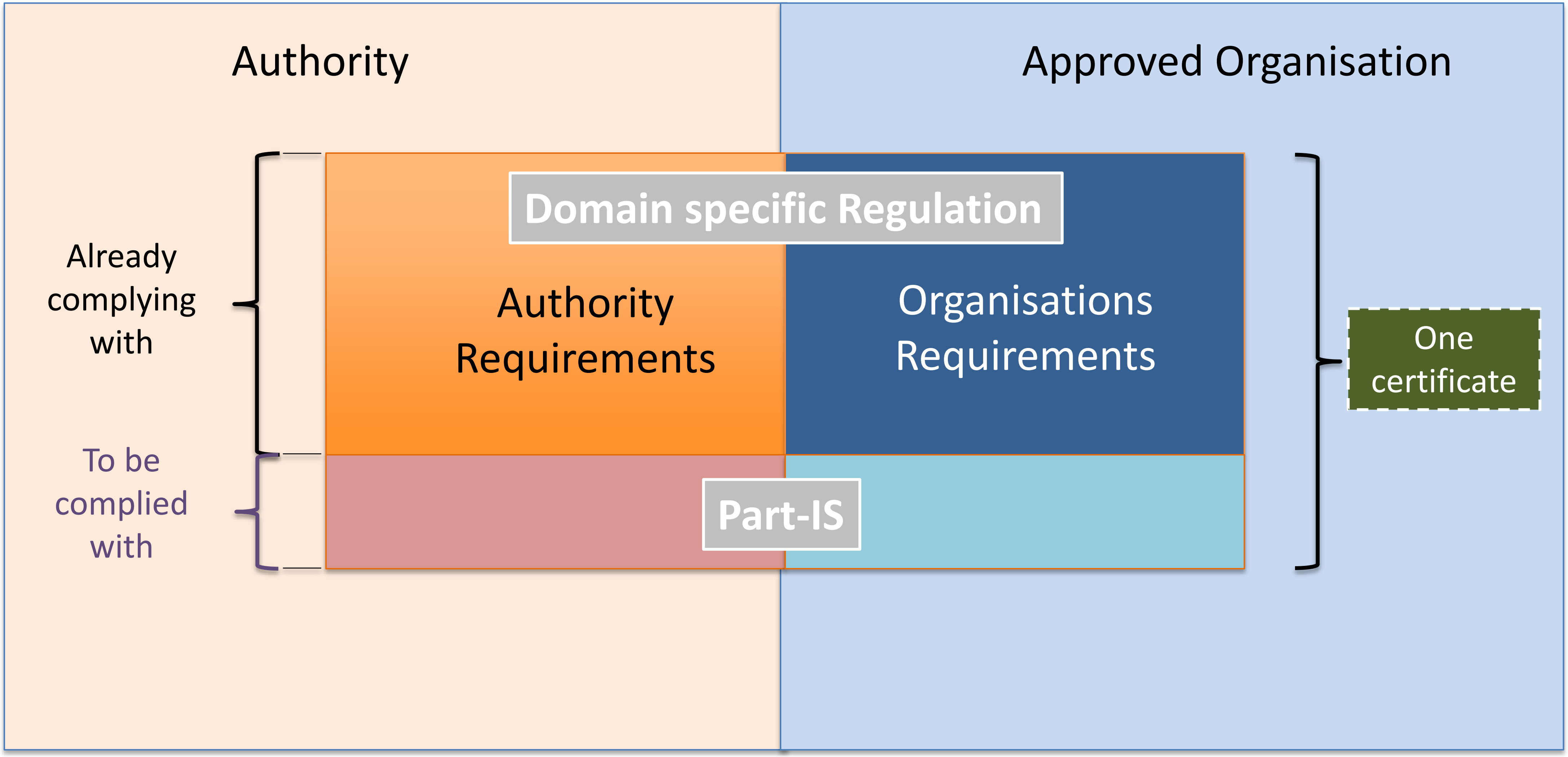
- Information Security Risk Treatment
- Information Security Incidents — Detection, Response, and Recovery



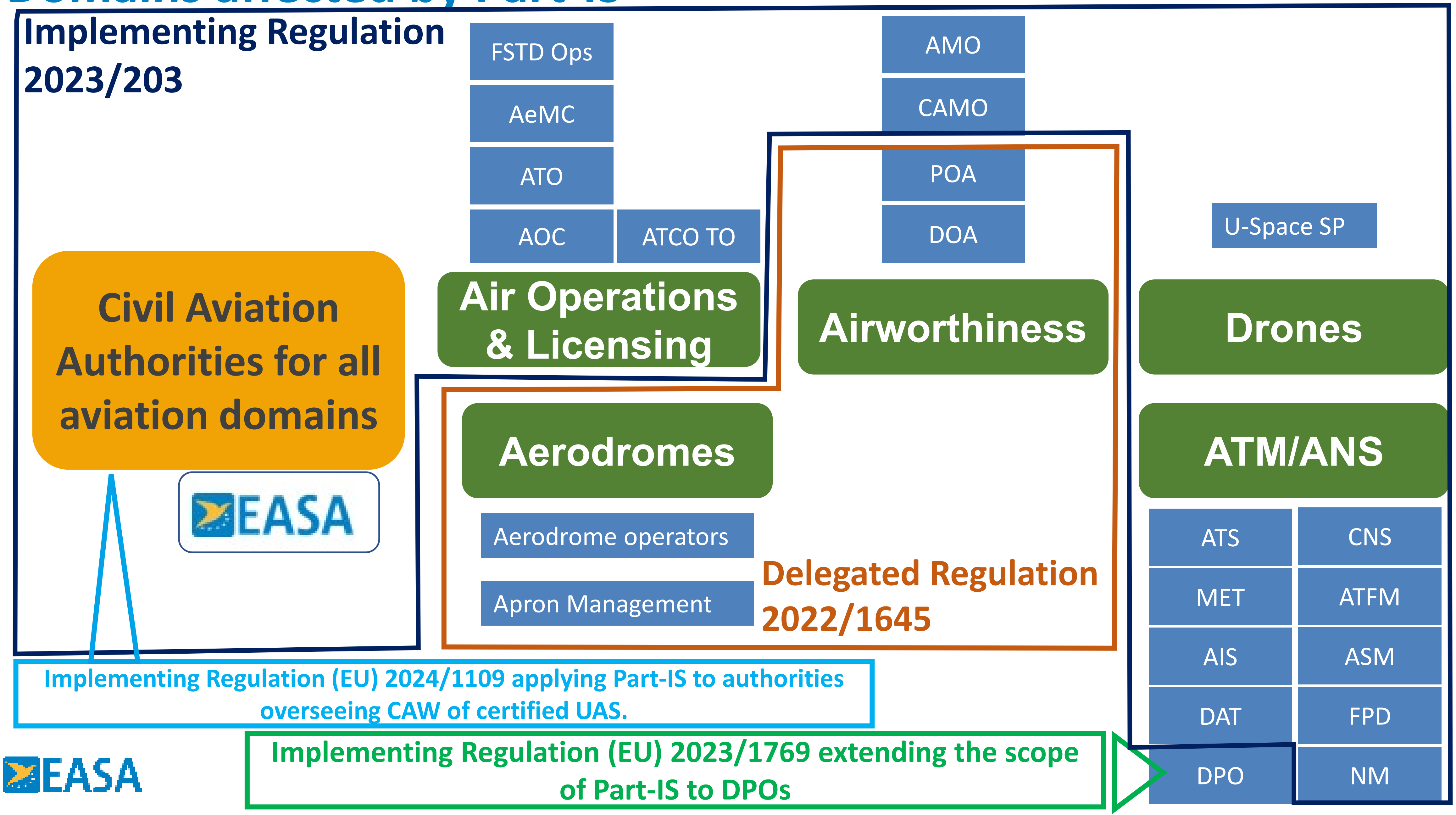
Reporting Regulation

- Information Security External Reporting Scheme

Part-IS and existing approvals/regulations



Domains affected by Part-IS



Implementing Regulation 2023/203

Civil Aviation Authorities for all aviation domains

EASA

FSTD Ops

AeMC

ATO

AOC

ATCO TO

Air Operations & Licensing

AMO

CAMO

POA

DOA

Airworthiness

U-Space SP

Drones

Aerodromes

Aerodrome operators

Apron Management

Delegated Regulation 2022/1645

ATM/ANS

ATS | CNS

MET | ATFM

AIS | ASM

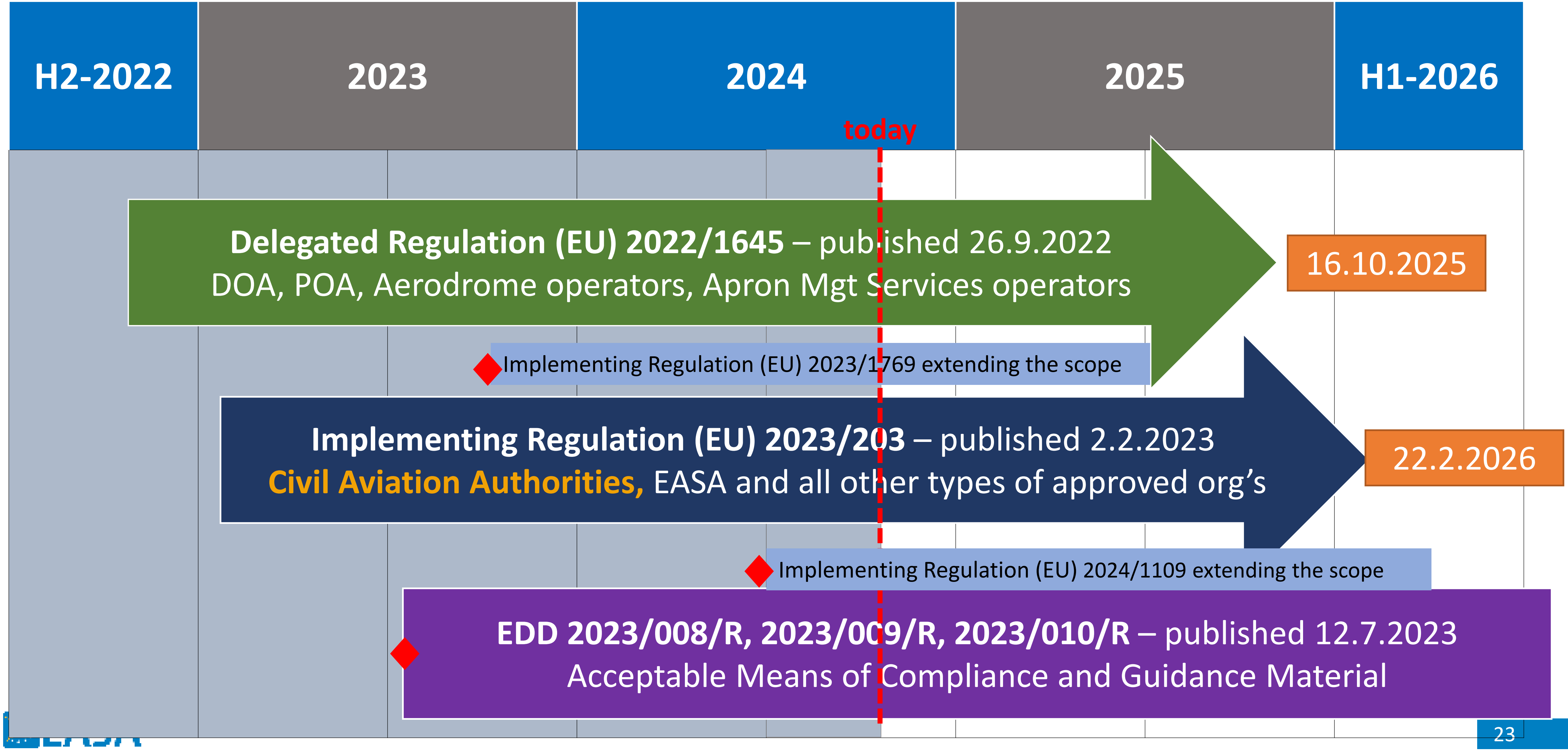
DAT | FPD

DPO | NM

Implementing Regulation (EU) 2024/1109 applying Part-IS to authorities overseeing CAW of certified UAS.

Implementing Regulation (EU) 2023/1769 extending the scope of Part-IS to DPOs

Part-IS implementation journey



H2-2022 | 2023 | 2024 | 2025 | H1-2026

today

Delegated Regulation (EU) 2022/1645 – published 26.9.2022
DOA, POA, Aerodrome operators, Apron Mgt Services operators

16.10.2025

Implementing Regulation (EU) 2023/1769 extending the scope

Implementing Regulation (EU) 2023/203 – published 2.2.2023
Civil Aviation Authorities, EASA and all other types of approved org's

22.2.2026

Implementing Regulation (EU) 2024/1109 extending the scope

EDD 2023/008/R, 2023/009/R, 2023/010/R – published 12.7.2023
Acceptable Means of Compliance and Guidance Material

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

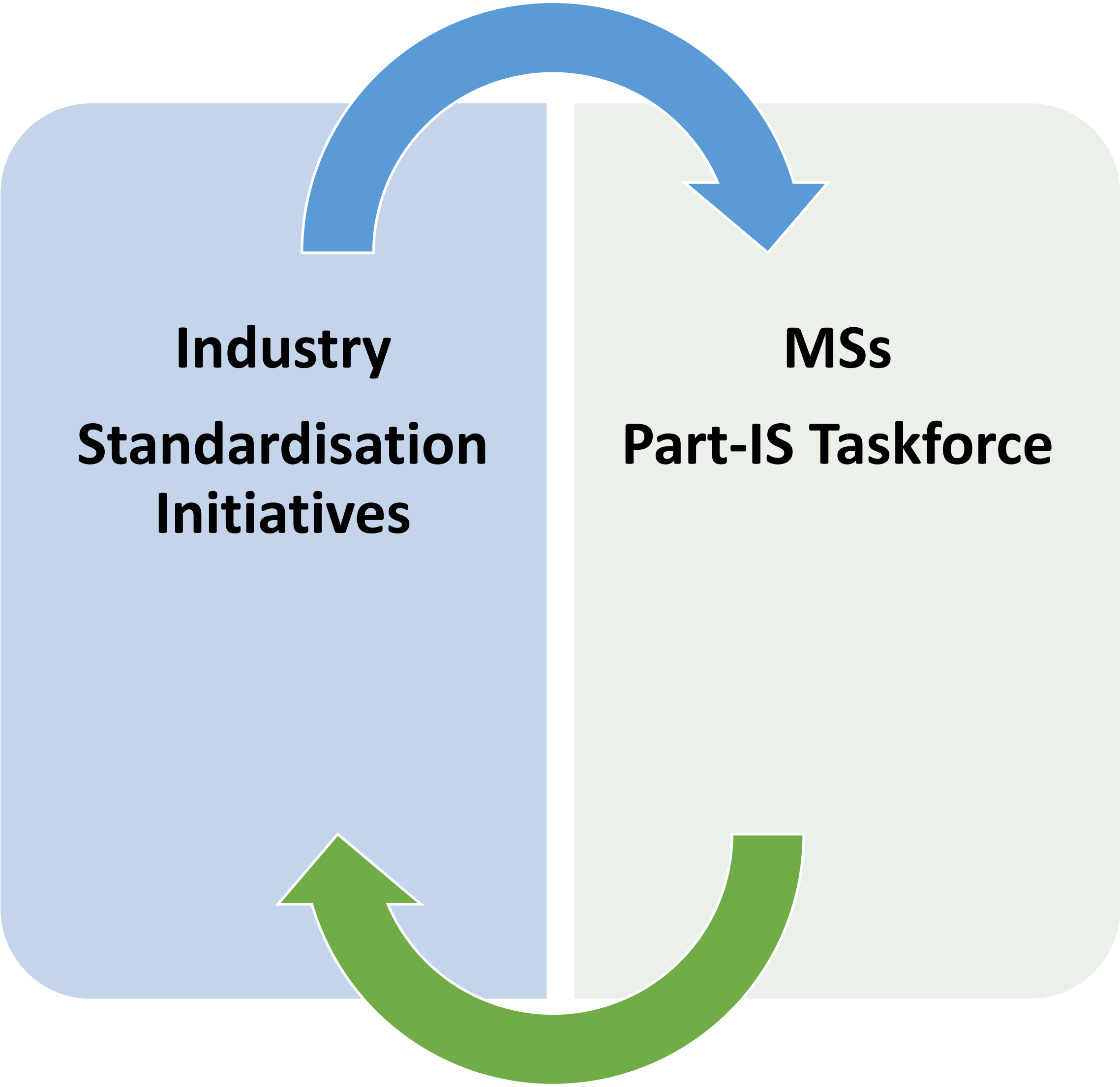
Acceptable Means of Compliance

- To address identified rule’s objectives and processes
- Possible ways to comply with the requirements

Guidance Material

- 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

Other initiatives supporting Part-IS implementation



Industry

Standardisation Initiatives

MSs

Part-IS Taskforce

AMC & GM update before Part-IS applicability

→ New guidance material has been/is being developed since the publication of AMC & GM

→ Some examples:

From the TF

- Part-IS compliance guideline for ISO/IEC 27001 certified organisations
- Assessment of requests for derogation

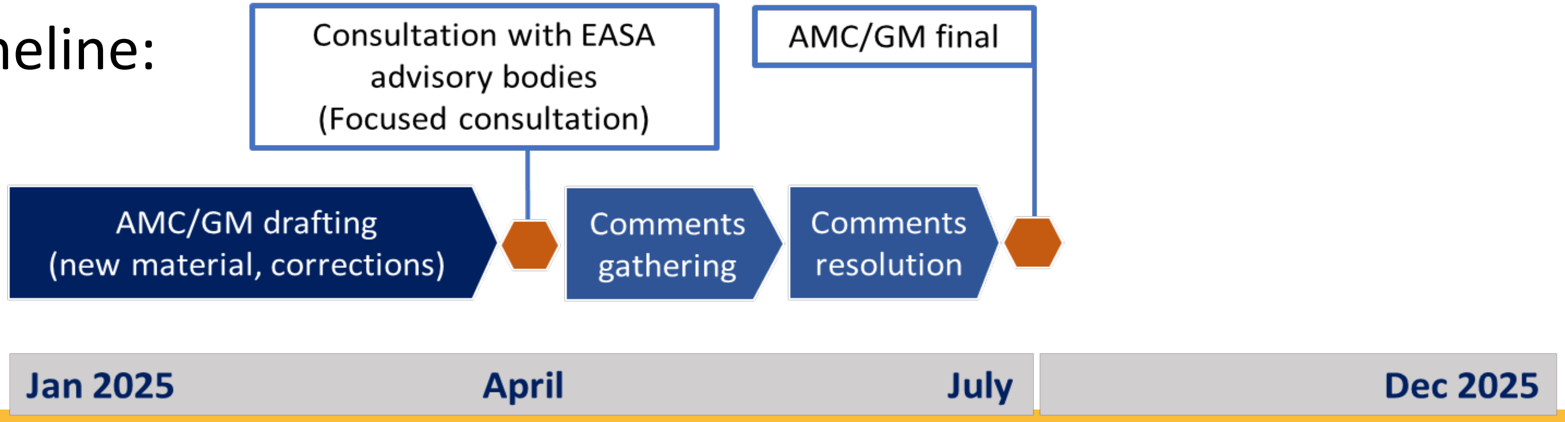
From EASA

- Adaptation of ENISA ECSF to Part-IS and the aviation domain

From Eurocae

- Updated ED-206 -> ED-206A
- ED-ISMS (maybe more likely in Q1 2025)

Tentative timeline:



Consultation with EASA advisory bodies (Focused consultation)

AMC/GM final

AMC/GM drafting (new material, corrections)

Comments gathering

Comments resolution

Jan 2025

April

July

Dec 2025

Introduction to Part-IS and Organisational Impact

Part-IS Implementation

Workshop

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		
IS.I.OR.220	Information security incidents — detection, response, and recovery	IS.AR.215
IS.I.OR.225		
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		
IS.I.OR.255		
IS.I.OR.260	Continuous improvement	IS.AR.235

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

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-specific regulations 2/2

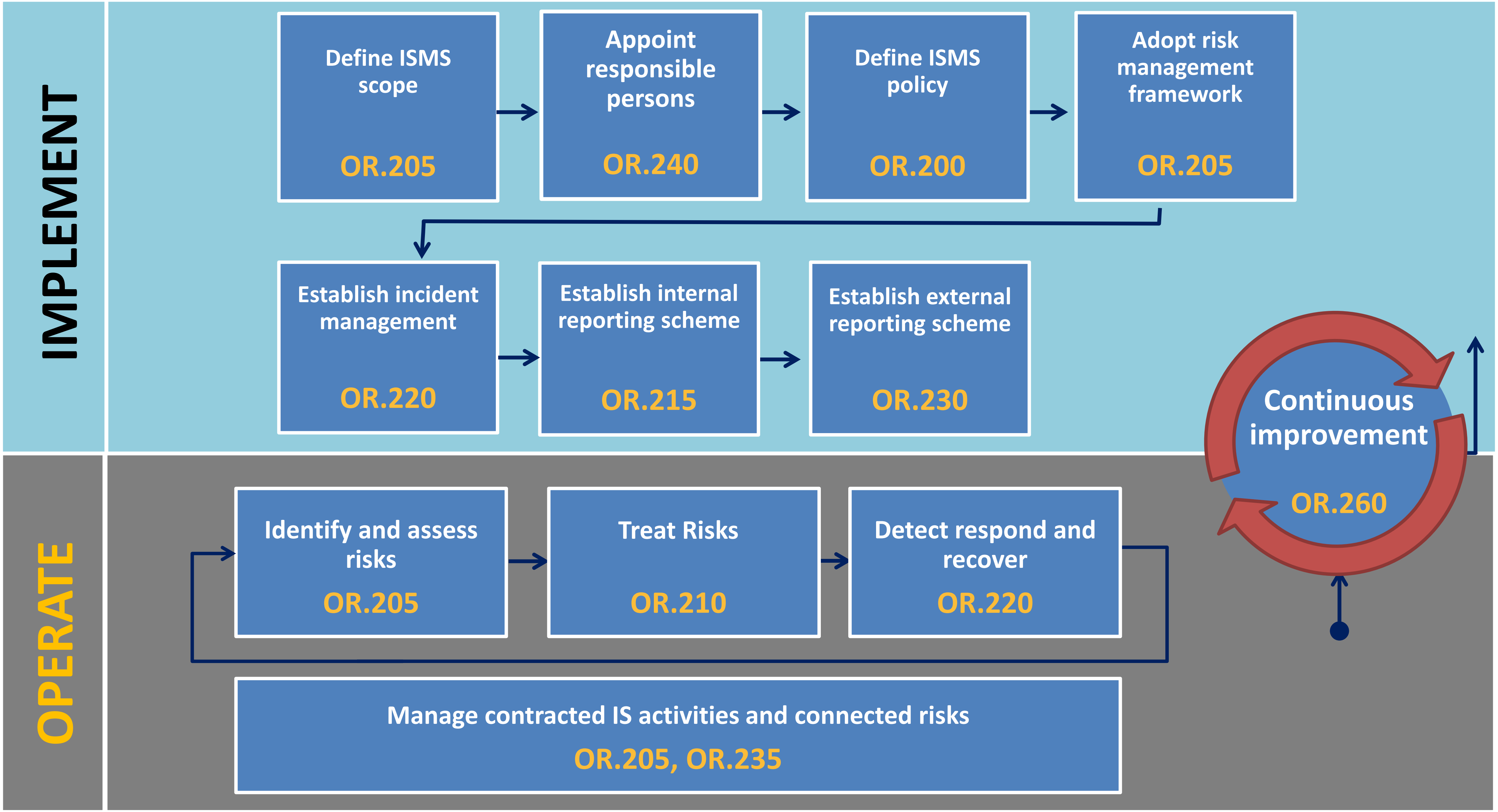
Part Area	Reg. 1178 ORA	Reg. 748 21	Reg. 965 ORO	Reg. 139 ADR	Reg. 340 ATCO	Reg. 373 ATM/ANS	Reg. 1321 CAMO	Reg. 1321 145
Hook to ISMS	.GEN.200A	.A.139A .A.239A	.GEN.200A	.OR.D.005A .OR.D.007 .OR.F.045A	.OR.C.001A	.OR.B.005A .OR.D.010	.A.200A	.A.200A

Part Area	Reg. 1178 ARA	Reg. 748 21	Reg. 965 ARO	Reg. 139 ADR	Reg. 340 ATCO	Reg. 373 ATM/ANS	Reg. 1321 CAMO	Reg. 1321 145	Reg. 1321 66
Hook to ISMS	.GEN.200	.B.25	.GEN.200	.AR.B.005	.AR.B.001	.AR.B.001	.B.200	.B.200	.B.15
Imm. React. to 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 .AR.C.040A	.AR.C.001 .AR.E.010A	.AR.C.010 .AR.C.025A	.B.300 .B.330A	.B.300 .B.330A	**N/A**
Allocation of tasks	.GEN.205	.B.30	.GEN.205	.AR.B.010	.AR.B.005	.AR.B.005	.B.205	.B.205	**N/A**

Provisions introduced in new domain-specific regulations (2023/1769 and 2024/1109)

Part Area	Reg. 1769 **DPO**
Hook to ISMS	.OR.B.001

Part Area	Reg. 1769 **DPO**	Reg. 1109 **AR.UAS**
Hook to ISMS	.AR.B.001	.GEN.200
Immediate reaction to IS Reports	.AR.A.015	.GEN.125 .GEN.135A
Oversight	.AR.C.010	**N/A**
Allocation of tasks	**N/A**	.GEN.205



IMPLEMENT

Define ISMS scope
OR.205

Appoint responsible persons
OR.240

Define ISMS policy
OR.200

Adopt risk management framework
OR.205

Establish incident management
OR.220

Establish internal reporting scheme
OR.215

Establish external reporting scheme
OR.230

Continuous improvement
OR.260

OPERATE

Identify and assess risks
OR.205

Treat Risks
OR.210

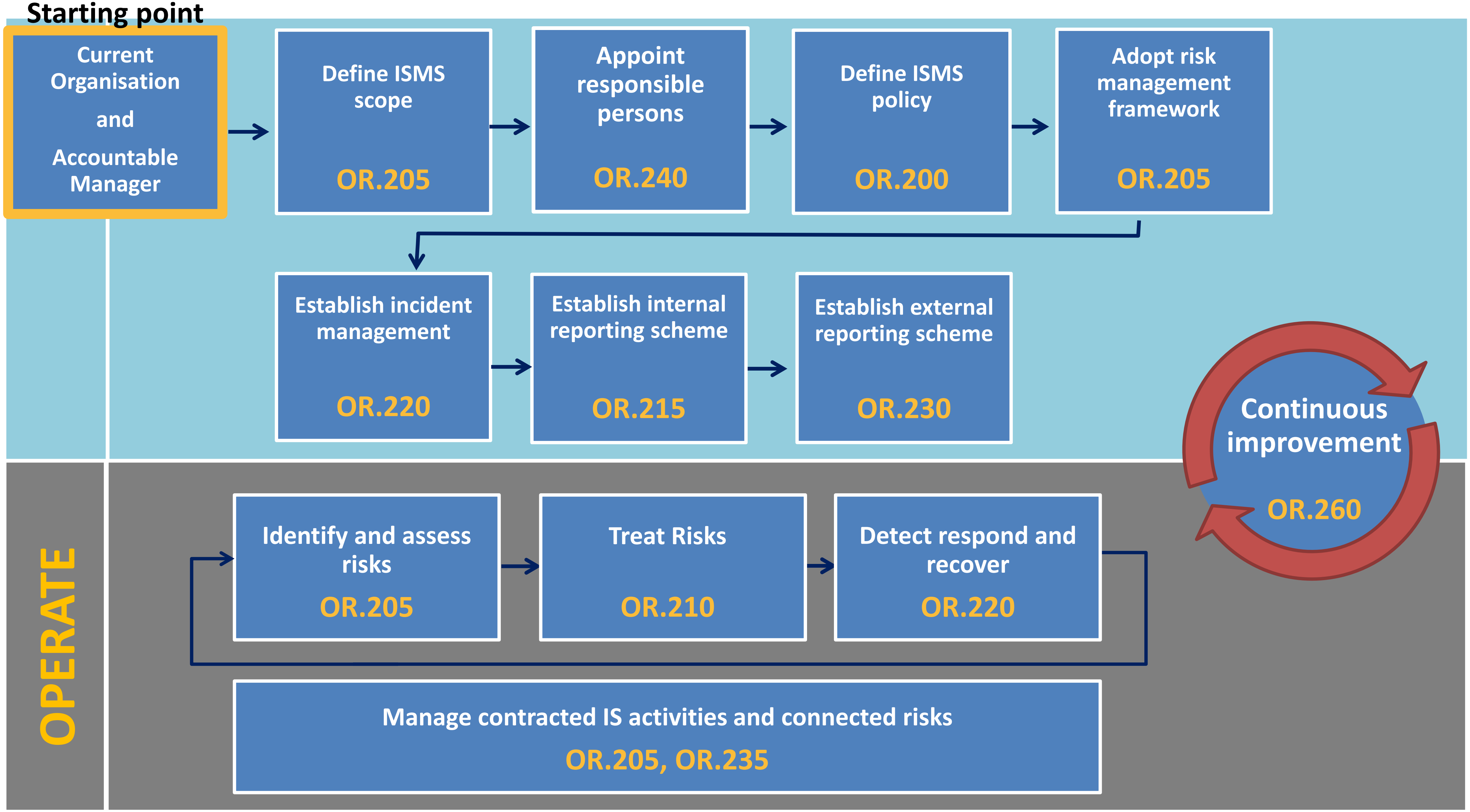
Detect respond and recover
OR.220

Manage contracted IS activities and connected risks
OR.205, OR.235

Organisational Impact

Part-IS Implementation

Workshop



Starting point

Current Organisation and Accountable Manager

Define ISMS scope OR.205

Appoint responsible persons OR.240

Define ISMS policy OR.200

Adopt risk management framework OR.205

Establish incident management OR.220

Establish internal reporting scheme OR.215

Establish external reporting scheme OR.230

Continuous improvement OR.260

OPERATE

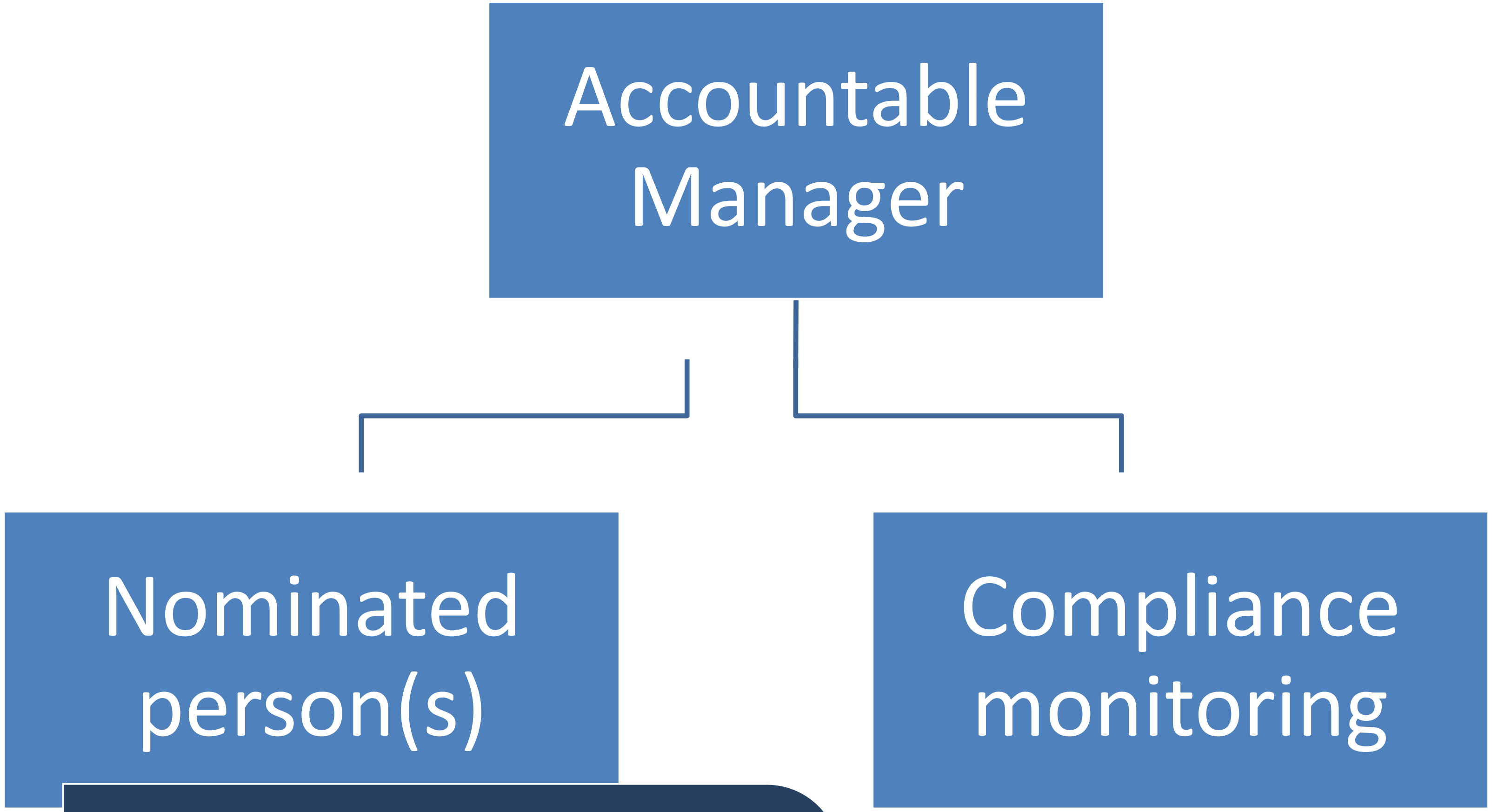
Identify and assess risks OR.205

Treat Risks OR.210

Detect respond and recover OR.220

Manage contracted IS activities and connected risks OR.205, OR.235

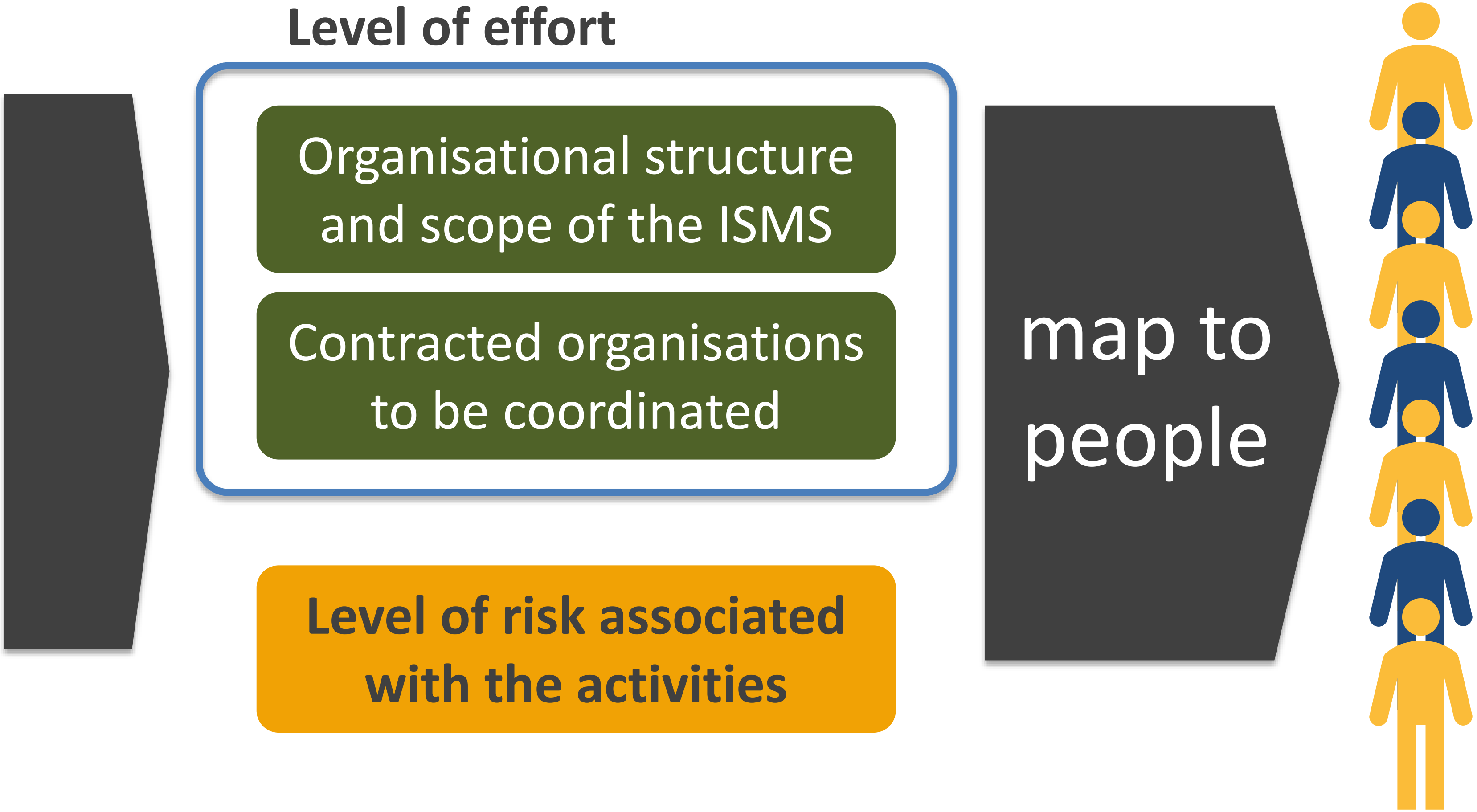
Organisational structure



How to make this delegation of responsibility effective?

Determination of sufficiency

Part-IS tasks*
Task 1
Task 2
Task 3
Task 4
Task ….



Level of effort

Organisational structure and scope of the ISMS

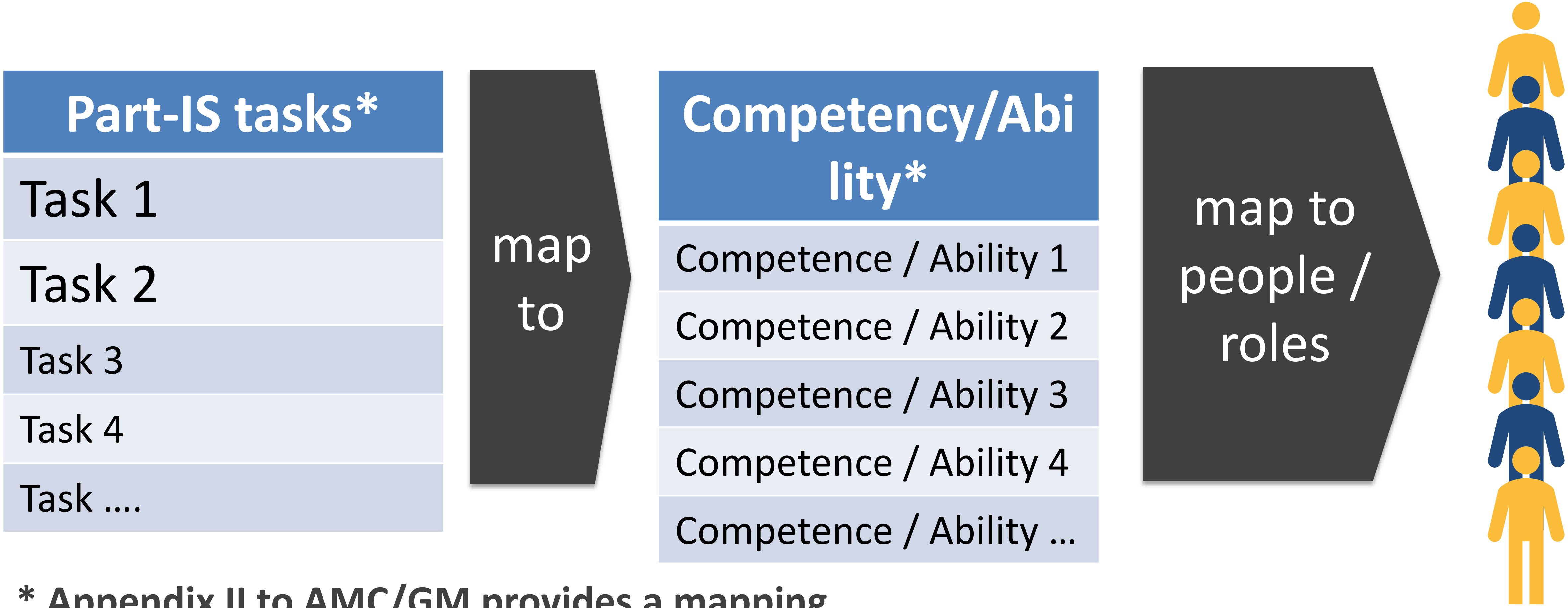
Contracted organisations to be coordinated

Level of risk associated with the activities

map to people

* Appendix II to AMC/GM of Part-IS

Personnel Competence



Part-IS tasks*
Task 1
Task 2
Task 3
Task 4
Task ….

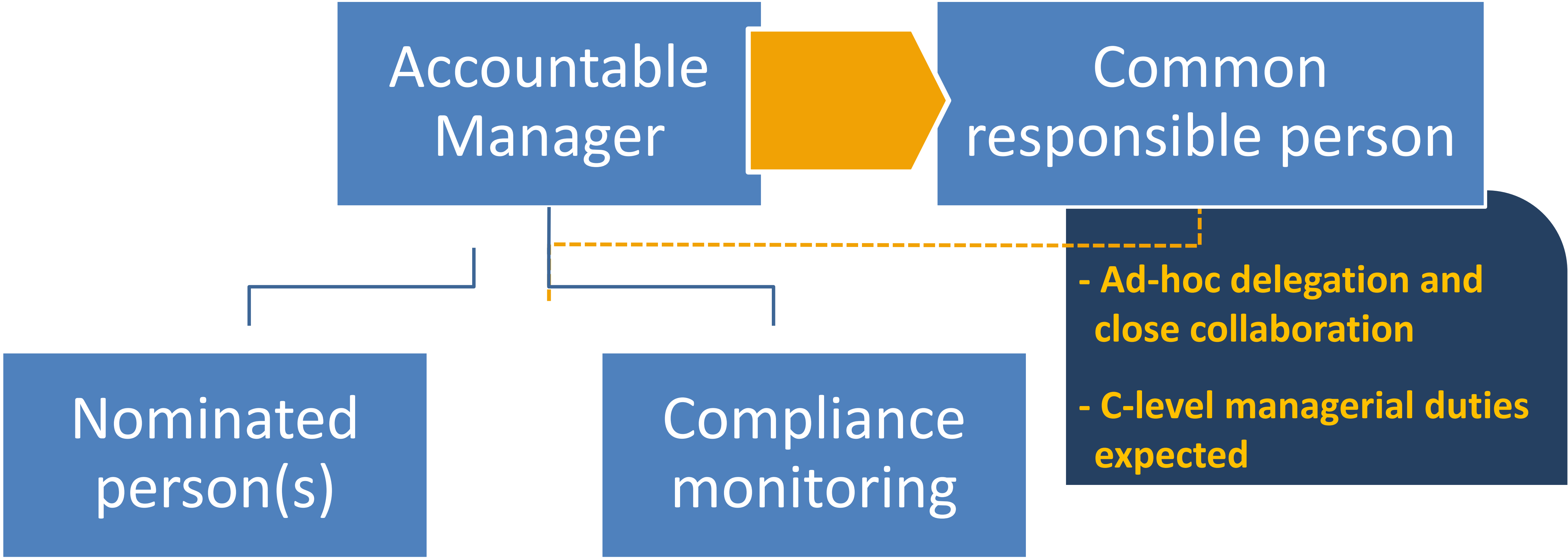
map to

Competency/Ability*
Competence / Ability 1
Competence / Ability 2
Competence / Ability 3
Competence / Ability 4
Competence / Ability …

map to people / roles

*** Appendix II to AMC/GM provides a mapping between Part-IS Tasks and NICE CSF v1.1**

Organisational structure



Accountable Manager

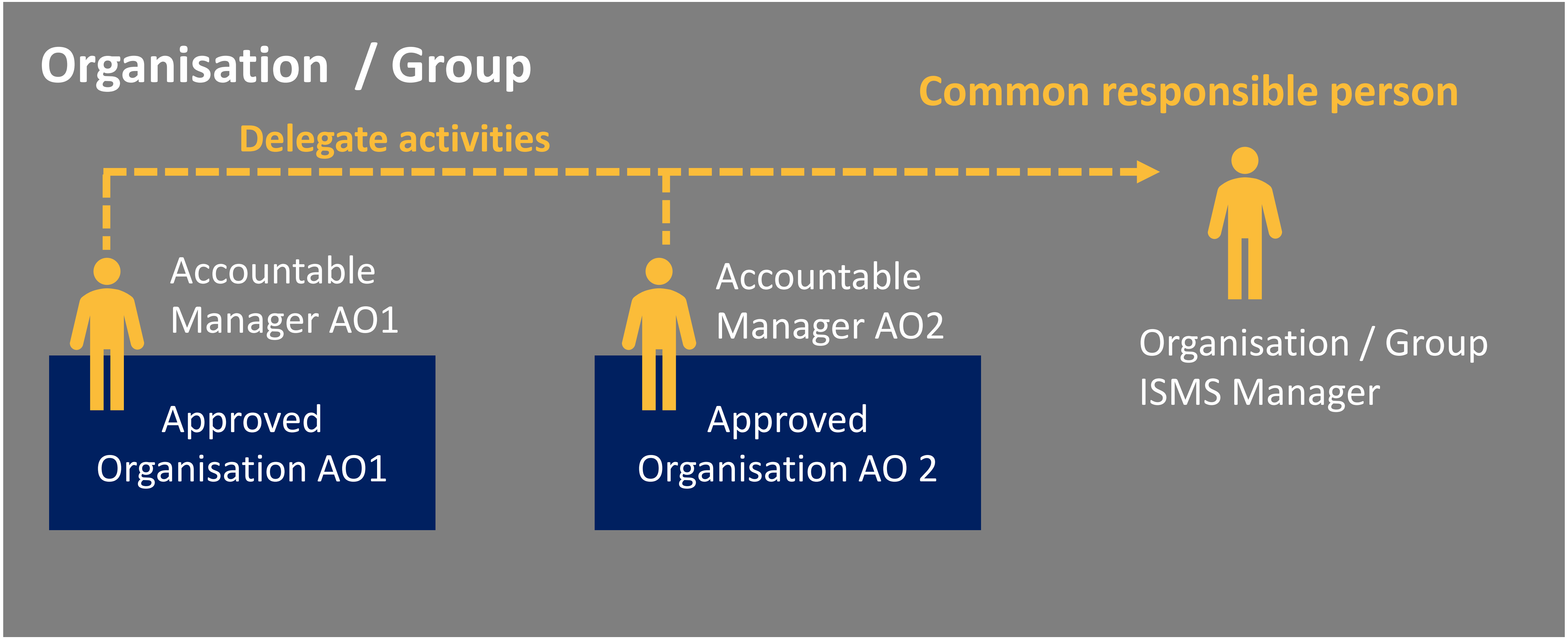
Common responsible person

Nominated person(s)

Compliance monitoring

- Ad-hoc delegation and close collaboration
- C-level managerial duties expected

Common responsible person



Organisation / Group

Common responsible person

Delegate activities

Accountable Manager AO1

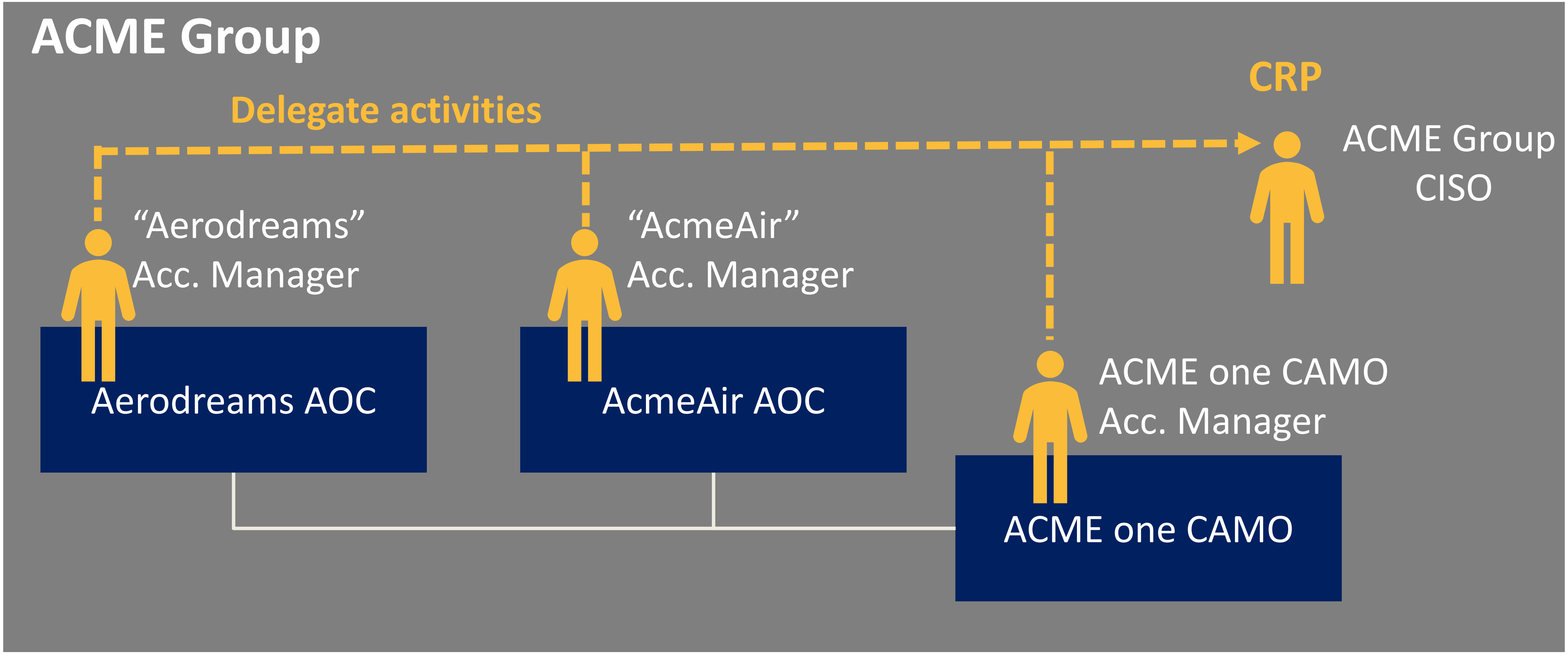
Approved Organisation AO1

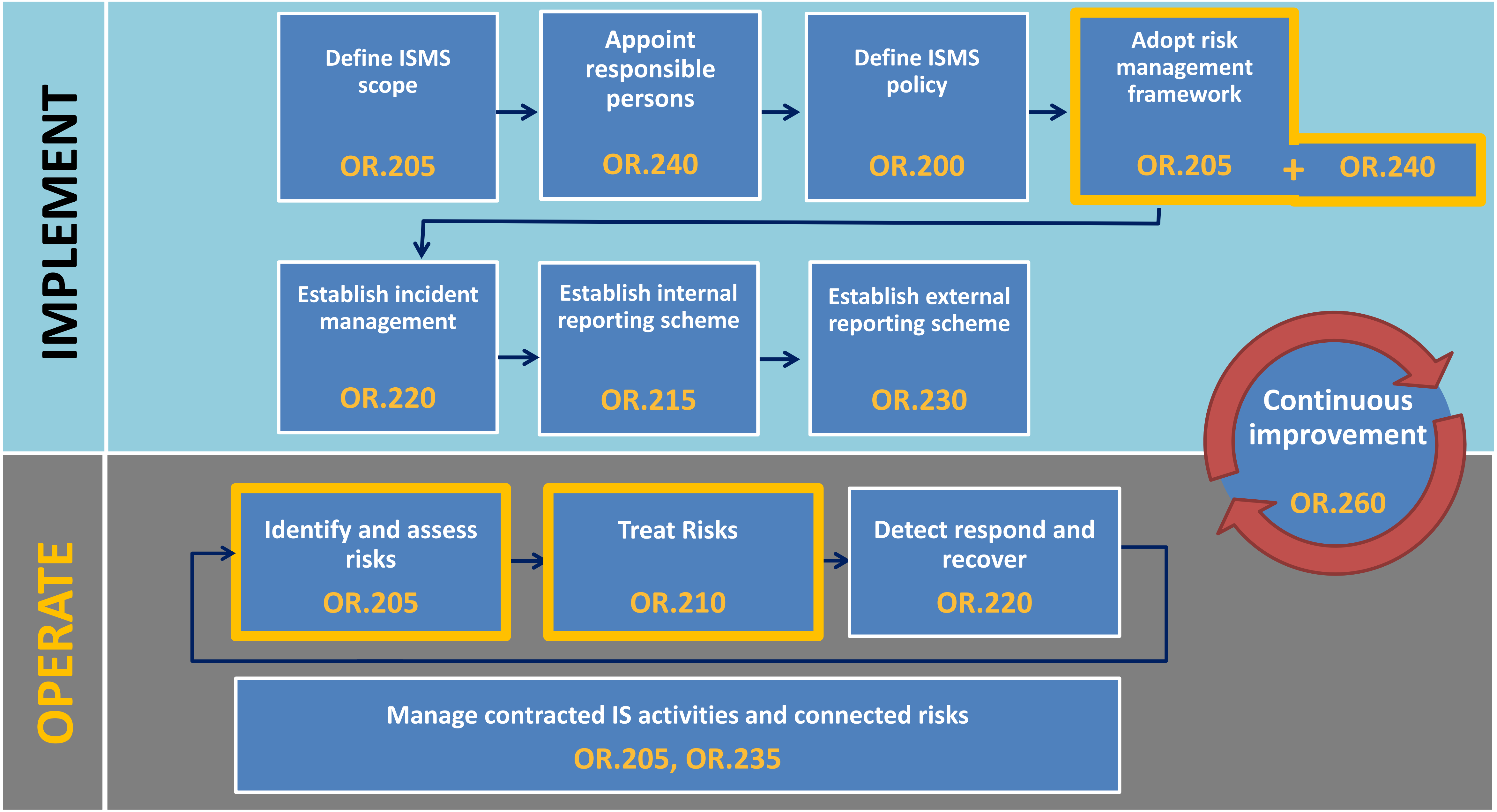
Accountable Manager AO2

Approved Organisation AO 2

Organisation / Group ISMS Manager

Example – Group controlling multiple AOs





IMPLEMENT

Define ISMS scope
OR.205

Appoint responsible persons
OR.240

Define ISMS policy
OR.200

Adopt risk management framework
OR.205 + OR.240

Establish incident management
OR.220

Establish internal reporting scheme
OR.215

Establish external reporting scheme
OR.230

Continuous improvement
OR.260

OPERATE

Identify and assess risks
OR.205

Treat Risks
OR.210

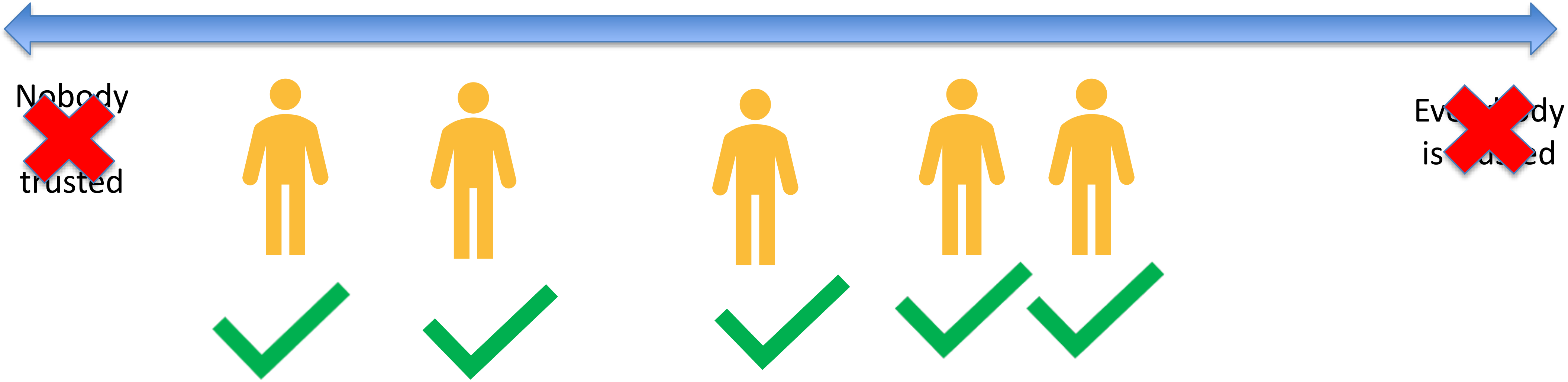
Detect respond and recover
OR.220

Manage contracted IS activities and connected risks
OR.205, OR.235

Trustworthiness

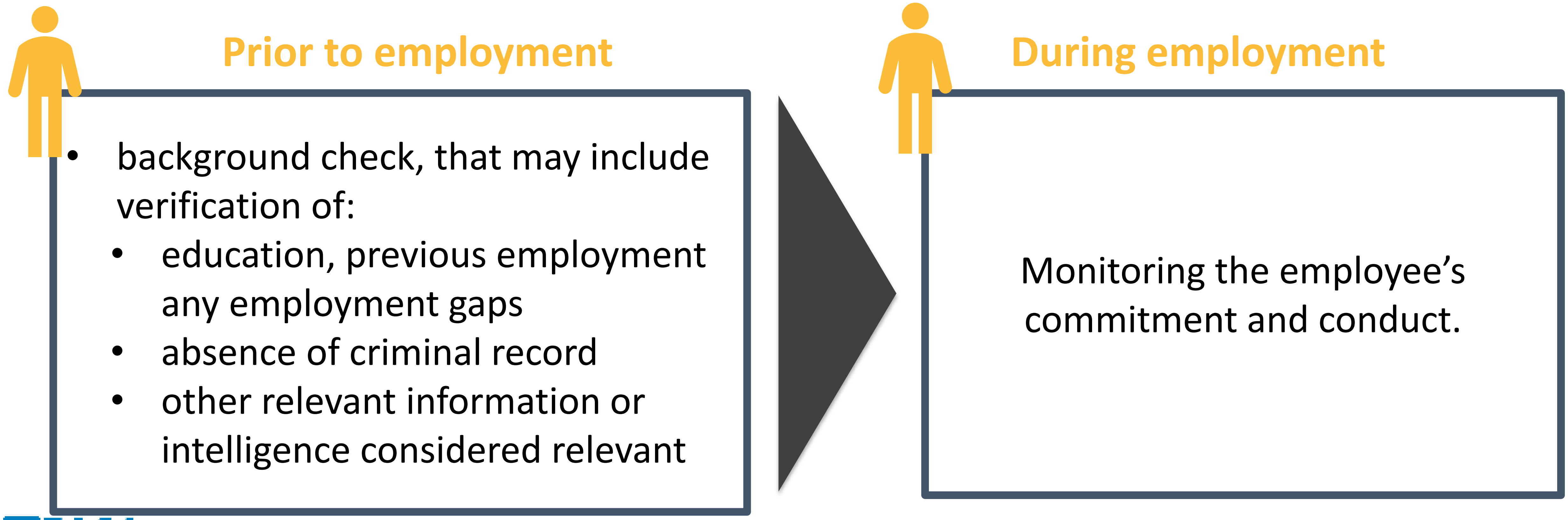
Level of trustworthiness should match the role:

- Extremes such as "everyone is trusted" or "nobody is trusted" should be avoided.



Trustworthiness

Trustworthiness criteria/procedures can be used to justify risk assessment assumptions.



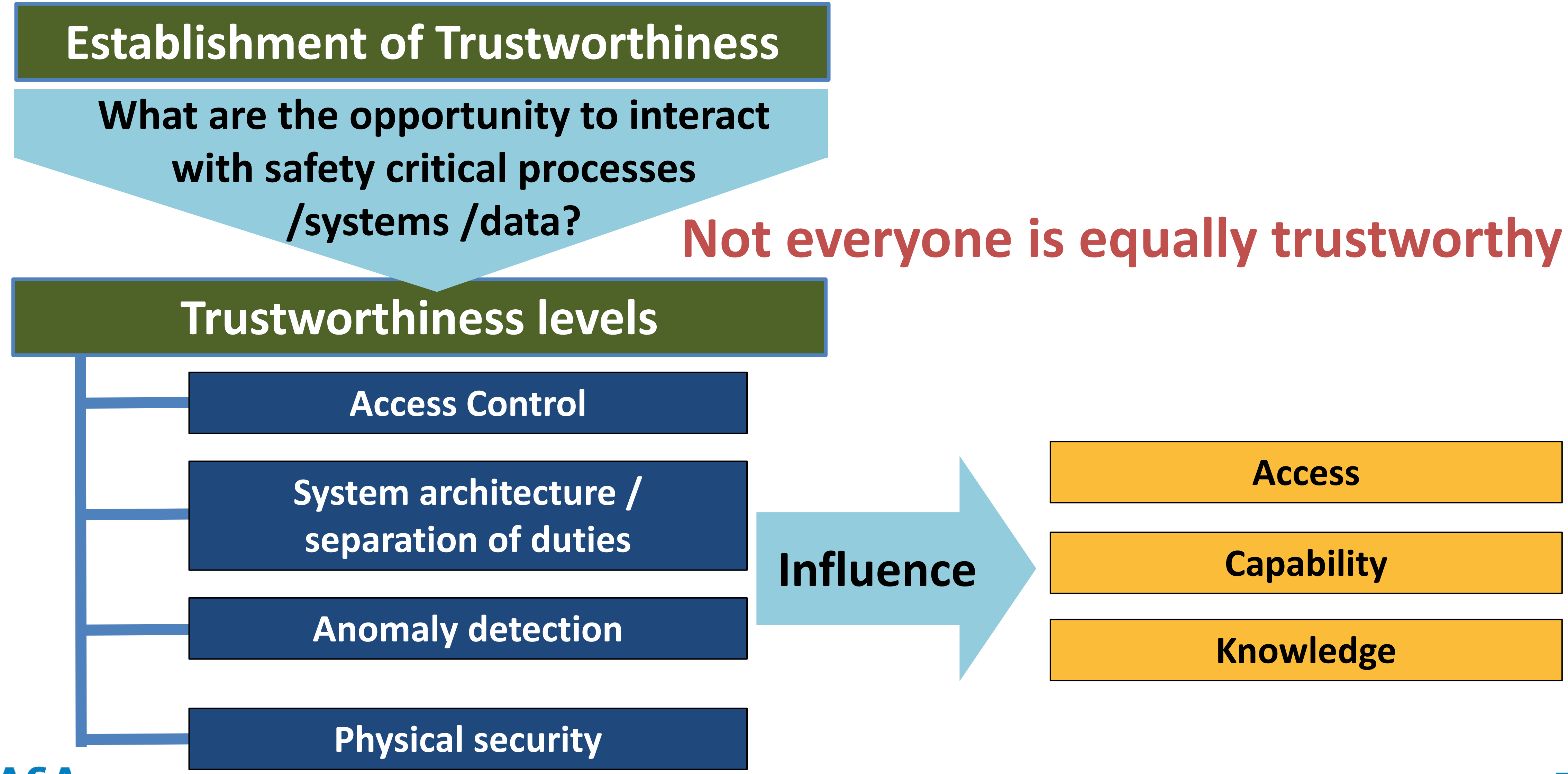
Prior to employment

- background check, that may include verification of:
  - education, previous employment any employment gaps
  - absence of criminal record
  - other relevant information or intelligence considered relevant

During employment

Monitoring the employee’s commitment and conduct.

Trustworthiness



Establishment of Trustworthiness

What are the opportunity to interact with safety critical processes /systems /data?

Not everyone is equally trustworthy

Trustworthiness levels

- Access Control
- System architecture / separation of duties
- Anomaly detection
- Physical security

Influence

- Access
- Capability
- Knowledge

Coffee break – *15 minutes*

Join us in the Main Foyer

Part-IS Implementation

Workshop

Panel 1 - Part-IS early implementers’ feedbacks

Part-IS Implementation

Workshop

EASA

Gian Andrea Bandieri is responsible, since November 2021, for the EASA team dealing with Cybersecurity in Aviation, which includes rulemaking, information sharing, threats identification, capacity building and research. In addition, Security and Conflict Zones are also under his responsibility.

He holds a Master degree in Aeronautical Engineering from Politecnico di Torino and a Master in Aviation Law from the University of Modena.

Arnold Hoessler joined the senior leadership team of Cyber Security and IT Management at Lufthansa Group in May 2024 and is responsible for the Information Security Management System and Cyber Assurance and Standards.

With an engineering and business management background, he has served the Lufthansa Group

companies for 25+ years in various leadership roles in technical fleet management, quality and

operations.

Part IS - we make cyber fly

Information Security

Aviation Safety

+ MRO & Services

- ✓ One LHG ISMS 27k1
- ✓ > 1,8m IT assets
- ⚡ Threats on rise

- 46 organizations 6 authorities
- > 800 aircraft
- Safety for 130m pax

! **Focus on initial compliance** by Feb 2026

! **Leverage robust standards** i.e. ISO27k1

! **Guidance for Supply Chain** & OEM support

! **PanEU authority standards** for implementation

Team wins – we are 130k cyber defenders

LUFTHANSA GROUP
Cyber Security

Jarno Ruotsalainen is Head of Operations Support at Nordic Regional Airlines, where he leads a multidisciplinary team of experts in various areas of operations and business support. He also acts as Head of IT and is responsible for IT services and solutions, including cyber security.

With almost 12 years of experience in airline operations and especially operational engineering, Jarno has a broad and an engineering-like approach and view of airline operations in a whole.

NORRA
Outstanding Aviation

Part-IS Implementation Project

Jarno Ruotsalainen
Head of Operations Support
Nordic Regional Airlines (Norra)

Introduction and starting point

- Regional operator based in Finland
  - Strategic partner of Finnair
  - Over 50 000 flights per year
  - Appr. 720 employees

- Safety Management System (SMS)
  - Maturity level good
  - Risk assessment processes in place
  - Good reporting culture
  - Continuous improvement

- Information security
  - Commonly known best practices mostly in use
    - Technical solutions and processes
  - High level of automation and digitalization
  - Not integrated into SMS
  - No dedicated Information Security Management Manual (ISMM)

Project so far

1. Inventory and mapping
   - Technical solutions
   - Processes
   - Resources
2. Identification of systems and information
   - Impact on flight safety
   - Classification of criticality -> priorisation
   - Risk assessments
3. Scoping of ISMS
   - Part-IS + other legislation
   - Required new processes, resources, training
4. Integration of ISMS into the SMS
5. Documentation required
   - ISMM
6. New technical solutions will be implemented, e.g. for asset and service management
   - Maximum use of automation

NORRA

Outstanding Aviation

Tomi Salmenpää is a Chief Adviser in Aviation Cybersecurity to Traficom, Civil Aviation Authority (CAA) Finland. In his current role he focuses on the implementation of information security to the civil aviation system. Tomi contributes actively to the international co-operation developing policies, - best practices and holistic information security to aviation.

He has nearly 20 years' experience in aviation security and cyber security, gained in the aviation industry and at the CAA.

TRAFICOM

Liikenne- ja viestintävirasto

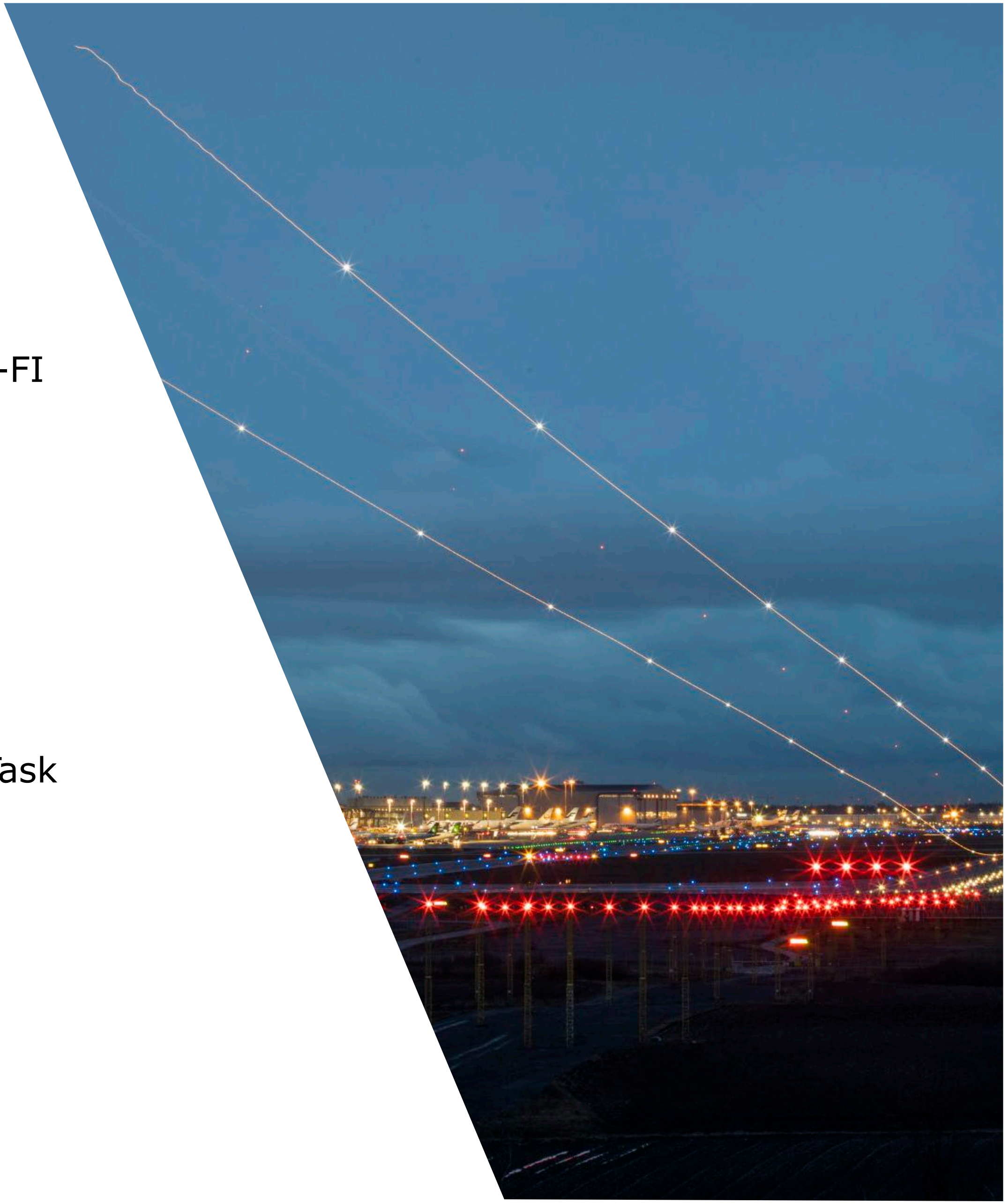
Part-IS Early Implementers’ Experiences

7.11.2024

Tomi Salmenpää

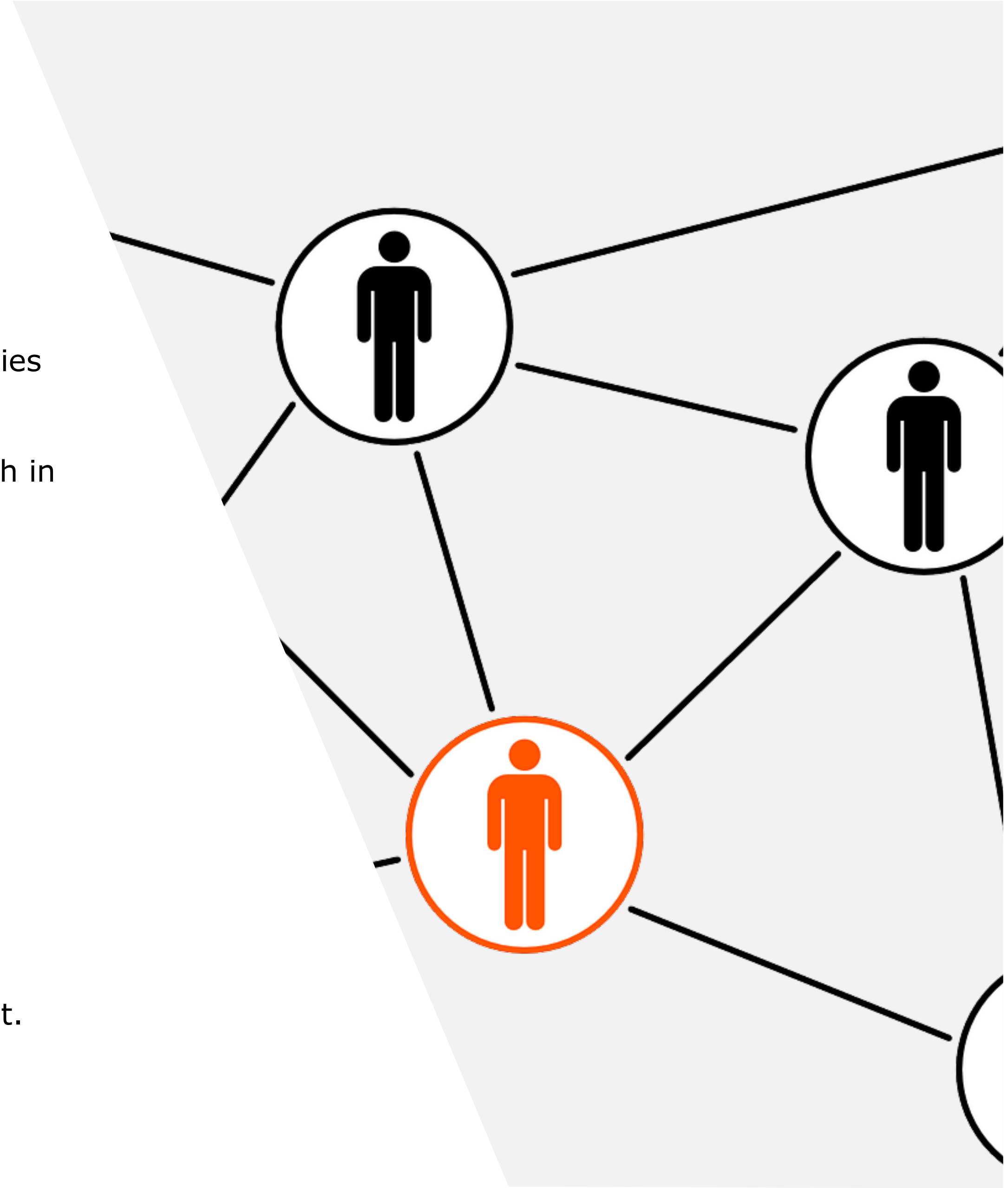
Part-IS early implementers’, Key Experiences, CAA Finland

- Traficom: All transport modes, communications agency and NCSC-FI
- Part-IS roles (also NIS2 and avsec)
  - Service provider: CAA for all aviation domains (Certificates, oversight and approvals)
  - Oversight
- History with Part-IS
  - Drafting of Part-IS and AM&GM, now in Part-IS implementing Task Force
  - Until early 2024, found appropriate approach to Traficom



Part-IS early implementers', Key Experiences, CAA Finland

- Integration of Part-IS into existing aviation governance (roles & responsibilities remains in as they are)
- Interconnect (collide) aviation safety and information security functions, both in organisations AND authorities
  - Not all aviation domains are similar
    - Culture (People, processes, ways of work, knowledge..)
    - Safety risks
    - Objective: Appropriate Part-IS implementation
  - Risk management
    - Ensure efficient risk management (avoid complexity)
    - Focus in crown jewels
- Theory and practise goes hand in hand. Theorizing perfect solution is difficult. Take the first step, evaluate & direct, take the second step..



Alain Combes is a product security expert in Airbus Commercial and leads the Part-IS ISMS implementation and operation for the Design Organisation Approval scope. He also chairs the ASD Europe Civil Aviation Cybersecurity Committee and the EUROCAE “Aeronautical Systems Security” WG-72 Subgroup responsible for ED-206 (Security Event Management Guidance document) and ED-204 (Information Security Guidance for Continuing Airworthiness).

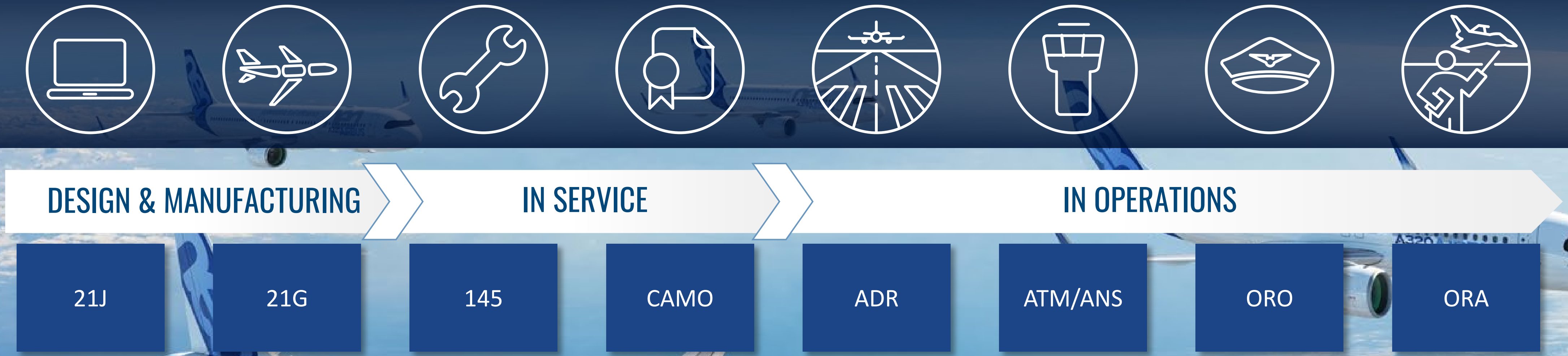
He holds a master’s degree in information processing technologies.

Airbus – Part-IS early implementers' feedback

Alain Combes, Airbus Commercial DOA ISMS Officer

November 2024

Part-IS Applicability in Airbus Commercial



DESIGN & MANUFACTURING

IN SERVICE

IN OPERATIONS

21J	21G	145	CAMO	ADR	ATM/ANS	ORO	ORA

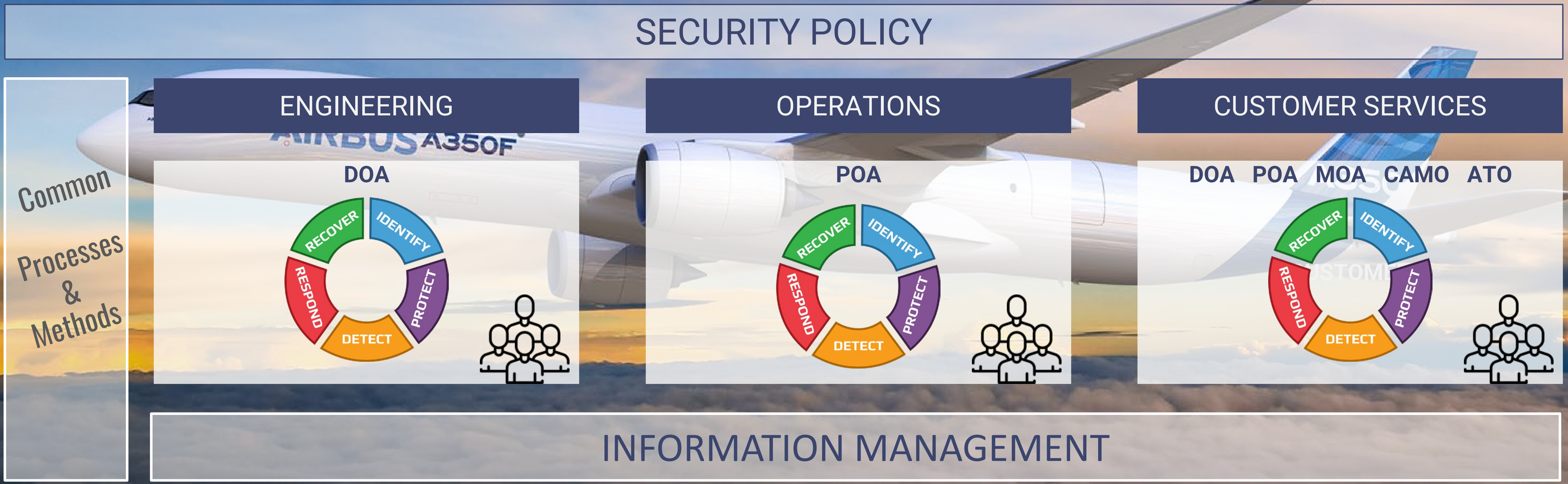
Part-IS: Federated ISMS Instances

(Airbus Commercial example)

ISMS Officer

Local ISMS Officers

Security Representatives



SECURITY POLICY

Common Processes & Methods

ENGINEERING

DOA

OPERATIONS

POA

CUSTOMER SERVICES

DOA POA MOA CAMO ATO

INFORMATION MANAGEMENT

Q&A – 30 minutes

Part-IS Implementation

Workshop

EASA

Davide Martini has been a Senior Cybersecurity Expert at EASA since 2016. He leads efforts in developing aviation cybersecurity regulations and the implementation of the European cybersecurity strategy for aviation. Previously, he spent over 15 years in the aviation industry.

He holds a Master degree in Aerospace Engineering from Politecnico di Milano.

Christophe Soriano is currently leading an Airbus project securing the Part-IS compliance of the DOA, POA, MOA, CAMO and ATO activities of Customer Services.

He holds a degree in Computer Science Engineering and has worked in the industrial software industry for 13 years in various business areas, including automotive and aerospace, from developer to project manager, gaining extensive experience ranging from security assurance for embedded software to building product security management systems.

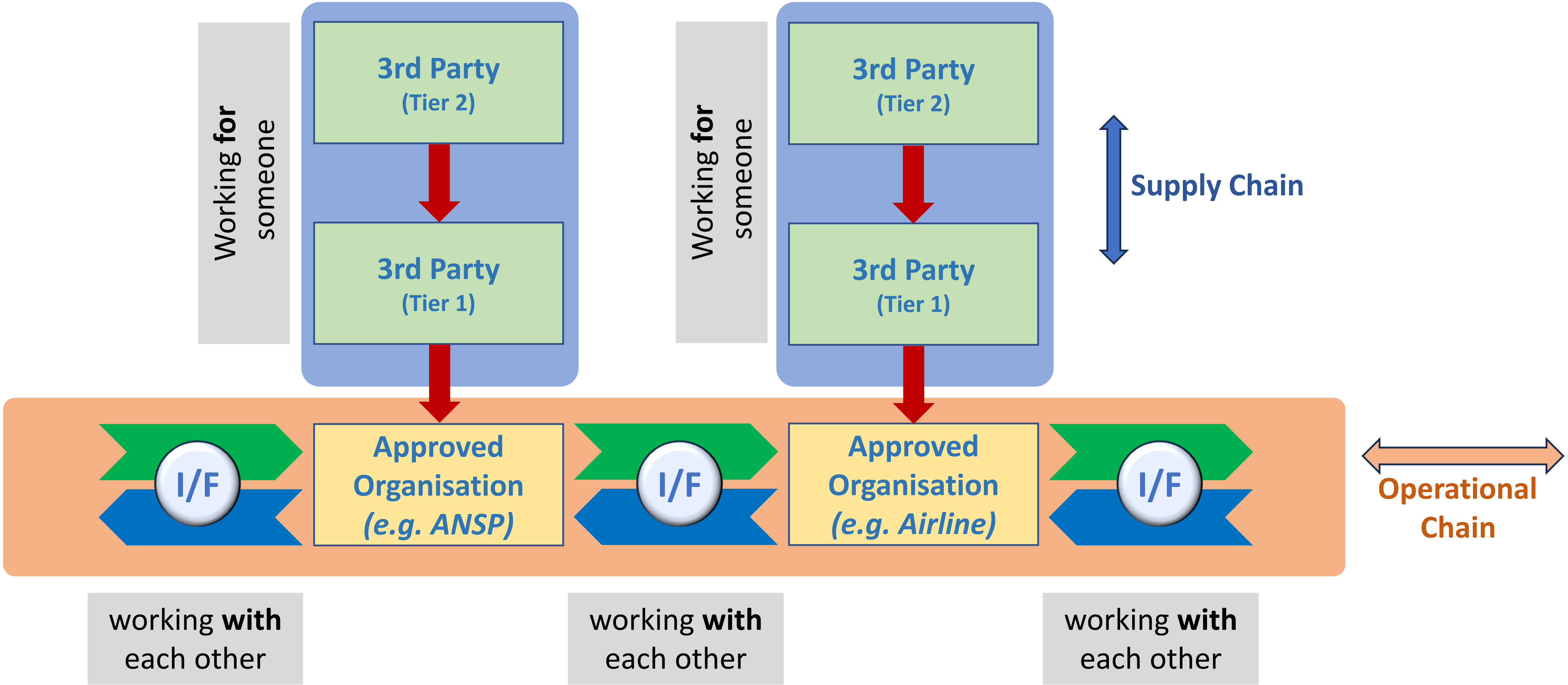
Alexander Kalev is a cybersecurty engineer at the Airbus Customer Services Security Team . He is currently working on risk assessments related to aircraft maintenance and ground support equipment.

Examples of functional chains and shared risks

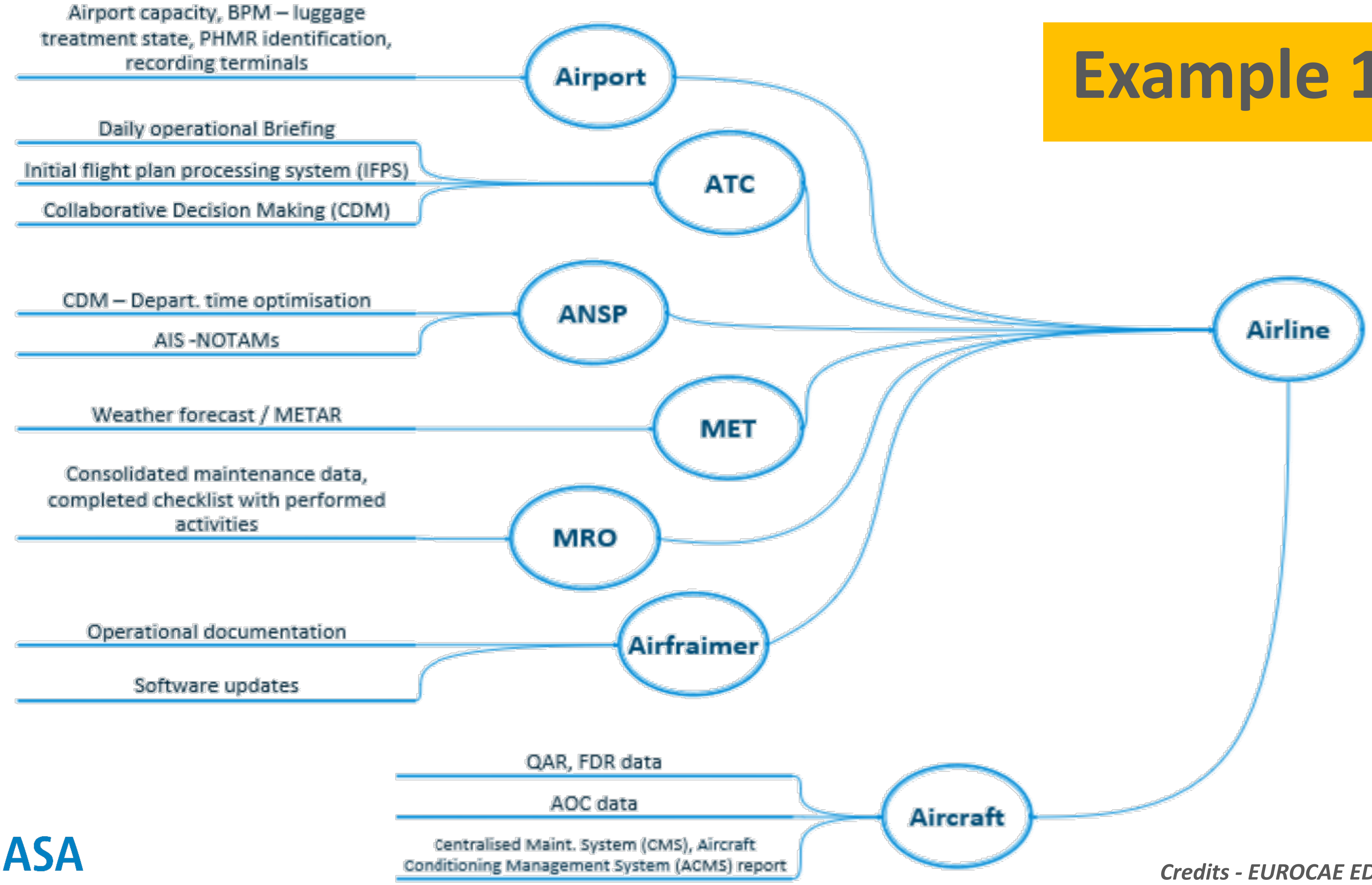
Part-IS Implementation

Workshop

What functional chain means

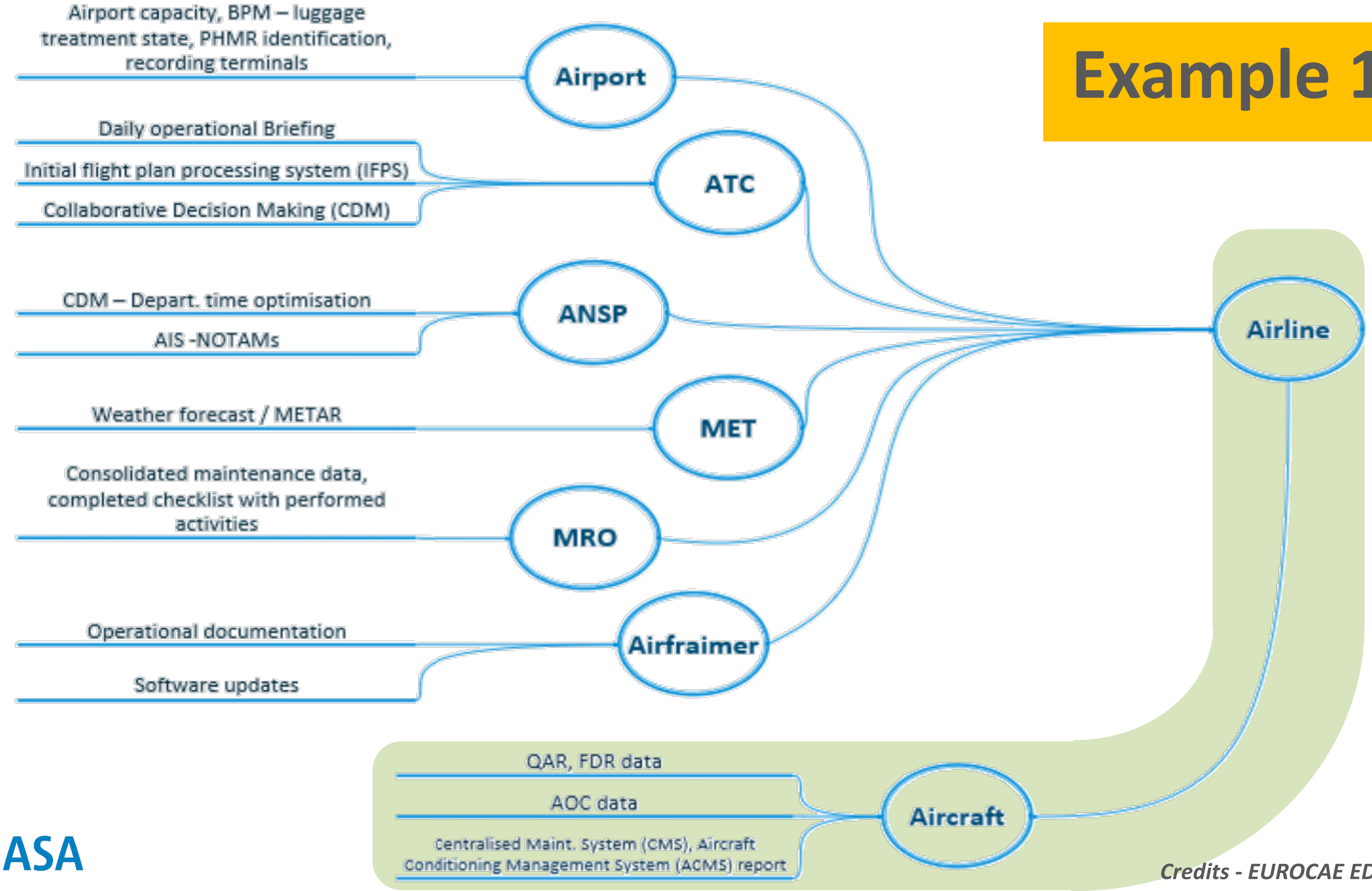

Working **for** someone
3rd Party
(Tier 2)
3rd Party
(Tier 1)
Working **for** someone
3rd Party
(Tier 2)
3rd Party
(Tier 1)
Supply Chain
I/F
Approved Organisation *(e.g. ANSP)*
I/F
Approved Organisation *(e.g. Airline)*
I/F
Operational Chain
working **with** each other
working **with** each other
working **with** each other

Example 1


Airport capacity, BPM – luggage treatment state, PHMR identification, recording terminals
Airport
Daily operational Briefing
Initial flight plan processing system (IFPS)
Collaborative Decision Making (CDM)
ATC
CDM – Depart. time optimisation
AIS -NOTAMs
ANSP
Weather forecast / METAR
MET
Consolidated maintenance data, completed checklist with performed activities
MRO
Operational documentation
Software updates
Airfraimer
QAR, FDR data
AOC data
Centralised Maint. System (CMS), Aircraft Conditioning Management System (ACMS) report
Aircraft
Airline

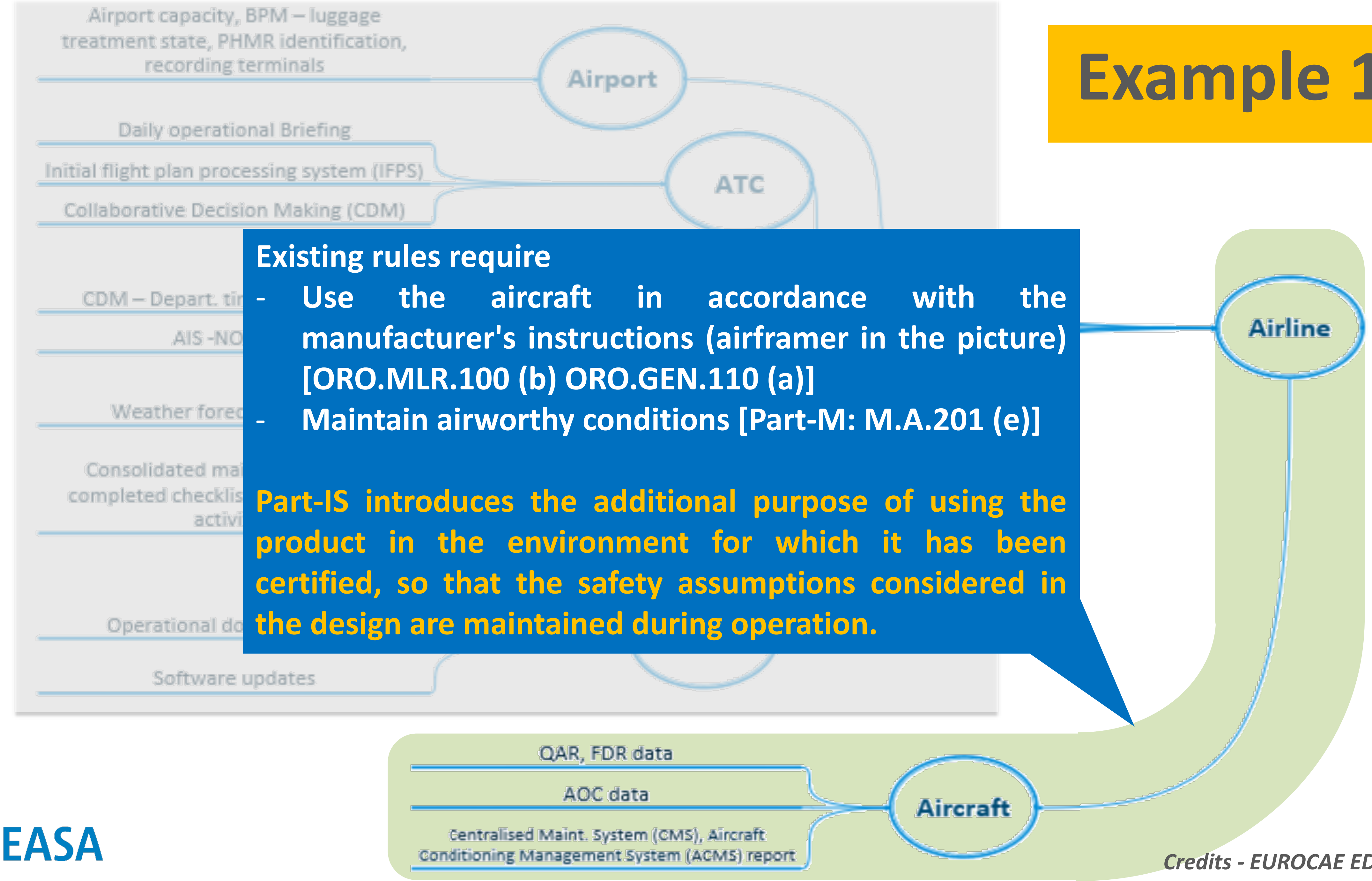
Credits - EUROCAE ED-201A for data

Example 1


Airport capacity, BPM – luggage treatment state, PHMR identification, recording terminals
Airport
Daily operational Briefing
Initial flight plan processing system (IFPS)
Collaborative Decision Making (CDM)
ATC
CDM – Depart. time optimisation
AIS -NOTAMs
ANSP
Weather forecast / METAR
MET
Consolidated maintenance data, completed checklist with performed activities
MRO
Operational documentation
Software updates
Airfraimer
Airline
QAR, FDR data
AOC data
Centralised Maint. System (CMS), Aircraft Conditioning Management System (ACMS) report
Aircraft

Credits - EUROCAE ED-201A for data

Example 1


Airport capacity, BPM – luggage treatment state, PHMR identification, recording terminals
Airport
Daily operational Briefing
Initial flight plan processing system (IFPS)
ATC
Collaborative Decision Making (CDM)
CDM – Depart. ti
AIS -NO
Weather fore
Consolidated ma
completed checklis
activi
Operational do
Software updates
Airline
QAR, FDR data
AOC data
Centralised Maint. System (CMS), Aircraft Conditioning Management System (ACMS) report
Aircraft

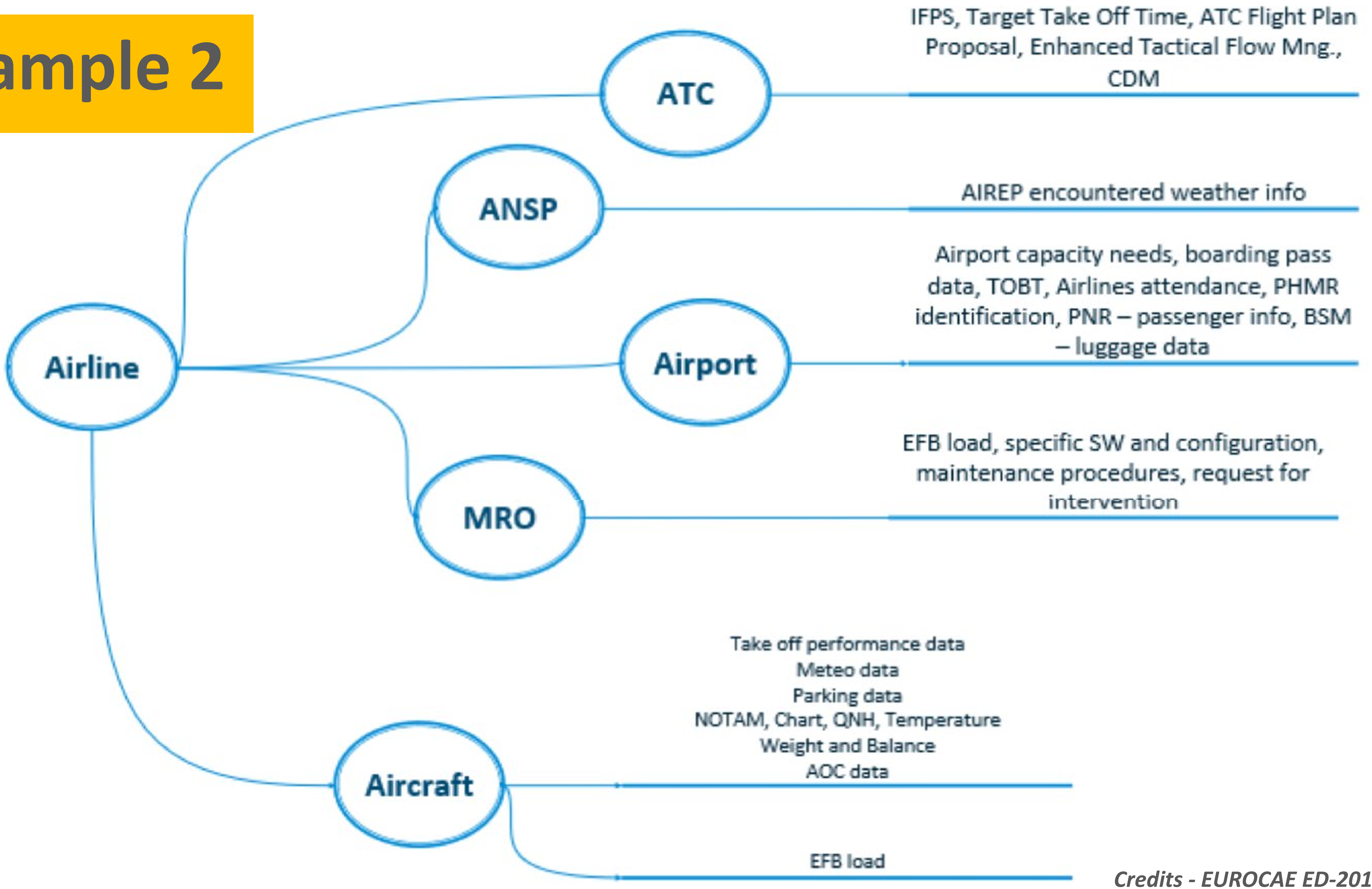
Existing rules require

- Use the aircraft in accordance with the manufacturer's instructions (airframer in the picture) [ORO.MLR.100 (b) ORO.GEN.110 (a)]
- Maintain airworthy conditions [Part-M: M.A.201 (e)]

Part-IS introduces the additional purpose of using the product in the environment for which it has been certified, so that the safety assumptions considered in the design are maintained during operation.

Credits - EUROCAE ED-201A for data

Example 2



IFPS, Target Take Off Time, ATC Flight Plan Proposal, Enhanced Tactical Flow Mng., CDM

AIREP encountered weather info

Airport capacity needs, boarding pass data, TOBT, Airlines attendance, PHMR identification, PNR – passenger info, BSM – luggage data

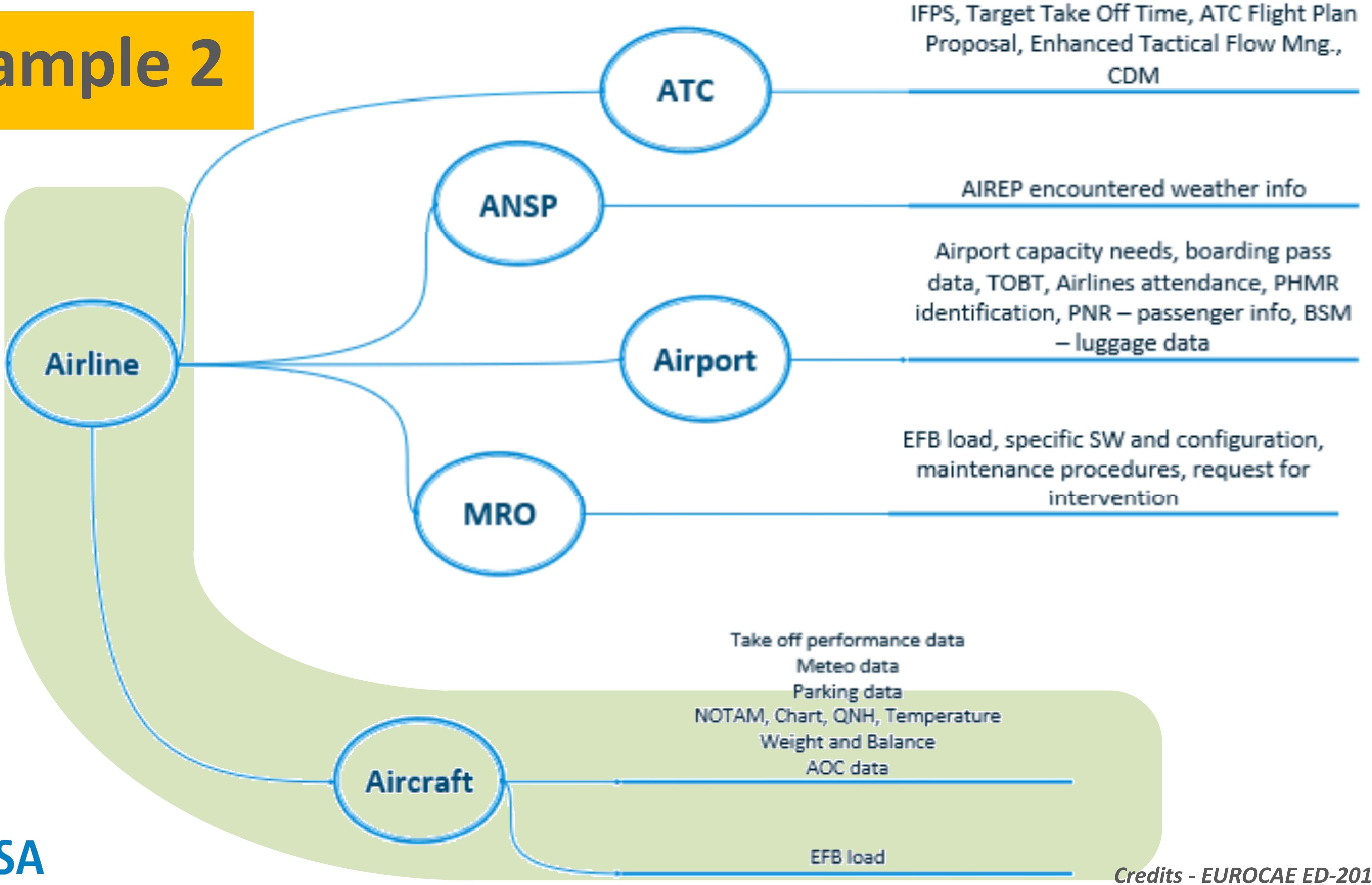
EFB load, specific SW and configuration, maintenance procedures, request for intervention

Take off performance data
Meteo data
Parking data
NOTAM, Chart, QNH, Temperature
Weight and Balance
AOC data

EFB load

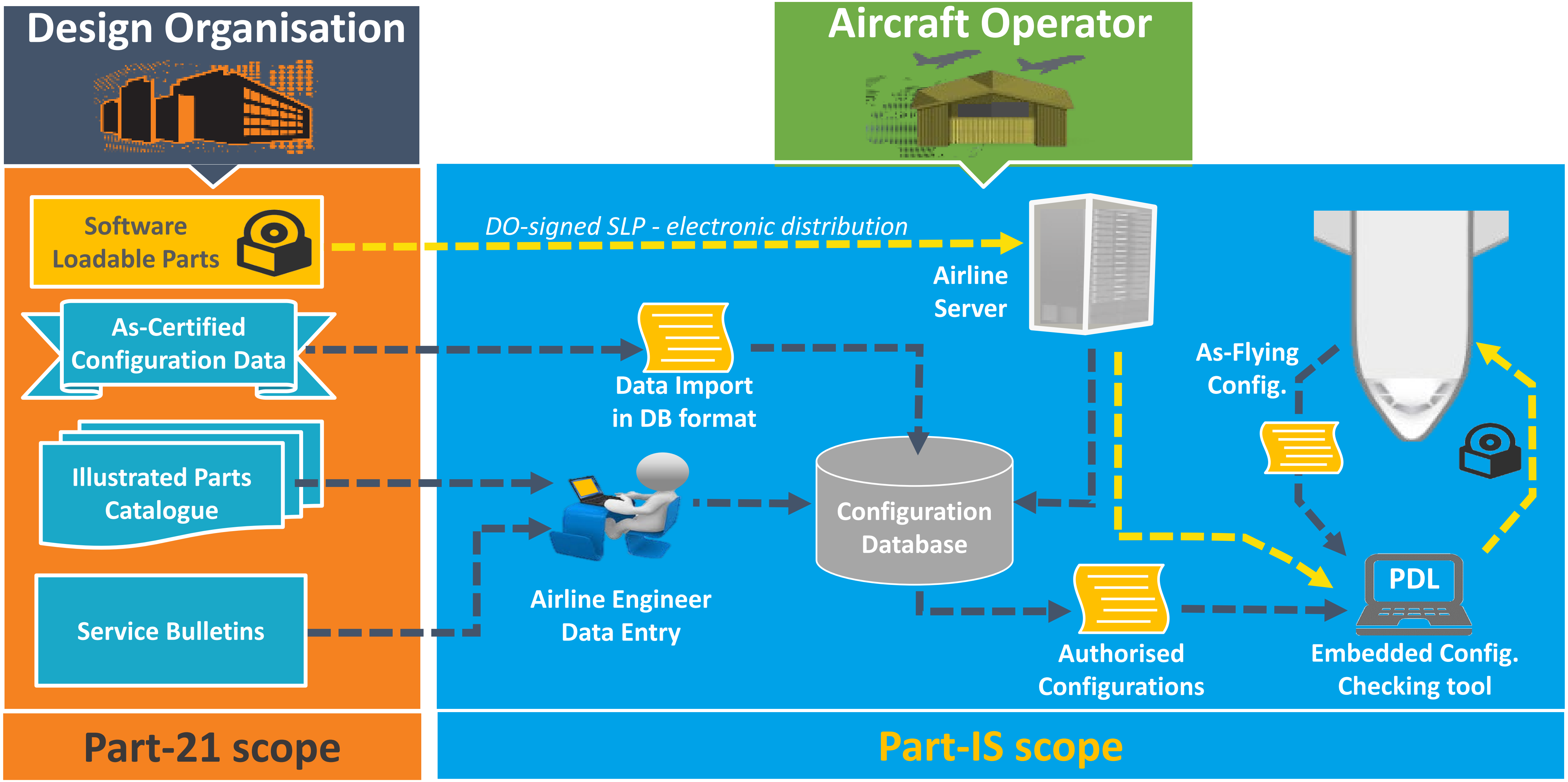
Credits - EUROCAE ED-201A for data

Example 2

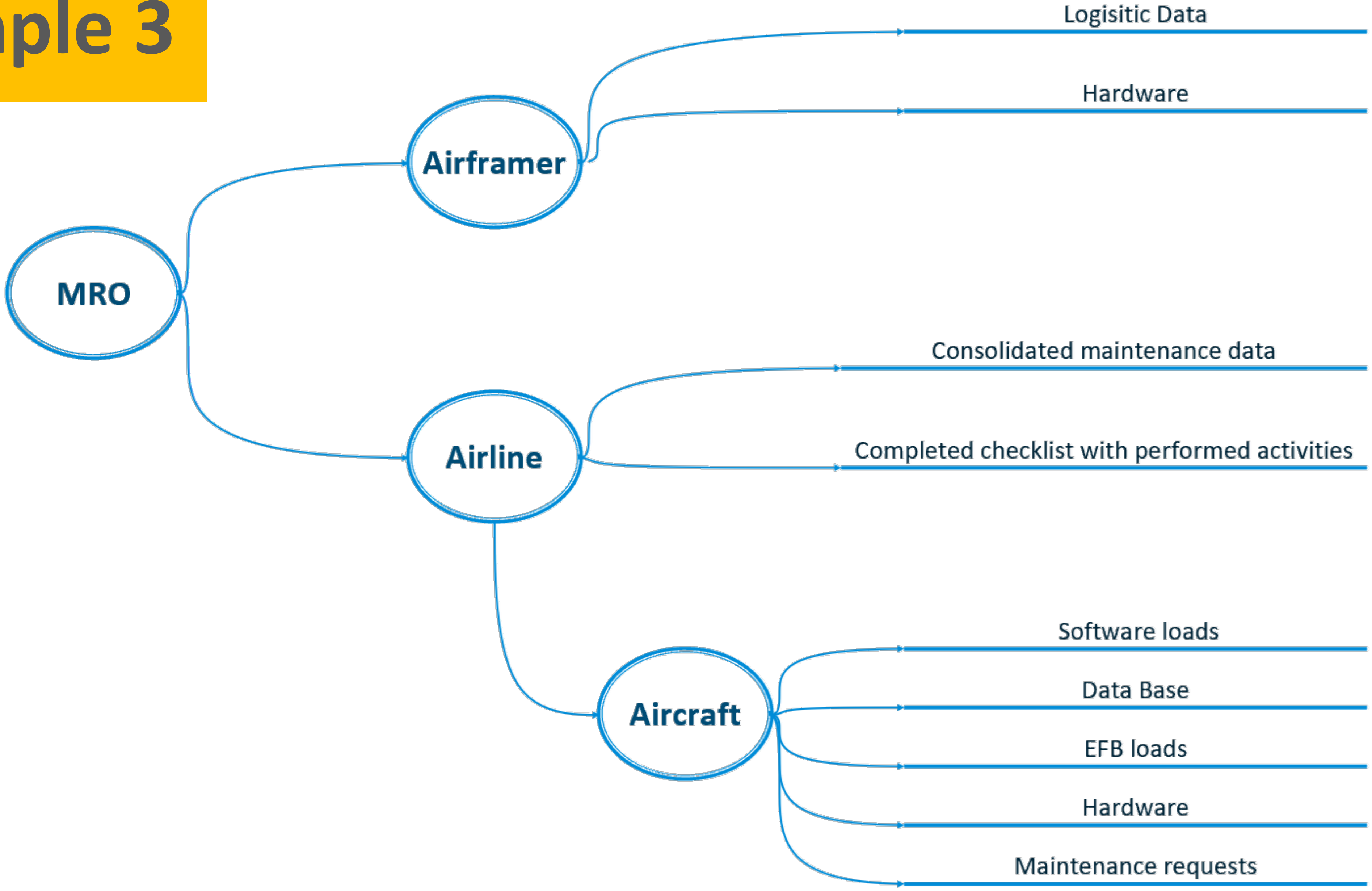

ATC
IFPS, Target Take Off Time, ATC Flight Plan Proposal, Enhanced Tactical Flow Mng., CDM
ANSP
AIREP encountered weather info
Airline
Airport
Airport capacity needs, boarding pass data, TOBT, Airlines attendance, PHMR identification, PNR – passenger info, BSM – luggage data
MRO
EFB load, specific SW and configuration, maintenance procedures, request for intervention
Aircraft
Take off performance data
Meteo data
Parking data
NOTAM, Chart, QNH, Temperature
Weight and Balance
AOC data
EFB load

Credits - EUROCAE ED-201A for data

Part-IS and Part-21 cont. airworthiness



Example 3



MRO

Airframer

Logisitic Data

Hardware

Airline

Consolidated maintenance data

Completed checklist with performed activities

Aircraft

Software loads

Data Base

EFB loads

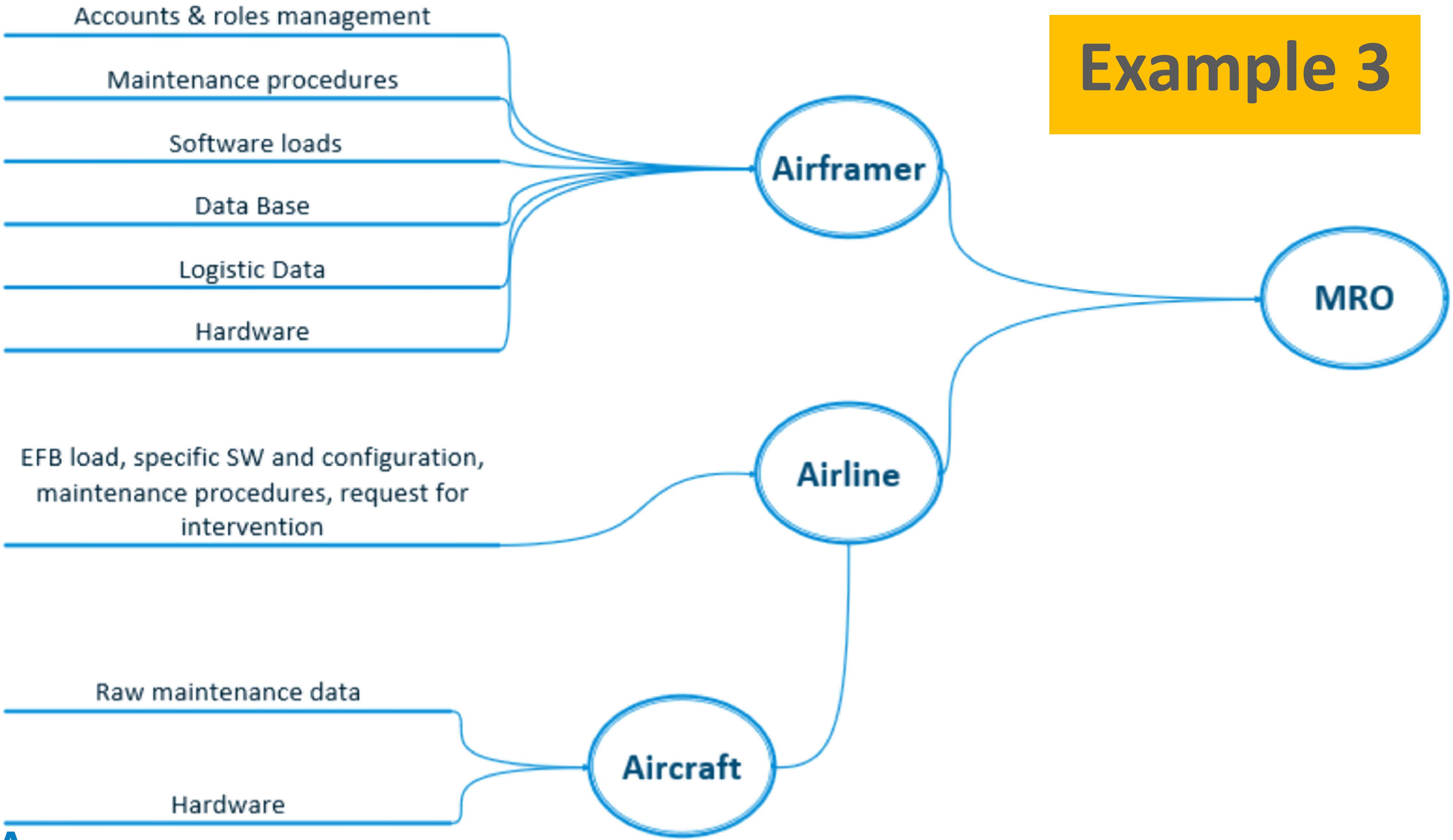
Hardware

Maintenance requests

EASA

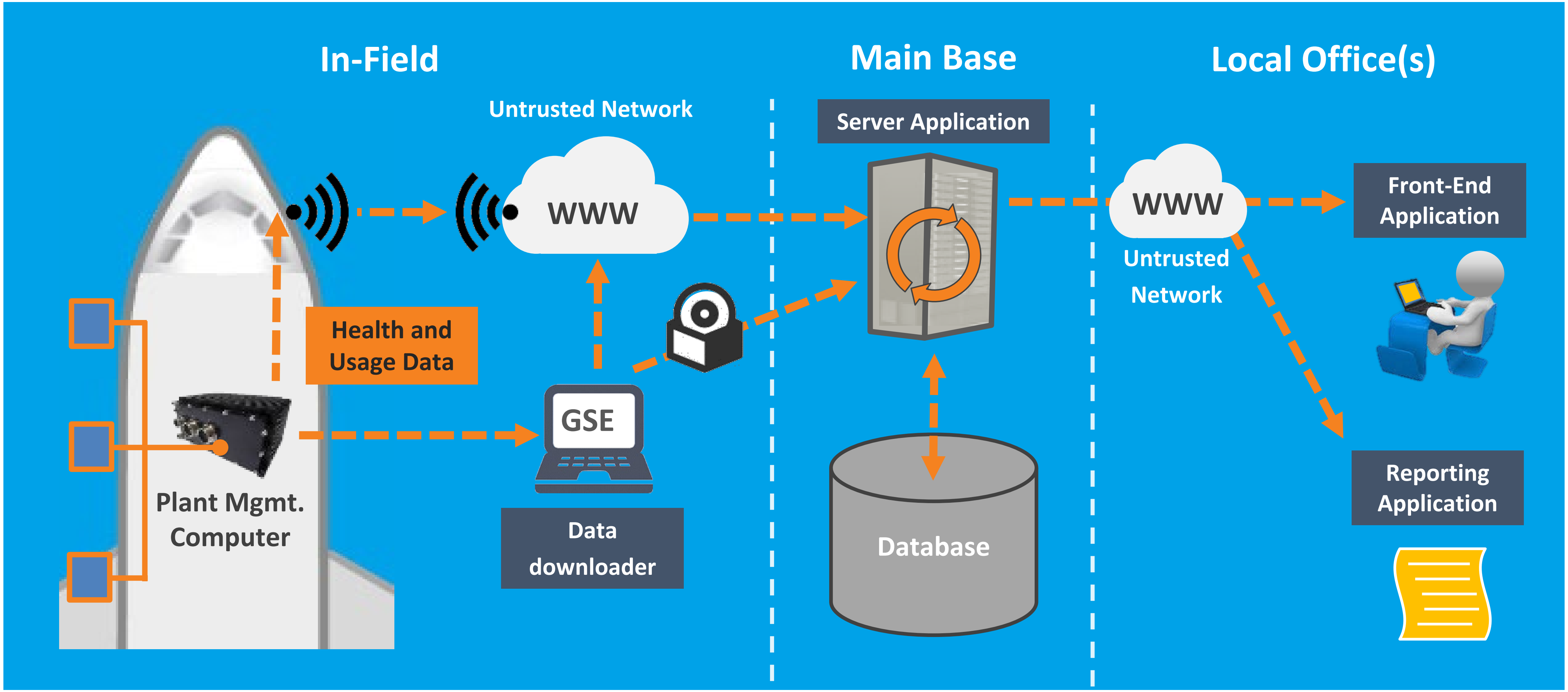
Credits - EUROCAE ED-201A for data

Example 3



Credits - EUROCAE ED-201A for data

Raw maintenance data scenario



Interface Management and Risk Information Sharing

Part-IS Implementation

Workshop

Outline

1. **Introduction**
   a. Part-IS at Airbus
   b. Risk Information Sharing Requirements
2. **A two-fold Approach**
   a. Interfaces with Customers
   b. Standardization Effort

Disclaimer

🚧

The information and materials provided during the presentation are considered work in progress and there may be errors, omissions, or inaccuracies.

⚠

The presented approaches to Part-IS conformity are subject to change and should be considered in context by each organization.

Part-IS at Airbus - Facts and Figures

5 Approved Organizations

- DOA
- POA
- MOA
- CAMO
- ATO

~100 Business Processes

- Directly impacted (related to approved organizations)
- Indirectly impacted (related to development)

Assets

- Potentially hundreds of digital assets
- ~ 500 GSE potentially relevant for Part-IS

Impacted Populations

- Processes Owners
- Business Asset Owners
- Development Teams
- Security Teams
- …

ISMS Network

- ~25 nominated ISMS Officers
- Potentially hundreds of ISMS representatives to be nominated
- Part of the ISMS Network common with the SMS

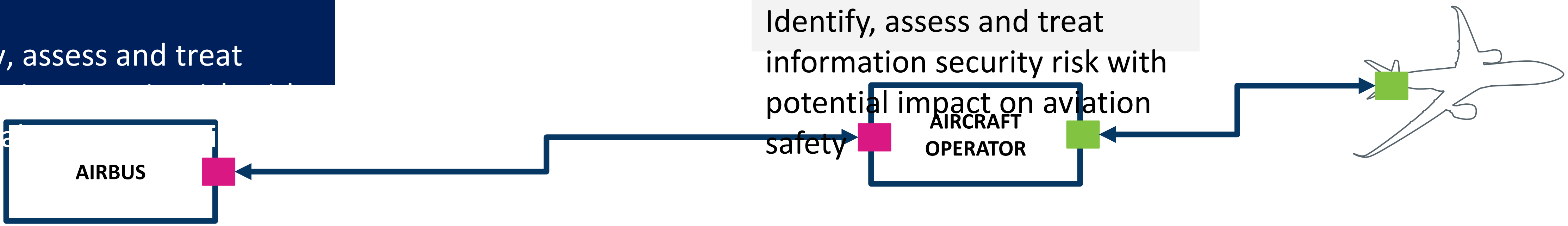
Risk Information Sharing Requirements

Security Risk Assessment (SRA)

Identify, assess and treat

Security Risk Assessment (SRA)

Identify, assess and treat information security risk with potential impact on aviation safety



Identify interfaces on which there could be mutual exposure to information security risks

IS.OR.205(b)

Inform connected organisations about shared risks

IS.OR.210 (b)

Identify interfaces on which there could be mutual exposure to information security risks

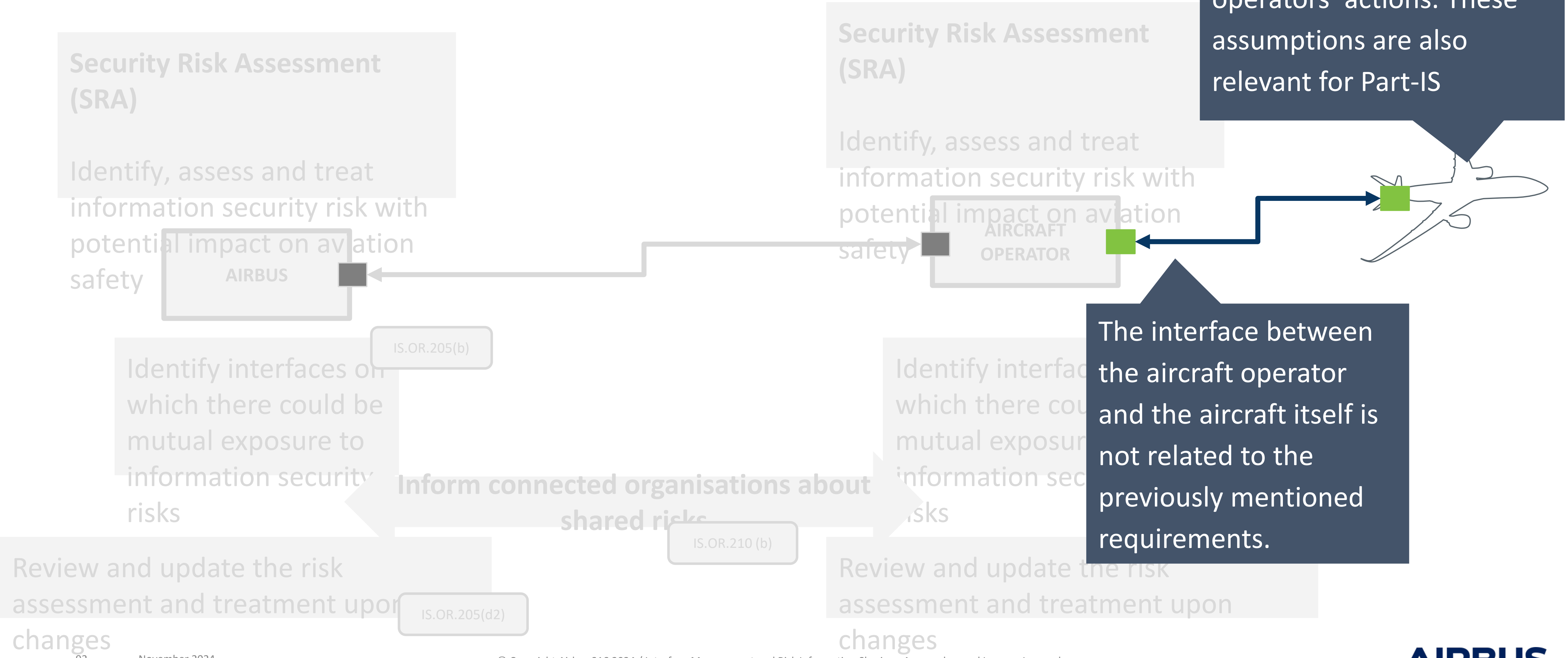
Review and update the risk assessment and treatment upon

IS.OR.205(d2)

Review and update the risk assessment and treatment upon changes

Risk Information Sharing Requirements

The product has been certified using specific assumptions impling operators' actions. These assumptions are also relevant for Part-IS



Security Risk Assessment (SRA)

Identify, assess and treat information security risk with potential impact on aviation safety

Identify interfaces on which there could be mutual exposure to information security risks

Inform connected organisations about shared risks

Review and update the risk assessment and treatment upon changes

Security Risk Assessment (SRA)

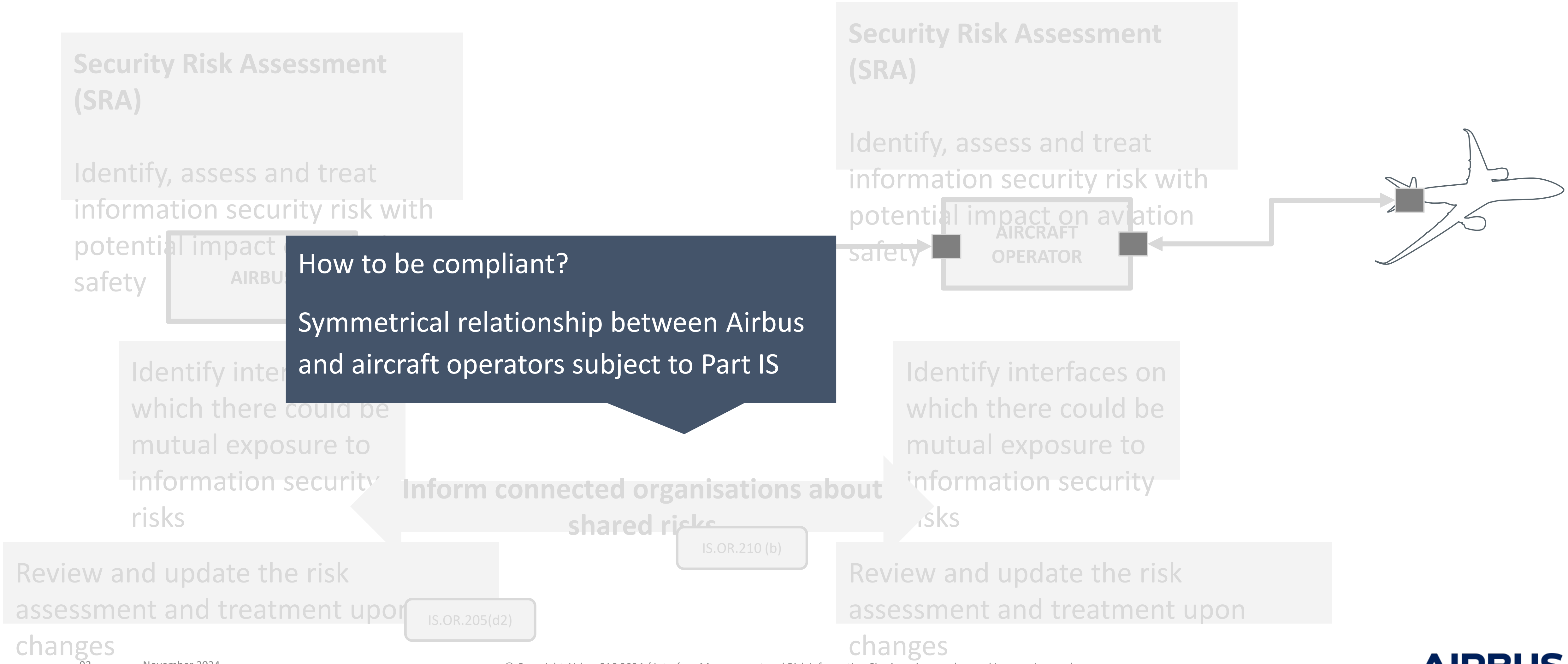
Identify, assess and treat information security risk with potential impact on aviation safety

Identify interfac which there cou mutual exposur information sec isks

Review and update the risk assessment and treatment upon changes

The interface between the aircraft operator and the aircraft itself is not related to the previously mentioned requirements.

Risk Information Sharing Requirements



Security Risk Assessment (SRA)

Identify, assess and treat information security risk with potential impact on aviation safety

Security Risk Assessment (SRA)

Identify, assess and treat information security risk with potential impact on aviation safety

How to be compliant?

Symmetrical relationship between Airbus and aircraft operators subject to Part IS

Identify inter which there could be mutual exposure to information securit risks

Identify interfaces on which there could be mutual exposure to information security isks

Inform connected organisations about shared risks

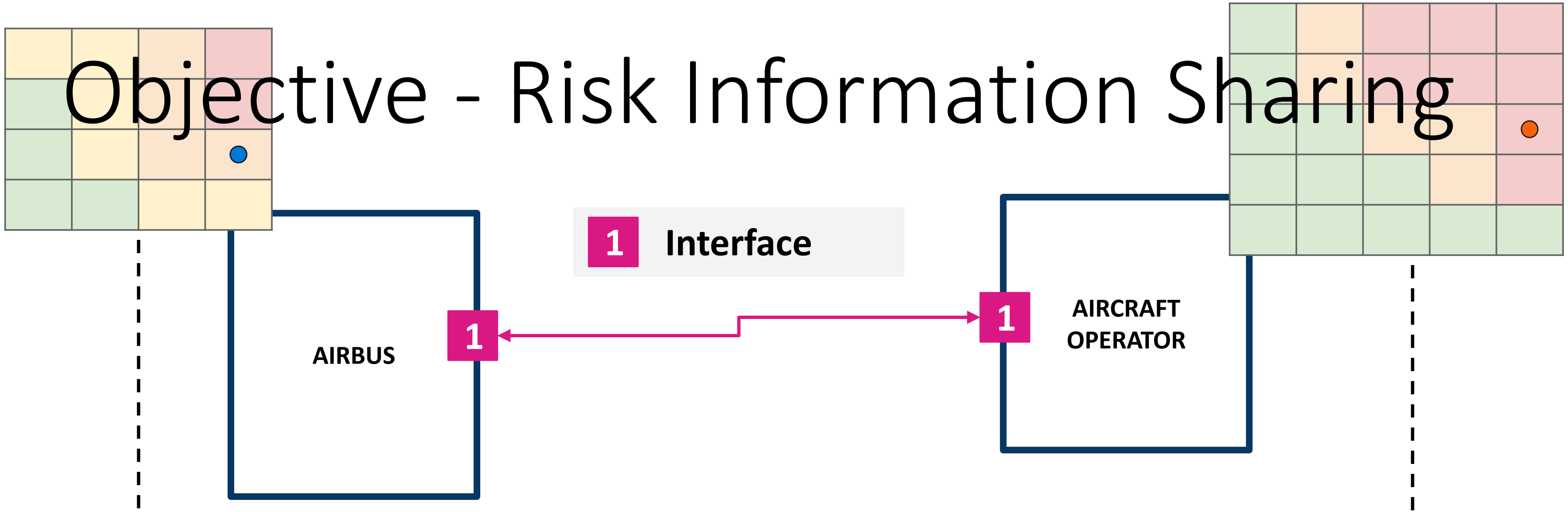
IS.OR.210 (b)

Review and update the risk assessment and treatment upor changes

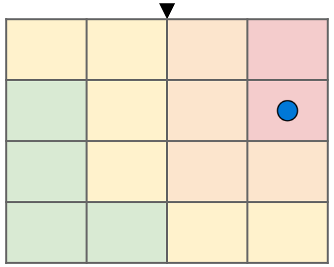
IS.OR.205(d2)

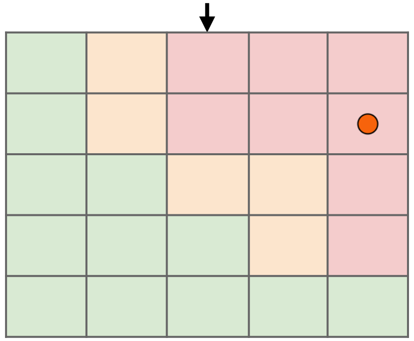
Review and update the risk assessment and treatment upon changes

Objective - Risk Information Sharing



	Severity of the Threat Condition		
Level of Threat	**Negligible Effect/Impact**	**Incident**	**Accident**
High	Conditionally Acceptable	Not acceptable	Not acceptable
Medium	Acceptable	Conditionally Acceptable	●●
Low	Acceptable	Acceptable	Conditionally Acceptable





The comparison risk acceptance matrix is extracted from the Annex B of the ED-201A Aeronautical Information System Security Framework Guidance.

A Two-fold Approach

EASA Part-IS Workshop - November 2024

A Two-fold Approach

Common considerations:

- Large number of interfaces between all organizations
- Interface commonality between organizations

Interfaces with Customers:

- Scope: Interfaces between aircraft operators and Airbus
- Issued from the ED-201A[1] and the AMC/GM[2]
- Bottom → Up

Standardization Effort:

- Scope: All types of interfaces (operators, suppliers, service providers, etc.)
- Based on Airbus & Dassault Aviation collaboration and the "likelihood of safety impact propagation"[3]
- Top → Down

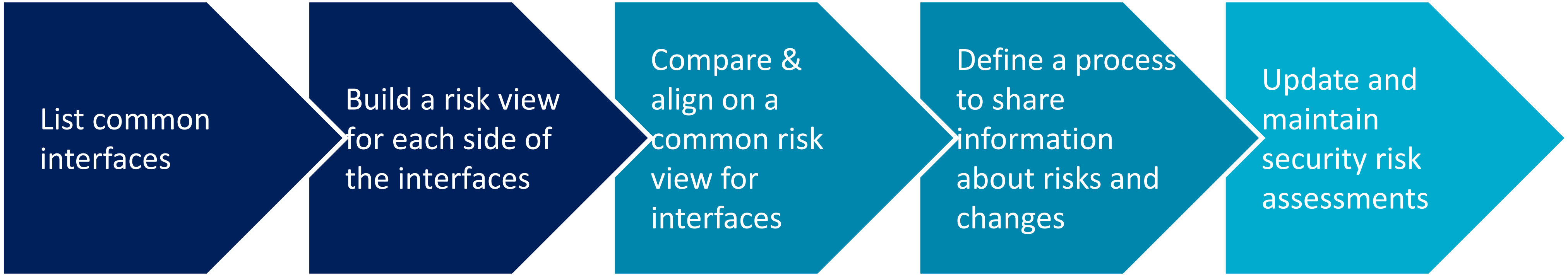
[1] Aeronautical Information System Security Framework Guidance
[2] Acceptable Means of Compliance and Guidance Material to Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645
[3] ED/DO-ISMS Guidance for Aviation White paper: Identification and Classification guidance for Part-IS assets

COMMERCIAL AIRCRAFT

Interfaces with Customers

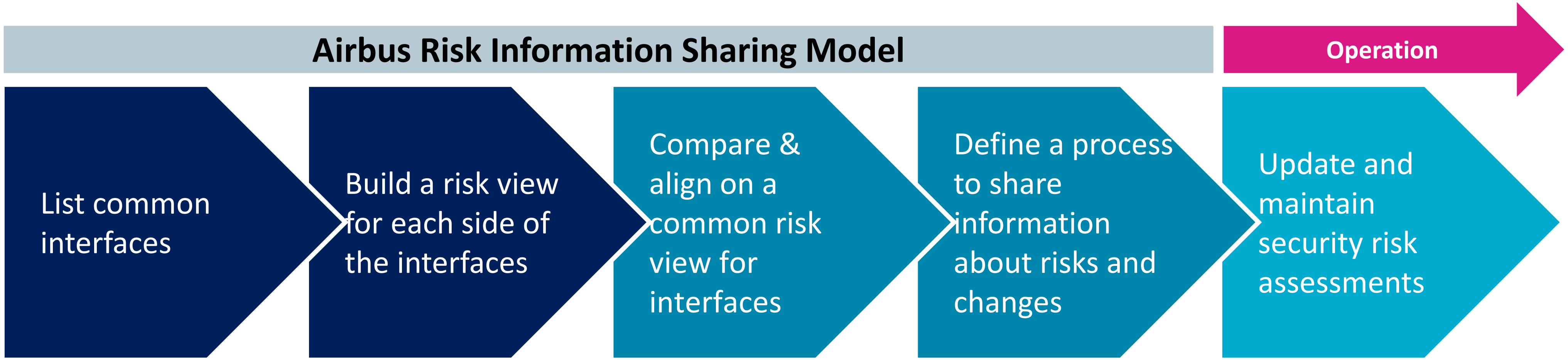
EASA Part-IS Workshop - November 2024

Approach



1. List common interfaces
2. Build a risk view for each side of the interfaces
3. Compare & align on a common risk view for interfaces
4. Define a process to share information about risks and changes
5. Update and maintain security risk assessments

Approach


Airbus Risk Information Sharing Model
Operation
List common interfaces
Build a risk view for each side of the interfaces
Compare & align on a common risk view for interfaces
Define a process to share information about risks and changes
Update and maintain security risk assessments

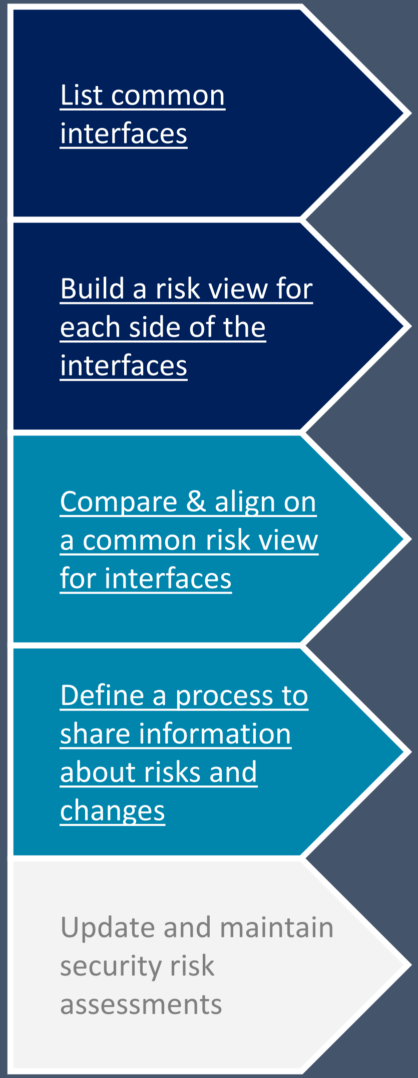
Risk Information Sharing Model

Represent relationships between security risk assessments and shared interfaces

Be able to represent the complex relationships between connected organizations

Enable collaboration and engage discussion

Perform real-world risk information sharing and prepare for day 1



List common interfaces

Build a risk view for each side of the interfaces

Compare & align on a common risk view for interfaces

Define a process to share information about risks and changes

Update and maintain security risk assessments

Risk Information Sharing Model

Represent relationships between security risk assessments and shared interfaces

“Compress security risk assessments”

Be able to represent the complex relationships between connected organizations

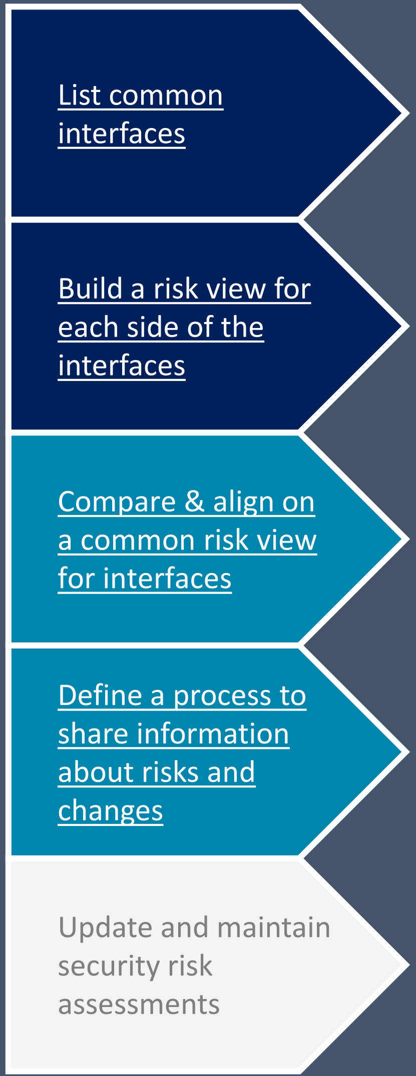
Use a visual methods

Enable collaboration and engage discussion

Use generic interfaces and fictitious data

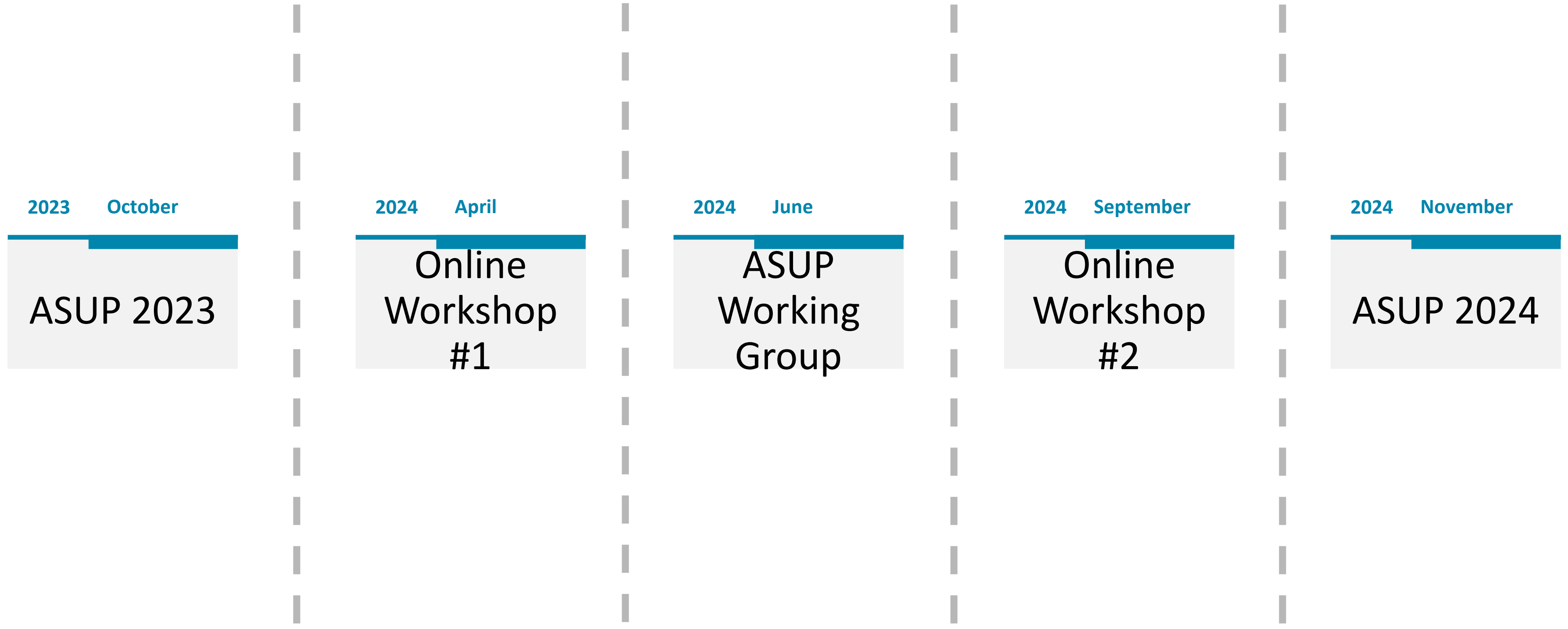
Perform real-world risk information sharing and prepare for day 1

Create report templates



List common interfaces
Build a risk view for each side of the interfaces
Compare & align on a common risk view for interfaces
Define a process to share information about risks and changes
Update and maintain security risk assessments

Risk Information Sharing Model



2023 October

ASUP 2023

2024 April

Online Workshop #1

2024 June

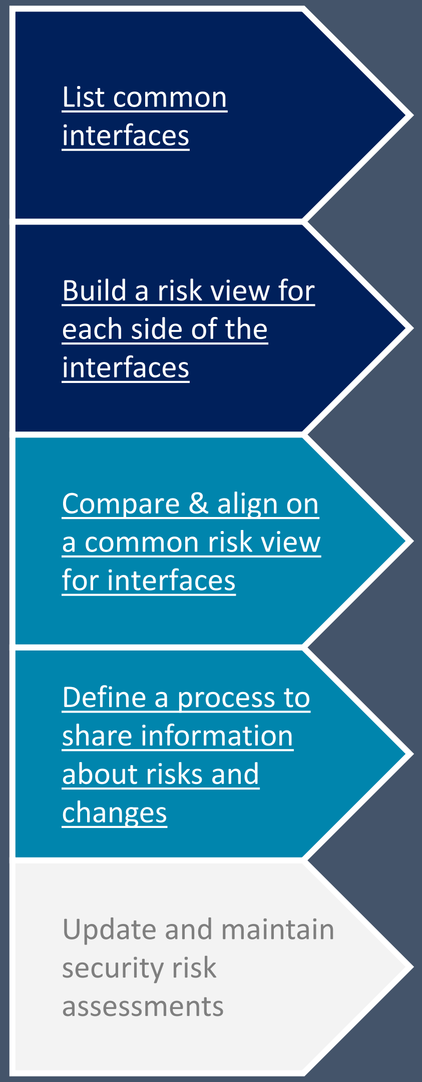
ASUP Working Group

2024 September

Online Workshop #2

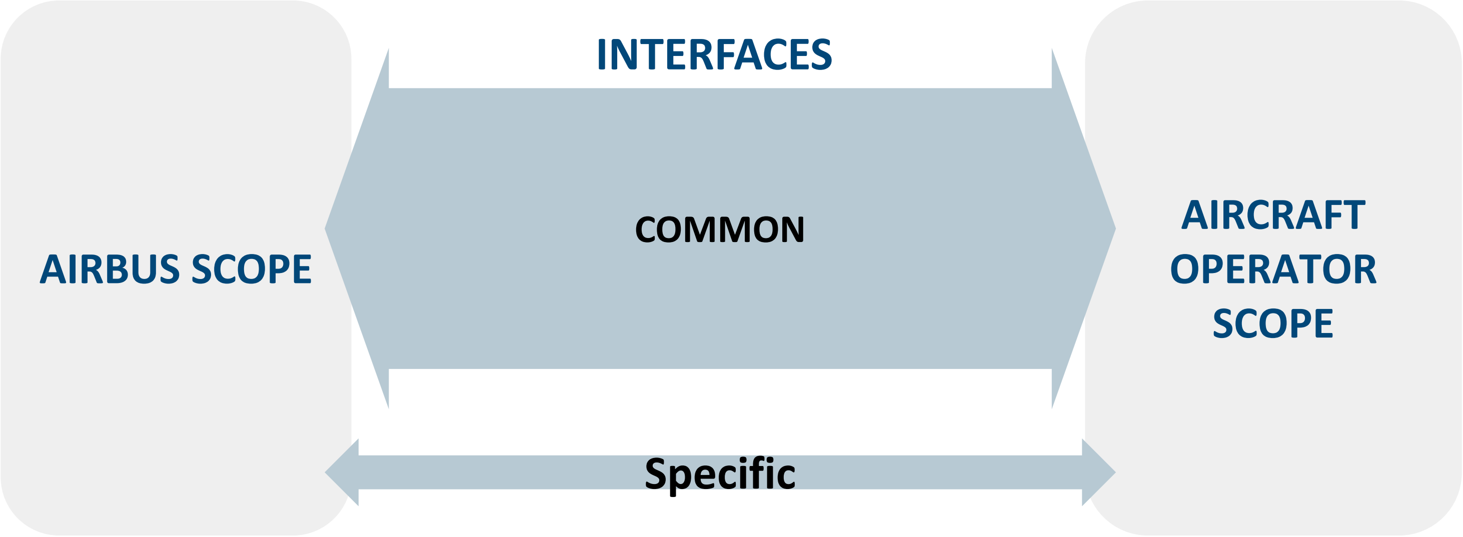
2024 November

ASUP 2024



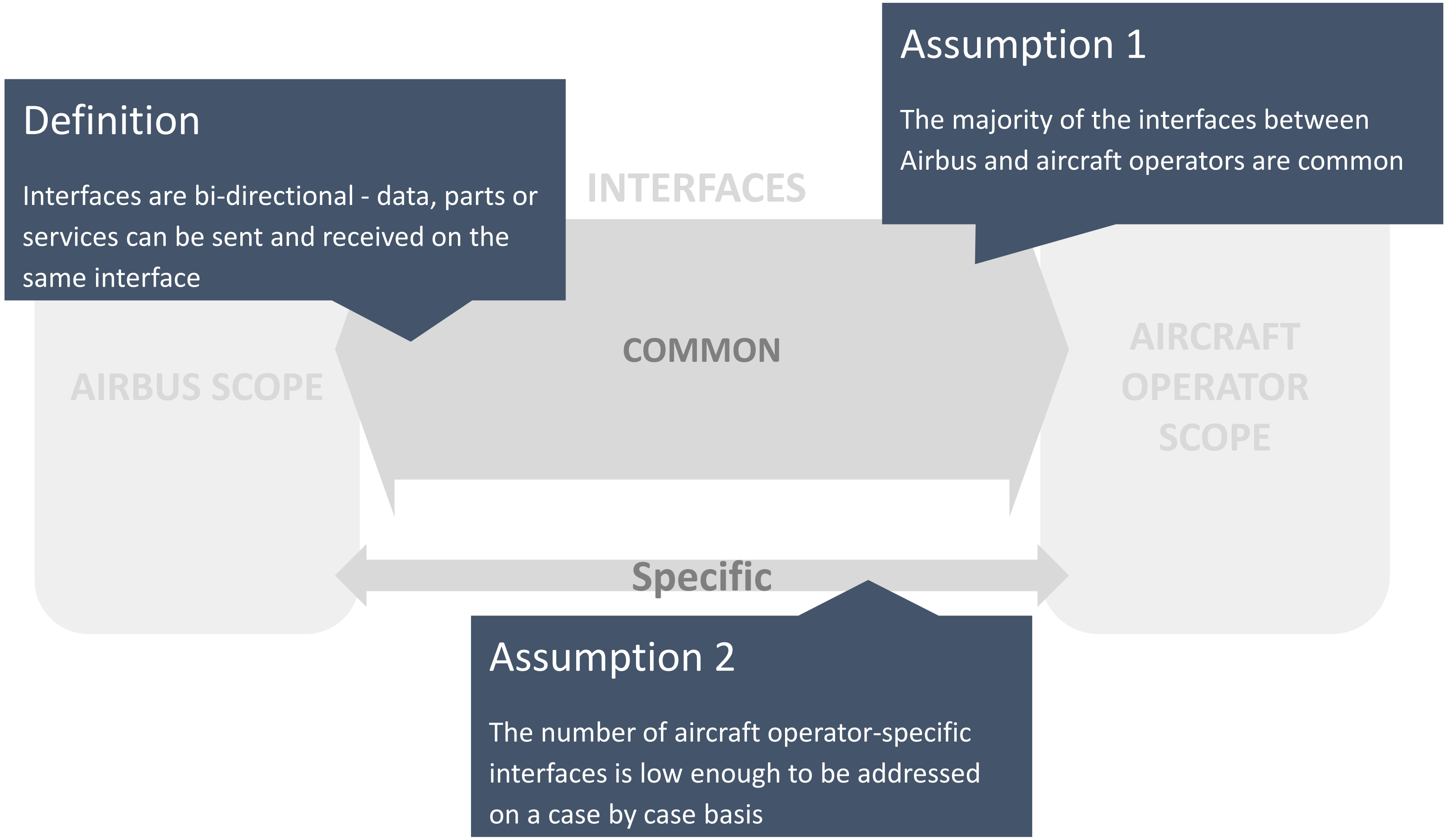
- List common interfaces
- Build a risk view for each side of the interfaces
- Compare & align on a common risk view for interfaces
- Define a process to share information about risks and changes
- Update and maintain security risk assessments

Common Interfaces



- List common interfaces
- Build a risk view for each side of the interfaces
- Compare & align on a common risk view for interfaces
- Define a process to share information about risks and changes
- Update and maintain security risk assessments

Common Interfaces



Definition

Interfaces are bi-directional - data, parts or services can be sent and received on the same interface

Assumption 1

The majority of the interfaces between Airbus and aircraft operators are common

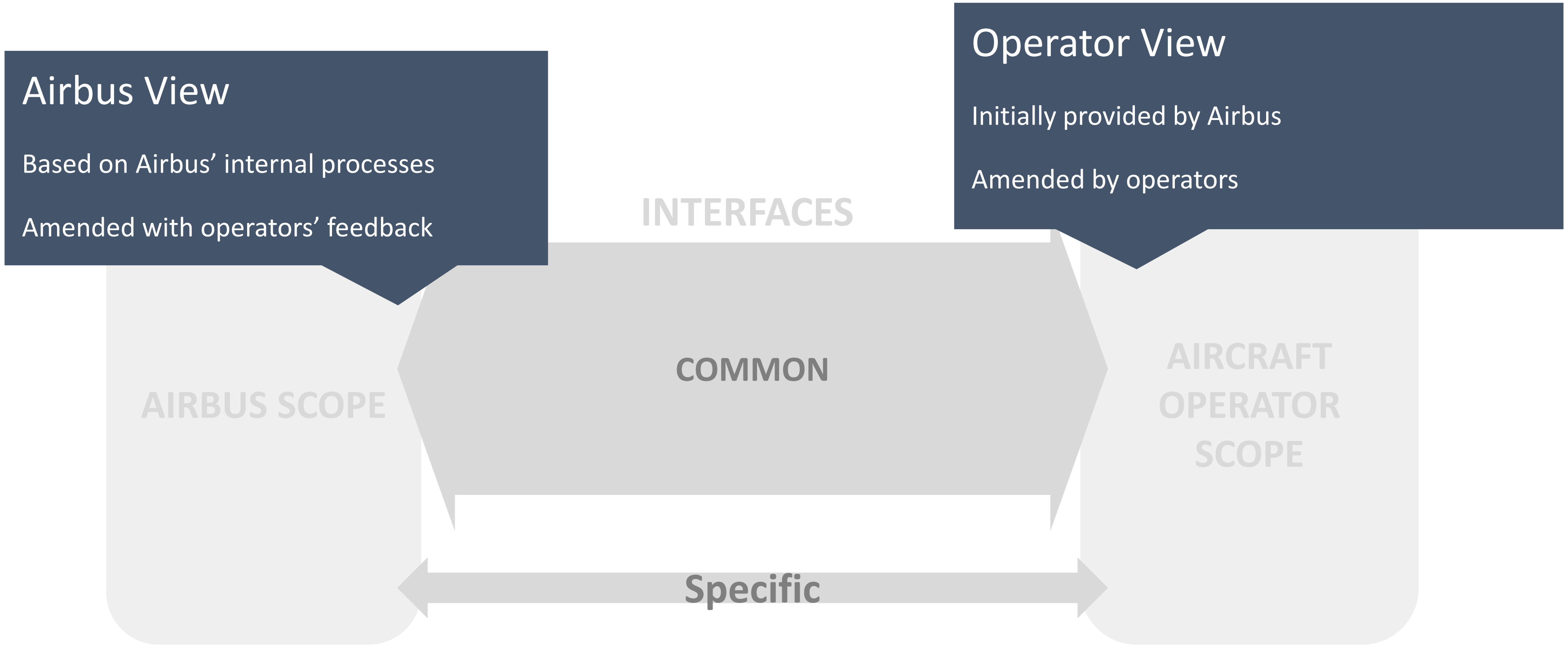
Assumption 2

The number of aircraft operator-specific interfaces is low enough to be addressed on a case by case basis

- List common interfaces
- Build a risk view for each side of the interfaces
- Compare & align on a common risk view for interfaces
- Define a process to share information about risks and changes
- Update and maintain security risk assessments

AIRBUS

Interfaces and Risks



Airbus View

Based on Airbus' internal processes

Amended with operators' feedback

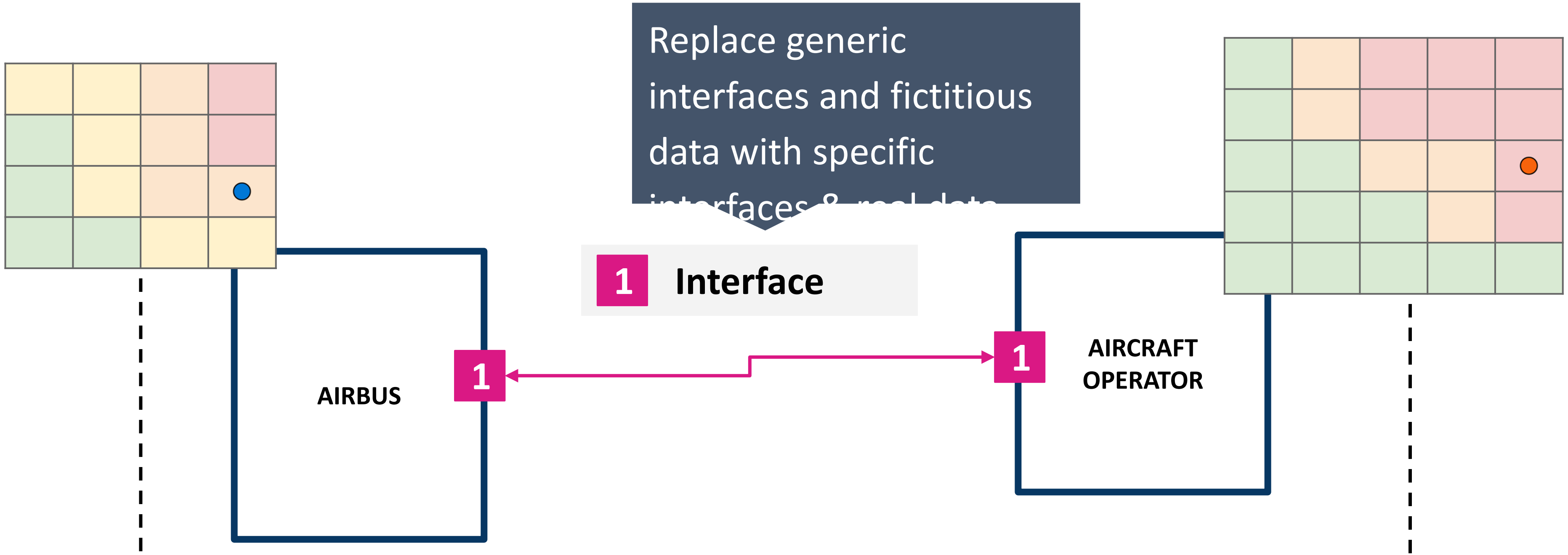
Operator View

Initially provided by Airbus

Amended by operators

- List common interfaces
- Build a risk view for each side of the interfaces
- Compare & align on a common risk view for interfaces
- Define a process to share information about risks and changes
- Update and maintain security risk assessments

Common View for Each Interface



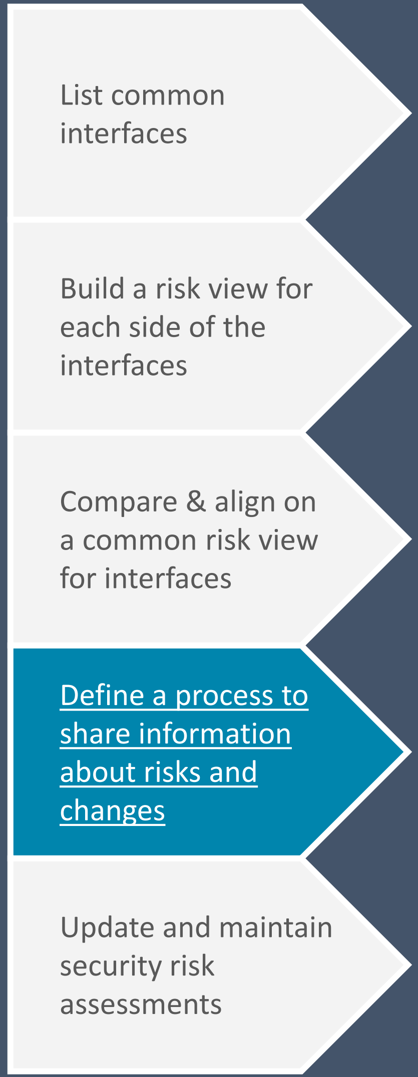
Replace generic interfaces and fictitious data with specific interfaces & real data

	Severity of the Threat Condition		
Level of Threat	Negligible Effect/Impact	Incident	Accident
High	Conditionally Acceptable	Not acceptable	Not acceptable
Medium	Acceptable	Conditionally Acceptable	●●
Low	Acceptable	Acceptable	Conditionally Acceptable

- List common interfaces
- Build a risk view for each side of the interfaces
- Compare & align on a common risk view for interfaces
- Define a process to share information about risks and changes
- Update and maintain security risk assessments

Process

- Put in place a specific risk information sharing template
- Extension of the Airbus Security Handbook documentation suite
- Ensure an yearly update
- Provide access to Aircraft Security Focal Points (ASFP)
- Put in place a specific Non-Disclosure Agreement (NDA)



List common interfaces

Build a risk view for each side of the interfaces

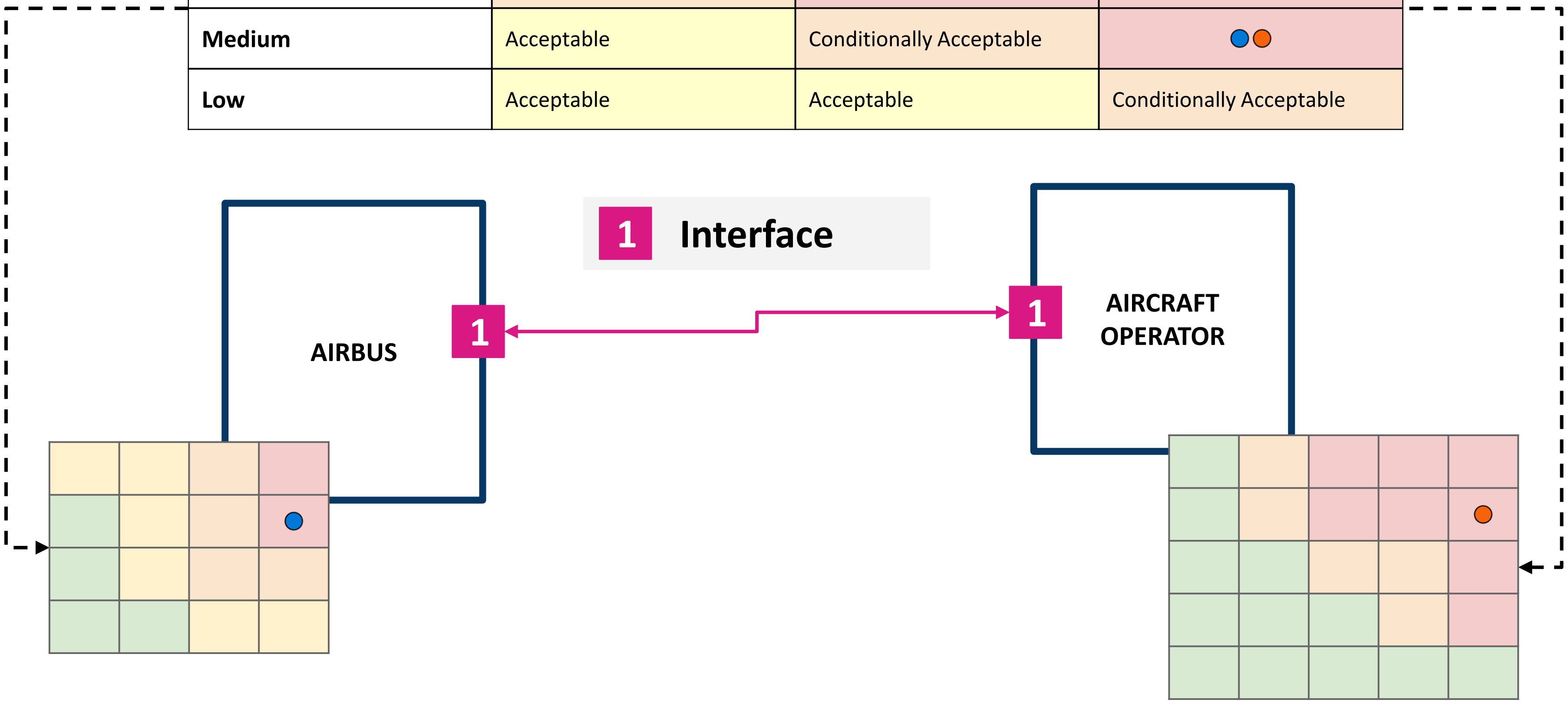
Compare & align on a common risk view for interfaces

Define a process to share information about risks and changes

Update and maintain security risk assessments

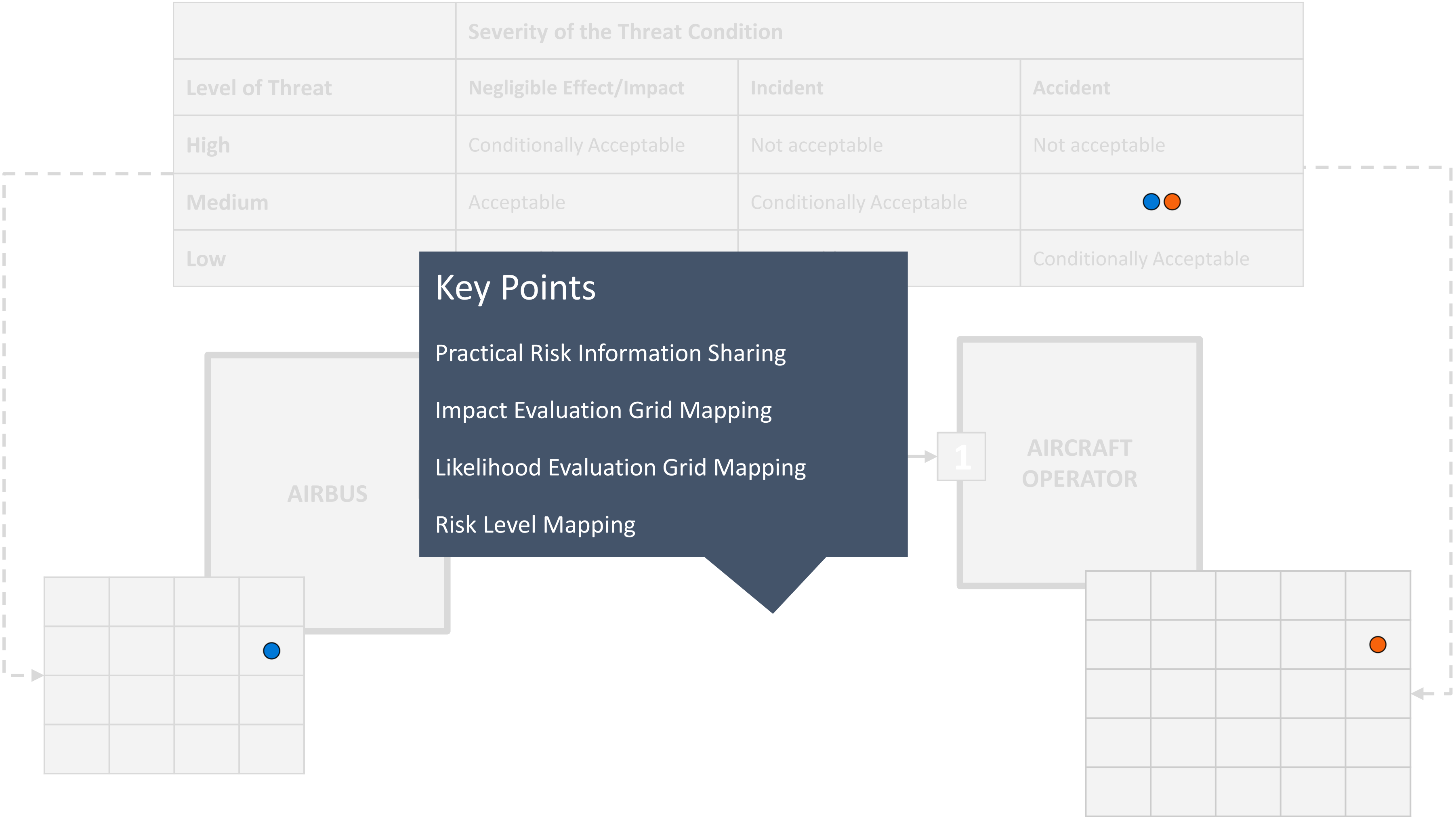
Update Security Risk Assessments

	Severity of the Threat Condition		
Level of Threat	**Negligible Effect/Impact**	**Incident**	**Accident**
High	Conditionally Acceptable	Not acceptable	Not acceptable
Medium	Acceptable	Conditionally Acceptable	●●
Low	Acceptable	Acceptable	Conditionally Acceptable



- List common interfaces
- Build a risk view for each side of the interfaces
- Compare & align on a common risk view for interfaces
- Define a process to share information about risks and changes
- Update and maintain security risk assessments

Update Security Risk Assessments



	Severity of the Threat Condition		
Level of Threat	Negligible Effect/Impact	Incident	Accident
High	Conditionally Acceptable	Not acceptable	Not acceptable
Medium	Acceptable	Conditionally Acceptable	●●
Low			Conditionally Acceptable

Key Points

Practical Risk Information Sharing

Impact Evaluation Grid Mapping

Likelihood Evaluation Grid Mapping

Risk Level Mapping

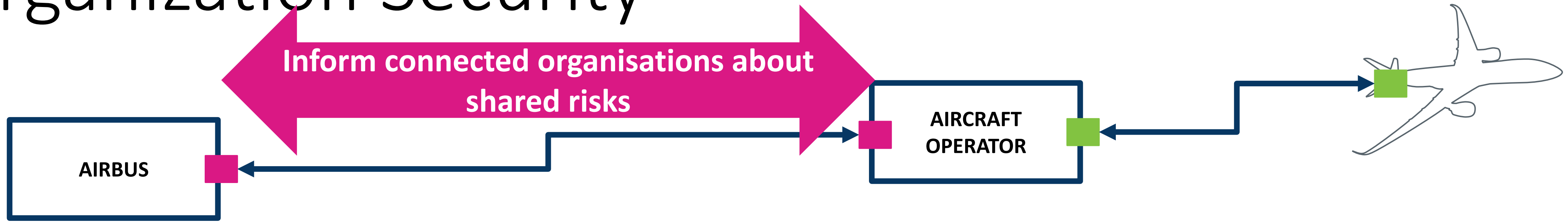
- List common interfaces
- Build a risk view for each side of the interfaces
- Compare & align on a common risk view for interfaces
- Define a process to share information about risks and changes
- Update and maintain security risk assessments

AIRBUS

Challenges & Issues

- Different understanding of what an interface is what is considered a connected organization
- Existence of trust assumptions
- Different maturity levels between operators
- Use different security risk assessment methods and different ways to represent risks
- Difficulty to see beyond the risk information sharing phase - what happens in case of a non-alignment about a given risk
- Difficulty to predict the impact on current and future contracts
- Tendency to mix up product security and organization security

Tendency to Mix up Product Security and Organization Security



Inform connected organisations about shared risks

AIRBUS

AIRCRAFT OPERATOR

Aircraft Certification Security Risk Assessment

Instructions for Continued Airworthiness (ICA)

Assumptions[1] to be verified by the operator (enable aircraft SRA validity)

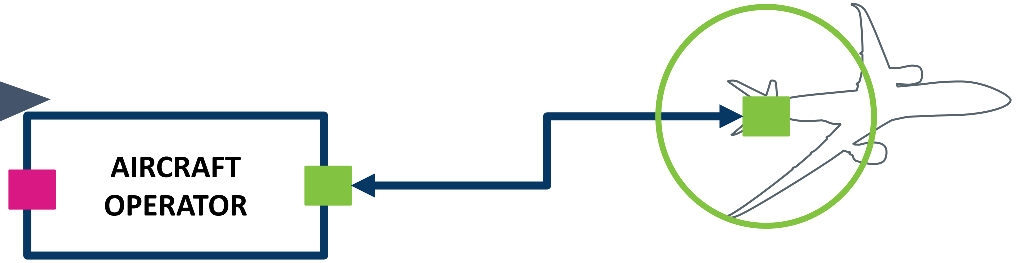
Security Handbook

Operator Part-IS Security Risk Assessment

[1] Example: *"All aircraft physical zones except the cabin area are considered as trustworthy" ("A350 XWB Security Handbook", 2023, p. 32)* - the aircraft operator has to ensure controlled access to all trusted zones of the aircraft.

Operator Security Risk Assessment and Aircraft Interfaces

When the aircraft operator identifies an attack path in its Part-IS assessment involving an interface with the aircraft, it is the aircraft operators' responsibility to assess the safety impact



Derived from GM1 IS.OR.205(c):

Where the aircraft certification[1] addresses product information security, the aircraft operator may take benefit of the associated ICA provided the assumptions are verified

[1] Aircraft types or modifications subject to EASA special conditions / CS25 1319.

COMMERCIAL AIRCRAFT

Standardization Effort

EASA Part-IS Workshop - November 2024

Asset Criticality

Potential Maximum Safety Impact	**Group 1** Assets with immediate, short-term or hidden safety impact	**Group 2** Assets with delayed detectable safety effect	**Group 3** Assets with contribution to **safety** scenarios	**Group 4** Assets with contribution to **security** scenarios
A/C unsafe condition (hazardous or catastrophic)	Critical	Essential	Essential	Routine
Reduction of safety margins (minor or major)	Essential	Routine	Routine	Routine

Ref. "An Identification and Classification guidance method for Part-IS assets", 19th July 2024, Dassault and Airbus, for EUROCAE WG-72 / RTCA SC-216 committees (ED-ISMS)

Classification of Organizations in Interface

Interface Classification:

- Asset Type
  (parts, software, services…)
- Organization Role
  (supplier, customer…)
- Link Type
  (IT connection, equipment or part delivery…)

Interface Criticality Depending on the Asset Type:

Potential Maximum Safety Impact	Group 1	Group 2	Group 3	Group 4
A/C unsafe condition	Critical	Essential	Essential	Routine
Reduction of safety margins	Essential	Routine	Routine	Routine

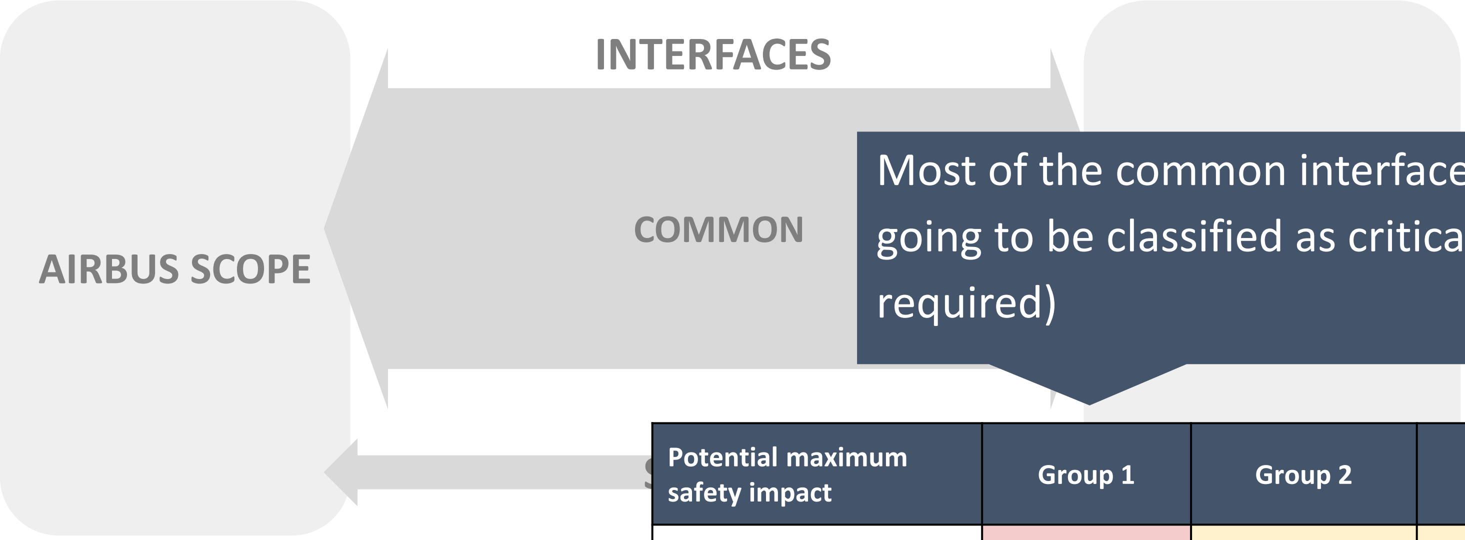
Thoroughness of the Security Assessment: (supplier role in interface)

Cyber Maturity framework

Interface Criticality	Security Activities - IT link
Critical	Detailed Security Risk Assessment Cyber Maturity "level 3" for supplier organization
Essential	Cyber Maturity "level 2" for supplier organization
Routine	Cyber Maturity "level 1" for supplier organization

Ref. "Identification and Classification guidance for Part-IS organizations in interface, 29th August 2024", Dassault and Airbus, for EUROCAE WG-72 / RTCA SC-216 committees (ED-ISMS)

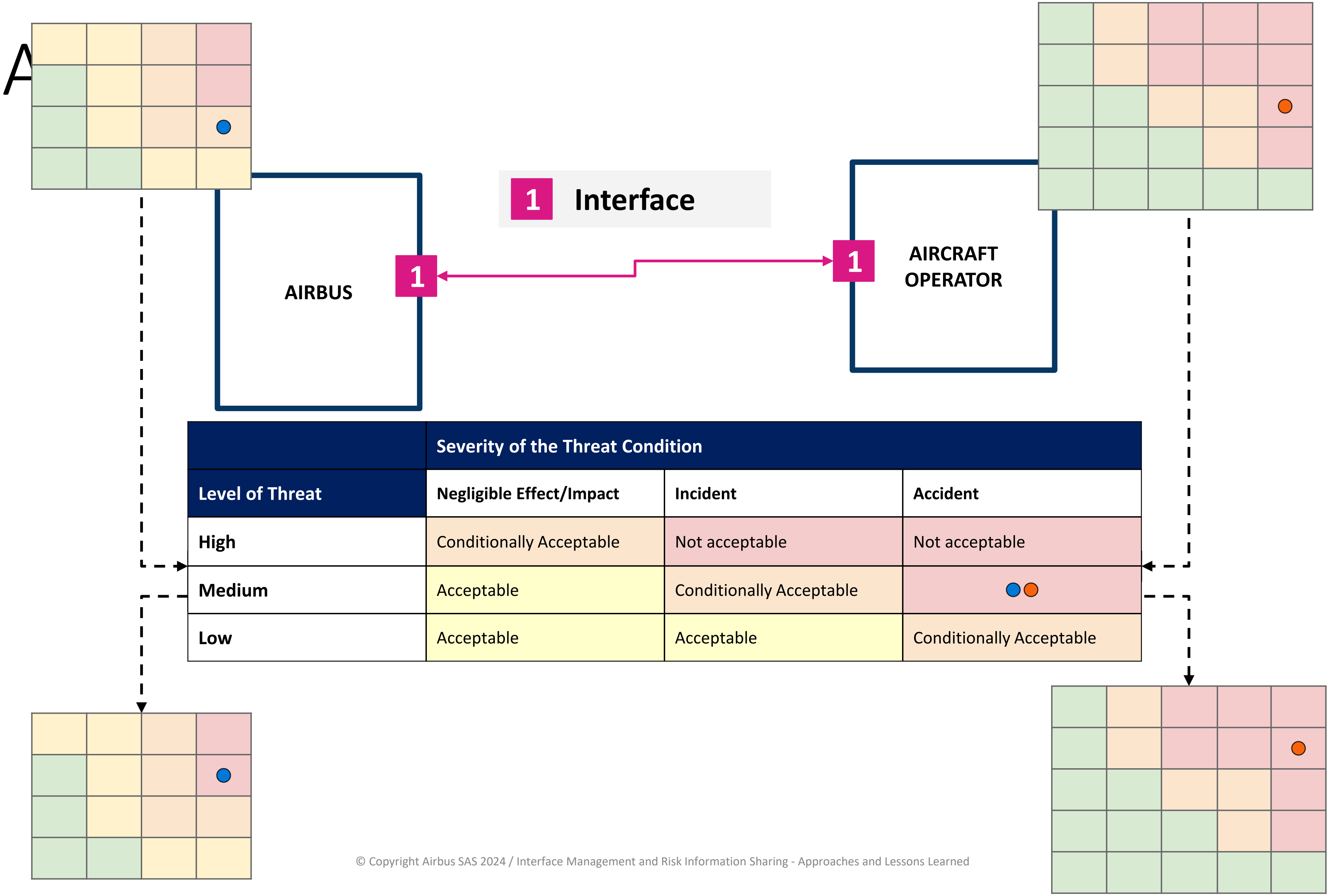
Interplay



Most of the common interfaces are going to be classified as critical (SRA required)

Potential maximum safety impact	Group 1	Group 2	Group 3	Group 4
A/C unsafe condition	Critical	Essential	Essential	Routine
Reduction of safety margins	Essential	Routine	Routine	Routine

Q & A



	Severity of the Threat Condition		
Level of Threat	**Negligible Effect/Impact**	**Incident**	**Accident**
High	Conditionally Acceptable	Not acceptable	Not acceptable
Medium	Acceptable	Conditionally Acceptable	● ●
Low	Acceptable	Acceptable	Conditionally Acceptable

External Reporting under Part-IS

Part-IS Implementation

Workshop

Gerry Ngu is a Senior Expert for Cybersecurity in Aviation, with over 20 years of experience at EASA in various roles, including in the Safety and Certification domain.

Over the past 8 years, Gerry has played a pivotal role in the establishment and operation of the European Cybersecurity Centre for Aviation (ECCSA), while also building and leading the Cyber Threat Intelligence capabilities within EASA.

Andris Sermulins is a Safety Data Manager at EASA, and also Co-chair of the Network of Analysts Data Quality and Taxonomy Working Group.

Andris has more than 10 years of experience in Safety Data Management, as well as extensive experience in flight operations and flight support.

Mandatory reporting

IS.OR.230 Information security external reporting scheme

(a) The organisation shall implement an **information security reporting system** that meets the requirements laid down in Regulation (EU) No 376/2014 and its delegated and implementing acts if such Regulation is applicable to the organisation.

(b) Without prejudice to point (a), the organisation shall ensure that any information security incident or vulnerability, which may represent a **significant risk** to aviation safety, is reported to their competent authority. In addition:

(1) when such an incident or vulnerability **affects an aircraft or associated system or component**, the organisation shall **also report it to the design approval holder**;

(2) when such an incident or vulnerability **affects a system or constituent used by the organisation**, the organisation shall **report it to the organisation responsible for the design of the system or constituent**.

[omitted]

PART-IS Reporting aspects overview 1/2

PART-IS
ANNEX I

Authority Requirements (AR)

IS.AR.200
ISMS

External Reporting

Organisations subject to its oversight & information received through **IS.I.OR.230**

PART-IS
ANNEX II

Organisations Requirements (OR)

IS.OR.215

Internal Reporting

IS.OR.230

External Reporting

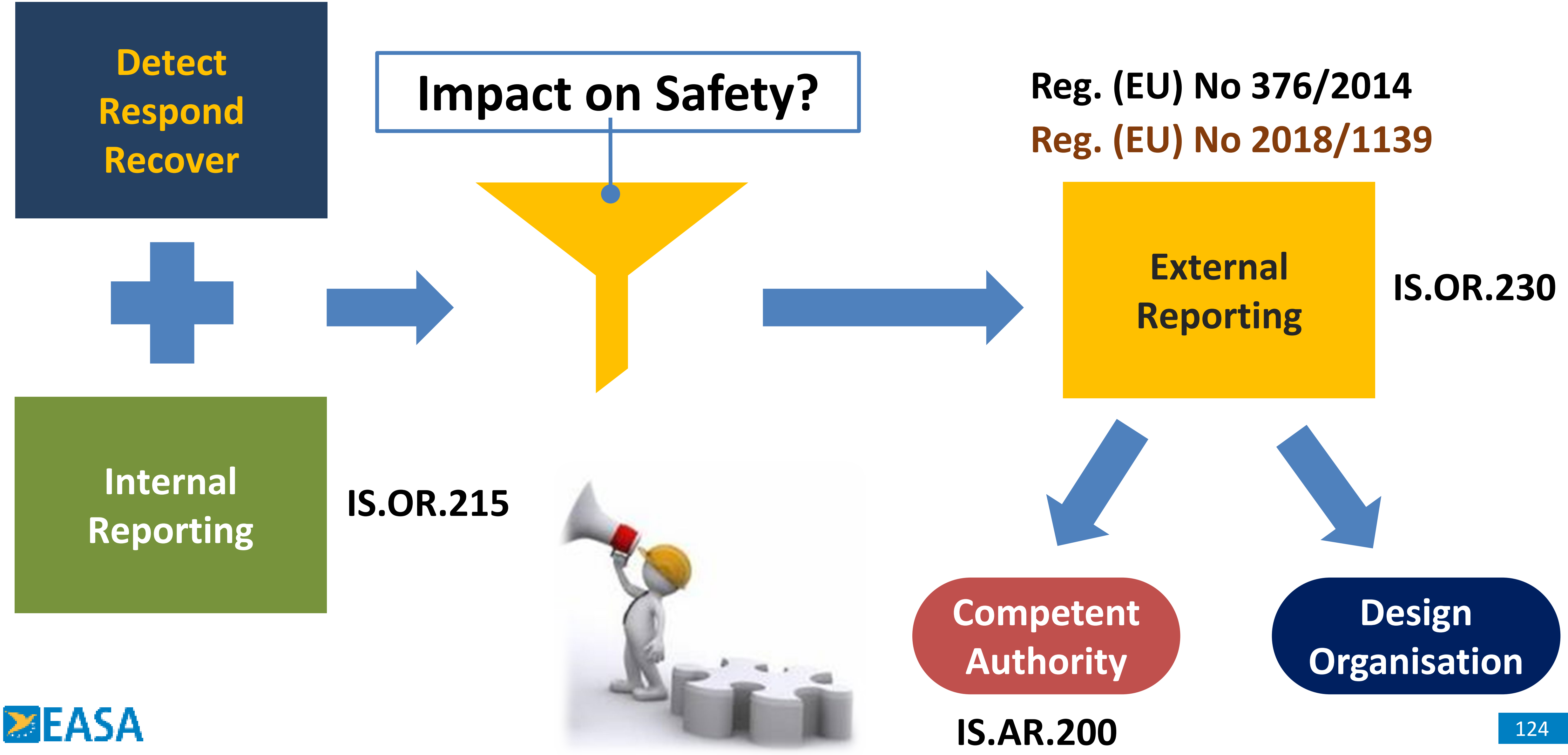
Internal Reporting

Cyber incidents
&
Vulnerabilities with a potential **impact on aviation safety**

External Reporting

Reg (EU) 376/2014
Reg (EU) 2018/1139
Report to:
- Competent Authority
- Design Approval Holder
- Design of system/ constituent
- **Not exceeding 72 h**

PART-IS Reporting aspects overview 2/2



Detect
Respond
Recover

Internal Reporting

IS.OR.215

Impact on Safety?

Reg. (EU) No 376/2014
Reg. (EU) No 2018/1139

External Reporting

IS.OR.230

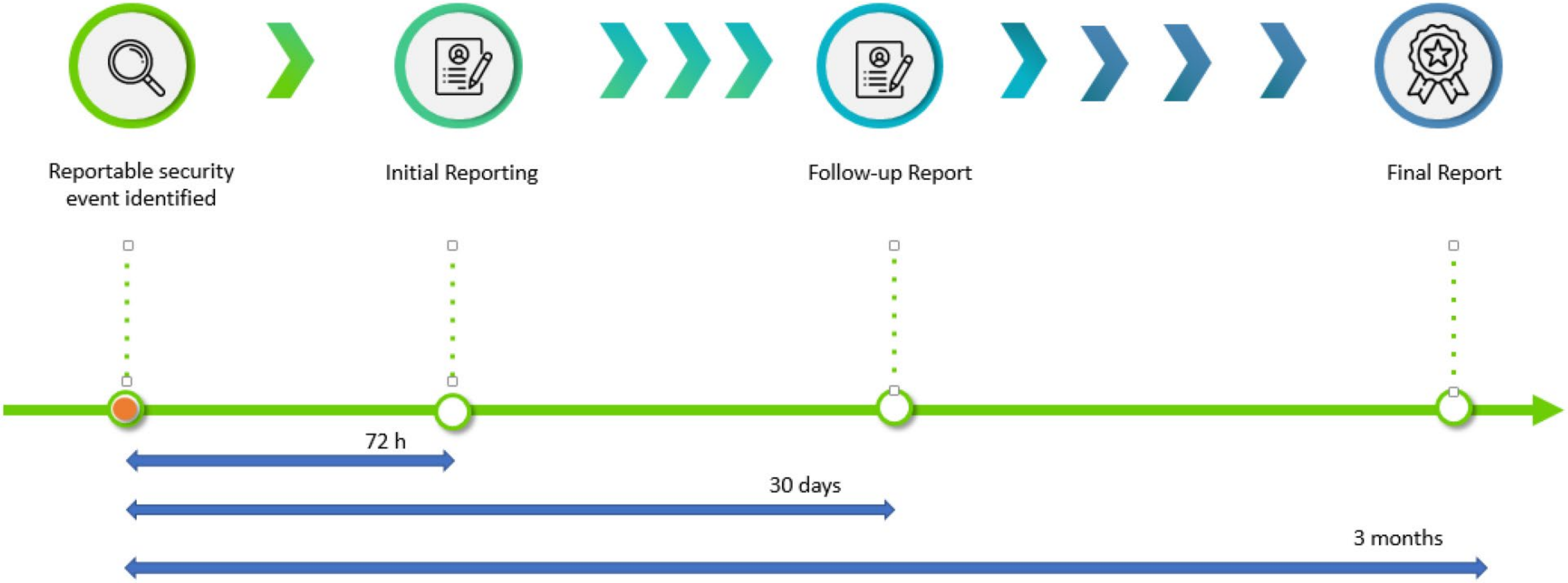
Competent Authority

IS.AR.200

Design Organisation

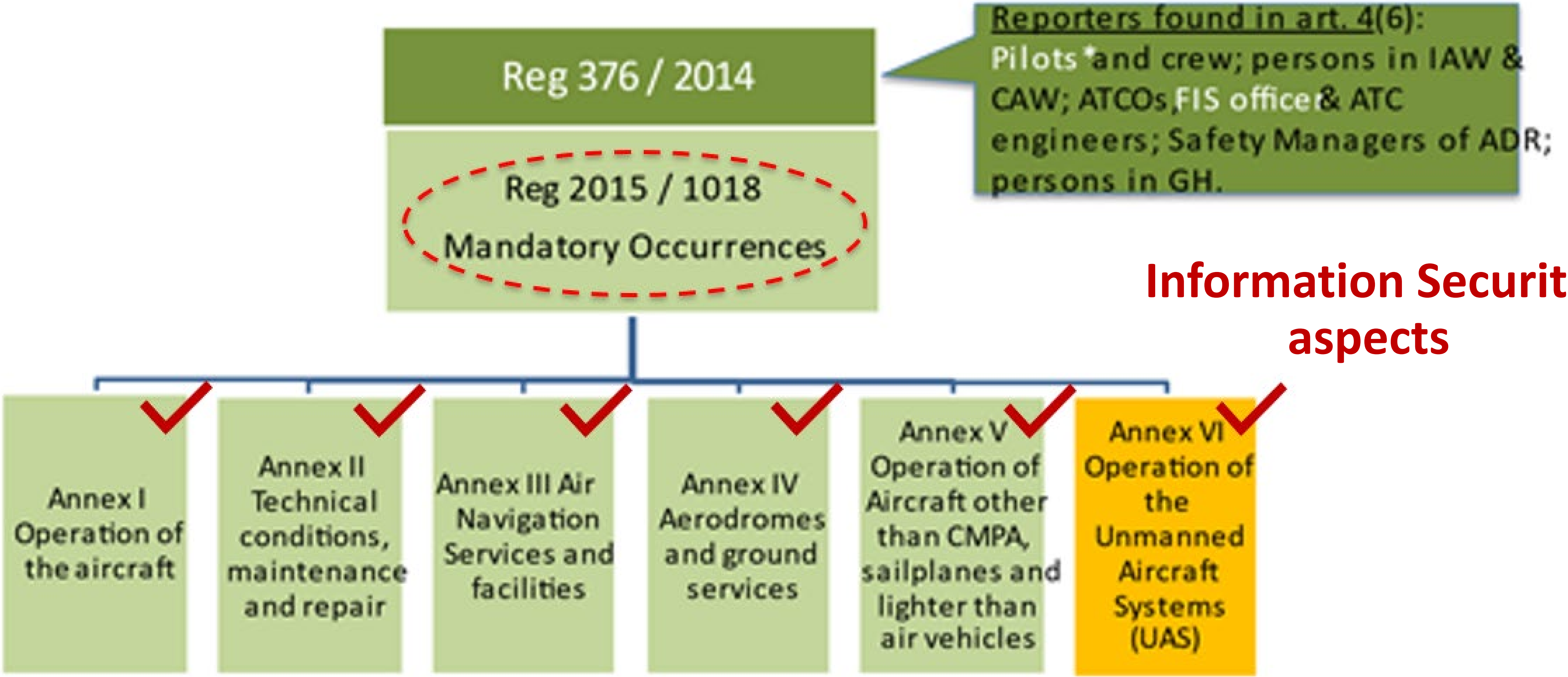
EASA

ED-206 6.4.2 Reporting timeline example



Mandatory occurrence reporting (Q4-2025)

Discuss future update EC Reg 376/2014 – 2015/1018 (annexes)



Reg 376 / 2014

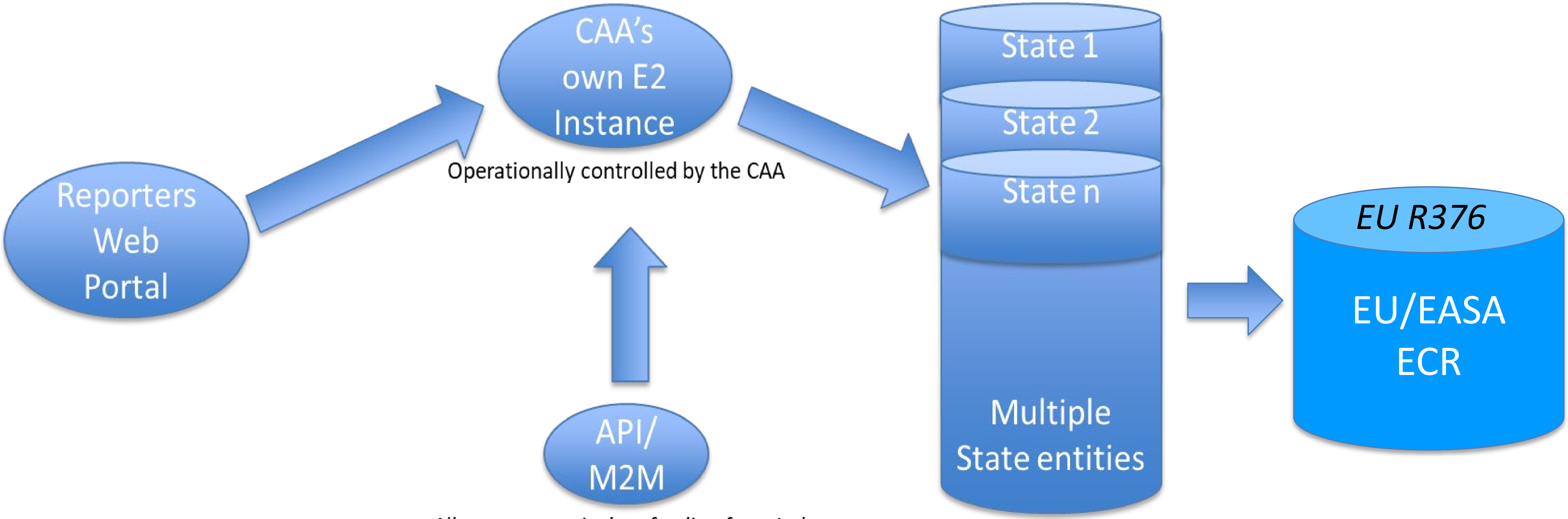
Reporters found in art. 4(6): Pilots *and crew; persons in IAW & CAW; ATCOs, FIS officer & ATC engineers; Safety Managers of ADR; persons in GH.

Reg 2015 / 1018 Mandatory Occurrences

- ✓ Annex I Operation of the aircraft
- ✓ Annex II Technical conditions, maintenance and repair
- ✓ Annex III Air Navigation Services and facilities
- ✓ Annex IV Aerodromes and ground services
- ✓ Annex V Operation of Aircraft other than CMPA, sailplanes and lighter than air vehicles
- ✓ Annex VI Operation of the Unmanned Aircraft Systems (UAS)

Information Security aspects

ECCAIRS2 enhanced scope for EU/EASA MS



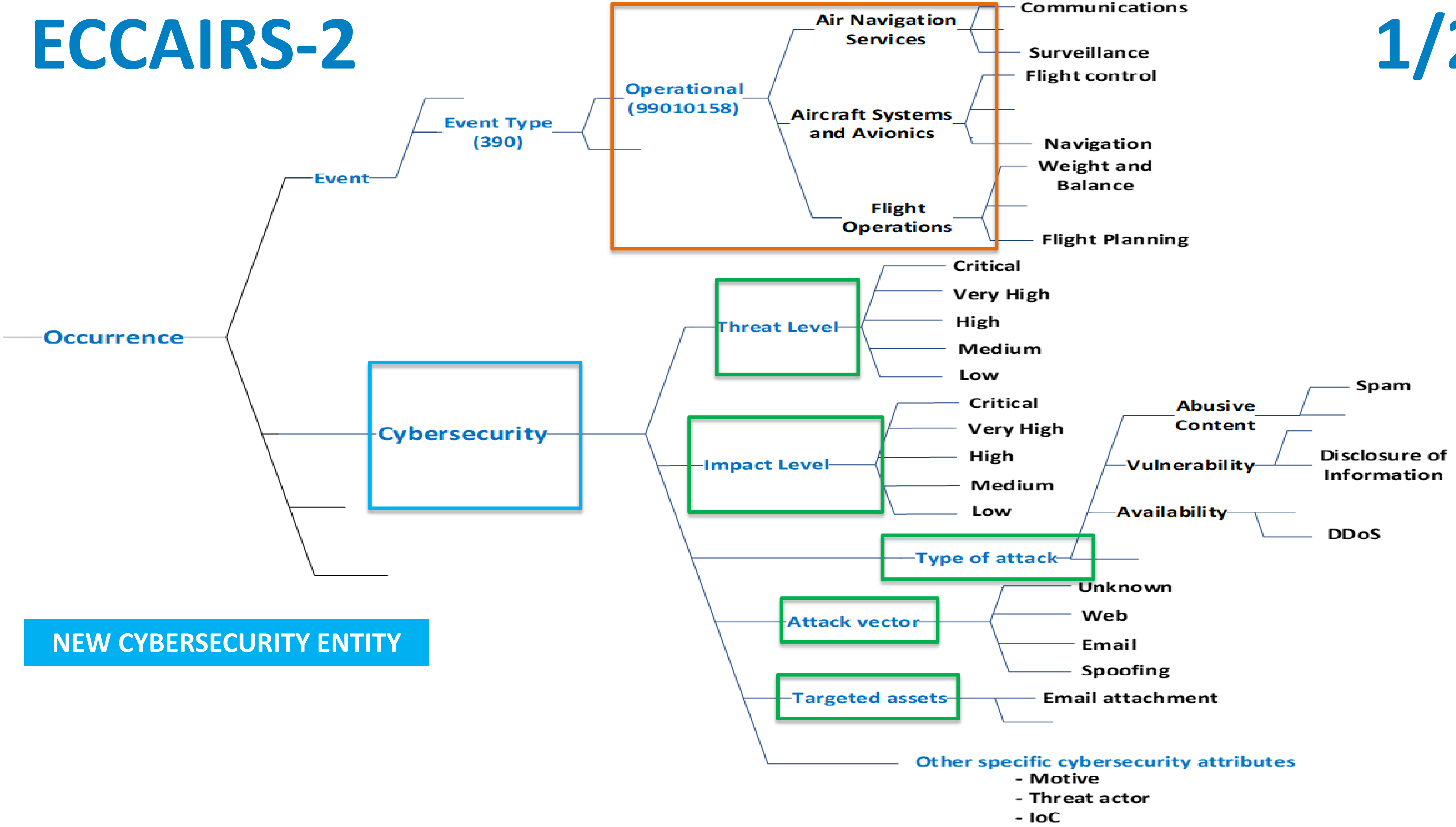
Operationally controlled by the CAA

Allows automatic data feeding from Industry Reporters' SMS software into E2 of their CAA

Central EU Cloud E2 Storage, with separate "State databases"

ECCAIRS-2

1/2



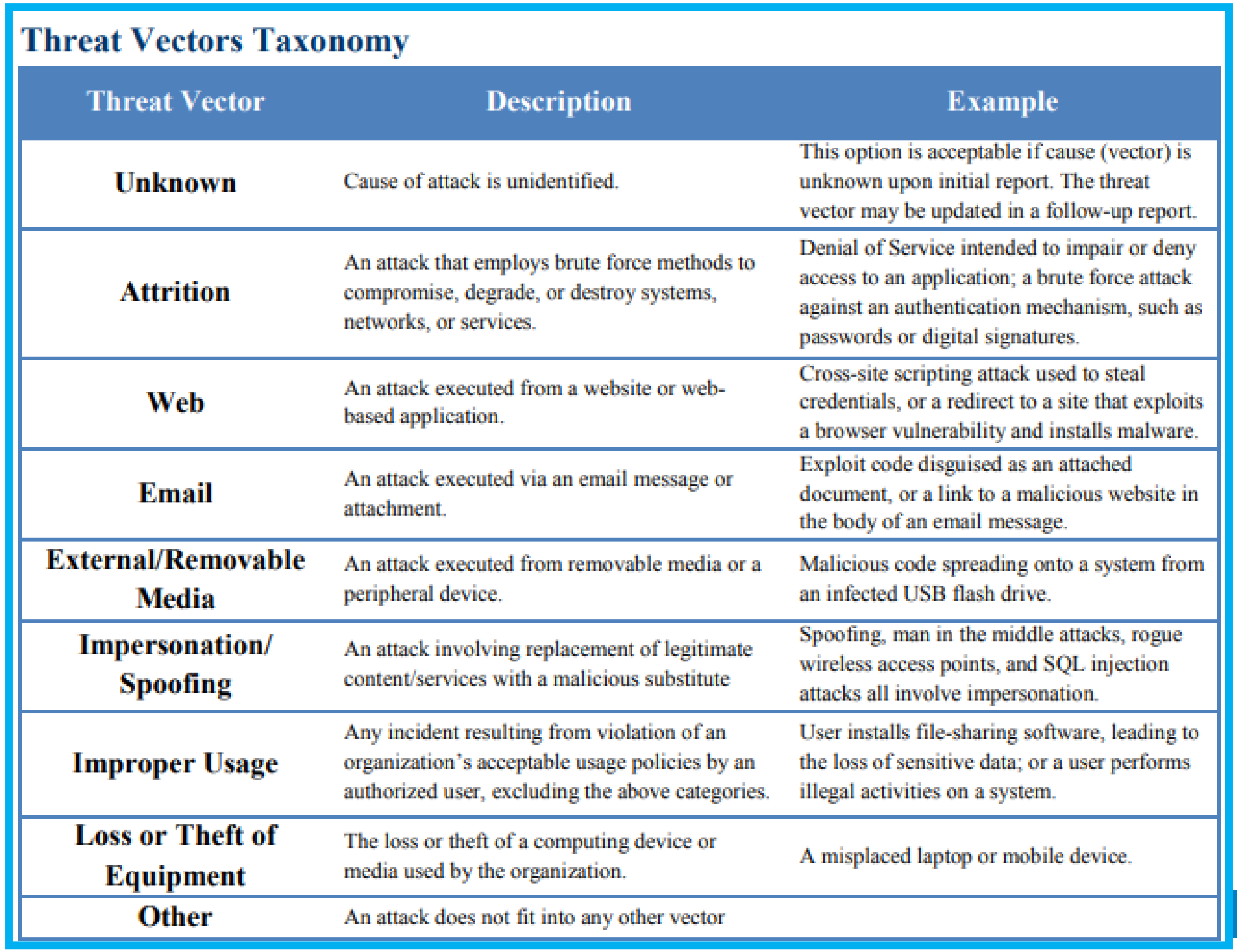
NEW CYBERSECURITY ENTITY

Implementation in ECCAIRS2 2/2

Discussions: EASA/ NoCA (WG1)/ NoA (DQT-WG)

New entities to consider: *Examples in brackets*

- Source of detection (e.g. Employee report)
- Detection method (Mail Security Gateway)
- Type of incident (Phishing)
- Targeted assets (Employee email accounts)
- Attack vector (Email attachment)
- Indicator of Compromise (IoC) (Malicious email attachment (SHA256 hash: xxx123...))
- Vulnerabilities exploited (xxx/none)
- Threat actor (External actor/unknown)
- Motive (Credential theft)

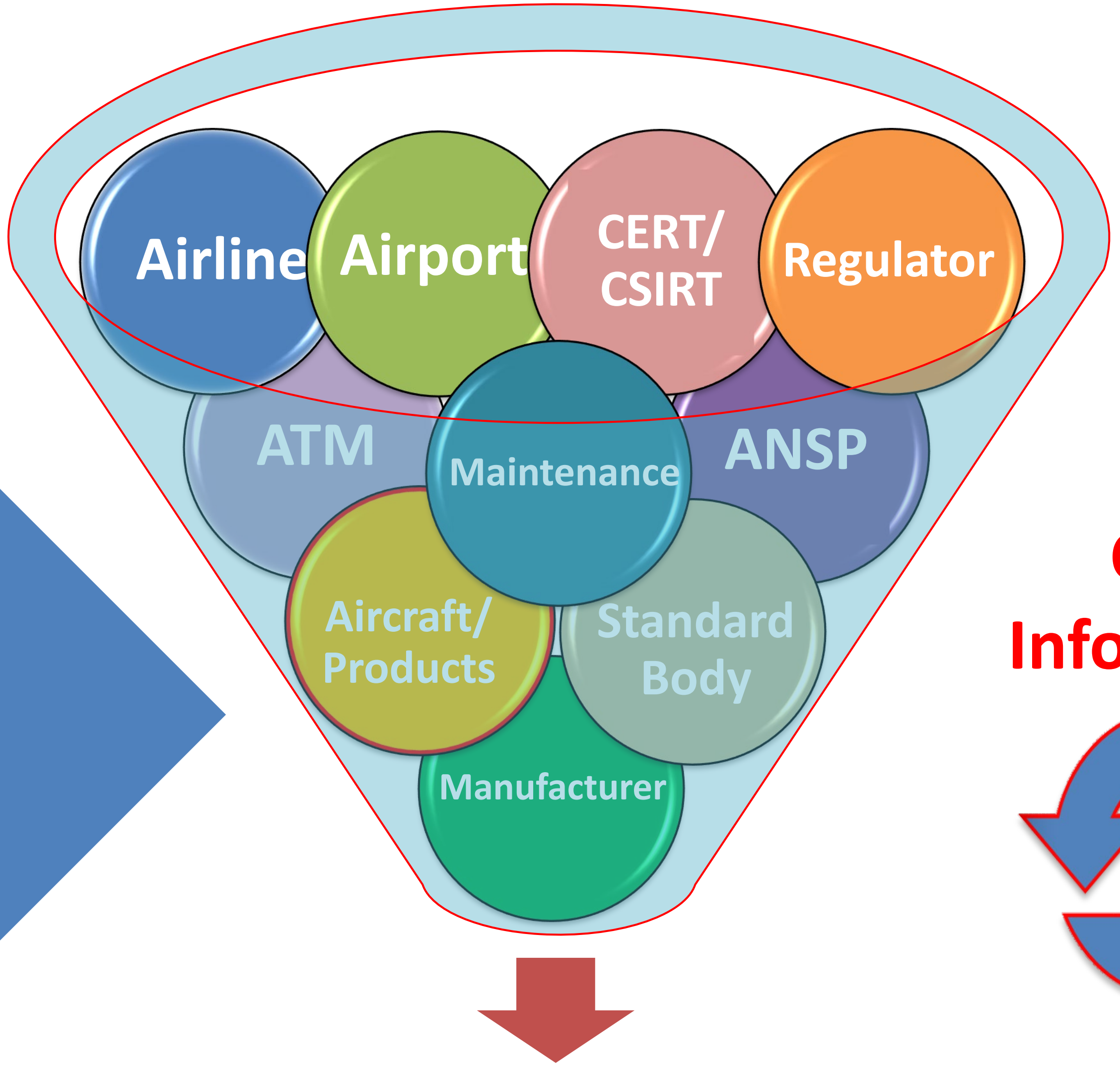


Threat Vectors Taxonomy

Threat Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The threat vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive.
Impersonation/ Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack does not fit into any other vector	

Goal information sharing

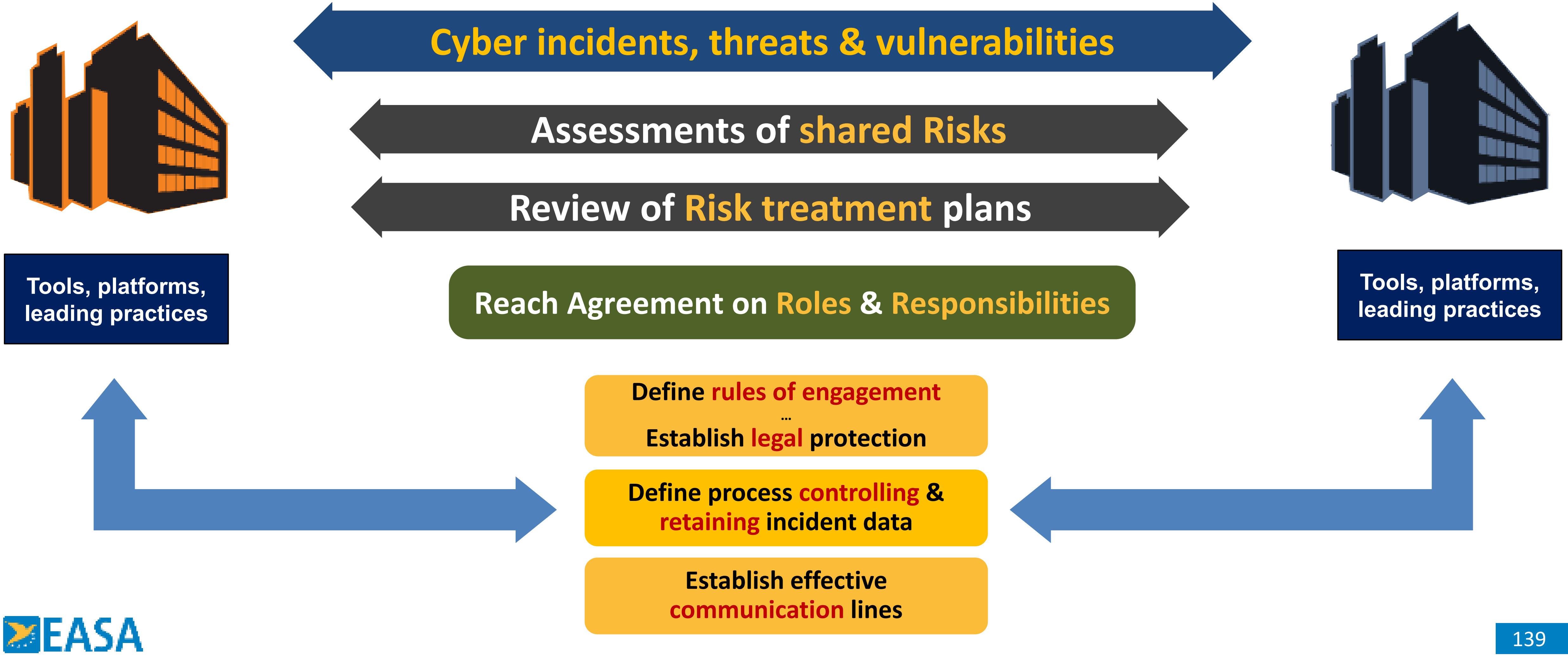
The cyber threat landscape is constantly shifting in the aviation sector…
It is important to share in a timely & rapid manner
cybersecurity related information



Resilience of the Aviation ECO-System

CTI & Info Sharing

Sharing information between organisations



Cyber incidents, threats & vulnerabilities

Assessments of shared Risks

Review of Risk treatment plans

Reach Agreement on Roles & Responsibilities

Tools, platforms, leading practices

Tools, platforms, leading practices

Define rules of engagement
…
Establish legal protection

Define process controlling & retaining incident data

Establish effective communication lines

ISO/IEC 27000 in relation to Part-IS

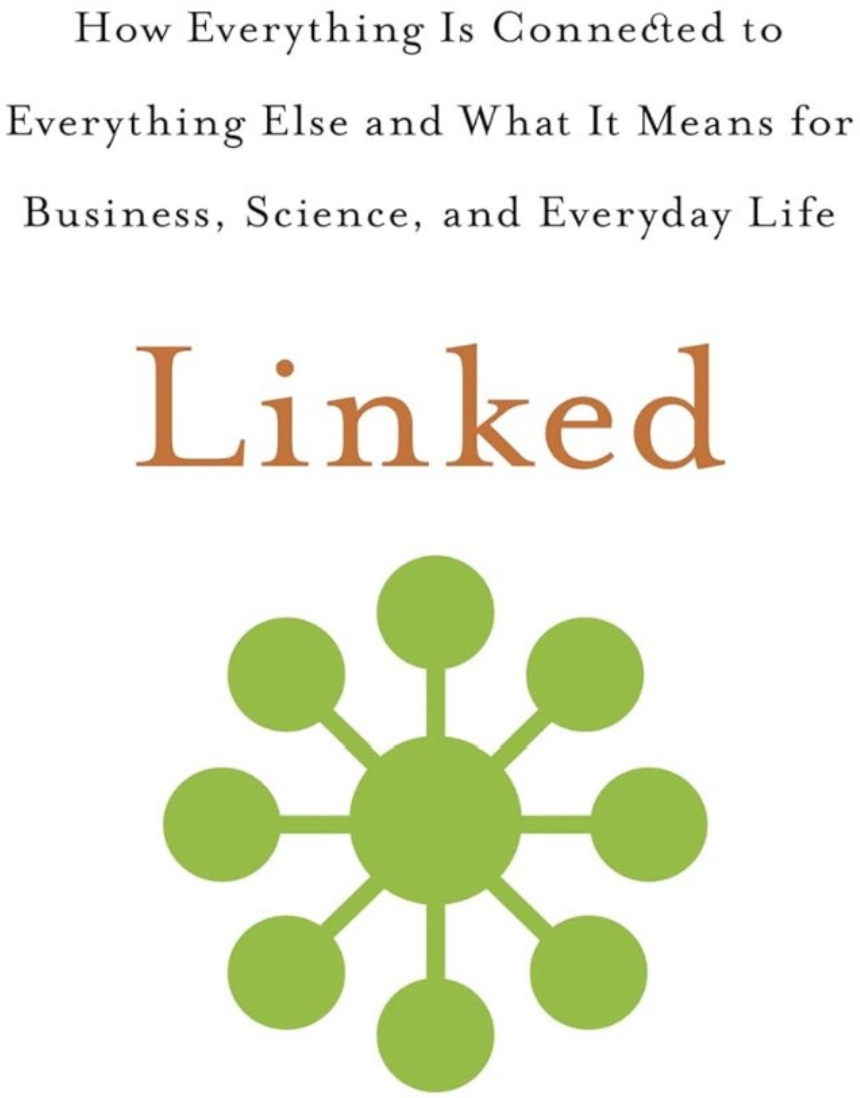
Part-IS Implementation

Workshop

EASA

Jean-Paul Moreaux has been a key figure in cybersecurity since the mid-90s, joining EASA in 2015 as Principal in cybersecurity in aviation after 27 years at Airbus, where he worked on avionics, ARINC protocols, and cybersecurity standards.

He has chaired EUROCAE's WG-72 for Aviation Cybersecurity and has been pivotal in ICAO and European cybersecurity regulations, including the recent Part-IS.



How Everything Is Connected to
Everything Else and What It Means for
Business, Science, and Everyday Life

Linked

Introduction

Some Expectation Management

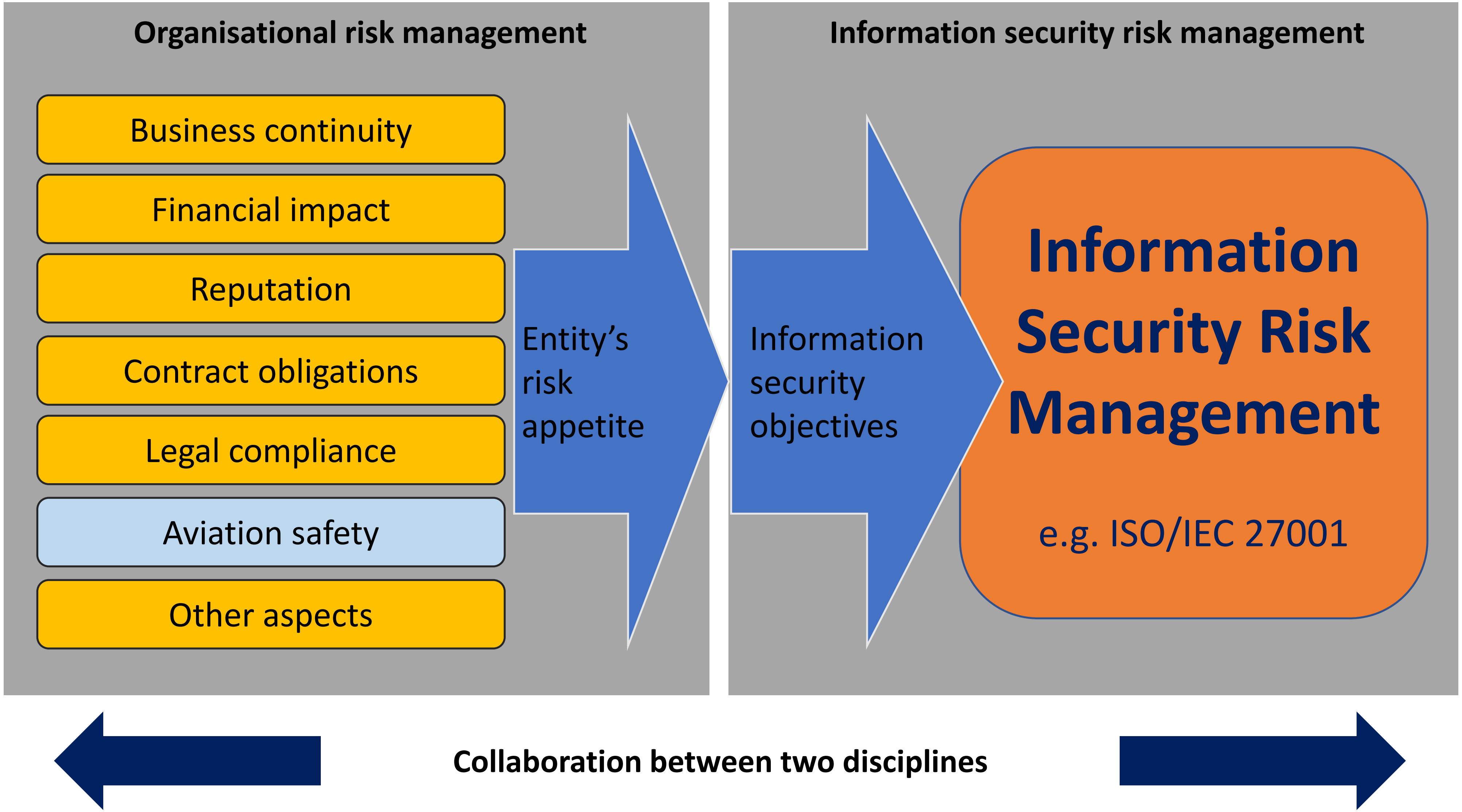
→ **I do not plan to interfere with other speakers by talking about**

- → ISO 27001 Requirements and their relationship to Part-IS
- → Details of Part-IS and the respective applicability

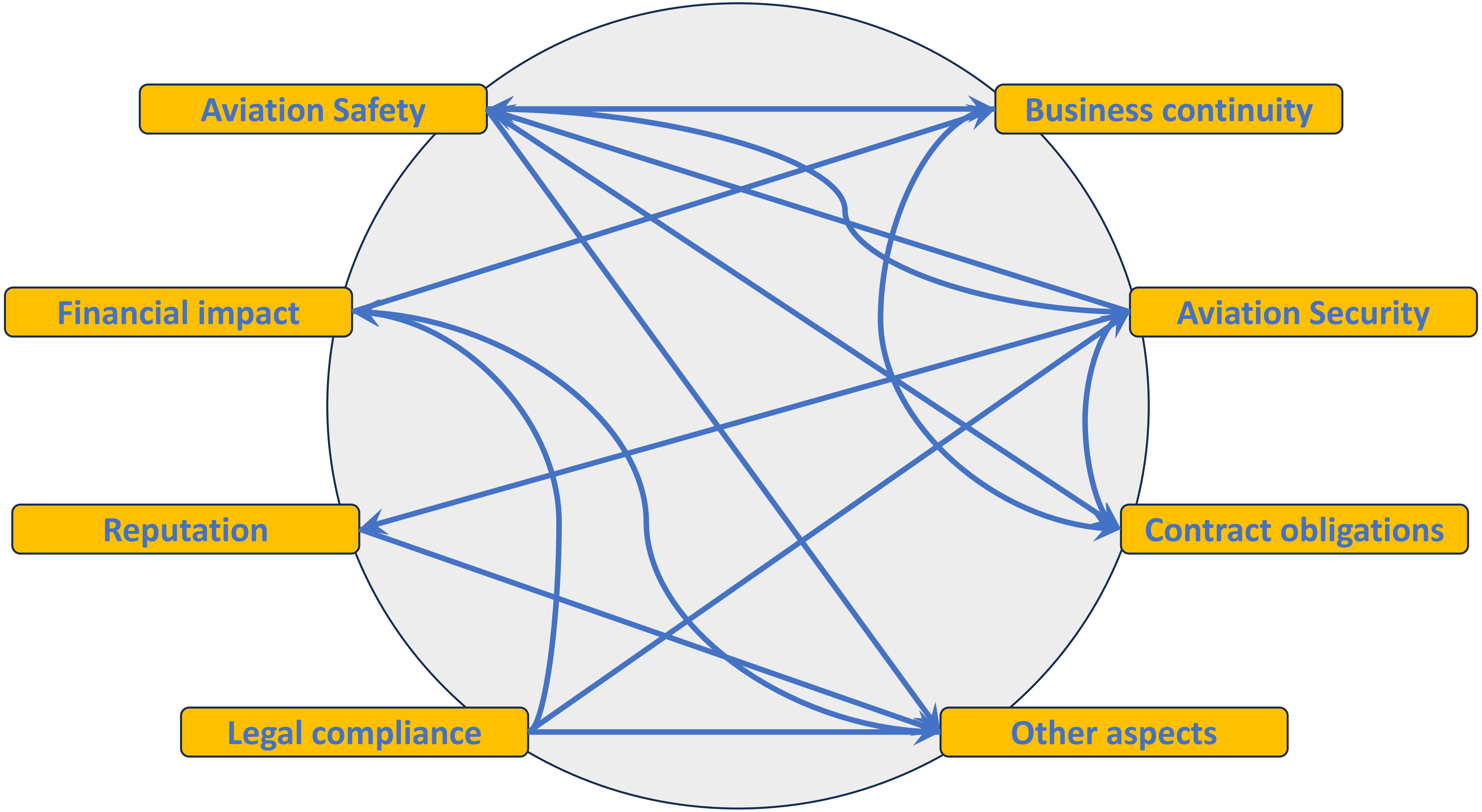
→ **What should not be underestimated, though, is**

- → The width of organisational risks driving Information Security Objectives
- → The notion of a System within a System-of-Systems
- → The complexity of all interacting organisational Risk Assessments

Safety is just one more Organisational Risk

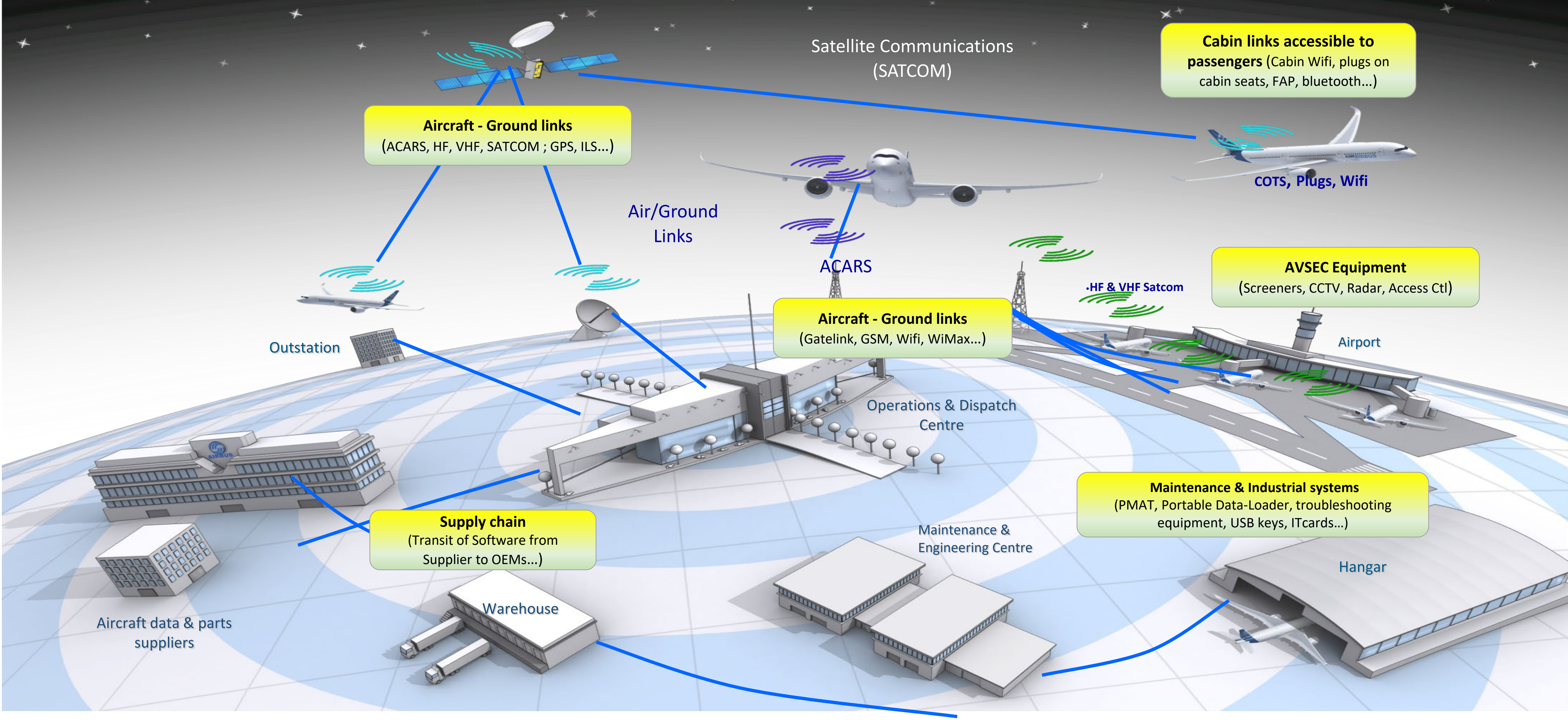

Organisational risk management
Business continuity
Financial impact
Reputation
Contract obligations
Legal compliance
Aviation safety
Other aspects
Entity's risk appetite
Information security risk management
Information security objectives
Information Security Risk Management
e.g. ISO/IEC 27001
Collaboration between two disciplines

In Aviation, Everything is Linked to Everything Else!



Nobody is an Island: System-of-Systems Notion

Aviation is a System-of-Systems



Cabin links accessible to passengers (Cabin Wifi, plugs on cabin seats, FAP, bluetooth…)

Aircraft - Ground links
(ACARS, HF, VHF, SATCOM ; GPS, ILS…)

Aircraft - Ground links
(Gatelink, GSM, Wifi, WiMax…)

AVSEC Equipment
(Screeners, CCTV, Radar, Access Ctl)

Maintenance & Industrial systems
(PMAT, Portable Data-Loader, troubleshooting equipment, USB keys, ITcards…)

Supply chain
(Transit of Software from Supplier to OEMs…)

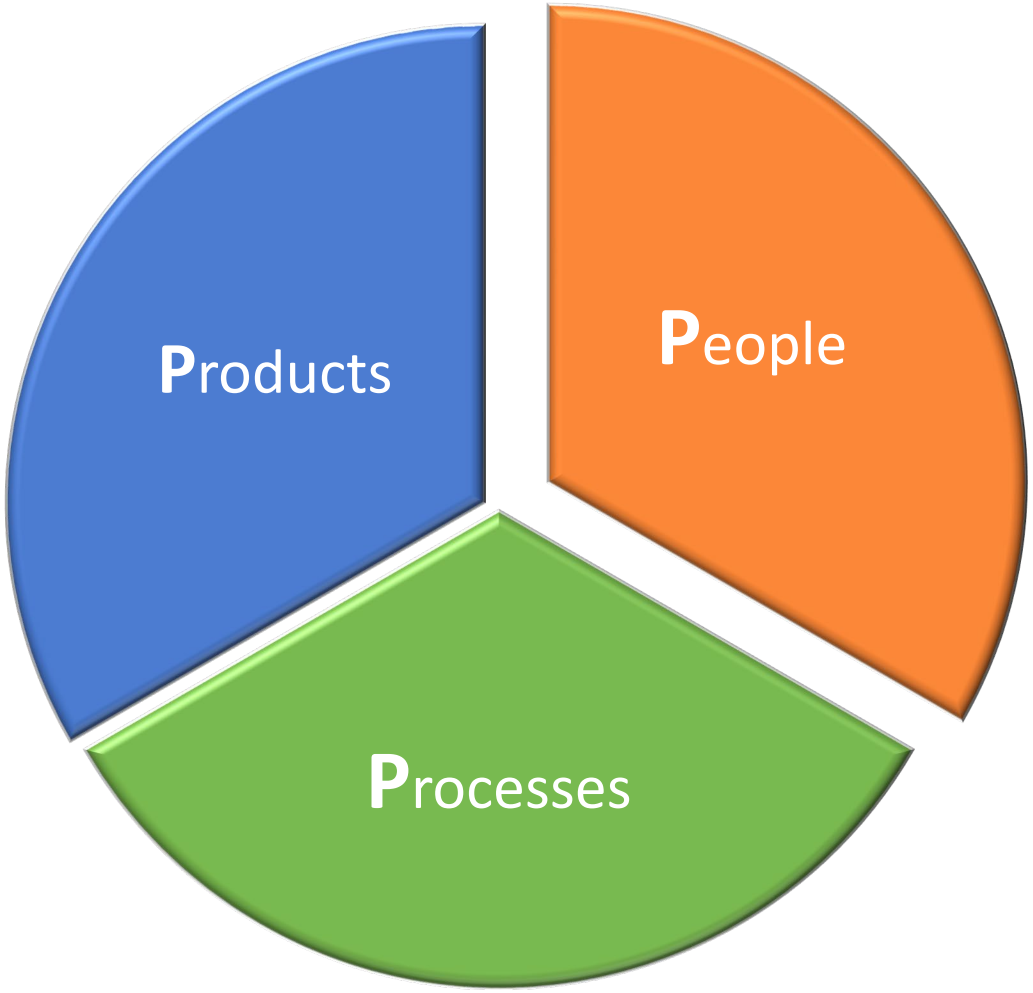
Satellite Communications (SATCOM)
COTS, Plugs, Wifi
Air/Ground Links
ACARS
•HF & VHF Satcom
Airport
Outstation
Operations & Dispatch Centre
Maintenance & Engineering Centre
Hangar
Warehouse
Aircraft data & parts suppliers

EASA

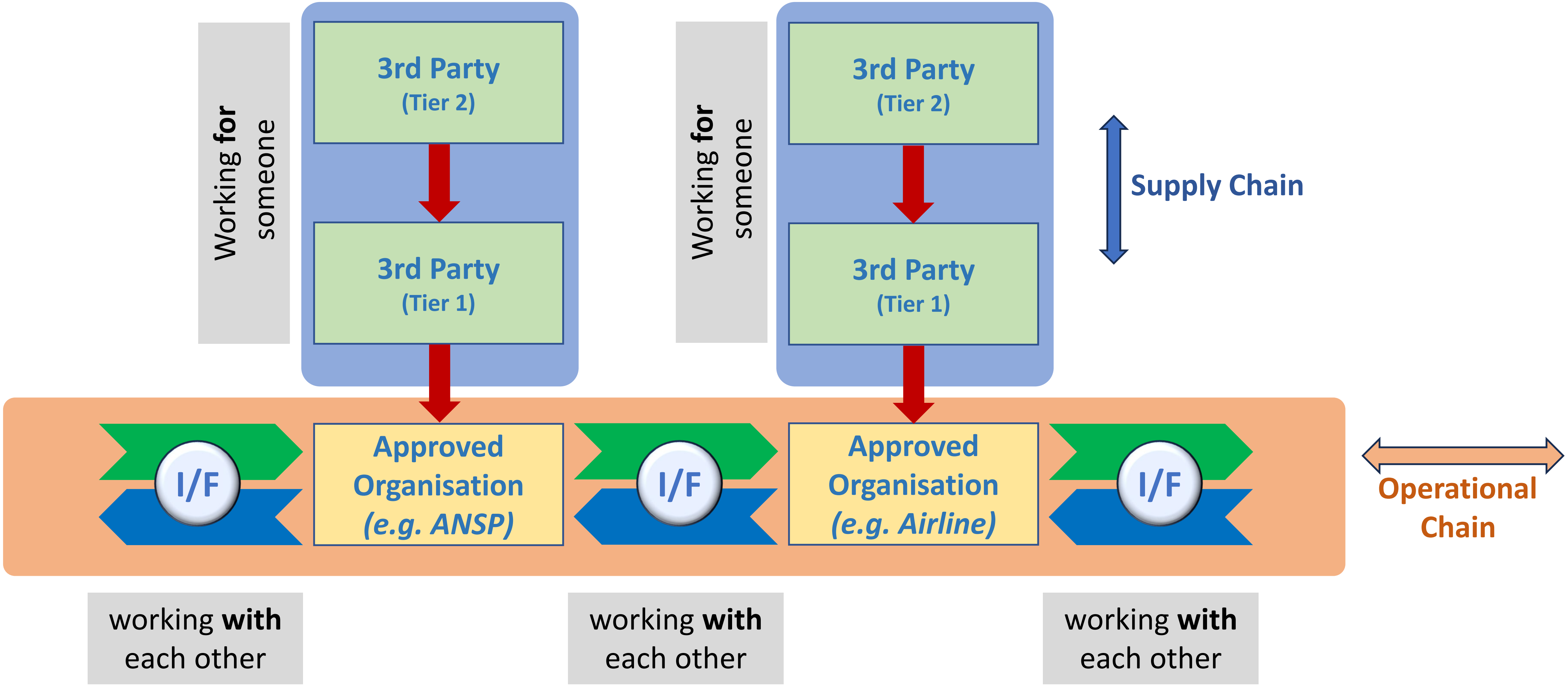
Courtesy Airbus

A System is

- → Composed of
  - → People, Processes, Products
- → Functionally structured
  - → As a System of Systems
- → Connected to Other Systems
  - → Horizontally, Vertically, or Both



STORM: An Risk-Sharing System-of-Systems


Working **for** someone
3rd Party
(Tier 2)
3rd Party
(Tier 1)
Working **for** someone
3rd Party
(Tier 2)
3rd Party
(Tier 1)
Supply Chain
I/F
Approved Organisation *(e.g. ANSP)*
I/F
Approved Organisation *(e.g. Airline)*
I/F
Operational Chain
working **with** each other
working **with** each other
working **with** each other

Yet Another Dimension: Interacting Risk Types

Risk Management is Interconnected

→ Safety Management

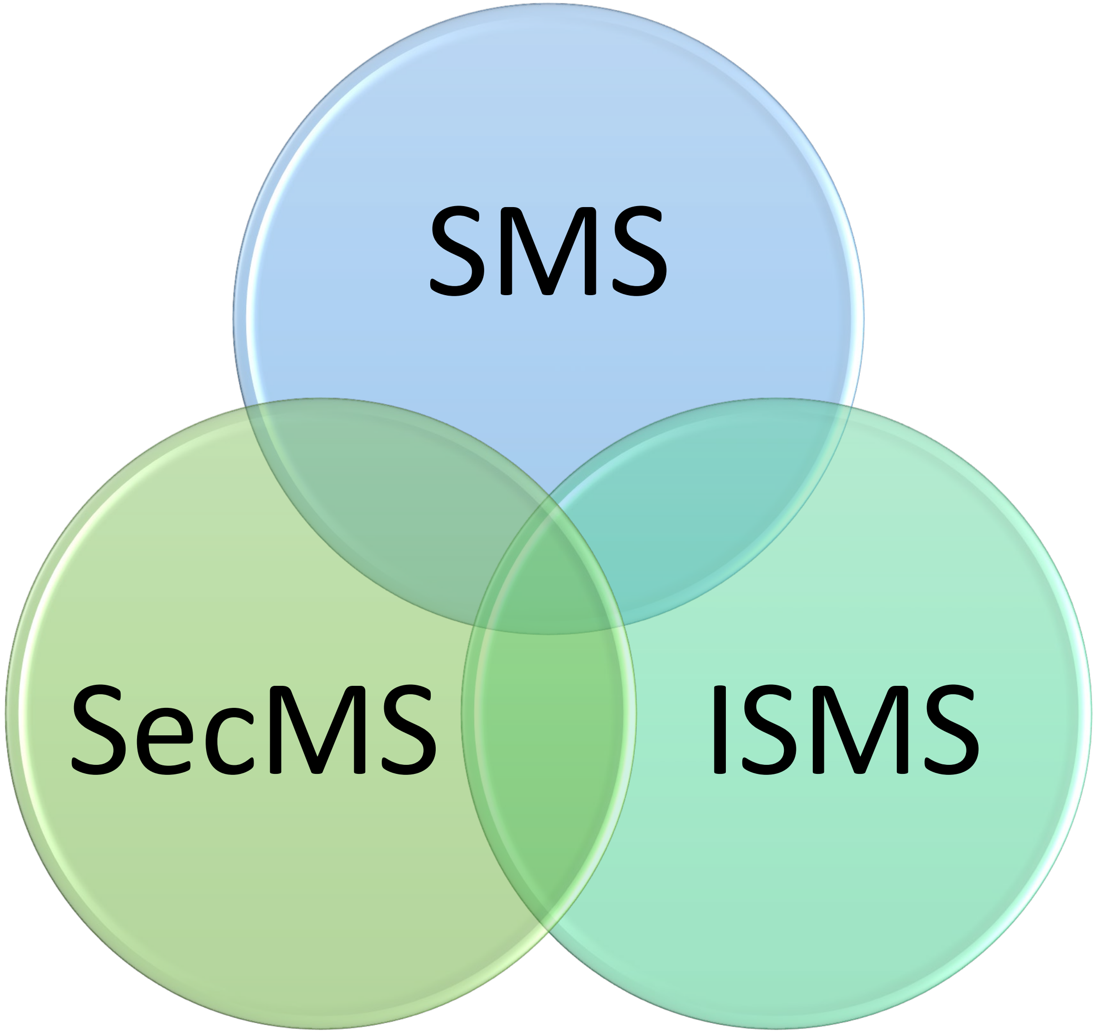
- **SMS**, ICAO Doc 9859

→ Aviation Security Management

- **SecMS**, ICAO Doc 8973

→ Information Security Management

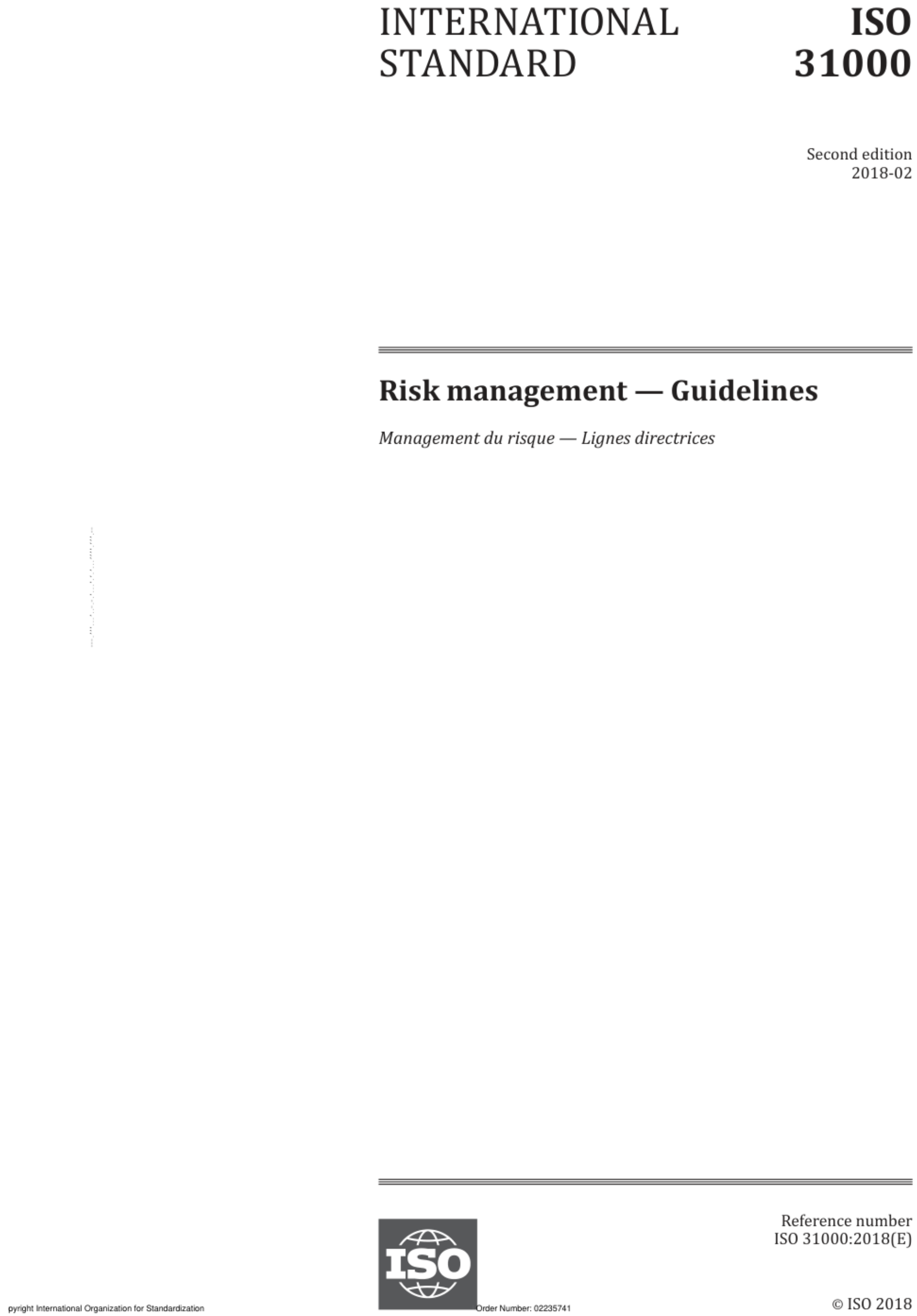
- **ISMS**, ICAO Doc 10204 (in publication)
- **ISMS,** EU/Part-IS



Comparison of Aviation Management Systems

SMS (Annex 19)	SeMS (Annex 17)	ISMS (ISO 27001-2013)
Effects-based risk-managed	**Threat**-based risk-managed (Plan-Do-Check-Act)	**Effects**-based risk-managed (Plan-Do-Check-Act)
1.1 Management commitment and responsibility	**1. Management commitment**	**5.1 Leadership and Commitment**
1.2 Safety accountabilities	3. Accountability and responsibilities	5.2 Policy
1.3 Appointment of key safety personnel		5.3 Roles, responsibilities and authorities
1.4 Coordination of emergency response planning	**6. Incident response**	**16. Incident response**
1.5 SMS documentation		7.5 Documented Information
2.1 Hazard identification **2.2 Safety risk assessment and mitigation**	**2. Threat and risk management**	**11.1 Impact and Threat Management Vulnerability Management**
3.1 Safety performance monitoring and measurement	**5. Performance monitoring, assessment and reporting**	**12.4 Performance monitoring, and assessment (Logging, Audits & Reviews, Security Testing)**
3.2 The management of change	**7. Management of change**	**12.1 Change Management**
3.3 Continuous improvement of SMS	**8. Continuous improvement**	**10.2 Continual improvement**
4.1 Training and education	**9. Training and education**	**7.2/7.3 Training, awareness and competence**
4.1 Safety communication	**10. Communication**	**7.4 Communication**
	4. Resources	7.1 Resources

Some Options: Managing Risks



INTERNATIONAL STANDARD

ISO 31000

Second edition
2018-02

Risk management — Guidelines

Management du risque — Lignes directrices

Reference number
ISO 31000:2018(E)

ISO31000 – Principles, Framework, Process

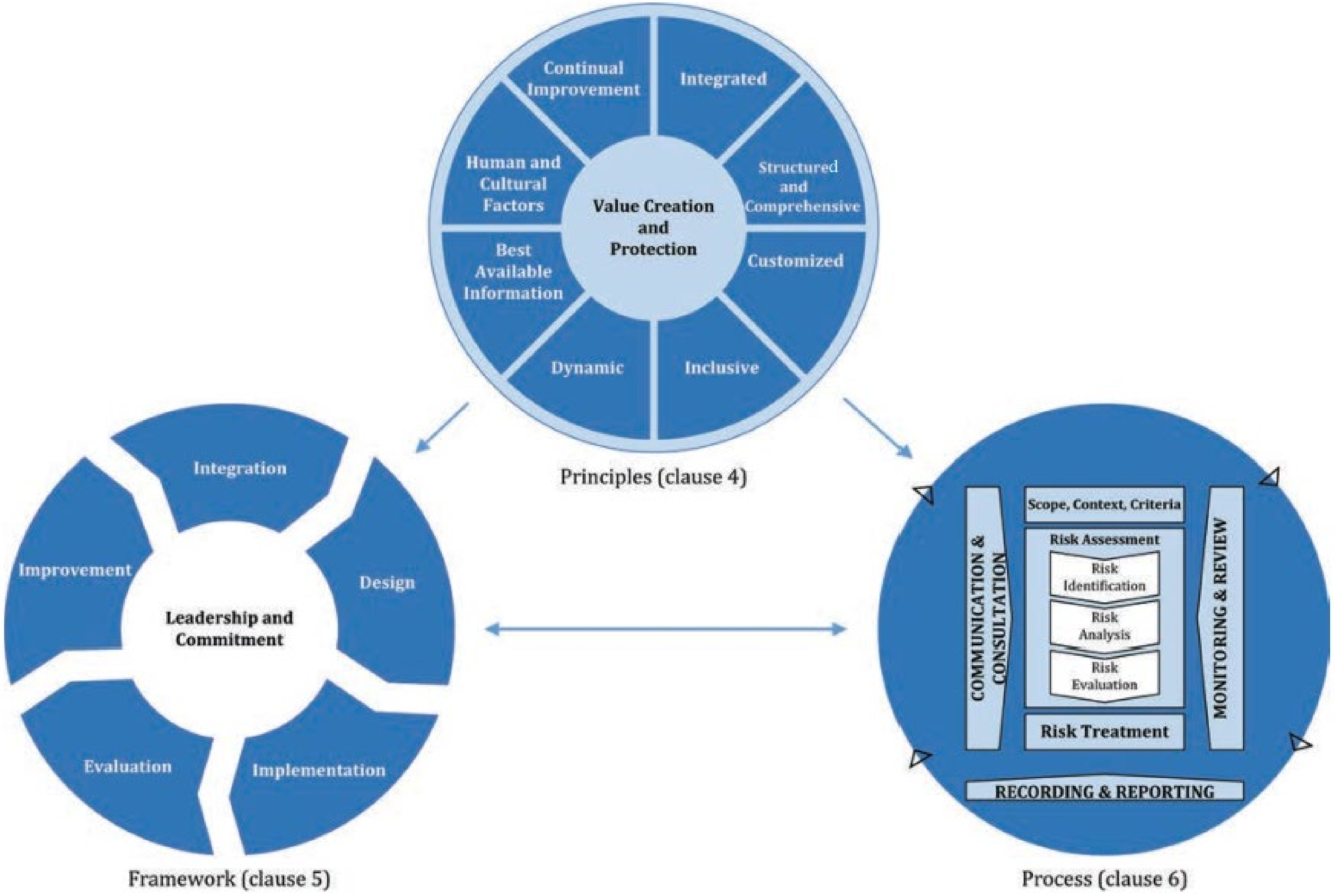
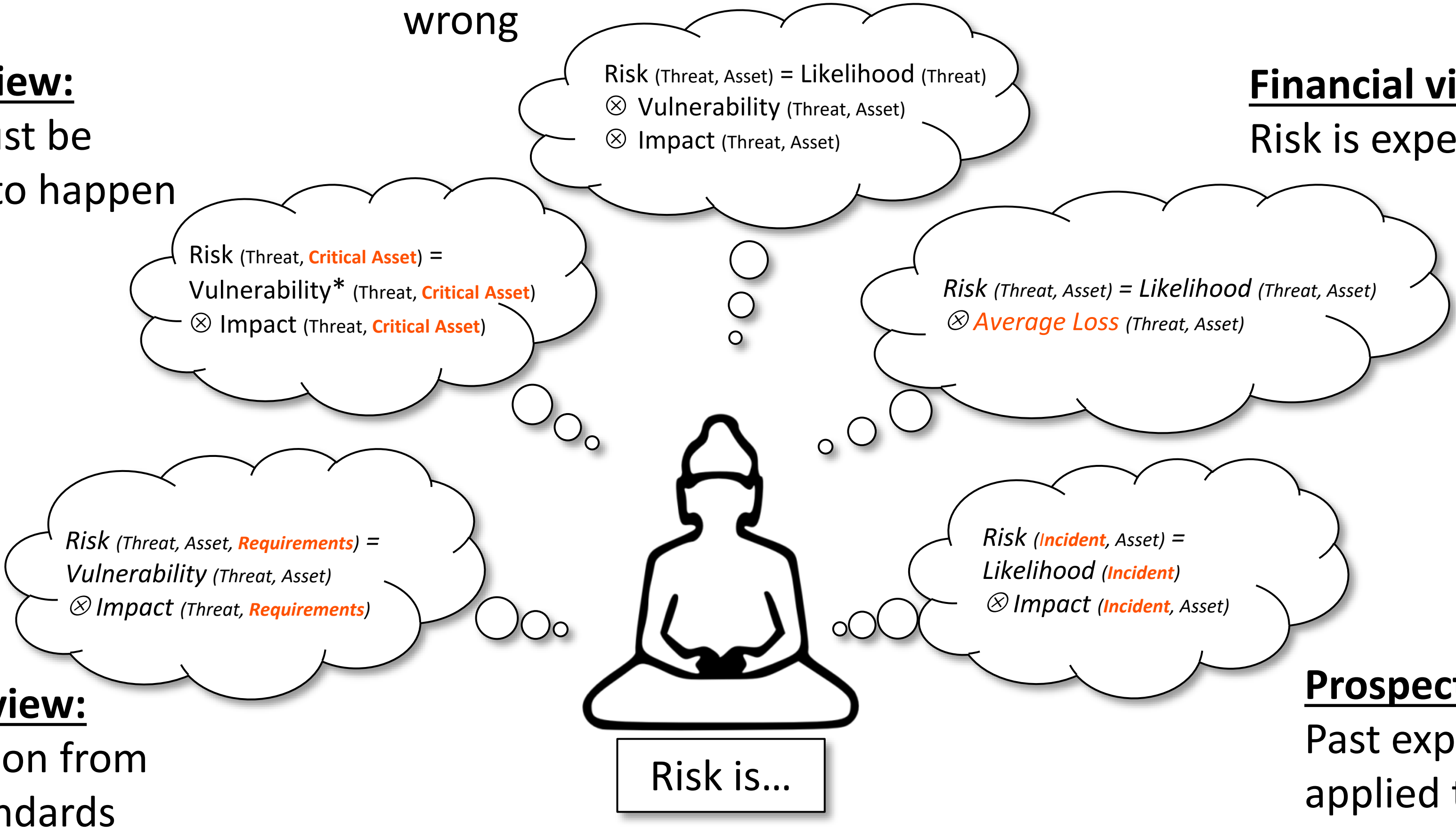


Figure 1 — Principles, framework and process

Which Class of Risk Assessment Do We Use for…?



Threat view:**
What could make things go wrong

Risk (Threat, Asset) = Likelihood (Threat)
⊗ Vulnerability (Threat, Asset)
⊗ Impact (Threat, Asset)

Impact view:
What must be avoided to happen

Risk (Threat, **Critical Asset**) =
Vulnerability* (Threat, **Critical Asset**)
⊗ Impact (Threat, **Critical Asset**)

Financial view:
Risk is expected loss ($)

Risk (Threat, Asset) = Likelihood (Threat, Asset)
⊗ Average Loss (Threat, Asset)

Compliance view:
Risk is deviation from rules and standards

*Risk (Threat, Asset, **Requirements**) =*
Vulnerability (Threat, Asset)
*⊗ Impact (Threat, **Requirements**)*

Prospective view:
Past experience applied to the future

*Risk (**Incident**, Asset) =*
*Likelihood (**Incident**)*
*⊗ Impact (**Incident**, Asset)*

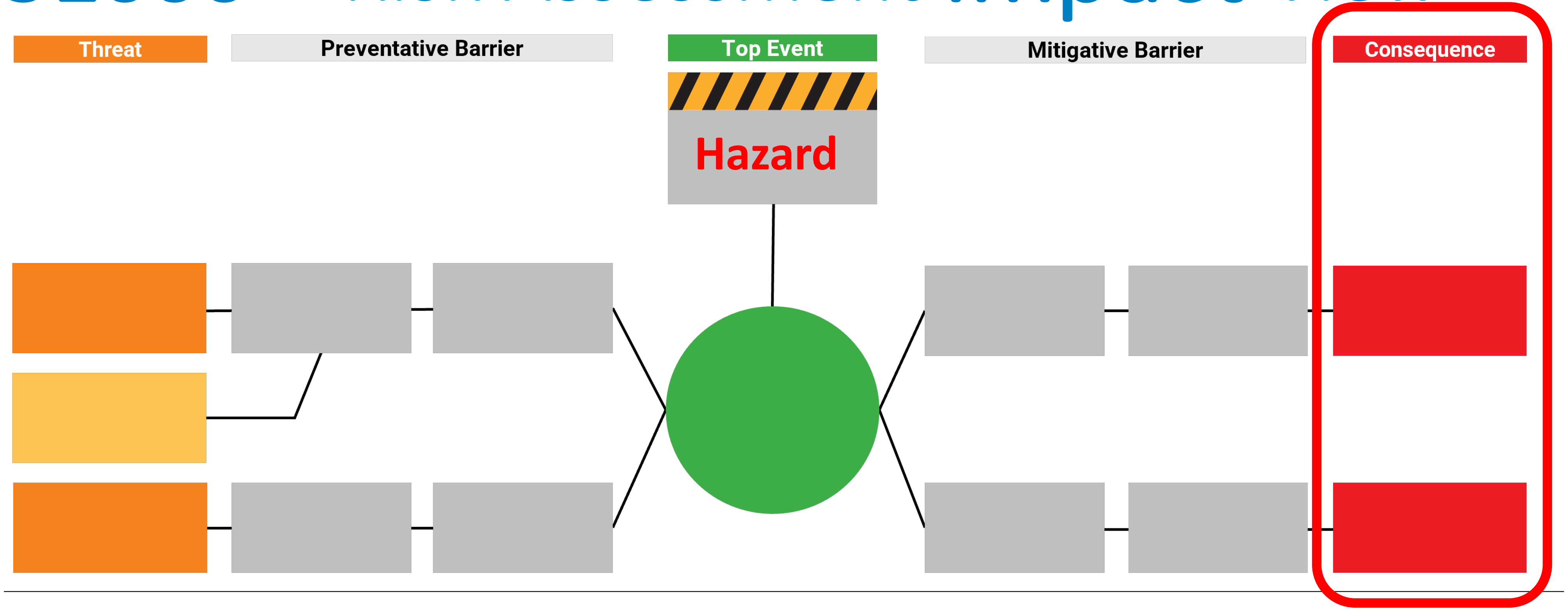
Risk is…

*) In Safety, "Hazard" would replace "Vulnerability"
**) In Safety, the term "Threat" is not limited to intentional acts

Classes from: Dan Iota: „*Current Established Risk Assessment Methodologies and Tools*", 2013

EASA

ISO31000 – Risk Assessment Impact View



Threat

Preventative Barrier

Top Event

Hazard

Mitigative Barrier

Consequence

Double click on the shapes above and input descriptions to complete the elements that make up the Bowtie Diagram. The element descriptions should conform to the questions asked below.

Step 1 Identify the Hazard

Hazard

- Is the hazard specific? (i.e. specify location, size etc if relevant)
- Has it been described in its controlled state?

Step 2 Identify the Top Event

Top Event

- Does it describe how control of the hazard has been lost?
- Does it describe what has been lost?
- Has the event been quantified (if relevant)?

Step 3 Identify Threats

Threat

- Does each threat identified directly cause the Top Event?

Step 4 Identify Consequences

Consequence

- Has it been described as [Damage] due to [Top Event]? (e.g Fire due to loss of containment)

Step 5 Identify Preventative Barriers

Preventative Barrier

- Is it specific?
- Is it capable of completely stopping the Top Event?
- Does it prevent the Threat from occurring?

Step 6 Identify Mitigative Barriers

Mitigative Barrier

- Is it specific?
- Does it prevent or limit the consequence?

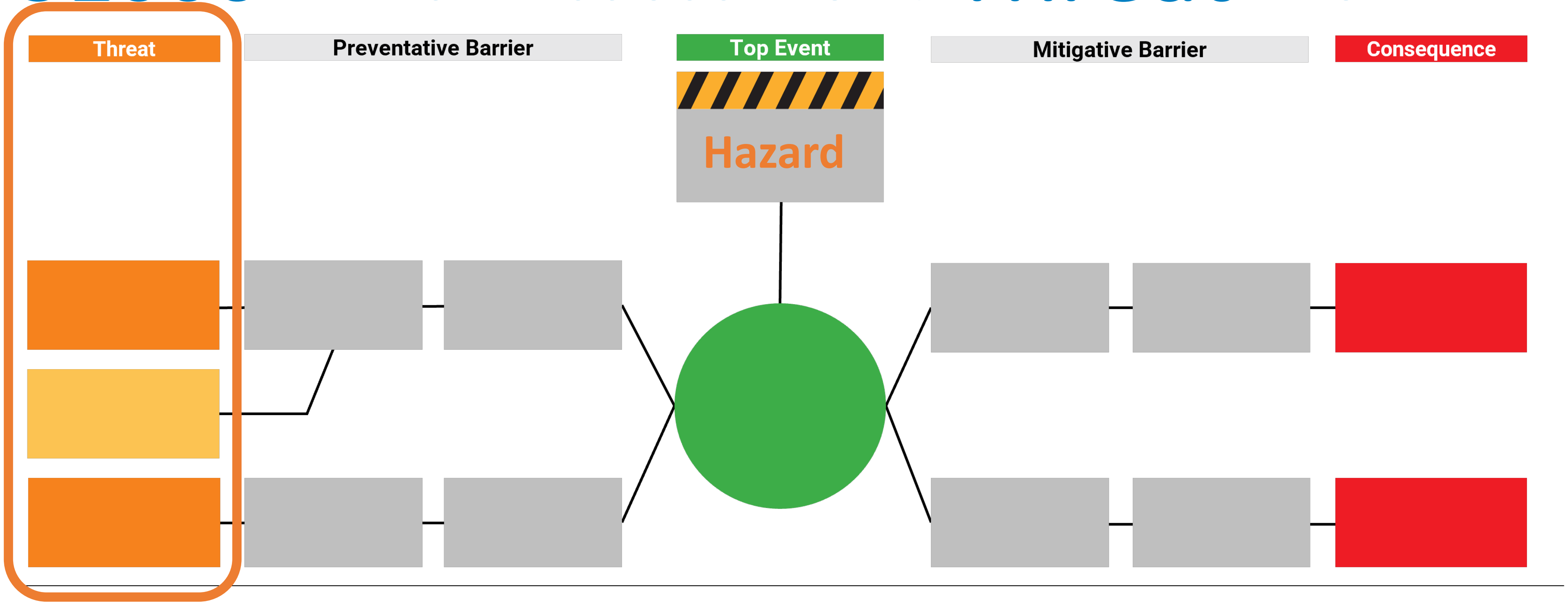
Step 7 Identify Escalation Factors

Escalation Factor

- Does it define how or why the barrier has degraded?
- Does it reduce the effectiveness of the barrier?
- Is it associated with a human or organisational factor?
- Is it realistic?

In Information Security, “Vulnerability” replaces “Hazard”

ISO31000 – Risk Assessment **Threat** View



Double click on the shapes above and input descriptions to complete the elements that make up the Bowtie Diagram. The element descriptions should conform to the questions asked below.

Step 1 Identify the Hazard

Hazard

- Is the hazard specific? (i.e. specify location, size etc if relevant)
- Has it been described in its controlled state?

Step 2 Identify the Top Event

Top Event

- Does it describe how control of the hazard has been lost?
- Does it describe what has been lost?
- Has the event been quantified (if relevant)?

Step 3 Identify Threats

Threat

- Does each threat identified directly cause the Top Event?

Step 4 Identify Consequences

Consequen ce

- Has it been described as [Damage] due to [Top Event]? (e.g Fire due to loss of containment)

Step 5 Identify Preventative Barriers

Preventative Barrier

- Is it specific?
- Is it capable of completely stopping the Top Event?
- Does it prevent the Threat from occurring?

Step 6 Identify Mitigative Barriers

Mitigative Barrier

- Is it specific?
- Does it prevent or limit the consequence?

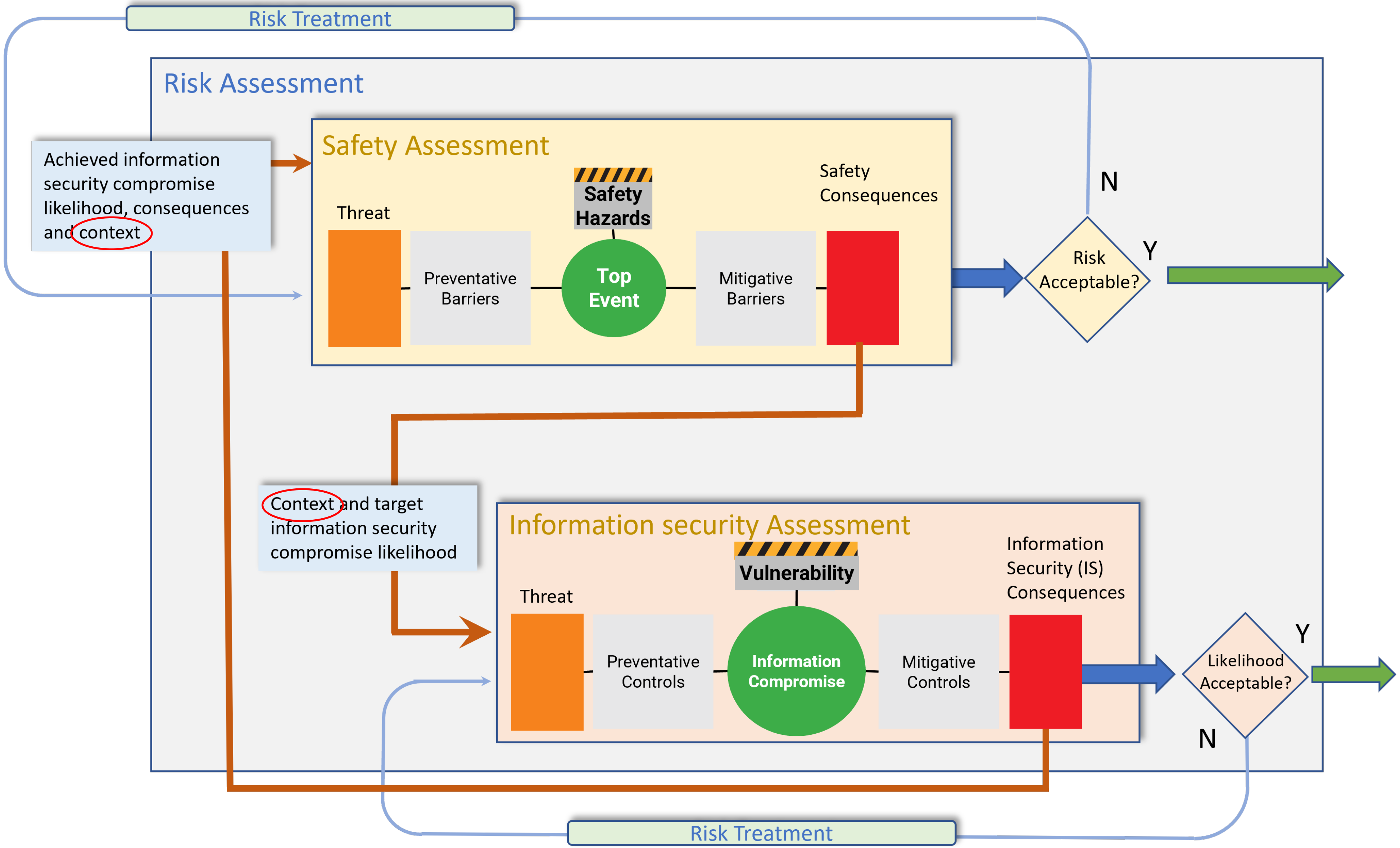
Step 7 Identify Escalation Factors

Escalation Factor

- Does it define how or why the barrier has degraded?
- Does it reduce the effectiveness of the barrier?
- Is it associated with a human or organisational factor?
- Is it realistic?

In Safety, the term "Threat" is not limited to intentional acts

Interacting Safety & Info Sec Risk Assessment



EASA

“One single event shall not cause a CAT effect”

Safety is our reference!

→ **CS-25.1309** Equipment, systems and installations” states:

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any catastrophic failure condition

(i) is extremely improbable; and

(ii) **does not result from a single failure**

➡ **There shall be at least two independent threat scenarios or causes to result in a Catastrophic safety consequence!**

ISO27005 – Safety Risk Treatment Options

→ Presumption: Only **unacceptable** safety risks will be treated

ISO27005:2022 (InfoSec) Risk Treatment Options	Safety Risk Treatment Options
avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk	available option
taking or increasing the risk in order to pursue an opportunity	Not possible, as risk needs to be made acceptable.
removing the risk source	available option
changing the likelihood	available option
changing the consequences	available option
sharing the risk (e.g. through contracts, buying insurance)	Not possible, as risk needs to be made acceptable.
retaining the risk by informed* decision	Not possible, as risk needs to be made acceptable.

*) Retaining an unacceptable risk despite being informed cannot even be considered gross neglect anymore!

Key Take Aways

Key Take Aways

All organisations are part of the Shared Trans-Organisational Risk Management (STORM)

All Risks Influence Any Other Risk:

- **Break The Silos!**
- **Learn Each Other's Language!**

Peace of Mind

© Caters News Agency

Industry Standardisation

Part-IS Implementation

Workshop

EASA

Cyrille Rosay is a Senior Expert in Cybersecurity in Aviation at EASA. He led RMT.648 for Aircraft Cybersecurity and co-chairs efforts on Part-IS guidance. Cyrille chairs EUROCAE WG-72 and the European Cybersecurity Standardisation Coordination Group (ECSCG).

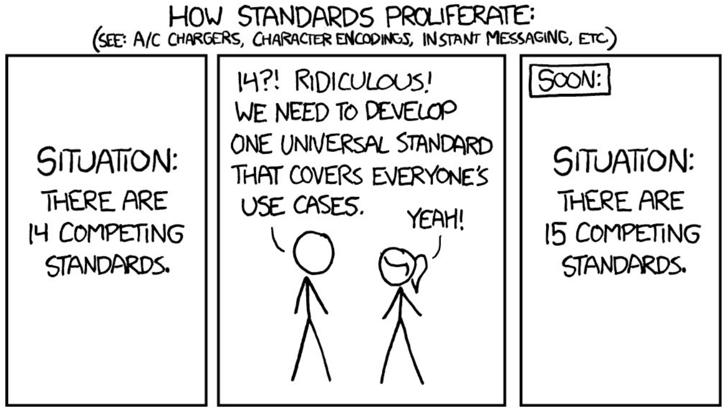
Before EASA, he was an airworthiness expert for the French Defence Agency and logged 2000 flight hours as an IFR multi-engine pilot.

Industry standards

- → Why do we need standards
- → ECSCG
- → EUROCAE WG-72
- → Which standards for part-IS?

Why Standards Matter

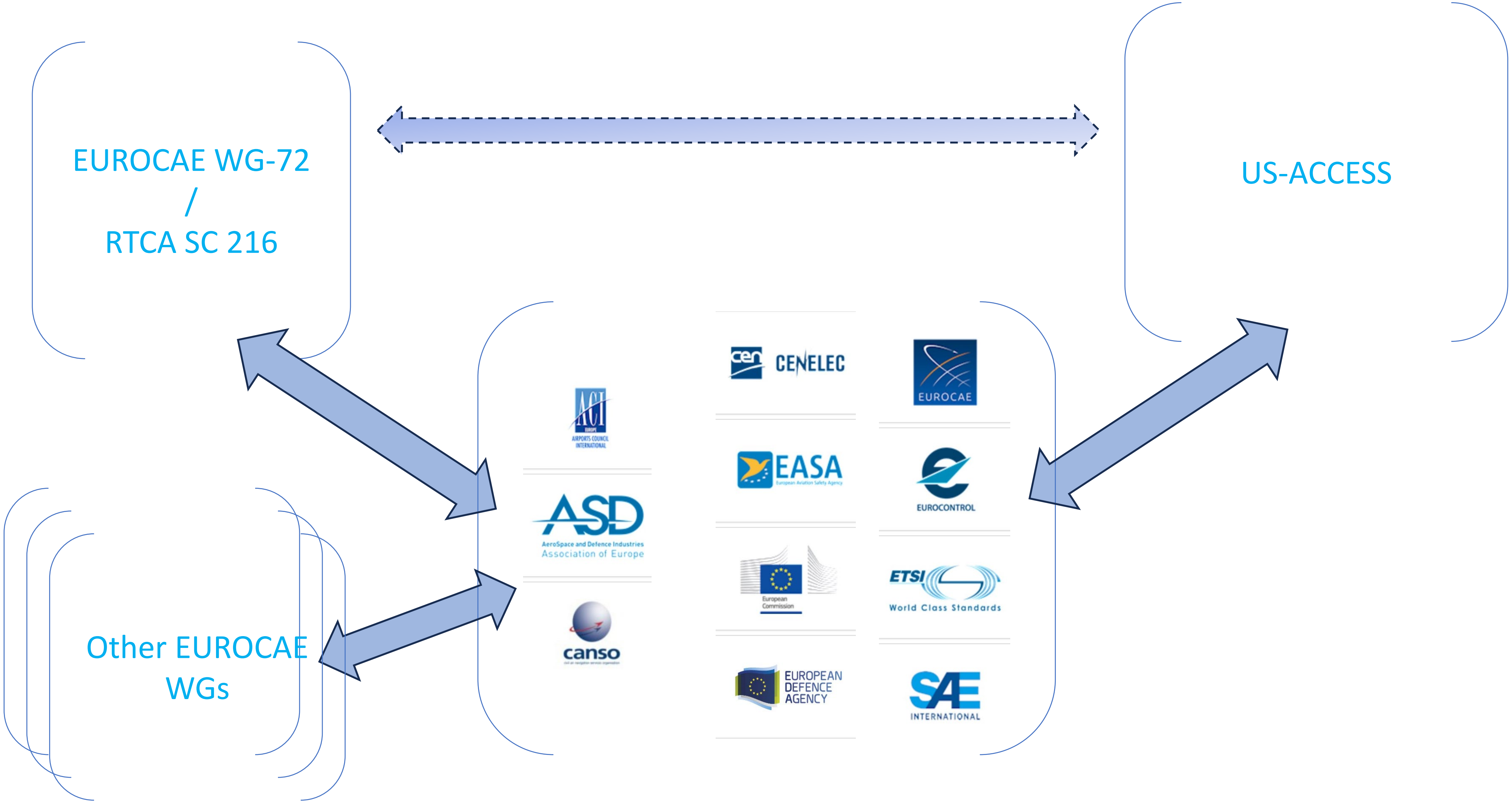
- agreed-upon norms, requirements, or guidelines that ensure
  - consistency,
  - quality,
  - Interoperability
  - (Conformity demonstration)
- foundation for shared understanding and compatibility
- simplify production, improve safety, reduce costs, and enhance reliability
- Developed by the industry for the industry


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

ECSCG

- European Cyber security for aviation Standards Coordination Group
  - **Joint** coordination and advisory group
    - coordinate the cyber security for aviation related standardisation activities
    - specific focus on activities stemming from the **EC and EASA regulations**
    - New Focus on SESAR implementation needs
    - does not exclude other market-driven standards

ECSCG



EUROCAE WG-72
/
RTCA SC 216

US-ACCESS

Other EUROCAE WGs

ACI EUROPE AIRPORTS COUNCIL INTERNATIONAL
CEN CENELEC
EUROCAE
ASD AeroSpace and Defence Industries Association of Europe
EASA European Aviation Safety Agency
EUROCONTROL
European Commission
ETSI World Class Standards
canso
EUROPEAN DEFENCE AGENCY
SAE INTERNATIONAL

ECSCG

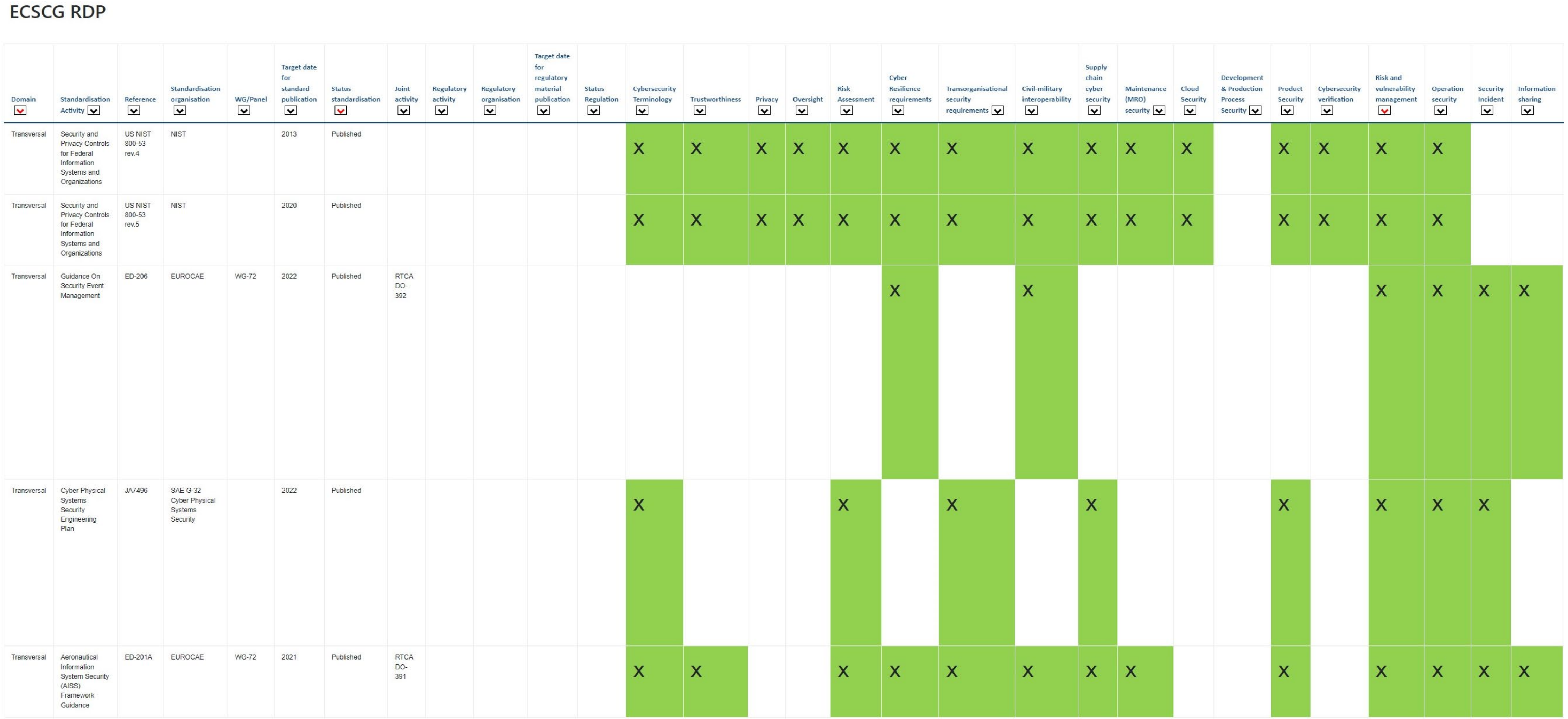
- Meeting 3 times a year

- EASA
  - Survey of existing standards
  - Gap identification

- SESAR 3
  - Gap identification
- Production of the Cybersecurity – Rolling Development Plan

https://rdptables.eurocae.net/Home/ECSCG

ECSCG – C-RDP



ECSCG RDP

Domain	Standardisation Activity	Reference	Standardisation organisation	WG/Panel	Target date for standard publication	Status standardisation	Joint activity	Regulatory activity	Regulatory organisation	Target date for regulatory material publication	Status Regulation	Cybersecurity Terminology	Trustworthiness	Privacy	Oversight	Risk Assessment	Cyber Resilience requirements	Transorganisational security requirements	Civil-military interoperability	Supply chain cyber security	Maintenance (MRO) security	Cloud Security	Development & Production Process Security	Product Security	Cybersecurity verification	Risk and vulnerability management	Operation security	Security Incident	Information sharing
Transversal	Security and Privacy Controls for Federal Information Systems and Organizations	US NIST 800-53 rev.4	NIST		2013	Published						X	X	X	X	X	X	X	X	X	X	X		X	X	X	X		
Transversal	Security and Privacy Controls for Federal Information Systems and Organizations	US NIST 800-53 rev.5	NIST		2020	Published						X	X	X	X	X	X	X	X	X	X	X		X	X	X	X		
Transversal	Guidance On Security Event Management	ED-206	EUROCAE	WG-72	2022	Published	RTCA DO-392										X		X							X	X	X	X
Transversal	Cyber Physical Systems Security Engineering Plan	JA7496	SAE G-32 Cyber Physical Systems Security		2022	Published						X				X		X		X				X		X	X	X	
Transversal	Aeronautical Information System Security (AISS) Framework Guidance	ED-201A	EUROCAE	WG-72	2021	Published	RTCA DO-391					X	X			X	X	X	X	X	X			X		X	X	X	X

→ “published transverse standards addressing Risk and Vulnerability Management”

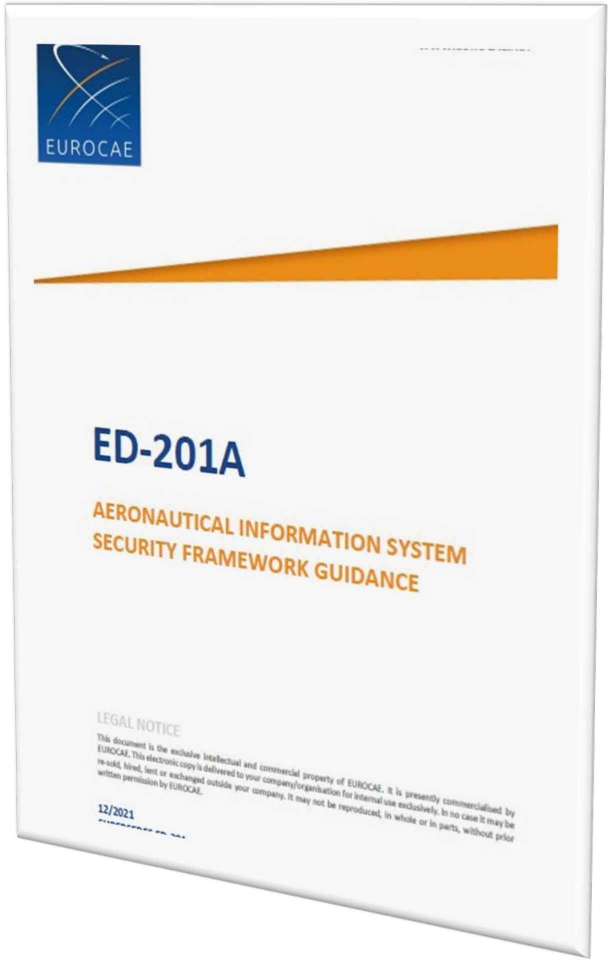
EUROCAE WG-72

- Created in 2006
- Subject: Aeronautical System Security
  - Focusing on potential impact on safety
- objectives rather than solutions

- addressing airborne systems, aviation ground systems, but also organizational aspects of information security (ISMS, ISEM).
- Joint Activity with RTCA SC-216
-

ED-201

- General concepts and frameworks on
  - Aviation security environment,
  - risk management and assurance,
  - supply chain,
  - ISMS in general,
  - Security Risk Assessment sharing and comparability,
  - Information Sharing,
  - External Agreements,
  - Threat Intelligence,
  - Protection of Sensitive Information and Disposal of Assets



EUROCAE

ED-201A

AERONAUTICAL INFORMATION SYSTEM SECURITY FRAMEWORK GUIDANCE

LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

12/2021

ED-202/ED-203/ED-204 the product suite

- → Airworthiness Security Process
- → Security scope
- → Security Risk Assessment
- → Security measure effectiveness
- → Security development
- → Scoring
- → Logging
- → Continuing airworthiness
  - → GSE, certificates, aircraft ISEM, roles and responsibilities

WWW.EUROCAE.NET

ED-202B

AIRWORTHINESS SECURITY PROCE
SPECIFICATION

LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is pr
EUROCAE. This electronic copy is delivered to your company/organisation for internal use ex
be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whol
written permission by EUROCAE.

10/2024
SUPERSEDES ED-202A

The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

AIRWORTHINESS SECURITY METHOD
CONSIDERATIONS

This document is the exclusive intellectual and commercial property of EUR
It is presently commercialised by EUROCAE.
This electronic copy is delivered to your company/organisation for internal u
In no case it may be re-sold, or hired, lent or exchanged outside your com

ED-203A
June 2018
Supersedes ED-203

9 – 23 rue Paul Lafargue
93200 Saint-Denis, France

ED-204A

INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

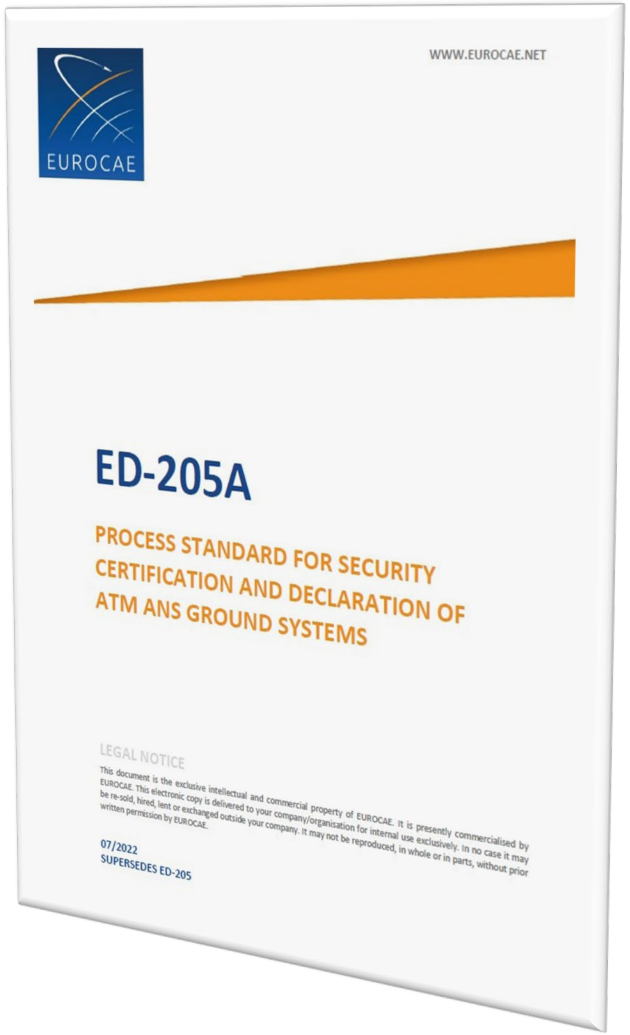
LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

09/2020
SUPERSEDES ED-204

ED-205 ATM ANS ground systems

- Security process
  - Organisation level (ISMS)
  - Risk management
  - Incident monitoring and reporting
  - Compliance demonstration



WWW.EUROCAE.NET

ED-205A

PROCESS STANDARD FOR SECURITY CERTIFICATION AND DECLARATION OF ATM ANS GROUND SYSTEMS

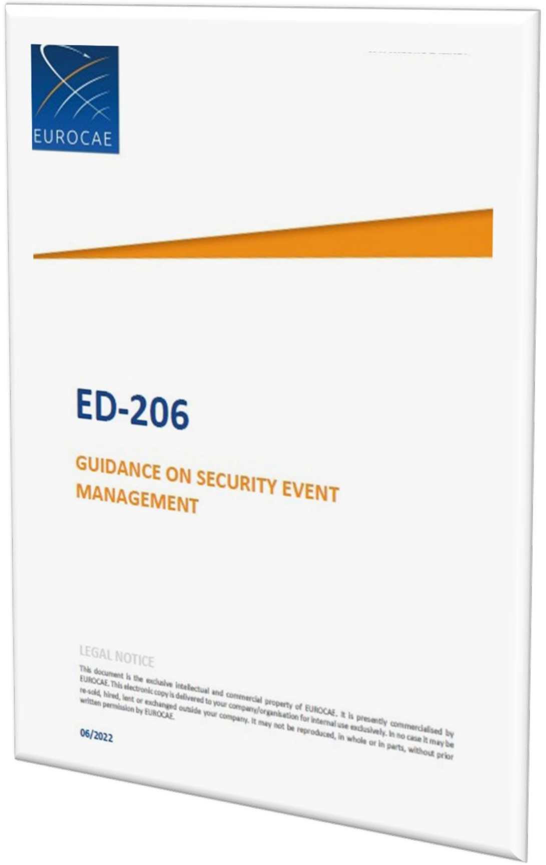
LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

07/2022
SUPERSEDES ED-205

ED-206 ISEM for organisation

- → ISEM framework (stakeholders, risk sharing, interfaces)
- → Prepare
- → Detect
- → Analyse
- → Respond
- → Recover



EUROCAE

ED-206

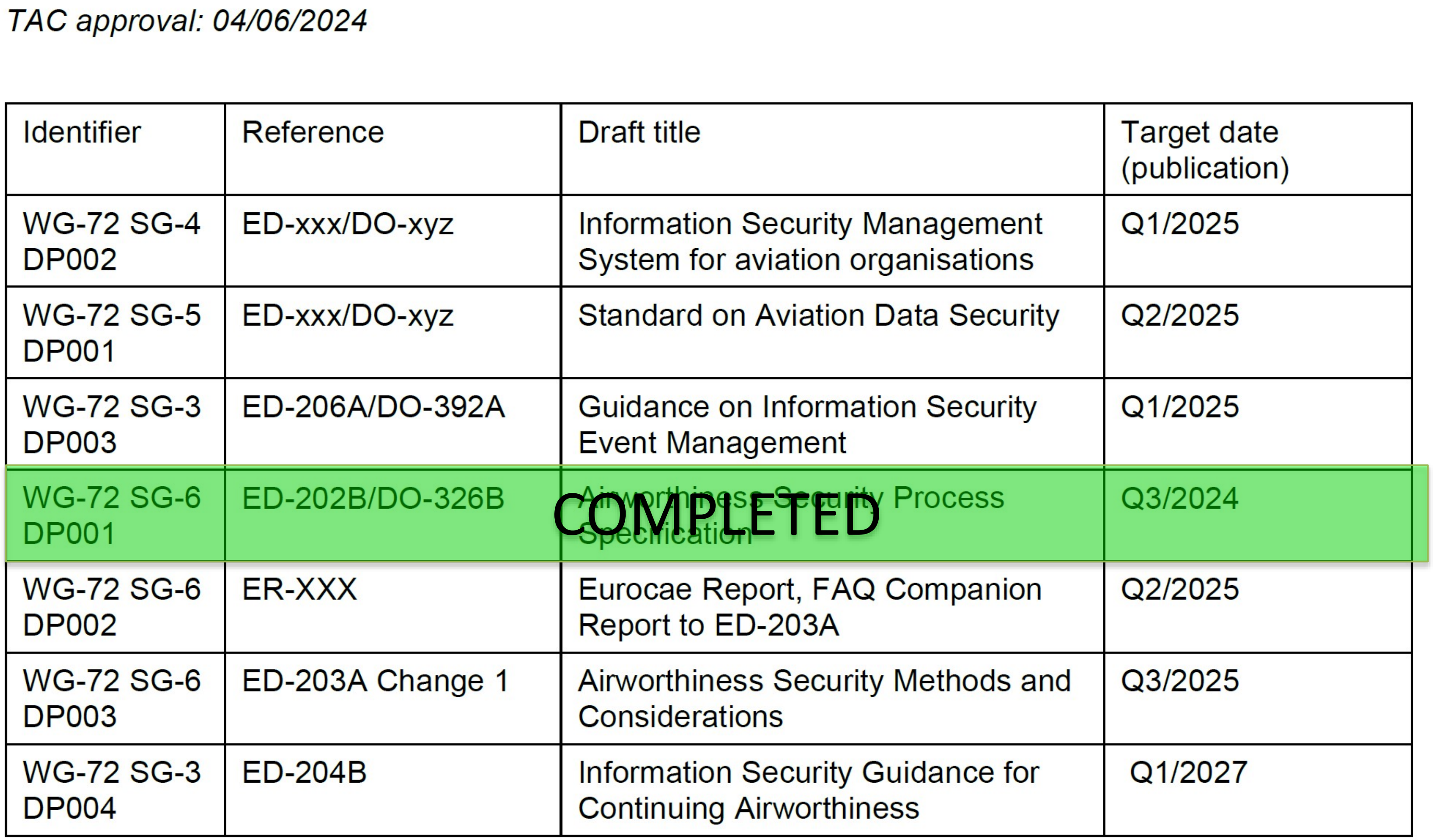
GUIDANCE ON SECURITY EVENT MANAGEMENT

LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

06/2022

Work programme

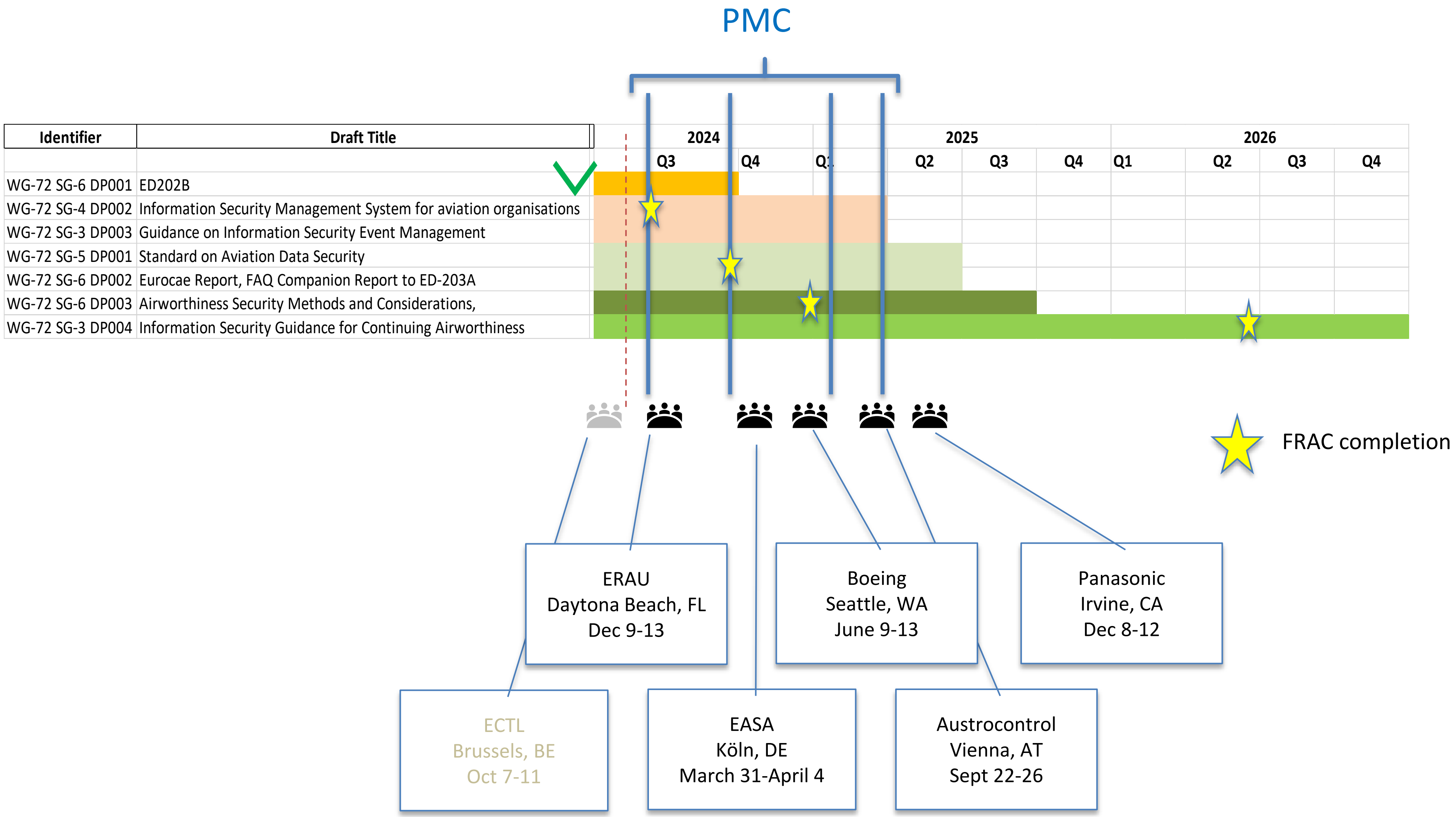


TAC approval: 04/06/2024

Identifier	Reference	Draft title	Target date (publication)
WG-72 SG-4 DP002	ED-xxx/DO-xyz	Information Security Management System for aviation organisations	Q1/2025
WG-72 SG-5 DP001	ED-xxx/DO-xyz	Standard on Aviation Data Security	Q2/2025
WG-72 SG-3 DP003	ED-206A/DO-392A	Guidance on Information Security Event Management	Q1/2025
WG-72 SG-6 DP001	ED-202B/DO-326B	Airworthiness Security Process Specification	Q3/2024
WG-72 SG-6 DP002	ER-XXX	Eurocae Report, FAQ Companion Report to ED-203A	Q2/2025
WG-72 SG-6 DP003	ED-203A Change 1	Airworthiness Security Methods and Considerations	Q3/2025
WG-72 SG-3 DP004	ED-204B	Information Security Guidance for Continuing Airworthiness	Q1/2027

COMPLETED

Schedule



Identifier	Draft Title
WG-72 SG-6 DP001	ED202B
WG-72 SG-4 DP002	Information Security Management System for aviation organisations
WG-72 SG-3 DP003	Guidance on Information Security Event Management
WG-72 SG-5 DP001	Standard on Aviation Data Security
WG-72 SG-6 DP002	Eurocae Report, FAQ Companion Report to ED-203A
WG-72 SG-6 DP003	Airworthiness Security Methods and Considerations,
WG-72 SG-3 DP004	Information Security Guidance for Continuing Airworthiness

★ FRAC completion

ECTL
Brussels, BE
Oct 7-11

ERAU
Daytona Beach, FL
Dec 9-13

EASA
Köln, DE
March 31-April 4

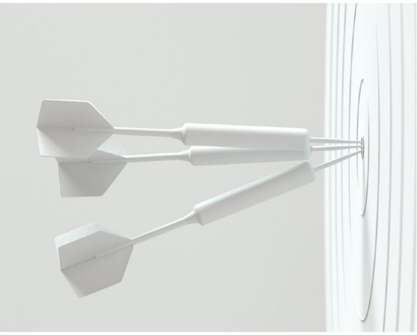
Boeing
Seattle, WA
June 9-13

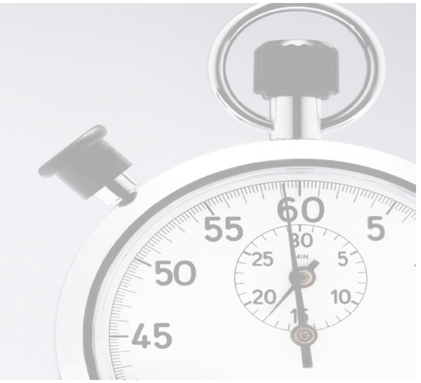
Austrocontrol
Vienna, AT
Sept 22-26

Panasonic
Irvine, CA
Dec 8-12

Eurocae WG-72 / SC-216 progresses

- ED-206A “Information Security Event Management”:
  1. ISMS vs ISEM objectives
  2. Vulnerability Scoring (Aviation customization)
  3. Timeline to report
     - organization to create timelines appropriate to their organiz
     - guidance on how to select appropriate timelines





Eurocae WG-72 / SC-216 progresses

ED-ISMS 1/2

- Alignment of ED-ISMS standard with ICAO work
- Proportionality for less complex organizations
  - guidance must support realistic maturity model
- Mechanisms for sharing audit results / minimizing audits
  - Suppliers expecting to see Part-IS language in contracts
  - need consensus on expectations
  - templates

Eurocae WG-72 / SC-216 progresses

ED-ISMS 2/2

- → Insider threat considerations
- → ISMS risk management process
- → Expanded on propagation to safety, distance and time, how many things need to happen in sequence before safety impact
- → Maturity model approach in ISMS

Eurocae WG-72 / SC-216 progresses

End to end Data security standard (ED-DSEC)

- 2 streams:
  - Framework:
    - blueprint on how to develop information security requirements for the data
    - 3 main steps
      - identify Data and the Stakeholders
      - determine the Data Flow and the Interfaces
      - protect the Data, based on the security properties hazard on safety effect
  - Supported by specific use cases
    - For example: aircraft data, from software provider to system upload

Standardisations: main takeaways

- Standards are key elements to:
  - Safety
  - Efficiency
  - Consistency
  - Level playing field
  - Developed by the industry for the industry
    - Share your experience and contribute☺

Q&A – 30 minutes

Part-IS Implementation

Workshop

Part-IS Workshop agenda – Day 2

Part-IS Task Force outcomes & harmonisation activities

Overview of the harmonisation activities carried out by the Task Force, i.e. approval of derogations and the implementation guidance for ISO/IEC 27001 certified organisations.

AESA, AUSTROCONTROL

Interplay with other EU rules (NIS2 and AVSEC)

Relationship beteen Part-IS and other EU cybersecurity legislation that may be applicable to aviation entities.

EASA, Polish CAA

Q&A

Panel 2 - Staff competence building

Discussion on cyber security competencies, & possible approaches to recruitment and upskilling the workforce, and the challenges associated with them.

EASA, ENISA, AESA, ILenT-NL, FOCA

ECSF adaptation for Part-IS roles

The tailored version of the ENISA Cybersecurity Skills Framework for use in the aviation context, taking into account in particular the roles introduced by Part-IS.

EASA

Q&A

See you tomorrow!

Thanks for being with us virtually and in presence

Part-IS Implementation

Workshop

EASA