EASA

European Union Aviation Safety Agency

Part-IS Implementation

Workshop 2025

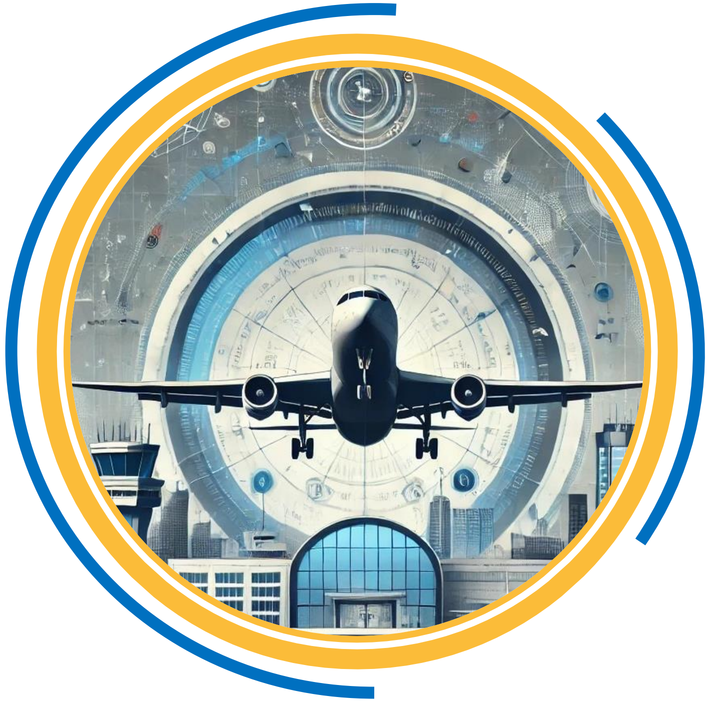
Cologne, June 25 - 26

Your safety is our mission.

An Agency of the European Union

Welcome!

Thanks for being with us virtually and in presence



Part-IS Implementation

Workshop

Opening Address – Florian Guillermet

Executive Director, EASA

Part-IS Workshop agenda – Day 1

Opening speech - Introduction to the event

Welcoming you to our workshop

EASA

Part-IS – An information security or a safety regulation?

The main objective of Part-IS will be presented by using the so-far experience by early implementers

EASA, Lufthansa Cargo AG, SECONDO MONA

Proportional Implementation of Part-IS & indicators of complexity

This session will cover the proportionality elements of Part-IS implementation by describing the challenges that different types of organisations are facing and the concept of the indicators of complexity will be presented as a tool to assess the implementation effort needed

EASA, Ryanair, ECOGAS

Q&A

Aviation product certification and Part-IS

The links and interplay between Part-IS and the aviation product security requirements will be presented

EASA

Enhancing CTI & Information Sharing for Part-IS compliance

The benefits of cyber threat intelligence and information sharing for Part-IS compliance will be explored providing guidance on implementing these practices in a proportionate manner

EASA

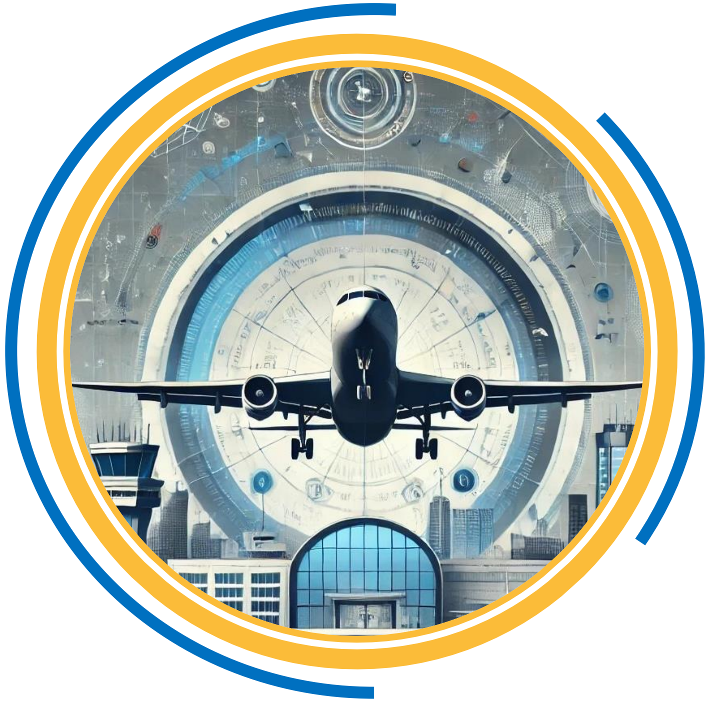
Meet the experts sessions (on-site only)

Participants will have the opportunity to exchange in 10min slots with EASA experts on-site on selected topics

Q&A

EASA

Part-IS - An information security or a safety regulation?



Part-IS Implementation

Workshop 2025

Jean-Paul Moreaux has been a key figure in cybersecurity in aviation 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.

EASA
European Union Aviation Safety Agency

So Long, and Thanks For All the Fish!

Your safety is our mission.

An Agency of the European Union

[Friendly Reminder] Part-IS is a Safety Regulation!

EASA
European Union Aviation Safety Agency

eRules

PART-IS

(IR/DR + AMC/GM)

One Part IS Requires **ONE** Extra Cause Having Safety Consequences To be taken Into Account

Two Part-IS Does **NOT** Establish New Safety Requirements!

Three Part-IS is **Integral to Traditional Principles** of Risk Management Sharing

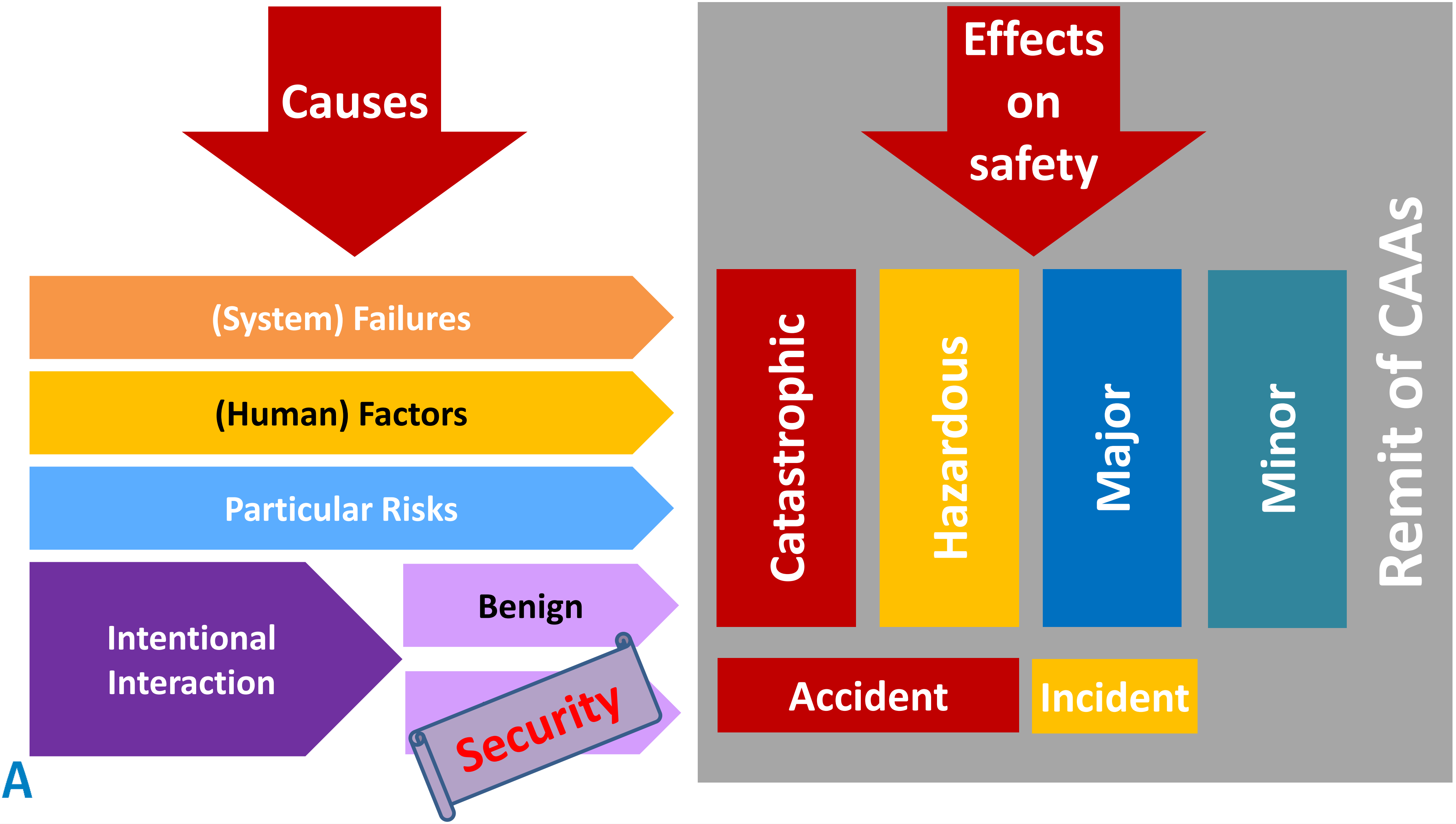
…changing perspective!

- → Now that we have an idea what the **extra safety risks** are, we cannot ignore them any longer!
- → At the same time, we now know where to find the answer to the question:

When is enough, enough?

YOU GUYS DO REALIZE I'M THE WOLF, RIGHT? WHY WON'T YOU RUN AWAY?
ONLY THE OLD AND SICK ARE ATTACKED BY WOLVES
A YOUNG & HEALTHY BODY CAN DEAL WITH WOLVE BITES
WE'RE COUNTING ON FLOCK IMMUNITY
WOLVES DON'T EXIST
ARGHXSEL 2020

Relation between Causes and Effects



Causes

(System) Failures

(Human) Factors

Particular Risks

Intentional Interaction

Benign

Security

Effects on safety

Catastrophic

Hazardous

Major

Minor

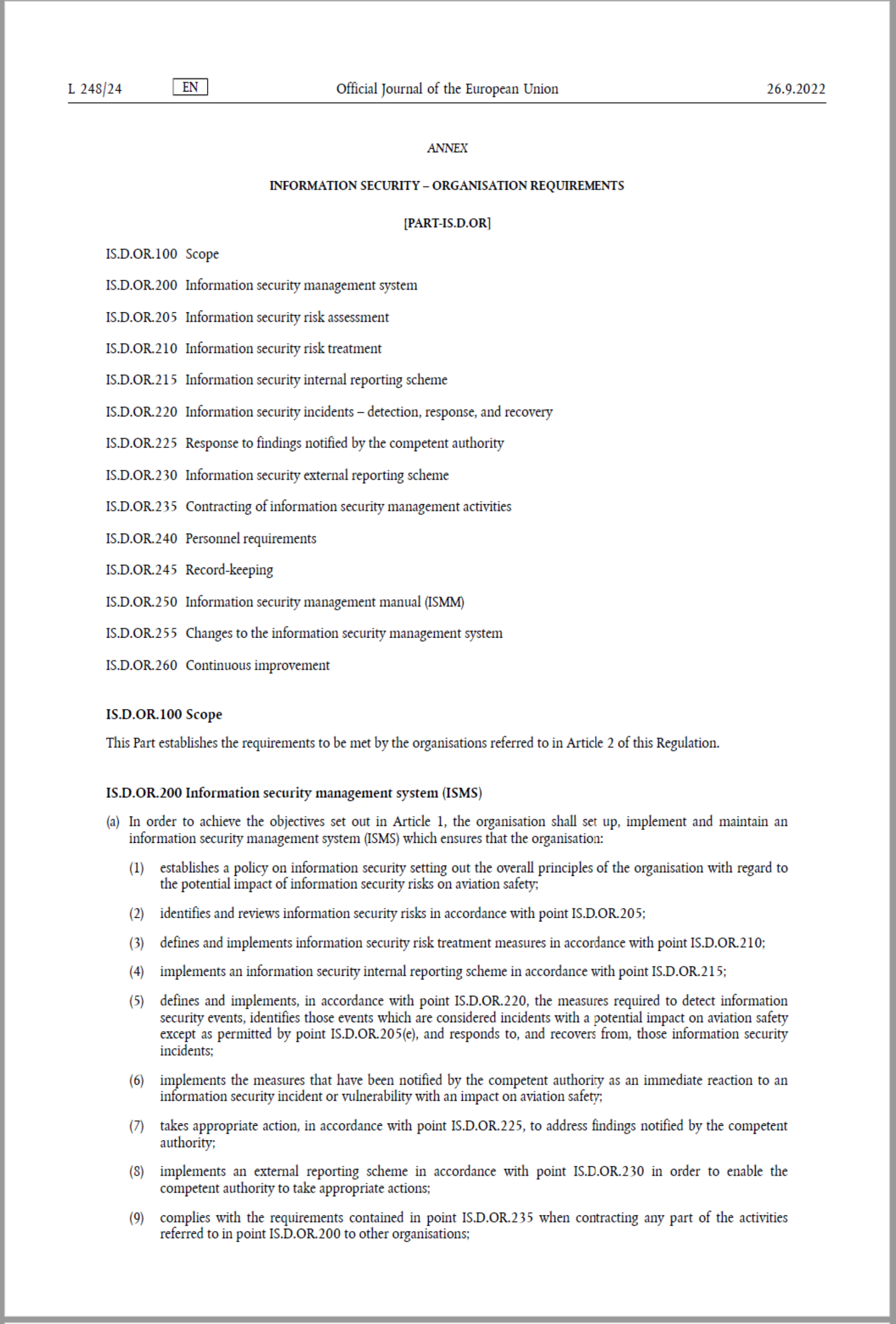
Remit of CAAs

Accident

Incident

EASA
European Union Aviation Safety Agency

The Legal Side of the Equation



L 248/24 EN Official Journal of the European Union 26.9.2022

ANNEX

INFORMATION SECURITY – ORGANISATION REQUIREMENTS

[PART-IS.D.OR]

IS.D.OR.100 Scope

This Part establishes the requirements to be met by the organisations referred to in Article 2 of this Regulation.

IS.D.OR.200 Information security management system (ISMS)

(a) In order to achieve the objectives set out in Article 1, the organisation shall set up, implement and maintain an information security management system (ISMS) which ensures that the organisation:

(1) establishes a policy on information security setting out the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;

(2) identifies and reviews information security risks in accordance with point IS.D.OR.205;

(3) defines and implements information security risk treatment measures in accordance with point IS.D.OR.210;

(4) implements an information security internal reporting scheme in accordance with point IS.D.OR.215;

(5) defines and implements, in accordance with point IS.D.OR.220, the measures required to detect information security events, identifies those events which are considered incidents with a potential impact on aviation safety except as permitted by point IS.D.OR.205(e), and responds to, and recovers from, those information security incidents;

(6) implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;

(7) takes appropriate action, in accordance with point IS.D.OR.225, to address findings notified by the competent authority;

(8) implements an external reporting scheme in accordance with point IS.D.OR.230 in order to enable the competent authority to take appropriate actions;

(9) complies with the requirements contained in point IS.D.OR.235 when contracting any part of the activities referred to in point IS.D.OR.200 to other organisations;

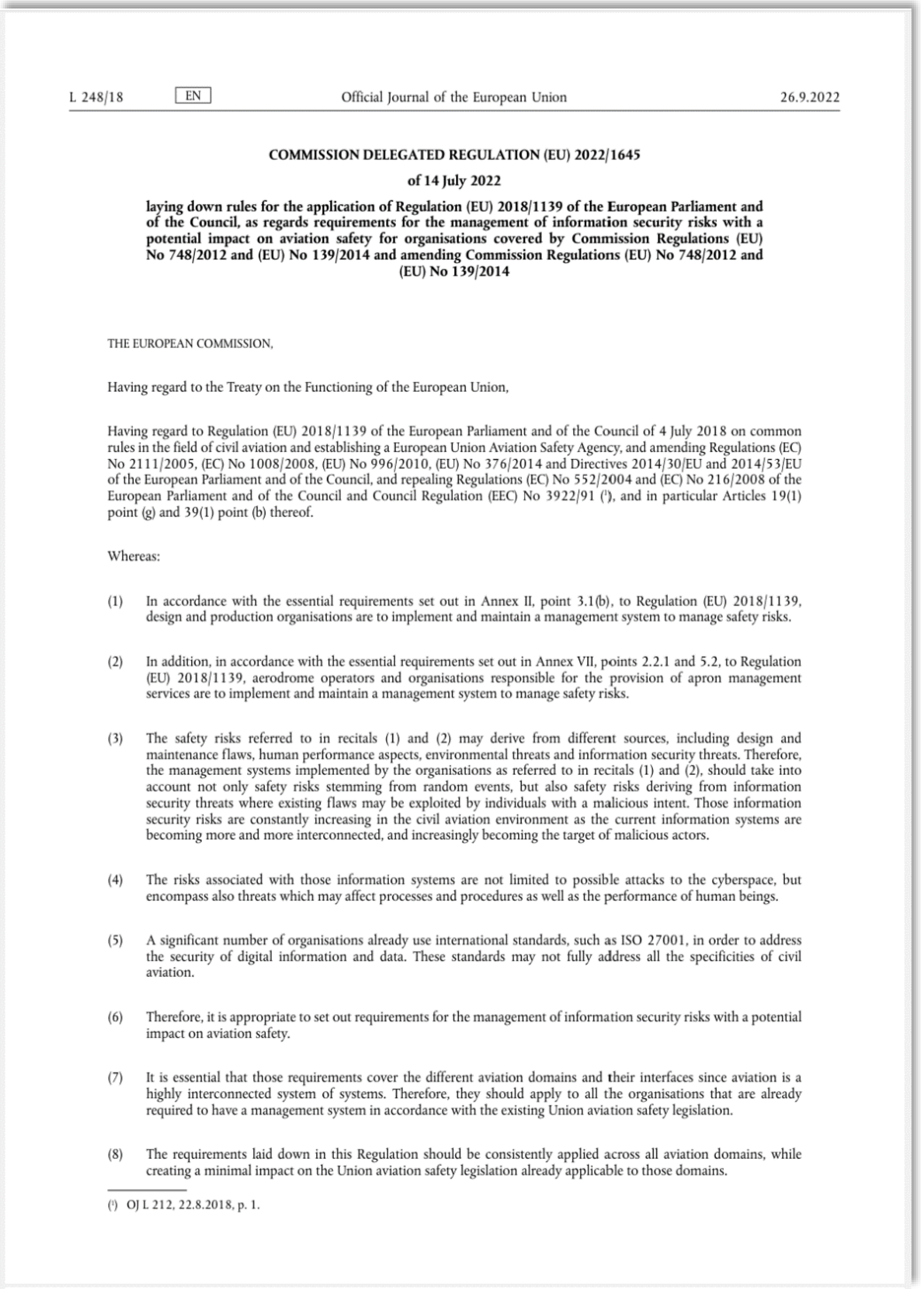
An Agency of the European Union

EU Regulation 2022/1645

Article 1

Subject matter

This Regulation sets out the requirements to be met by the organisations referred to in Article 2 in *order to identify and manage information security risks with potential impact on aviation safety* which could affect information and communication technology systems and data used for civil aviation purposes and to *detect information security events and identify those which are considered information security incidents with potential impact on aviation safety* and respond to, and recover from, those information security incidents.



L 248/18 EN Official Journal of the European Union 26.9.2022

COMMISSION DELEGATED REGULATION (EU) 2022/1645

of 14 July 2022

laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 ([1]), and in particular Articles 19(1) point (g) and 39(1) point (b) thereof.

Whereas:

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

(2) In addition, in accordance with the essential requirements set out in Annex VII, points 2.2.1 and 5.2, to Regulation (EU) 2018/1139, aerodrome operators and organisations responsible for the provision of apron management services are to implement and maintain a management system to manage safety risks.

(3) The safety risks referred to in recitals (1) and (2) may derive from different sources, including design and maintenance flaws, human performance aspects, environmental threats and information security threats. Therefore, the management systems implemented by the organisations as referred to in recitals (1) and (2), should take into account not only safety risks stemming from random events, but also safety risks deriving from information security threats where existing flaws may be exploited by individuals with a malicious intent. Those information security risks are constantly increasing in the civil aviation environment as the current information systems are becoming more and more interconnected, and increasingly becoming the target of malicious actors.

(4) The risks associated with those information systems are not limited to possible attacks to the cyberspace, but encompass also threats which may affect processes and procedures as well as the performance of human beings.

(5) A significant number of organisations already use international standards, such as ISO 27001, in order to address the security of digital information and data. These standards may not fully address all the specificities of civil aviation.

(6) Therefore, it is appropriate to set out requirements for the management of information security risks with a potential impact on aviation safety.

(7) It is essential that those requirements cover the different aviation domains and their interfaces since aviation is a highly interconnected system of systems. Therefore, they should apply to all the organisations that are already required to have a management system in accordance with the existing Union aviation safety legislation.

(8) The requirements laid down in this Regulation should be consistently applied across all aviation domains, while creating a minimal impact on the Union aviation safety legislation already applicable to those domains.

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

Basic Regulation (2018/1139)

Article 4

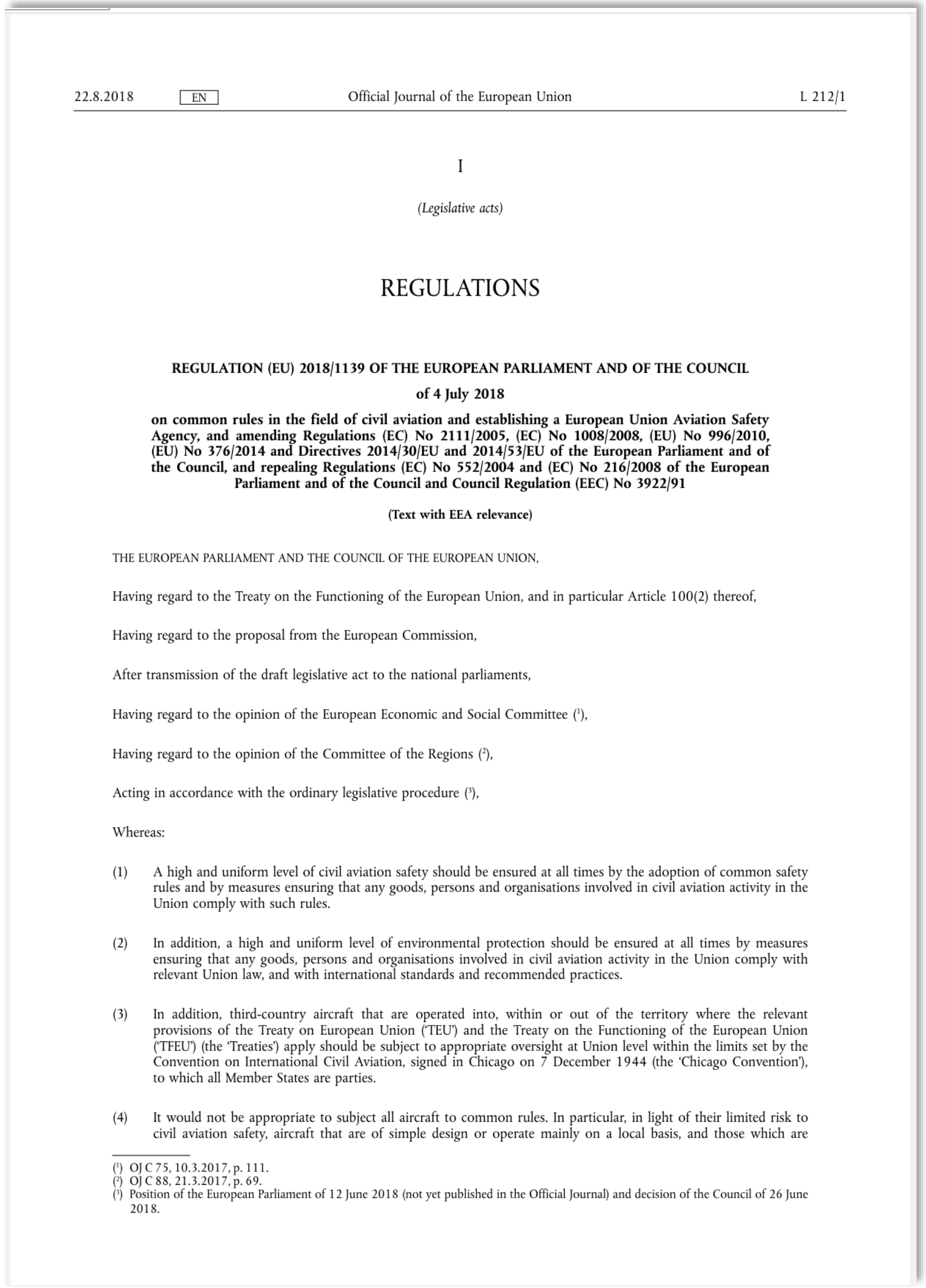
Principles for measures under this Regulation

1. When taking measures under this Regulation the Commission, the Agency and the Member States shall:

…

(c) allow for immediate reaction to established causes of accidents, serious incidents and intentional security breaches;

(d) take into account **interdependencies** between the different domains of aviation safety, and between **aviation safety, cyber security** and other technical domains of aviation regulation;



22.8.2018 EN Official Journal of the European Union L 212/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 4 July 2018

on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 100(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1) A high and uniform level of civil aviation safety should be ensured at all times by the adoption of common safety rules and by measures ensuring that any goods, persons and organisations involved in civil aviation activity in the Union comply with such rules.

(2) In addition, a high and uniform level of environmental protection should be ensured at all times by measures ensuring that any goods, persons and organisations involved in civil aviation activity in the Union comply with relevant Union law, and with international standards and recommended practices.

(3) In addition, third-country aircraft that are operated into, within or out of the territory where the relevant provisions of the Treaty on European Union ('TEU') and the Treaty on the Functioning of the European Union ('TFEU') (the 'Treaties') apply should be subject to appropriate oversight at Union level within the limits set by the Convention on International Civil Aviation, signed in Chicago on 7 December 1944 (the 'Chicago Convention'), to which all Member States are parties.

(4) It would not be appropriate to subject all aircraft to common rules. In particular, in light of their limited risk to civil aviation safety, aircraft that are of simple design or operate mainly on a local basis, and those which are

[1] OJ C 75, 10.3.2017, p. 111.
[2] OJ C 88, 21.3.2017, p. 69.
[3] Position of the European Parliament of 12 June 2018 (not yet published in the Official Journal) and decision of the Council of 26 June 2018.

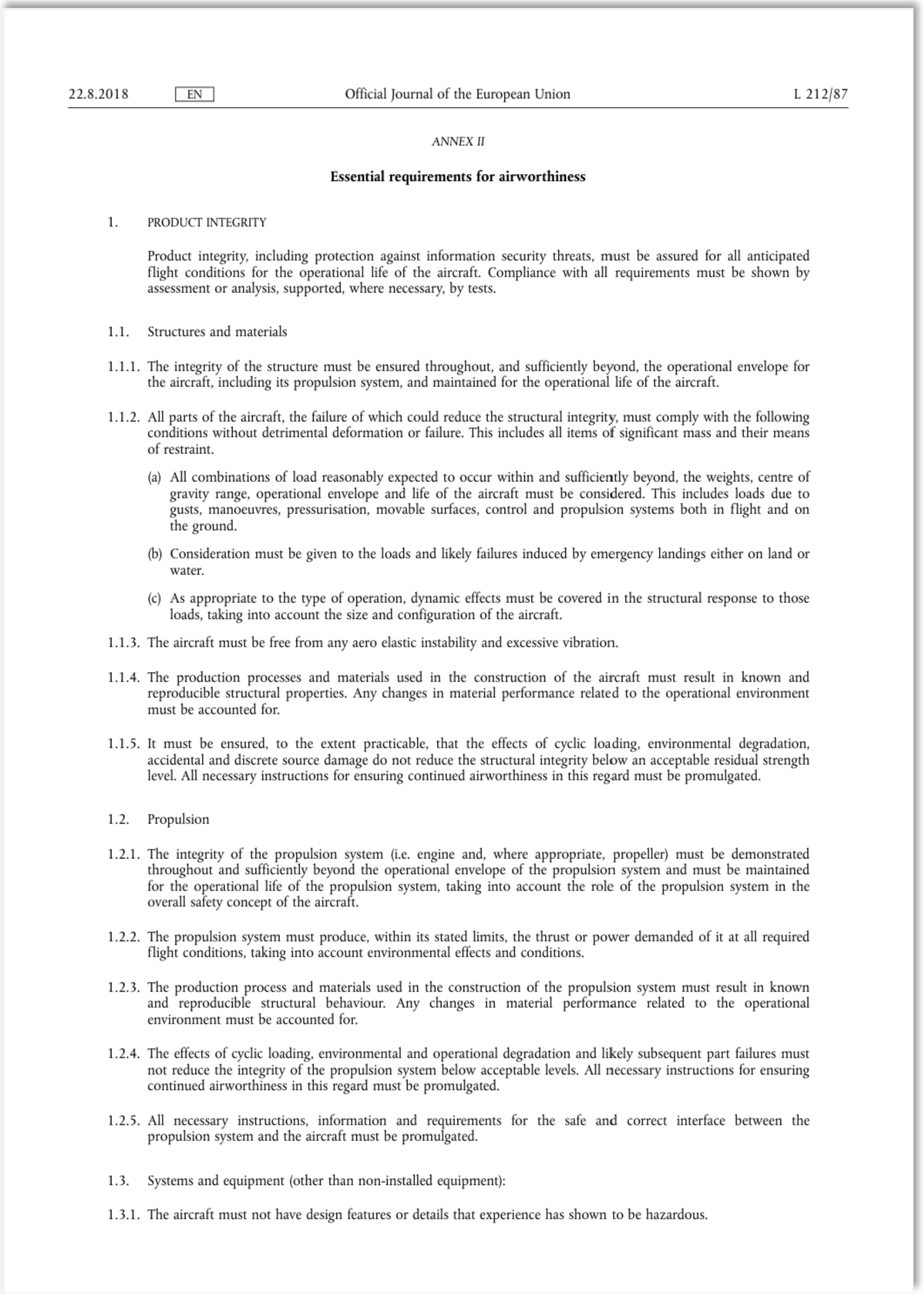
Basic Regulation (2018/1139)

ANNEX II

Essential requirements for airworthiness

1. PRODUCT INTEGRITY

Product integrity, including protection against **information security** threats, must be assured for all anticipated flight conditions for the operational life of the aircraft. Compliance with all requirements must be shown by assessment or analysis, supported, where necessary, by tests.



22.8.2018 EN Official Journal of the European Union L 212/87

ANNEX II

Essential requirements for airworthiness

1. PRODUCT INTEGRITY

Product integrity, including protection against information security threats, must be assured for all anticipated flight conditions for the operational life of the aircraft. Compliance with all requirements must be shown by assessment or analysis, supported, where necessary, by tests.

1.1. Structures and materials

1.1.1. The integrity of the structure must be ensured throughout, and sufficiently beyond, the operational envelope for the aircraft, including its propulsion system, and maintained for the operational life of the aircraft.

1.1.2. All parts of the aircraft, the failure of which could reduce the structural integrity, must comply with the following conditions without detrimental deformation or failure. This includes all items of significant mass and their means of restraint.

(a) All combinations of load reasonably expected to occur within and sufficiently beyond, the weights, centre of gravity range, operational envelope and life of the aircraft must be considered. This includes loads due to gusts, manoeuvres, pressurisation, movable surfaces, control and propulsion systems both in flight and on the ground.

(b) Consideration must be given to the loads and likely failures induced by emergency landings either on land or water.

(c) As appropriate to the type of operation, dynamic effects must be covered in the structural response to those loads, taking into account the size and configuration of the aircraft.

1.1.3. The aircraft must be free from any aero elastic instability and excessive vibration.

1.1.4. The production processes and materials used in the construction of the aircraft must result in known and reproducible structural properties. Any changes in material performance related to the operational environment must be accounted for.

1.1.5. It must be ensured, to the extent practicable, that the effects of cyclic loading, environmental degradation, accidental and discrete source damage do not reduce the structural integrity below an acceptable residual strength level. All necessary instructions for ensuring continued airworthiness in this regard must be promulgated.

1.2. Propulsion

1.2.1. The integrity of the propulsion system (i.e. engine and, where appropriate, propeller) must be demonstrated throughout and sufficiently beyond the operational envelope of the propulsion system and must be maintained for the operational life of the propulsion system, taking into account the role of the propulsion system in the overall safety concept of the aircraft.

1.2.2. The propulsion system must produce, within its stated limits, the thrust or power demanded of it at all required flight conditions, taking into account environmental effects and conditions.

1.2.3. The production process and materials used in the construction of the propulsion system must result in known and reproducible structural behaviour. Any changes in material performance related to the operational environment must be accounted for.

1.2.4. The effects of cyclic loading, environmental and operational degradation and likely subsequent part failures must not reduce the integrity of the propulsion system below acceptable levels. All necessary instructions for ensuring continued airworthiness in this regard must be promulgated.

1.2.5. All necessary instructions, information and requirements for the safe and correct interface between the propulsion system and the aircraft must be promulgated.

1.3. Systems and equipment (other than non-installed equipment):

1.3.1. The aircraft must not have design features or details that experience has shown to be hazardous.

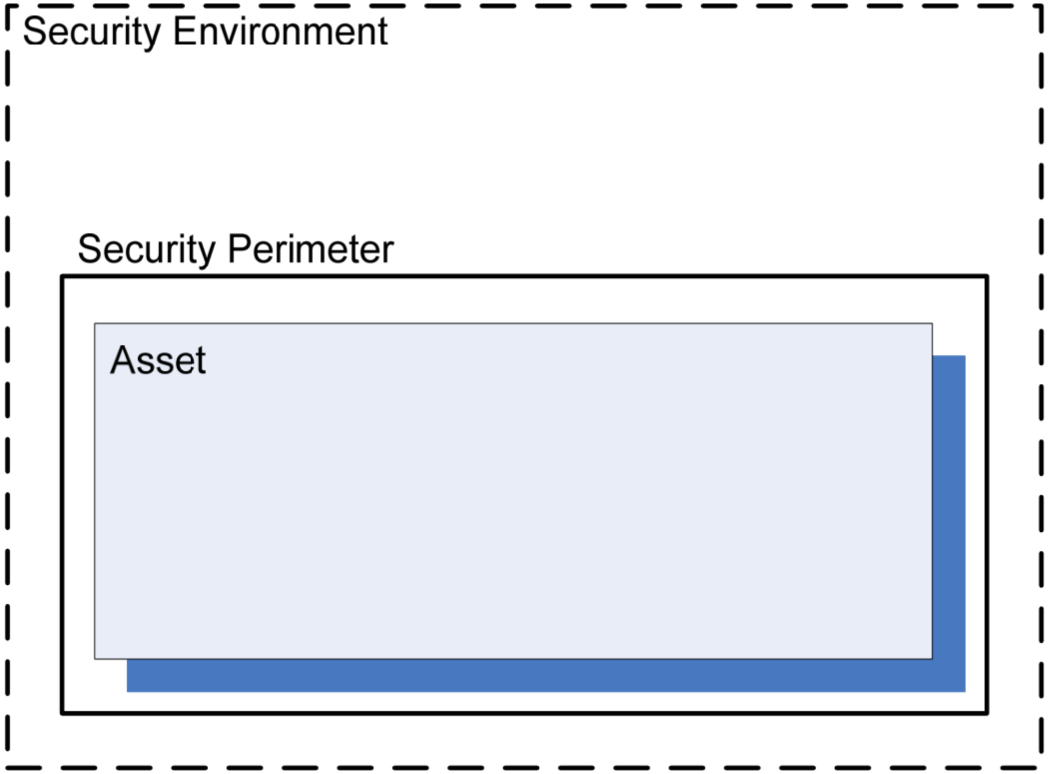
The Two Approaches

Scoping (OR/AR.100…)

→ Part-IS is a Safety Regulation!

- Scope = *potential impact on aviation safety*

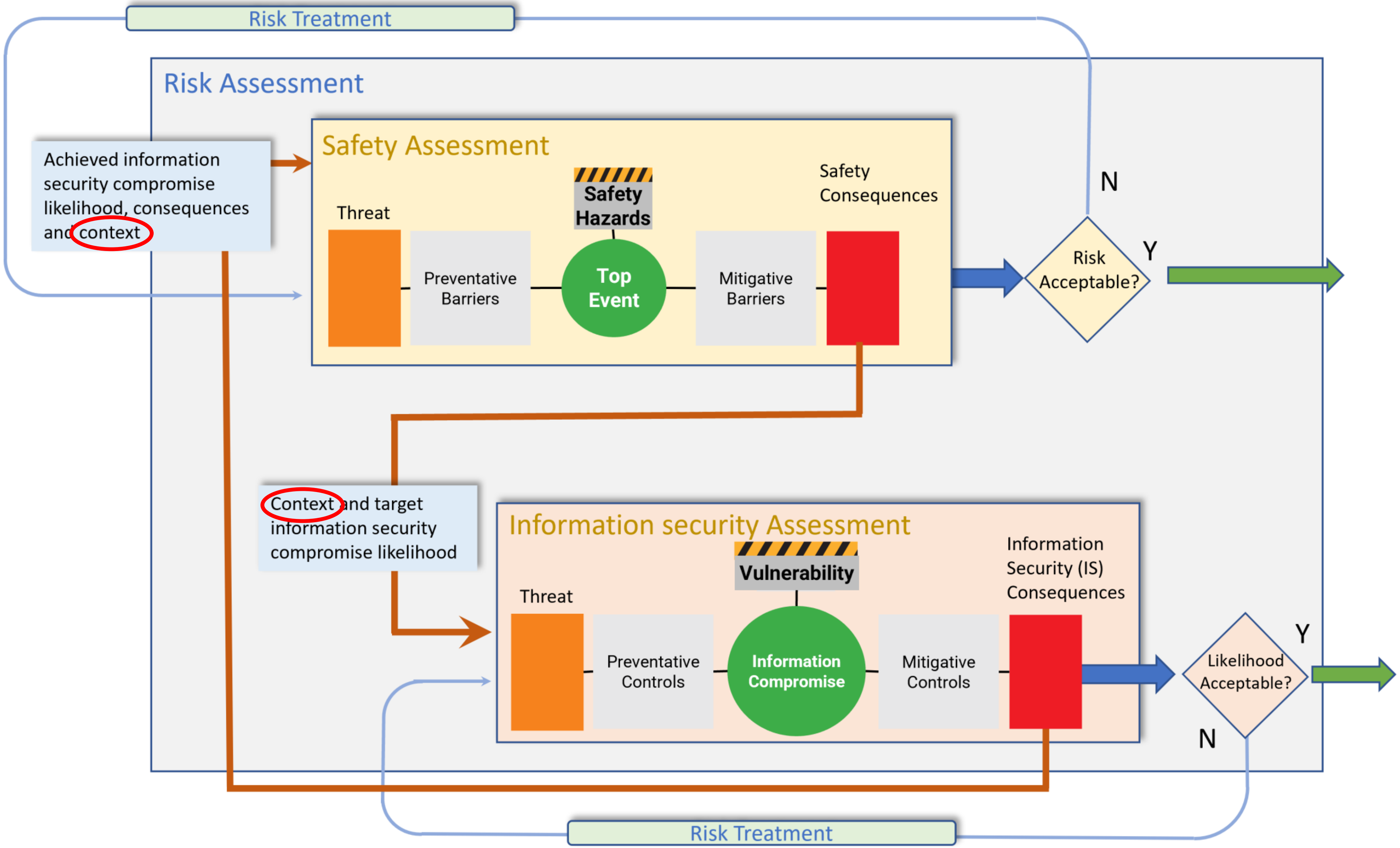
Security Environment = Outside Influence
Security Perimeter = Boundary of Safety Control
Asset = **Safety** Evaluation Item



- **Step One** =
  Safety Impact Assessment
- **Step Two** =
  Safety Risk Assessment

EASA

Interacting Safety & Info Sec Risk Assessment

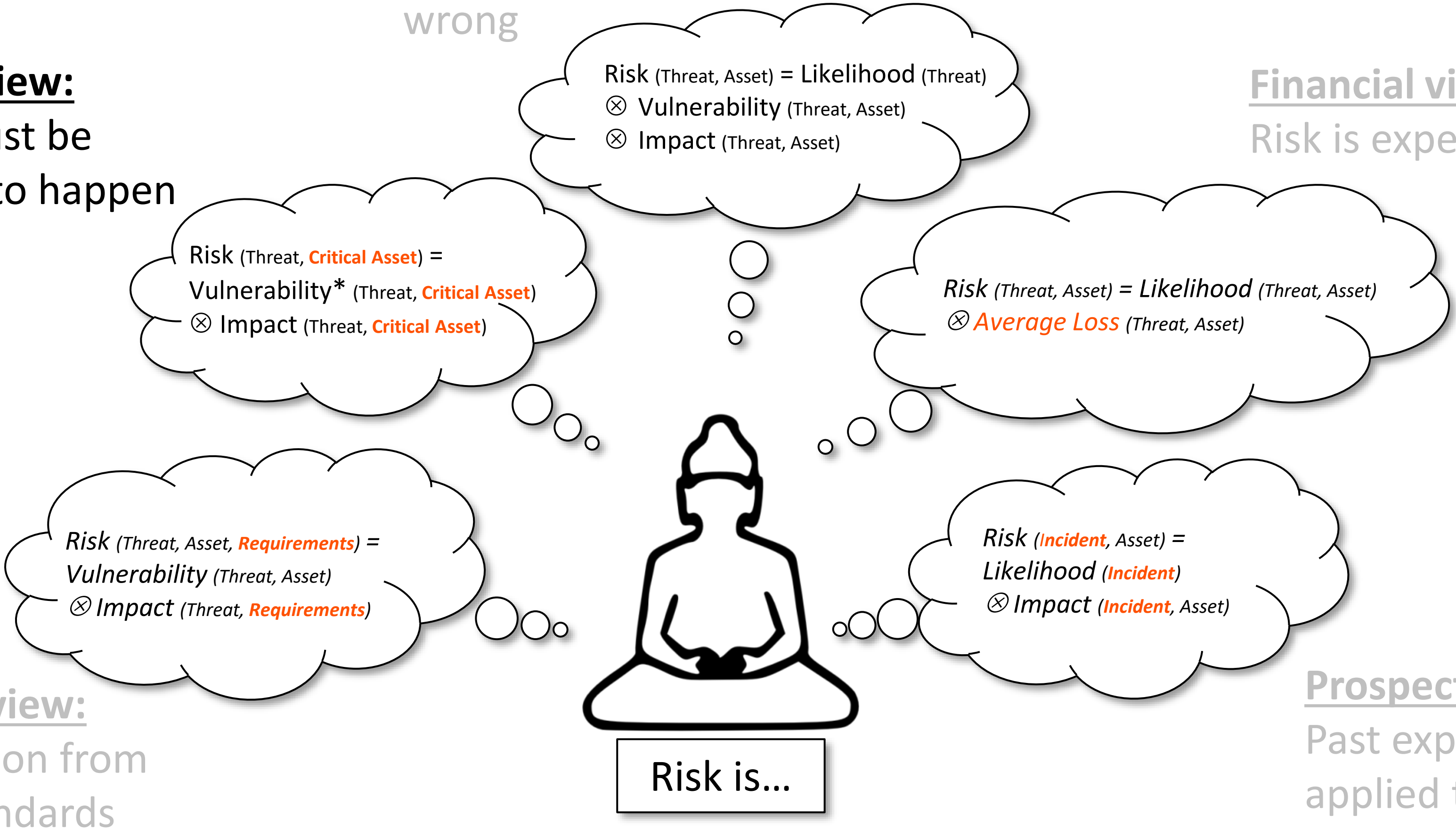


Which Class of Risk Assessment Do We Use for…?

Threat view:**
What could make things go wrong

Impact view:
What must be avoided to happen

Financial view:
Risk is expected loss ($)



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

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

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

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

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

Risk is…

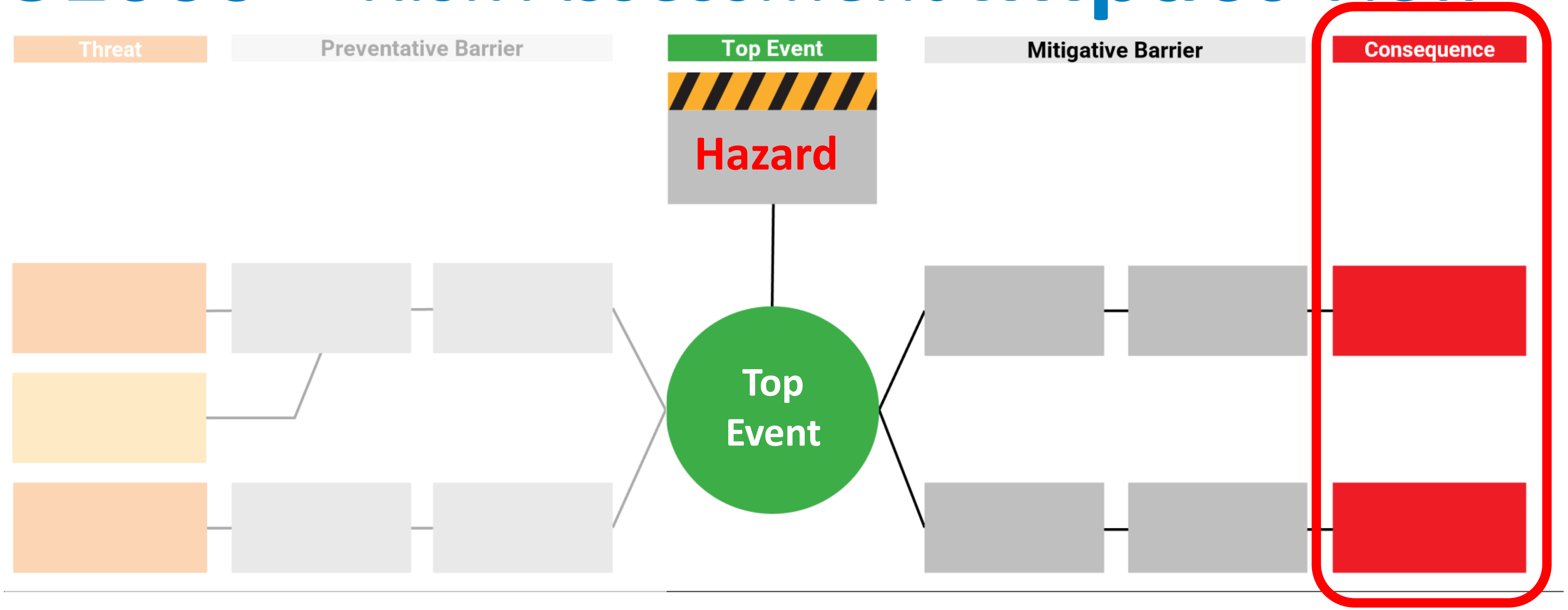
Compliance view:
Risk is deviation from rules and standards

Prospective view:
Past experience applied to the future

*) 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

ISO31000 – Risk Assessment Impact 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

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

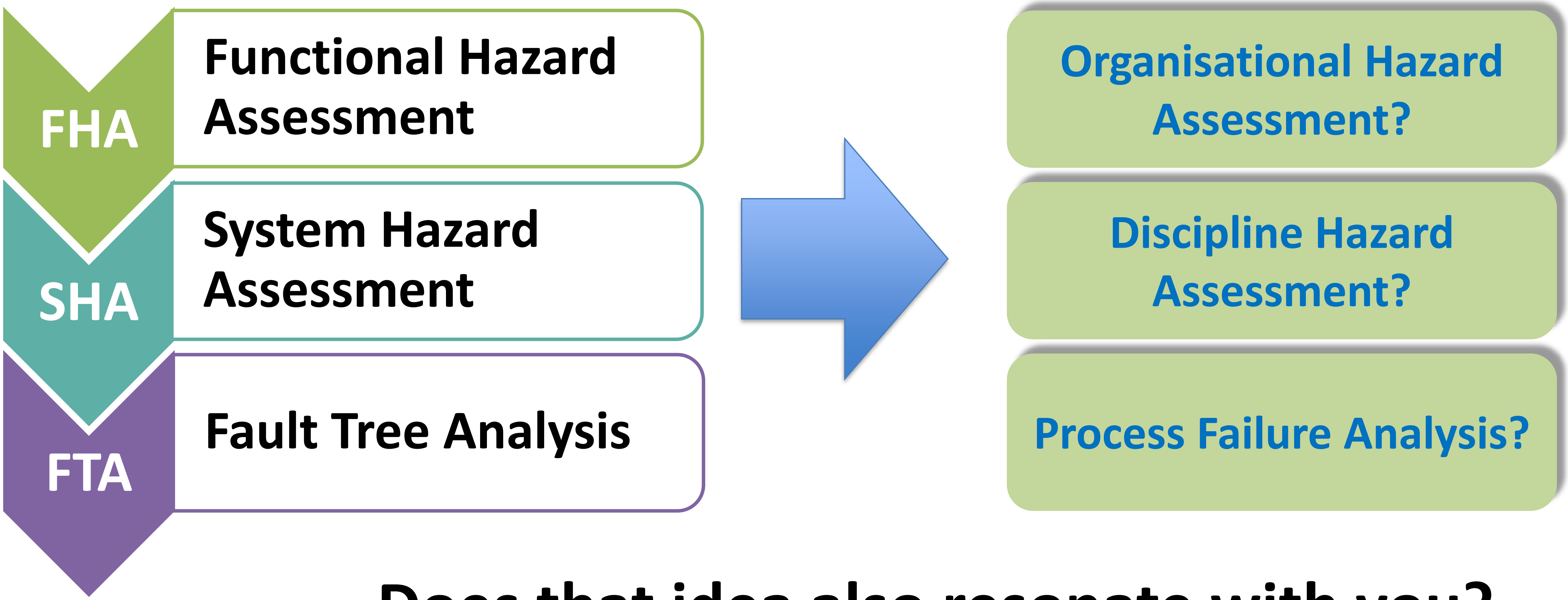
Escalation Factor

- 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”

Idea: Structural approach to Impact Identification

Transpose from Functional to Org Hazard Assessment:



FHA

Functional Hazard Assessment

SHA

System Hazard Assessment

FTA

Fault Tree Analysis

Organisational Hazard Assessment?

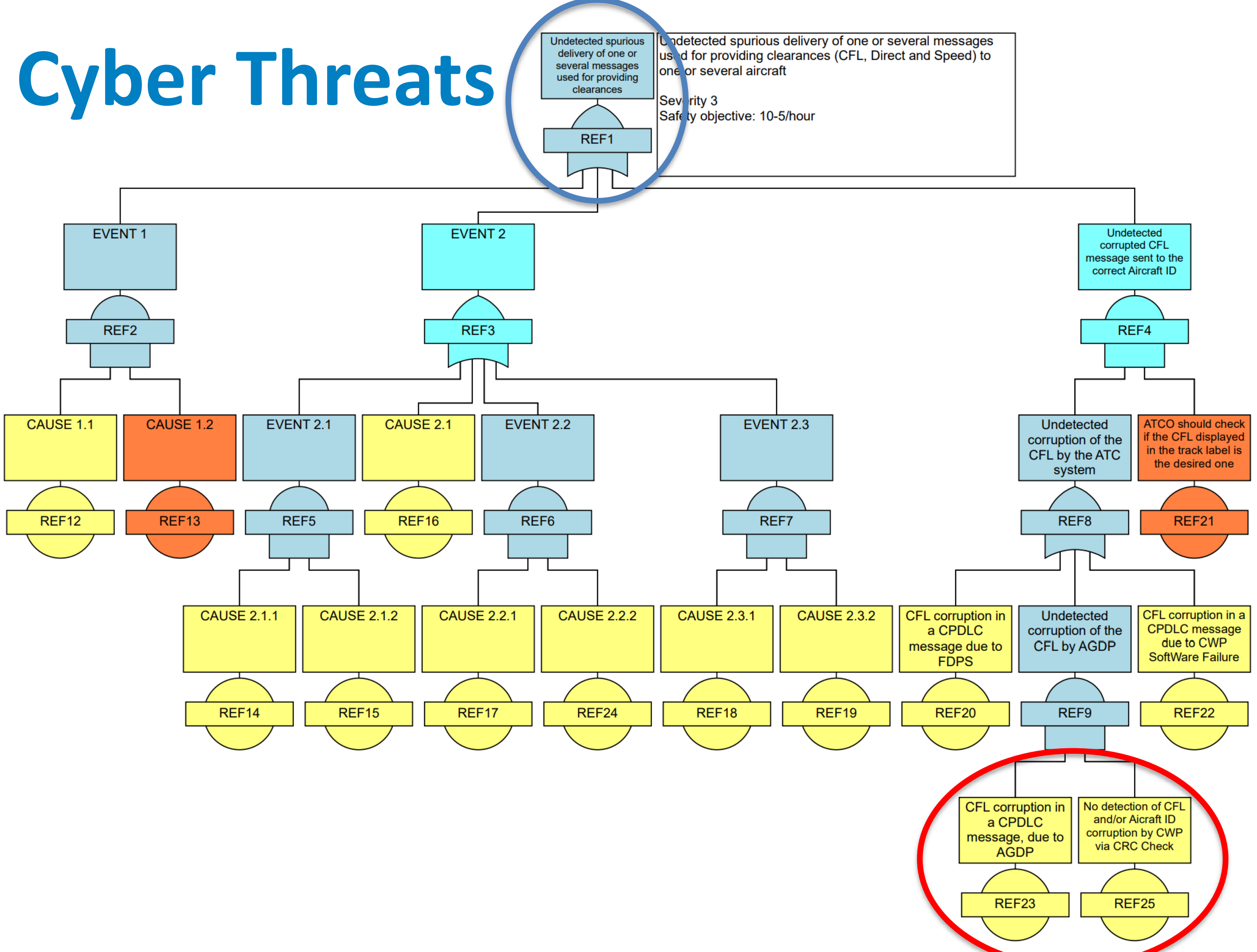
Discipline Hazard Assessment?

Process Failure Analysis?

Does that idea also resonate with you?

FTA Example w Cyber Threats

- → Look for the Information Security **Threat** on the **bottom**
- → Manifestation of the hazard is the **Top Event** on the top



Undetected spurious delivery of one or several messages used for providing clearances

Undetected spurious delivery of one or several messages used for providing clearances (CFL, Direct and Speed) to one or several aircraft

Severity 3

Safety objective: 10-5/hour

REF1

EVENT 1

REF2

EVENT 2

REF3

Undetected corrupted CFL message sent to the correct Aircraft ID

REF4

CAUSE 1.1

REF12

CAUSE 1.2

REF13

EVENT 2.1

REF5

CAUSE 2.1

REF16

EVENT 2.2

REF6

EVENT 2.3

REF7

Undetected corruption of the CFL by the ATC system

REF8

ATCO should check if the CFL displayed in the track label is the desired one

REF21

CAUSE 2.1.1

REF14

CAUSE 2.1.2

REF15

CAUSE 2.2.1

REF17

CAUSE 2.2.2

REF24

CAUSE 2.3.1

REF18

CAUSE 2.3.2

REF19

CFL corruption in a CPDLC message due to FDPS

REF20

Undetected corruption of the CFL by AGDP

REF9

CFL corruption in a CPDLC message due to CWP SoftWare Failure

REF22

CFL corruption in a CPDLC message, due to AGDP

REF23

No detection of CFL and/or Aicraft ID corruption by CWP via CRC Check

REF25

Which Class of Risk Assessment Do We Use for…?

Threat** view:

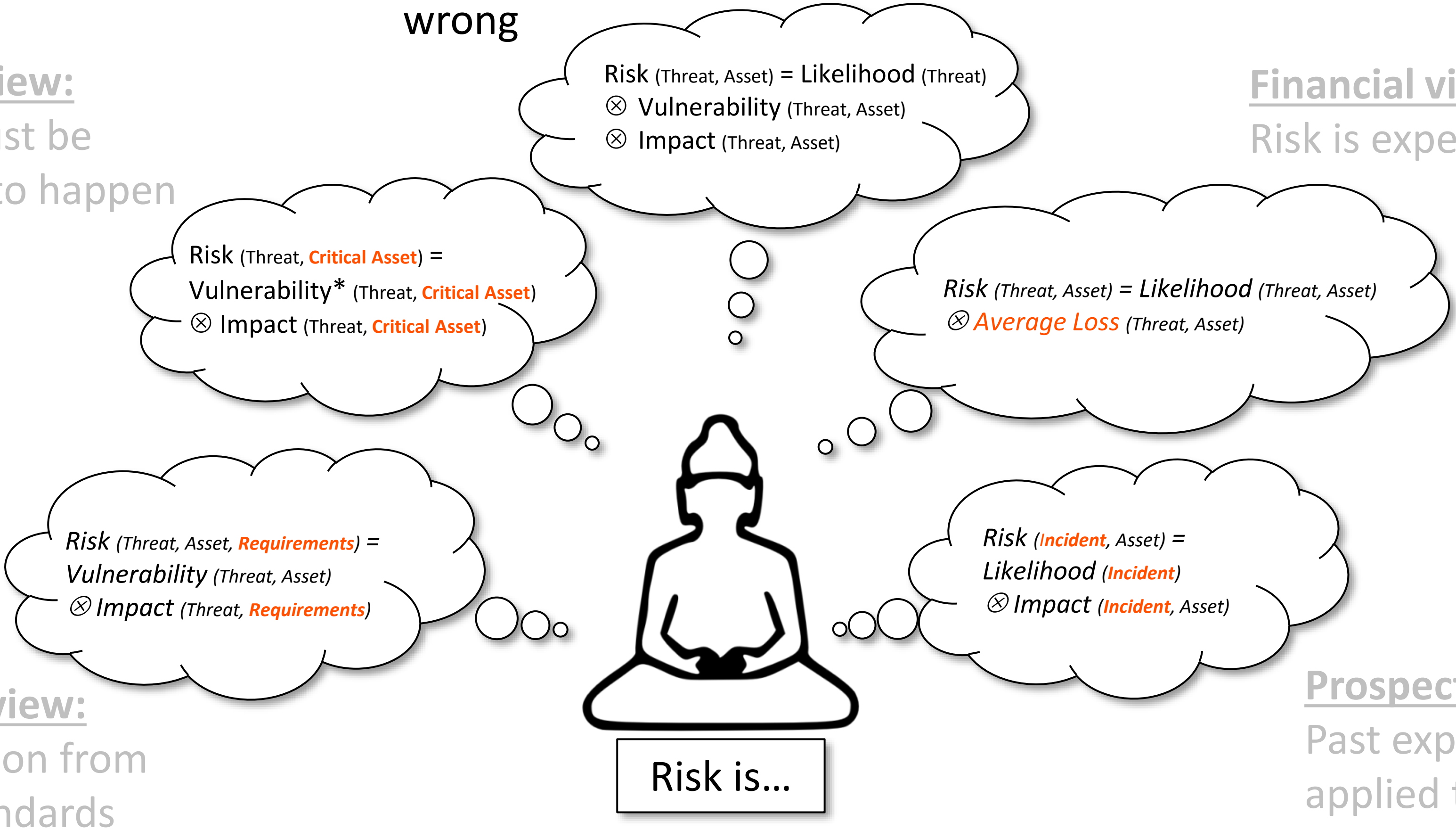
What could make things go wrong

Impact view:

What must be avoided to happen

Financial view:

Risk is expected loss ($)



Risk (Threat, Asset) = Likelihood (Threat) $\otimes$ Vulnerability (Threat, Asset) $\otimes$ Impact (Threat, Asset)

Risk (Threat, **Critical Asset**) = Vulnerability* (Threat, **Critical Asset**) $\otimes$ Impact (Threat, **Critical Asset**)

Risk (Threat, Asset) = Likelihood (Threat, Asset) $\otimes$ Average Loss (Threat, Asset)

*Risk (Threat, Asset, **Requirements**) = Vulnerability (Threat, Asset) $\otimes$ Impact (Threat, **Requirements**)*

*Risk (**Incident**, Asset) = Likelihood (**Incident**) $\otimes$ Impact (**Incident**, Asset)*

Risk is…

Compliance view:

Risk is deviation from rules and standards

Prospective view:

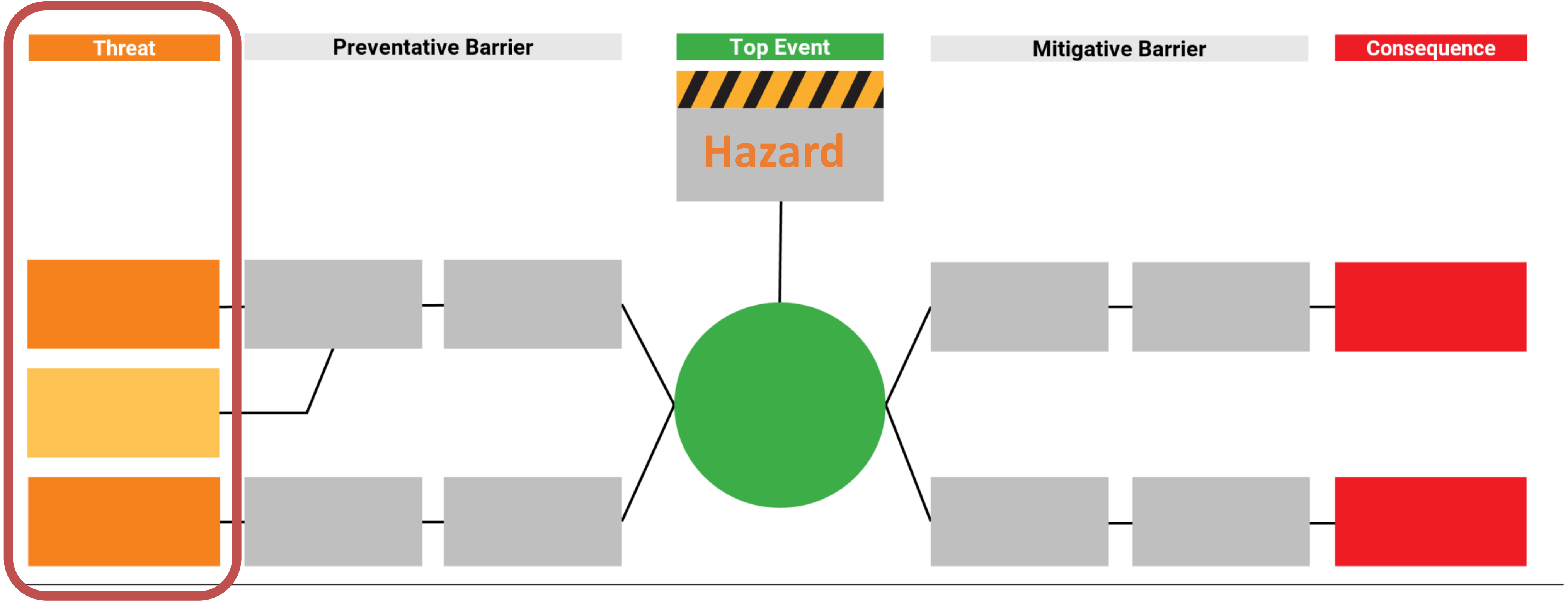
Past experience applied to the future

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

*) In Safety, “Hazard” would replace “Vulnerability”

**) In Safety, the term “Threat” is not limited to intentional acts

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

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 Safety, the term “Threat” is not limited to intentional acts

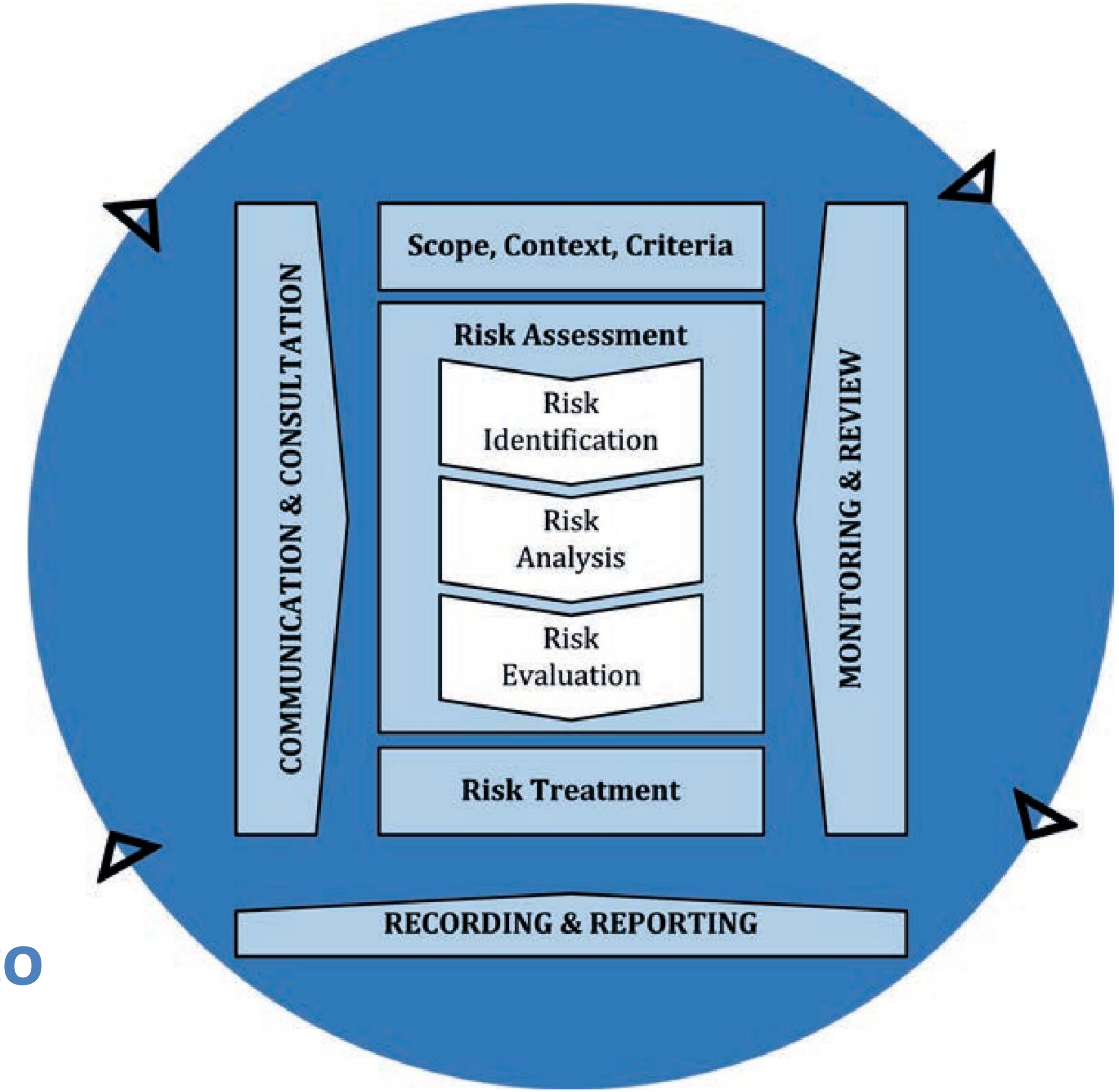
ISO 31000/27005

→ Information Security Risk Management Process

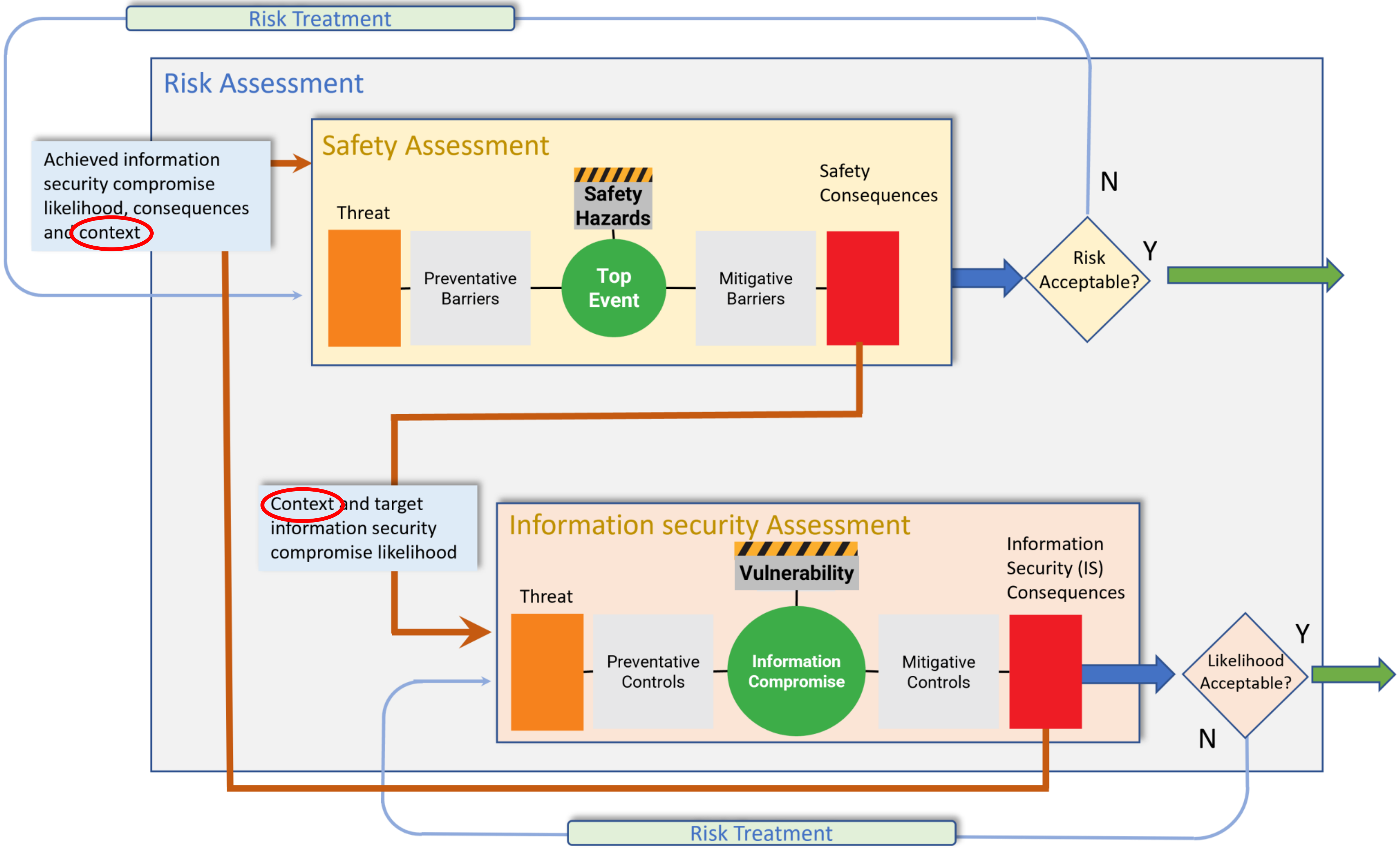
- → Treatment focuses on Information Security (which is not the full aviation scope)

- → Interdependencies between Information Security and Safety are not considered

→ **How to tie separate scopes into one common perspective?**



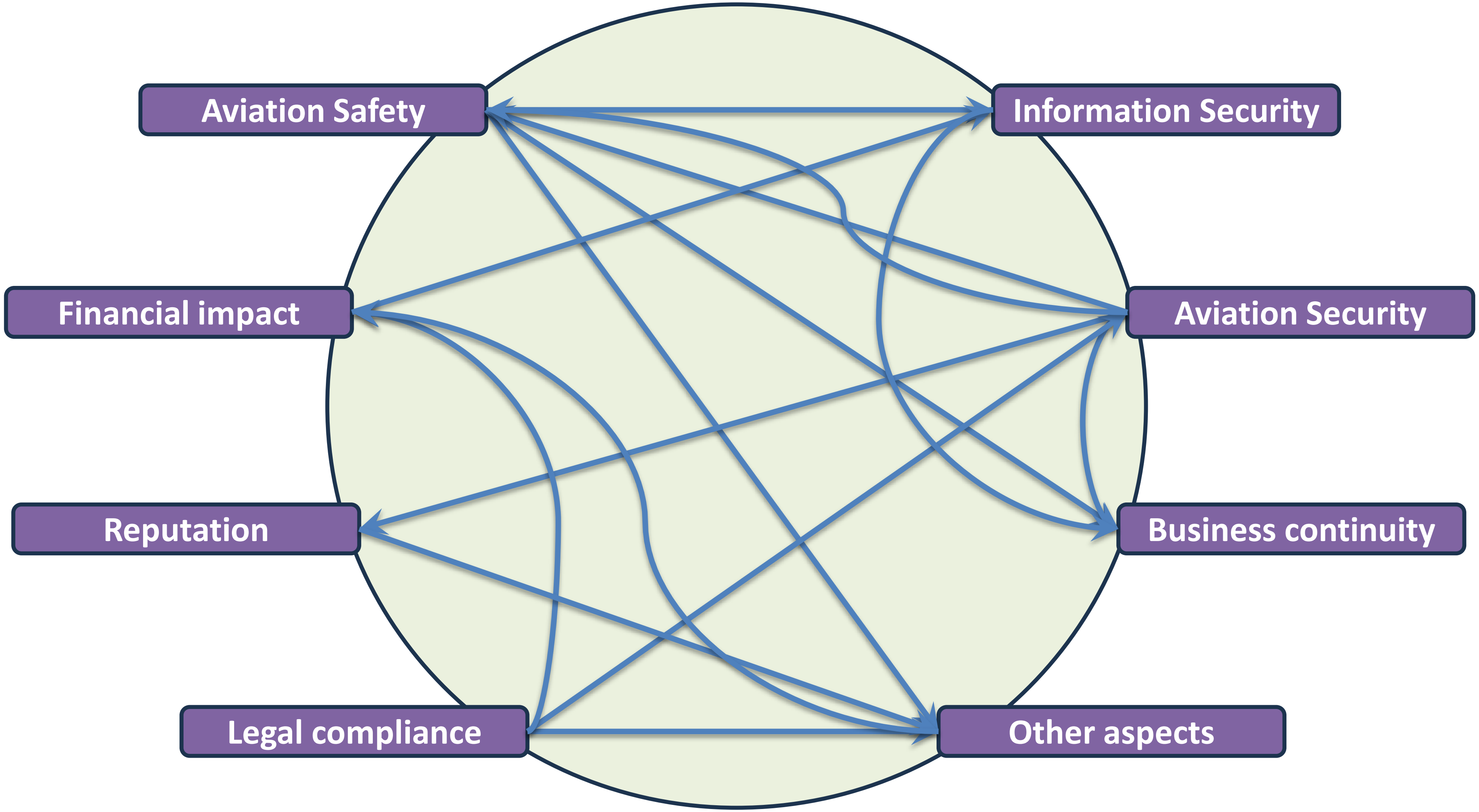
Interacting Safety & Info Sec Risk Assessment



EASA
European Union Aviation Safety Agency

The Final Message

Everything is Linked to Everything Else!



Aviation Safety

Information Security

Financial impact

Aviation Security

Reputation

Business continuity

Legal compliance

Other aspects

Safety Reminder

- → All requirements related to **Safety** are applicable to any Information Security measure, as they are part of the same context:

  Architecture, Perimeter, Environment

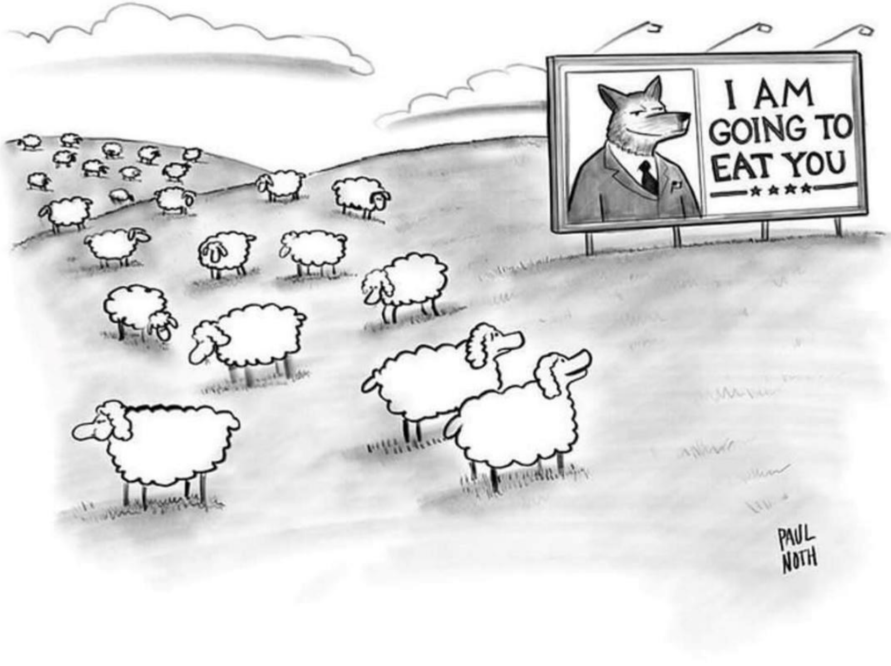
- → The level of (**Safety**) severity determines, how “badly” an organisation has to avoid them happening

  Acceptable Risks, Assurance Level

Safety Reminder, cont'd

Safety related requirements, in particular for Catastrophic / Hazardous Events, continue to be applicable:

"… to prevent a single information security failure from leading to unacceptable safety consequences."



"He tells it like it is."

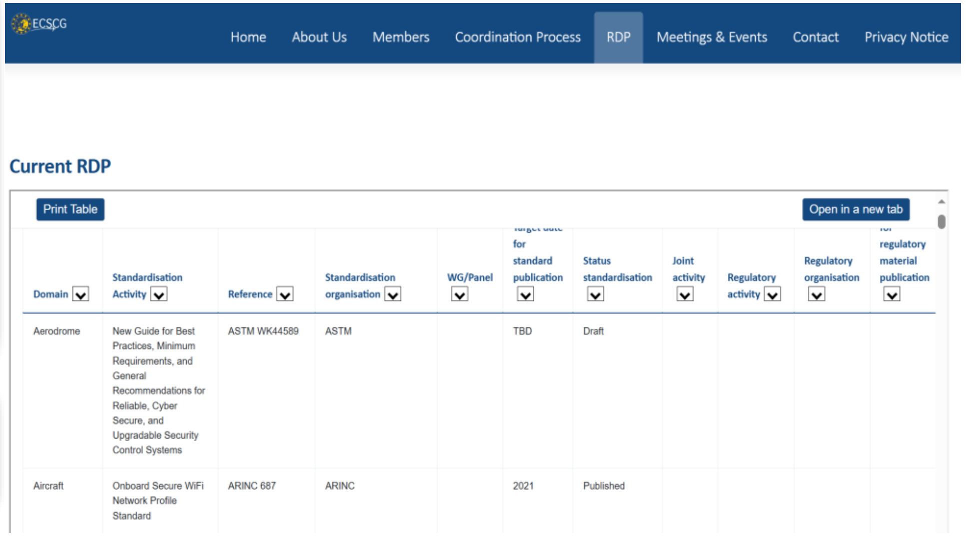
Safety Reminder, cont'd

Safety relevant specifications or standards can be found either on the **EASA** website or on the ones of **Eurocae/RTCA** or **SAE**, for example:

→ EASA CS25, SAE ARP 4754, RTCA DO-178B, Eurocae ED-153

Consult [ECSCG - ECAE RDP Tables] to find all standards relevant to Information Security in Aviation!

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



Current RDP

Domain	Standardisation Activity	Reference	Standardisation organisation	WG/Panel	Target date for standard publication	Status standardisation	Joint activity	Regulatory activity	Regulatory organisation	for regulatory material publication
Aerodrome	New Guide for Best Practices, Minimum Requirements, and General Recommendations for Reliable, Cyber Secure, and Upgradable Security Control Systems	ASTM WK44589	ASTM		TBD	Draft				
Aircraft	Onboard Secure WiFi Network Profile Standard	ARINC 687	ARINC		2021	Published				

EASA
European Union Aviation Safety Agency

A few Questions

An Agency of the European Union

A Few Questions for you (to answer on Slido):

- ✓ When is enough “enough”?
- ✓ How does Safety generally deal with threats?
- ✓ How to determine the correct assurance level?
- ✓ When to start with an IS assessment?

EASA

European Union Aviation Safety Agency

Question Resolution

An Agency of the European Union

✓ When is enough “enough”?

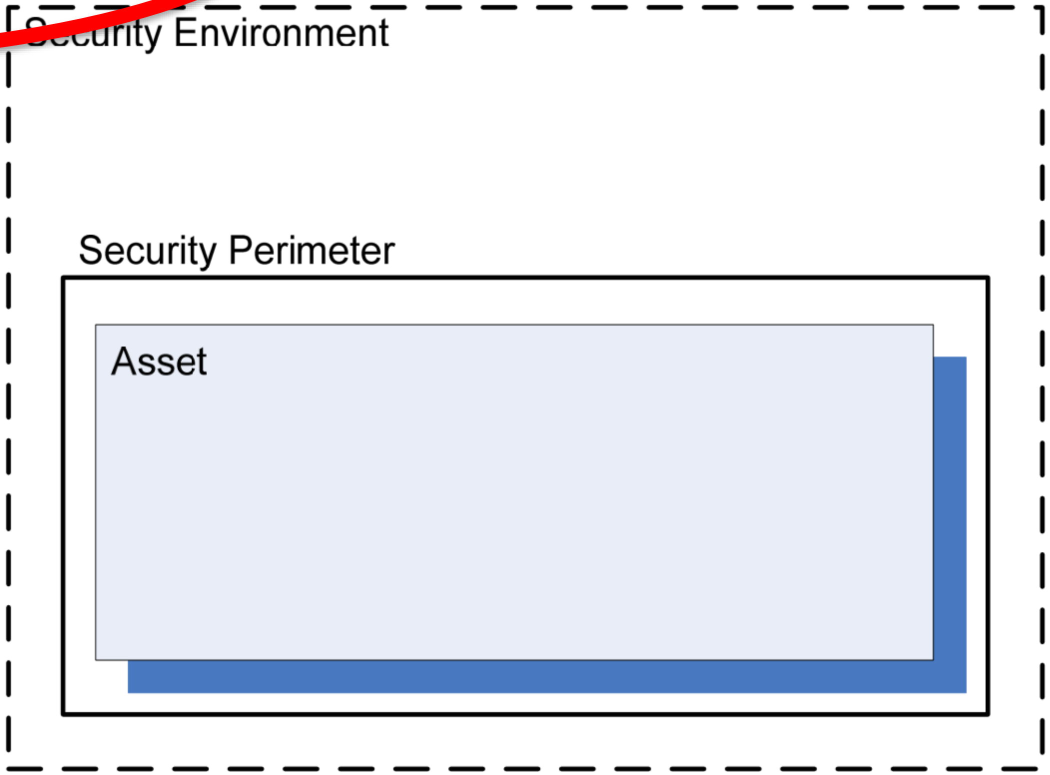
→ Part-IS is a Safety Regulation!

- Scope = *potential impact on aviation safety*

Security Environment = Outside Influence

Security Perimeter = Boundary of Safety Control

Asset = **Safety** Evaluation Item



- **Step One =**

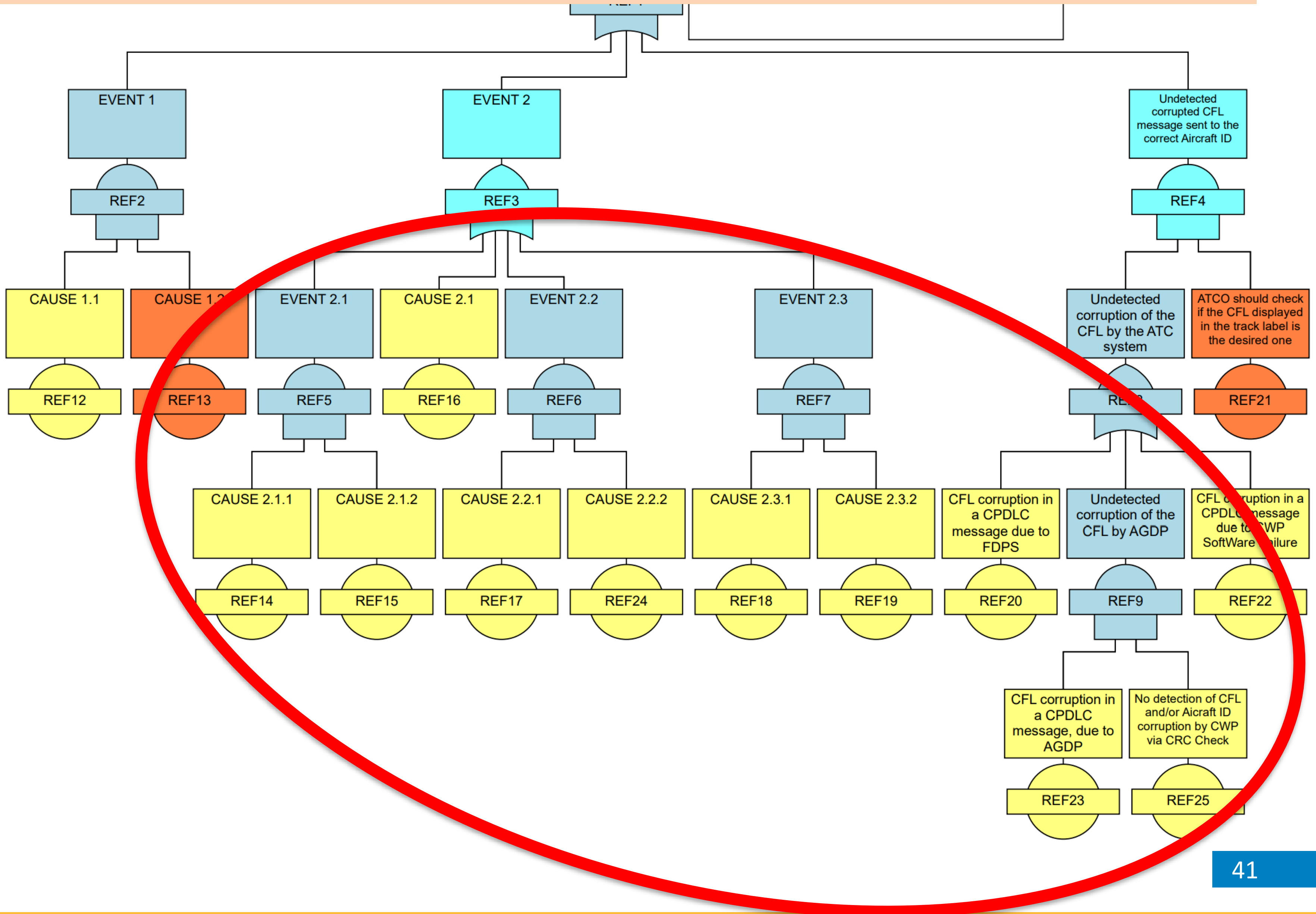
  Safety Impact Assessment

- **Step Two =**

  Safety Risk Assessment

✓ How does Safety generally deal with threats?

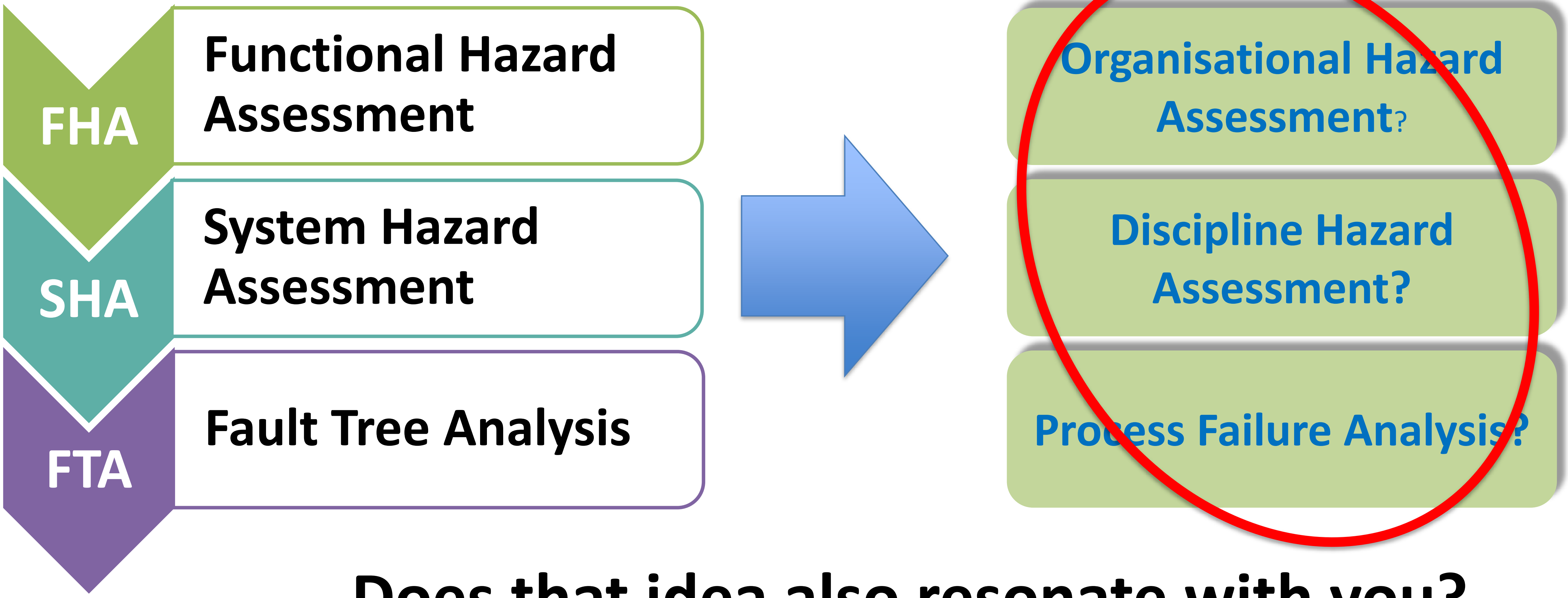
- → Look for the Information Security **Threat** on the **bottom**
- → Manifestation of the hazard is the **Top Event** on the top



REF1
EVENT 1
REF2
EVENT 2
REF3
Undetected corrupted CFL message sent to the correct Aircraft ID
REF4
CAUSE 1.1
REF12
CAUSE 1.2
REF13
EVENT 2.1
REF5
CAUSE 2.1
REF16
EVENT 2.2
REF6
EVENT 2.3
REF7
Undetected corruption of the CFL by the ATC system
REF8
ATCO should check if the CFL displayed in the track label is the desired one
REF21
CAUSE 2.1.1
REF14
CAUSE 2.1.2
REF15
CAUSE 2.2.1
REF17
CAUSE 2.2.2
REF24
CAUSE 2.3.1
REF18
CAUSE 2.3.2
REF19
CFL corruption in a CPDLC message due to FDPS
REF20
Undetected corruption of the CFL by AGDP
REF9
CFL corruption in a CPDLC message due to CWP SoftWare failure
REF22
CFL corruption in a CPDLC message, due to AGDP
REF23
No detection of CFL and/or Aicraft ID corruption by CWP via CRC Check
REF25

✓ How to determine the correct assurance level?

Transpose from Functional to Org Hazard Assessment:



FHA

Functional Hazard Assessment

SHA

System Hazard Assessment

FTA

Fault Tree Analysis

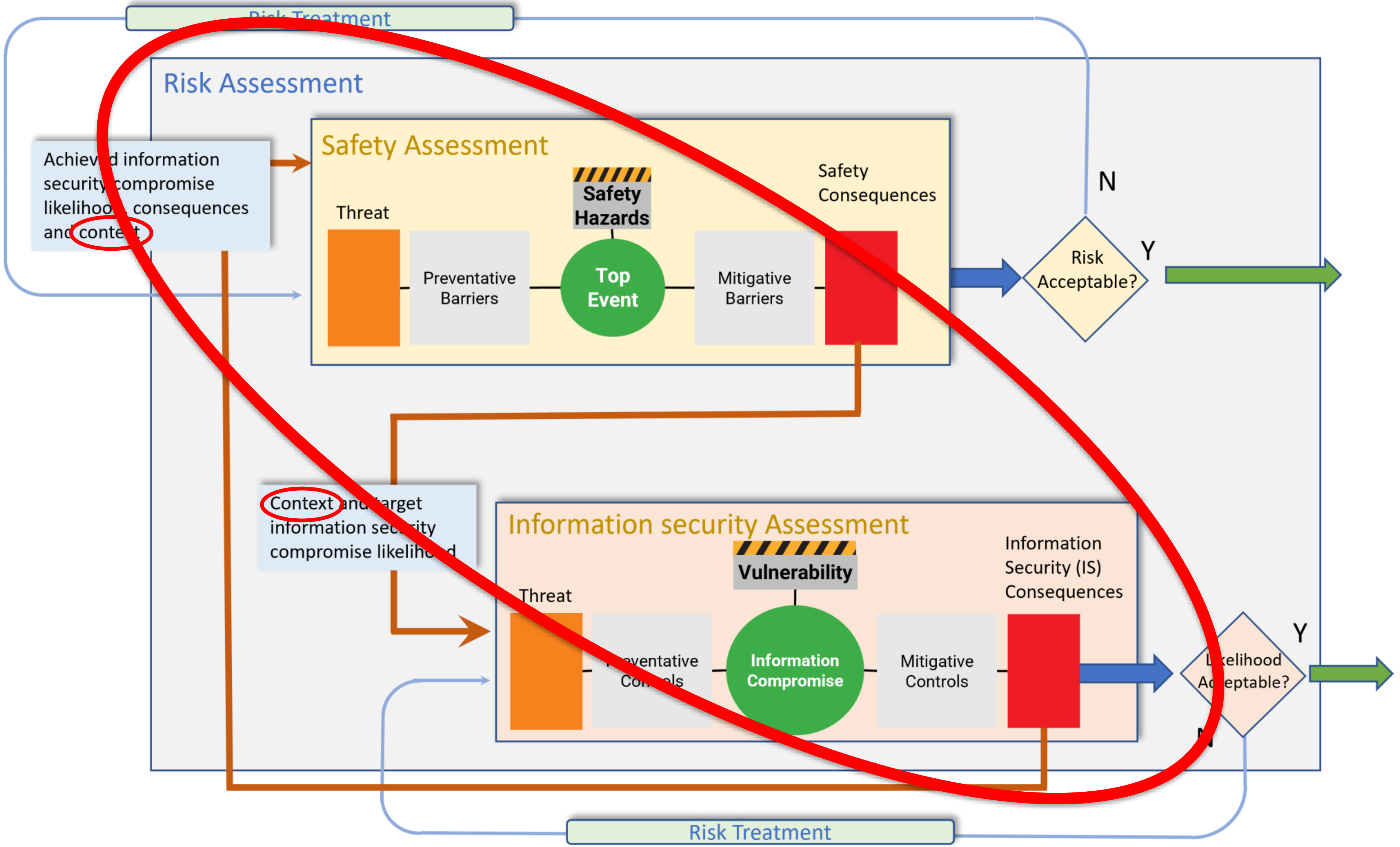
Organisational Hazard Assessment?

Discipline Hazard Assessment?

Process Failure Analysis?

Does that idea also resonate with you?

✓ When to start with an IS assessment?



So Long, and…

Thanks For All the Fish!

In other words:

This is my last event in EASA!

So long,
And thanks for all the fish.

With a background in engineering, **Gerardo Nardiello** began his professional journey in research before moving into the airline business, a field he's always been passionate about. He started his aviation career in quality management and followed its evolution into compliance monitoring. Over the years, he has been actively involved in consulting projects, auditing of operators, and training activities. He has contributed to the development of safety management systems and more recently engaged with the growing area of information security. He values continuous learning and a pragmatic approach to change.

Unlocking Synergy

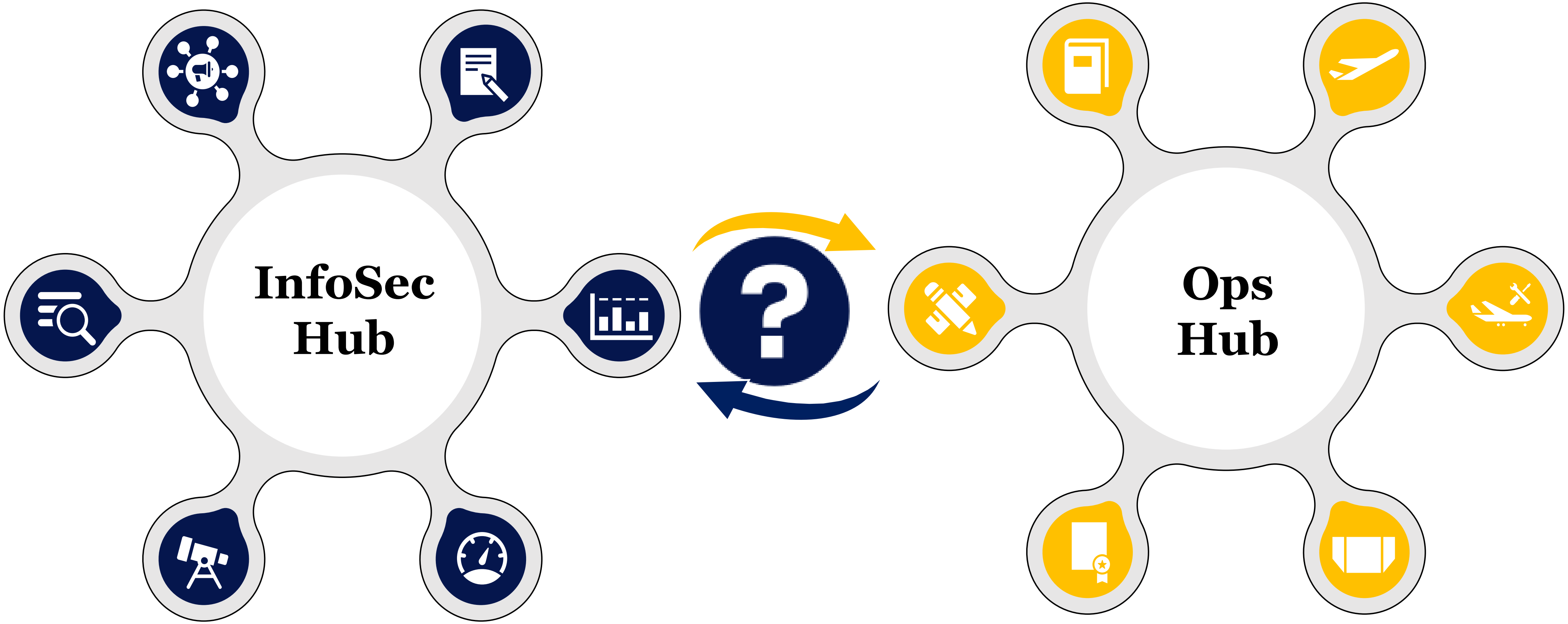
The Lufthansa Cargo Journey through Part-IS

25.06.2025, FRA F/OQ

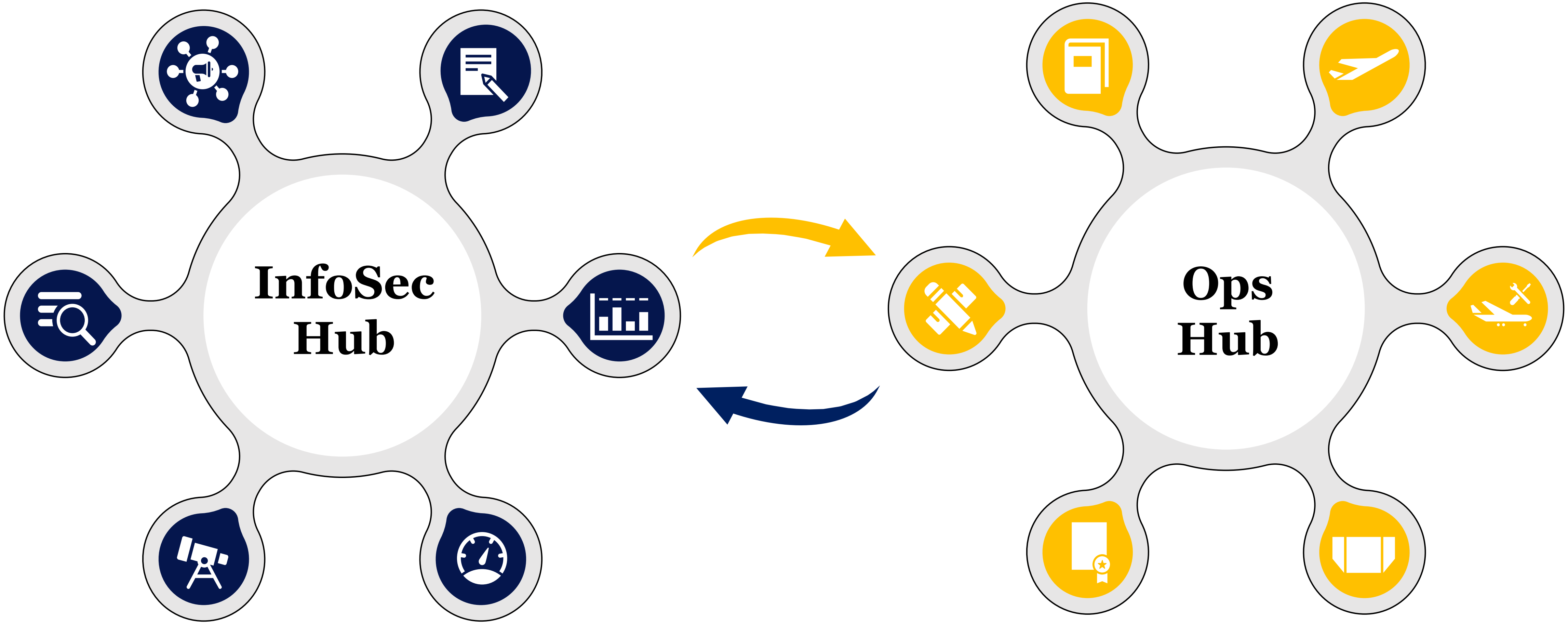
Lufthansa Cargo

COURSE
107
A/T ARM
OFF
IAS/MACH
C/O
SPEED
N1
LVL CHG
V NAV
HEADING
019
HDG SEL
L NAV
VOR LOC
APP
ALTITUDE
39000
ALT HLD
V/S
VERT SPEED
DN
UP
A/P ENGAGE
CMD A
CMD B
CWS A
CWS B
DISENGAGE
F/D ON
OFF
N1 SET
SPD REF
FUEL FLOW
AUTO BRAKE

One Objective - Two Hubs – One BIG Question

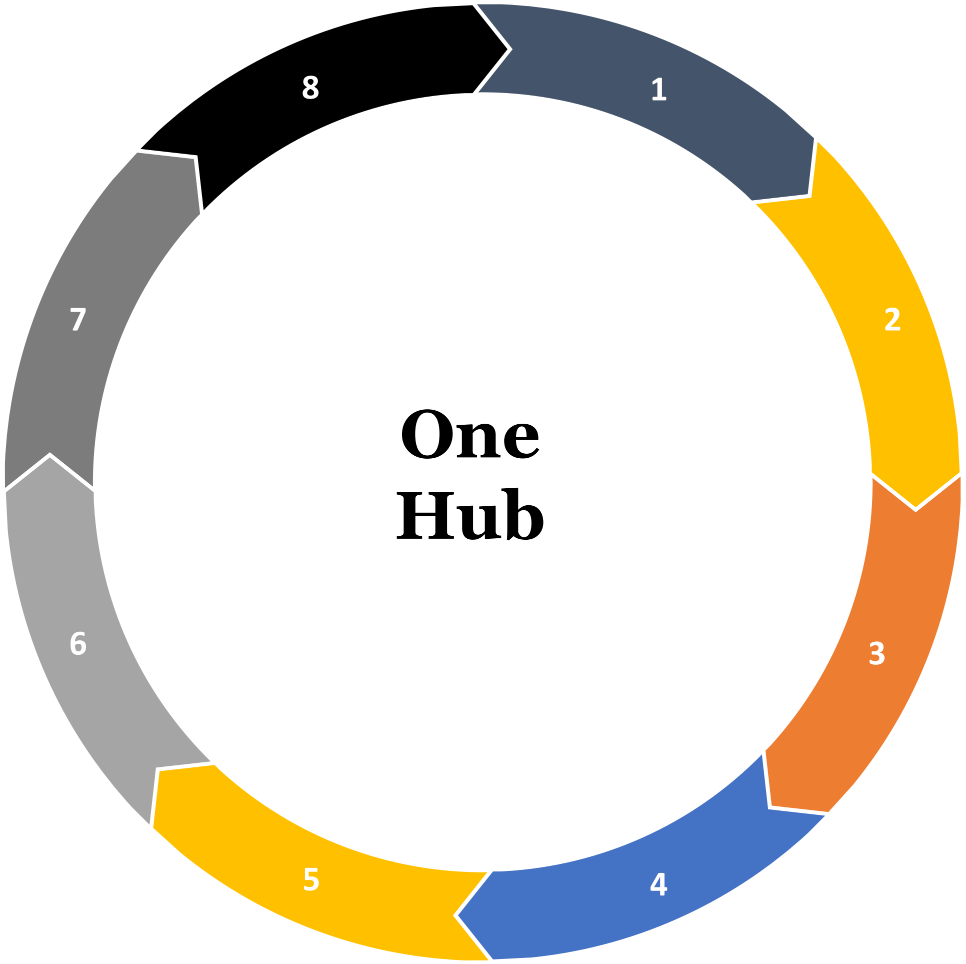


One Objective - Two Hubs – One BIG Question



Building Information Security into Operations

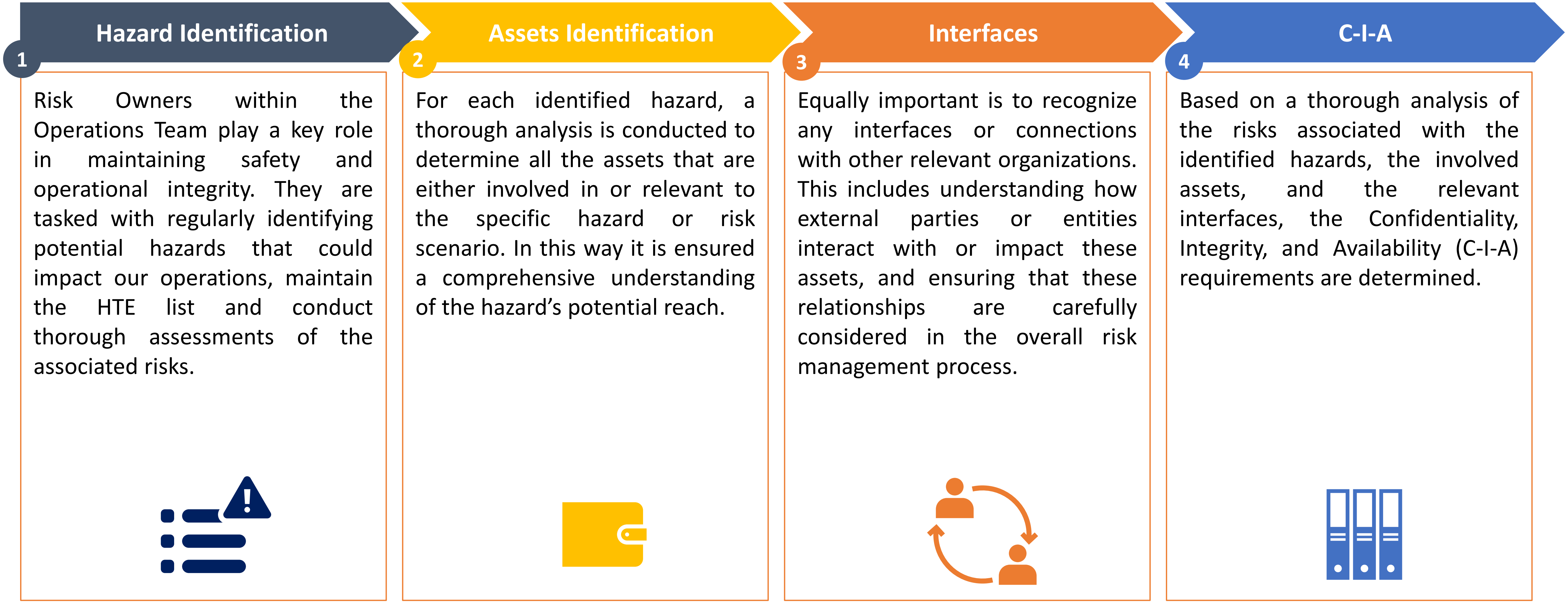
The 8-Step Part-IS Integration



1. Hazard Identification;
2. Assets Identification;
3. Interfaces;
4. C-I-A;
5. RTO/RPO;
6. Handover;
7. InfoSec Link;
8. Feedback Loop.

Process Breakdown

Steps 1 to 4



1 Hazard Identification

Risk Owners within the Operations Team play a key role in maintaining safety and operational integrity. They are tasked with regularly identifying potential hazards that could impact our operations, maintain the HTE list and conduct thorough assessments of the associated risks.

2 Assets Identification

For each identified hazard, a thorough analysis is conducted to determine all the assets that are either involved in or relevant to the specific hazard or risk scenario. In this way it is ensured a comprehensive understanding of the hazard’s potential reach.

3 Interfaces

Equally important is to recognize any interfaces or connections with other relevant organizations. This includes understanding how external parties or entities interact with or impact these assets, and ensuring that these relationships are carefully considered in the overall risk management process.

4 C-I-A

Based on a thorough analysis of the risks associated with the identified hazards, the involved assets, and the relevant interfaces, the Confidentiality, Integrity, and Availability (C-I-A) requirements are determined.

Process Breakdown

Steps 5 to 8

5 RTO/RPO

In connection with the identified relevant assets, both the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) are also established. These objectives are crucial for determining the maximum acceptable downtime and the point to which data and system functionality must be restored, ensuring that business continuity and disaster recovery plans are aligned with the criticality of the assets and the operational needs.

6 Handover

All the evaluations conducted are systematically passed on to the Appointed Person for Information Security (APIS) in the form of an HTE Control Card. This ensures that the APIS has access to comprehensive and up-to-date information on the identified risks, assets, and security requirements, allowing for informed decision-making and enhanced coordination of information security efforts.

7 InfoSec Link

The APIS serves as the crucial link between the Operations Team and the Information Security Team, ensuring seamless communication and collaboration between the two. The APIS is responsible for making sure that the specific security requirements dictated by operations are continuously upheld and integrated into the overall security framework.

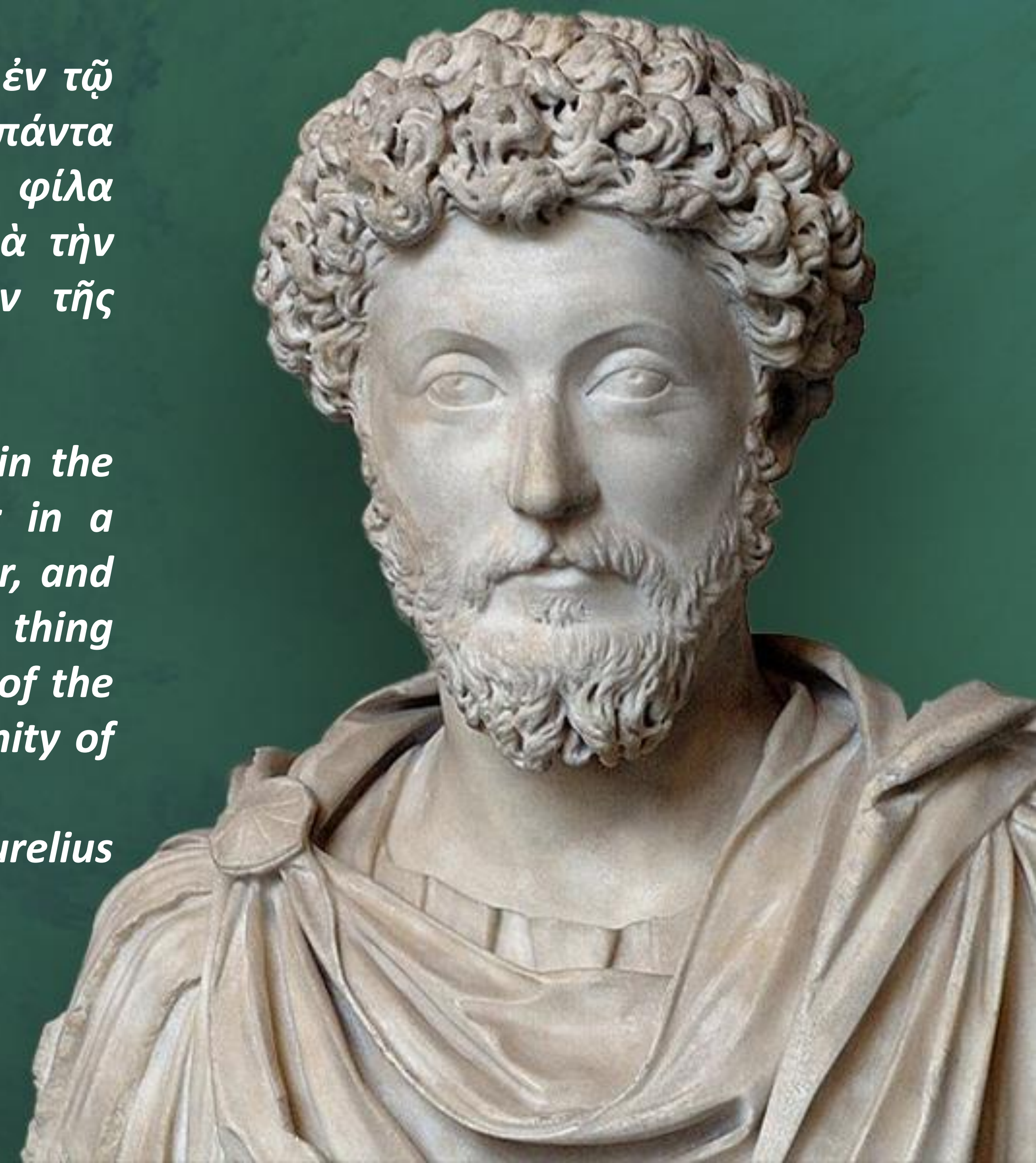
8 Feedback Loop

A feedback loop is established to ensure that critical information is promptly communicated in the event of incidents occurred or newly identified vulnerabilities.

“Πολλάκις ἐνθυμοῦ τὴν ἐπισύνδεσιν πάντων τῶν ἐν τῷ κόσμῳ καὶ σχέσιν πρὸς ἄλληλα. τρόπον γάρ τινα πάντα ἀλλήλοις ἐπιπέπλεκται καὶ πάντα κατὰ τοῦτο φίλα ἀλλήλοις ἐστί: καὶ γὰρ ἄλλῳ ἑξῆς ἐστι τοῦτο διὰ τὴν τονικὴν κίνησιν καὶ σύμπνοιαν καὶ τὴν ἕνωσιν τῆς οὐσίας.”

“Frequently consider the connection of all things in the universe and their relation to one another. For in a manner all things are implicated with one another, and all in this way are friendly to one another; for one thing comes in order after another, and this is by virtue of the active movement and mutual sympathy and the unity of the substance.”

M. Aurelius



Gerardo Nardiello
Deputy Compliance Monitoring Manager
Email: gerardo.nardiello@dlh.de
Phone: +49 69 696-55744

Lufthansa Cargo
Networking the world.

Alessio Piroli is the focal point for Safety Management System and Information Security Management System implementation in Secondo Mona approved maintenance and production organizations. He belongs to the Company Quality and Safety Department, with also the role of auditor and trainer.

Alessio has previously held also roles as Training Manager, instructor and examiner in Part-147 certified training organizations.

Alessio holds a master’s degree in Aerospace Engineering.

EASA Part-IS IMPLEMENTATION IN SECONDO MONA CERTIFIED ORGANIZATIONS

Alessio Piroli

EASA Part-IS Implementation Workshop - Cologne, 25 June 2025

SECONDO MONA S.P.A. COMPANY PRESENTATION

Secondo Mona, an Italian company founded in 1903, with its sole headquarters in Somma Lombardo (Italy), has been active in the aerospace sector since 1913 with the repair of the first aircraft engines. Today Secondo Mona is established in the global aerospace market, employing about 340 employees, and has become a preferred supplier of fuel systems and subsystems for fixed and rotary wing aircraft and UAVs, both civil and military.

120 YEARS of History and Aerospace Technology

PRESSURE REFUEL AND DEFUEL SYSTEMS

FUEL MANAGEMENT SYSTEMS, LEVEL SENSORS

NLG LOCK LINK

ELECTRICAL SHUT OFF VALVES AND MANIFOLDS

HYDRAULIC EQUIPMENT

PITCH TRIM ACTUATOR

FREE-WHEEL ACTUATOR

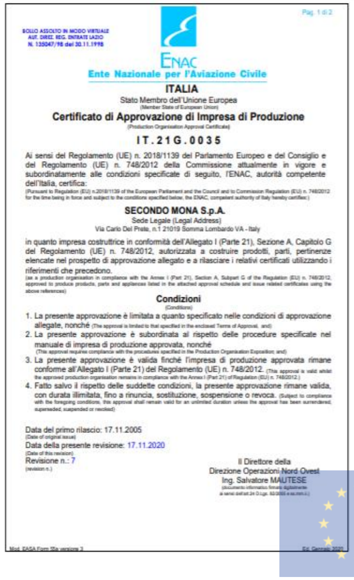
AC AND DC PUMPS, EJECTOR PUMPS

APPROVALS

CERTIFICATIONS – CIVIL REQUIREMENTS

PRODUCTION

EASA Part 21.G POA
IT.21G.0035



BOLLO ASSOLTO IN MODO VIRTUALE
AUT. DIREZ. REG. ENTRATE LAZIO
N. 135047/98 del 30.11.1998

Pag. 1 di 2

ENAC
Ente Nazionale per l'Aviazione Civile
ITALIA
Stato Membro dell'Unione Europea
(Member State of European Union)

Certificato di Approvazione di Impresa di Produzione
(Production Organisation Approval Certificate)

IT.21G.0035

Ai sensi del Regolamento (UE) n. 2018/1139 del Parlamento Europeo e del Consiglio e del Regolamento (UE) n. 748/2012 della Commissione attualmente in vigore e subordinatamente alle condizioni specificate di seguito, l'ENAC, autorità competente dell'Italia, certifica:
(Pursuant to Regulation (EU) n.2018/1139 of the European Parliament and the Council and to Commission Regulation (EU) n. 748/2012 for the time being in force and subject to the conditions specified below, the ENAC, competent authority of Italy hereby certifies:)

SECONDO MONA S.p.A.
Sede Legale (Legal Address)
Via Carlo Del Prete, n.1 21019 Somma Lombardo VA - Italy

in quanto impresa costruttrice in conformità dell'Allegato I (Parte 21), Sezione A, Capitolo G del Regolamento (UE) n. 748/2012, autorizzata a costruire prodotti, parti, pertinenze elencate nel prospetto di approvazione allegato e a rilasciare i relativi certificati utilizzando i riferimenti che precedono.
(as a production organisation in compliance with the Annex I (Part 21), Section A, Subpart G of the Regulation (EU) n. 748/2012, approved to produce products, parts and appliances listed in the attached approval schedule and issue related certificates using the above references)

Condizioni
(Conditions)

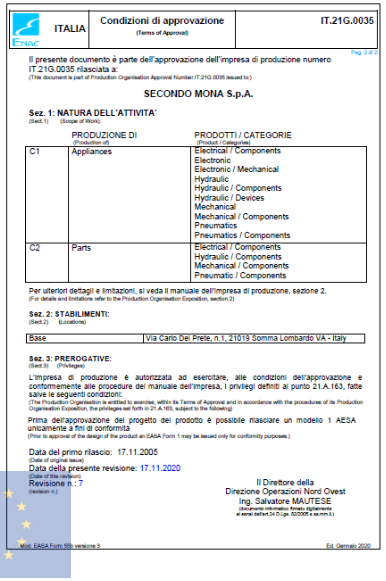
1. La presente approvazione è limitata a quanto specificato nelle condizioni di approvazione allegate, nonché (The approval is limited to that specified in the enclosed Terms of Approval, and)
2. La presente approvazione è subordinata al rispetto delle procedure specificate nel manuale di impresa di produzione approvata, nonché (This approval requires compliance with the procedures specified in the Production Organisation Exposition; and)
3. La presente approvazione è valida finché l'impresa di produzione approvata rimane conforme all'Allegato I (Parte 21) del Regolamento (UE) n. 748/2012. (This approval is valid whilst the approved production organisation remains in compliance with the Annex I (Part 21) of Regulation (EU) n. 748/2012.)
4. Fatto salvo il rispetto delle suddette condizioni, la presente approvazione rimane valida, con durata illimitata, fino a rinuncia, sostituzione, sospensione o revoca. (Subject to compliance with the foregoing conditions, this approval shall remain valid for an unlimited duration unless the approval has been surrendered, superseded, suspended or revoked)

Data del primo rilascio: 17.11.2005
(Date of original issue)
Data della presente revisione: 17.11.2020
(Date of this revision)
Revisione n.: 7
(revision n.)

Il Direttore della
Direzione Operazioni Nord Ovest
Ing. Salvatore MAUTESE
(documento informatico firmato digitalmente
ai sensi dell'art.24 D.Lgs. 82/2005 e ss.mm.ii.)

Mod. EASA Form 55a versione 3

Ed. Gennaio 2020



ENAC ITALIA	Condizioni di approvazione (Terms of Approval)	IT.21G.0035

Pag. 2 di 2

Il presente documento è parte dell'approvazione dell'impresa di produzione numero IT.21G.0035 rilasciata a:
(This document is part of Production Organisation Approval Number IT.21G.0035 issued to:)

SECONDO MONA S.p.A.

Sez. 1: NATURA DELL'ATTIVITA'
(Sect.1) (Scope of Work):

	PRODUZIONE DI (Production of)	PRODOTTI / CATEGORIE (Product / Categories)
C1	Appliances	Electrical / Components Electronic Electronic / Mechanical Hydraulic Hydraulic / Components Hydraulic / Devices Mechanical Mechanical / Components Pneumatics Pneumatics / Components
C2	Parts	Electrical / Components Hydraulic / Components Mechanical / Components Pneumatic / Components

Per ulteriori dettagli e limitazioni, si veda il manuale dell'impresa di produzione, sezione 2.
(For details and limitations refer to the Production Organisation Exposition, section 2)

Sez. 2: STABILIMENTI:
(Sect.2) (Locations)

Base	Via Carlo Del Prete, n.1, 21019 Somma Lombardo VA - Italy

Sez. 3: PREROGATIVE:
(Sect.3) (Privileges)

L'impresa di produzione è autorizzata ad esercitare, alle condizioni dell'approvazione e conformemente alle procedure del manuale dell'impresa, i privilegi definiti al punto 21.A.163, fatte salve le seguenti condizioni:
(The Production Organisation is entitled to exercise, within its Terms of Approval and in accordance with the procedures of its Production Organisation Exposition, the privileges set forth in 21.A.163, subject to the following)

Prima dell'approvazione del progetto del prodotto è possibile rilasciare un modello 1 AESA unicamente a fini di conformità
(Prior to approval of the design of the product an EASA Form 1 may be issued only for conformity purposes.)

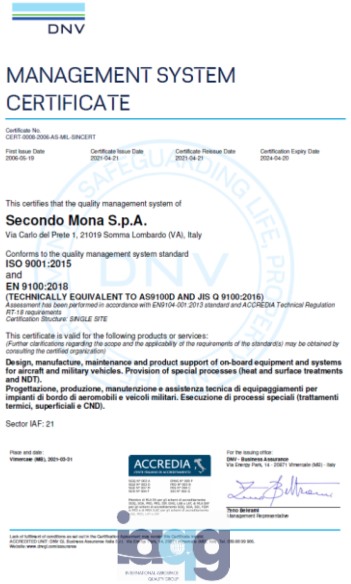
Data del primo rilascio: 17.11.2005
(Date of original issue)
Data della presente revisione: 17.11.2020
(Date of this revision)
Revisione n.: 7
(revision n.)

Il Direttore della
Direzione Operazioni Nord Ovest
Ing. Salvatore MAUTESE
(documento informatico firmato digitalmente
ai sensi dell'art.24 D.Lgs. 82/2005 e ss.mm.ii.)

Mod. EASA Form 55b versione 3

Ed. Gennaio 2020

EN 9100:2018



DNV

MANAGEMENT SYSTEM
CERTIFICATE

Certificate No.
CERT-0008-2006-AS-MIL-SINCERT

First Issue Date	Certificate Issue Date	Certificate Reissue Date	Certification Expiry Date
2006-05-19	2021-04-21	2021-04-21	2024-04-20

This certifies that the quality management system of
Secondo Mona S.p.A.
Via Carlo del Prete 1, 21019 Somma Lombardo (VA), Italy

Conforms to the quality management system standard
ISO 9001:2015
and
EN 9100:2018
(TECHNICALLY EQUIVALENT TO AS9100D AND JIS Q 9100:2016)
Assessment has been performed in accordance with EN9104-001:2013 standard and ACCREDIA Technical Regulation RT-18 requirements
Certification Structure: SINGLE SITE

This certificate is valid for the following products or services:
(Further clarifications regarding the scope and the applicability of the requirements of the standard(s) may be obtained by consulting the certified organization)

Design, manufacture, maintenance and product support of on-board equipment and systems for aircraft and military vehicles. Provision of special processes (heat and surface treatments and NDT).
Progettazione, produzione, manutenzione e assistenza tecnica di equipaggiamenti per impianti di bordo di aeromobili e veicoli militari. Esecuzione di processi speciali (trattamenti termici, superficiali e CND).

Sector IAF: 21

Place and date:
Vimercate (MB), 2021-03-31

ACCREDIA

For the issuing office:
DNV - Business Assurance
Via Energy Park, 14 - 20871 Vimercate (MB) - Italy

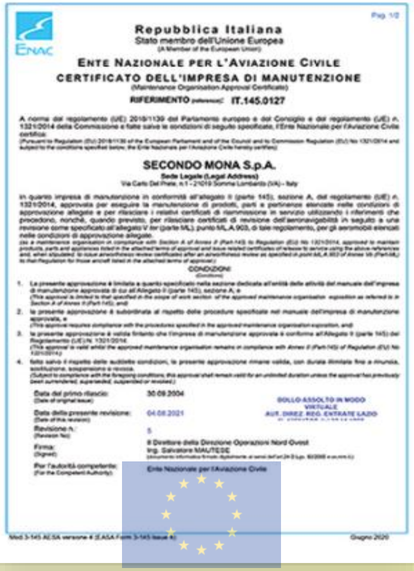
Zeno Beltrami
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
ACCREDITED UNIT: DNV GL Business Assurance Italia S.r.l., Via Energy Park, 14, 20871 Vimercate (MB) - Italy. Tel. 039.68 99 905.
Website: www.dnvgl.com/assurance

IAQG
INTERNATIONAL AEROSPACE QUALITY GROUP

MAINTENANCE

EASA MOA
Part 145
IT.145.0127



Pag. 1/2

ENAC

Repubblica Italiana
Stato membro dell'Unione Europea
(A Member of the European Union)

ENTE NAZIONALE PER L'AVIAZIONE CIVILE
CERTIFICATO DELL'IMPRESA DI MANUTENZIONE
(Maintenance Organisation Approval Certificate)
RIFERIMENTO (reference): **IT.145.0127**

A norma del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio e del regolamento (UE) n. 1321/2014 della Commissione e fatte salve le condizioni di seguito specificate, l'Ente Nazionale per l'Aviazione Civile certifica:
(Pursuant to Regulation (EU) 2018/1139 of the European Parliament and of the Council and to Commission Regulation (EU) No 1321/2014 and subject to the conditions specified below, the Ente Nazionale per l'Aviazione Civile hereby certifies)

SECONDO MONA S.p.A.
Sede Legale (Legal Address)
Via Carlo Del Prete, n.1 - 21019 Somma Lombardo (VA) – Italy

in quanto impresa di manutenzione in conformità all'allegato II (parte 145), sezione A, del regolamento (UE) n. 1321/2014, approvata per eseguire la manutenzione di prodotti, parti e pertinenze elencate nelle condizioni di approvazione allegate e per rilasciare i relativi certificati di riammissione in servizio utilizzando i riferimenti che precedono, nonché, quando previsto, per rilasciare certificati di revisione dell'aeronavigabilità in seguito a una revisione come specificato all'allegato V ter (parte ML), punto ML.A.903, di tale regolamento, per gli aeromobili elencati nelle condizioni di approvazione allegate.
(as a maintenance organisation in compliance with Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014, approved to maintain products, parts and appliances listed in the attached terms of approval and issue related certificates of release to service using the above references and, when stipulated, to issue airworthiness review certificates after an airworthiness review as specified in point ML.A.903 of Annex Vb (Part-ML) to that Regulation for those aircraft listed in the attached terms of approval.)

CONDIZIONI
(Conditions)

1. La presente approvazione è limitata a quanto specificato nella sezione dedicata all'entità delle attività del manuale dell'impresa di manutenzione approvata di cui all'Allegato II (parte 145), sezione A, e
(This approval is limited to that specified in the scope of work section of the approved maintenance organisation exposition as referred to in Section A of Annex II (Part-145), and)
2. la presente approvazione è subordinata al rispetto delle procedure specificate nel manuale dell'impresa di manutenzione approvata, e
(This approval requires compliance with the procedures specified in the approved maintenance organisation exposition, and)
3. la presente approvazione è valida fintanto che l'impresa di manutenzione approvata è conforme all'Allegato II (parte 145) del Regolamento (UE) N. 1321/2014.
(This approval is valid whilst the approved maintenance organisation remains in compliance with Annex II (Part-145) of Regulation (EU) No 1321/2014.)
4. fatto salvo il rispetto delle suddette condizioni, la presente approvazione rimane valida, con durata illimitata fino a rinuncia, sostituzione, sospensione o revoca.
(Subject to compliance with the foregoing conditions, this approval shall remain valid for an unlimited duration unless the approval has previously been surrendered, superseded, suspended or revoked.)

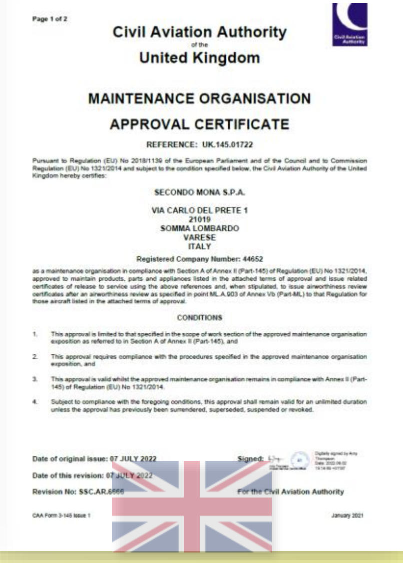
Data del primo rilascio: (Date of original issue)	30.09.2004
Data della presente revisione: (Date of this revision)	04.08.2021
Revisione n.: (Revision No)	5
Firma: (Signed)	Il Direttore della Direzione Operazioni Nord Ovest Ing. Salvatore MAUTESE [illegible]
Per l'autorità competente: (For the Competent Authority)	Ente Nazionale per l'Aviazione Civile

BOLLO ASSOLTO IN MODO VIRTUALE
AUT. DIREZ. REG. ENTRATE LAZIO
[illegible]

Mod 3-145 AESA versione 4 (EASA Form 3-145 Issue 4)

Giugno 2020

UK MOA
UK Part 145
UK.145.01722



Page 1 of 2

Civil Aviation Authority
of the
United Kingdom

MAINTENANCE ORGANISATION
APPROVAL CERTIFICATE

REFERENCE: UK.145.01722

Pursuant to Regulation (EU) No 2018/1139 of the European Parliament and of the Council and to Commission Regulation (EU) No 1321/2014 and subject to the condition specified below, the Civil Aviation Authority of the United Kingdom hereby certifies:

SECONDO MONA S.P.A.

VIA CARLO DEL PRETE 1
21019
SOMMA LOMBARDO
VARESE
ITALY

Registered Company Number: 44652

as a maintenance organisation in compliance with Section A of Annex II (Part-145) of Regulation (EU) No 1321/2014, approved to maintain products, parts and appliances listed in the attached terms of approval and issue related certificates of release to service using the above references and, when stipulated, to issue airworthiness review certificates after an airworthiness review as specified in point ML.A.903 of Annex Vb (Part-ML) to that Regulation for those aircraft listed in the attached terms of approval.

CONDITIONS

1. This approval is limited to that specified in the scope of work section of the approved maintenance organisation exposition as referred to in Section A of Annex II (Part-145), and
2. This approval requires compliance with the procedures specified in the approved maintenance organisation exposition, and
3. This approval is valid whilst the approved maintenance organisation remains in compliance with Annex II (Part-145) of Regulation (EU) No 1321/2014.
4. Subject to compliance with the foregoing conditions, this approval shall remain valid for an unlimited duration unless the approval has previously been surrendered, superseded, suspended or revoked.

Date of original issue: 07 JULY 2022
Date of this revision: 07 JULY 2022
Revision No: SSC.AR.6666

Signed:
Digitally signed by Amy Thompson
Date: 2022.08.02 [illegible]
For the Civil Aviation Authority

CAA Form 3-145 Issue 1

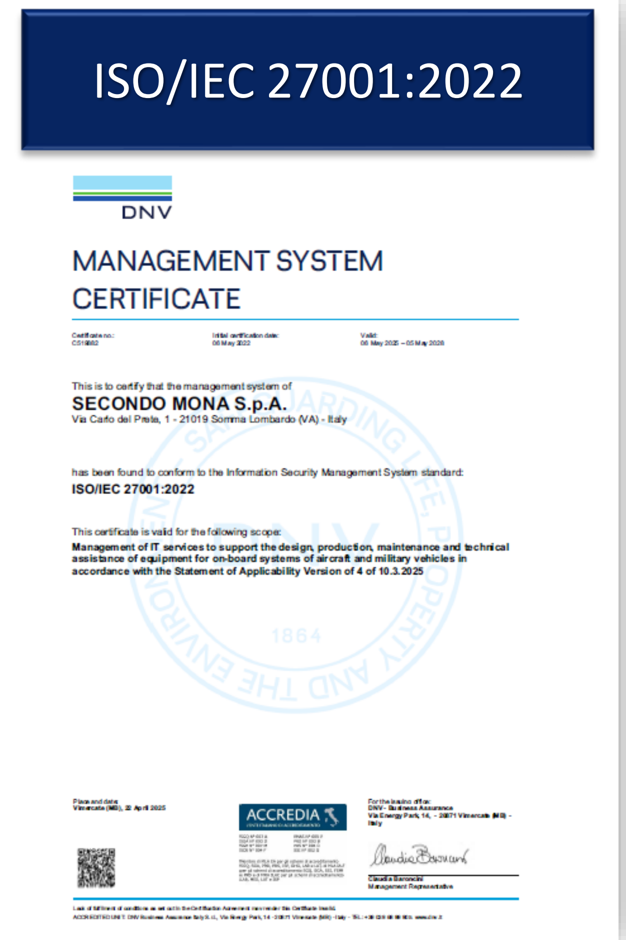
January 2021

FAA Repair Station
14 CFR Part 145
1E8Y986C

APPROVALS

CERTIFICATIONS – CYBERSECURITY

ISO/IEC 27001:2022



MANAGEMENT SYSTEM CERTIFICATE

Certificate no.:	Initial certification date:	Valid:
C519882	06 May 2022	06 May 2025 – 05 May 2028

This is to certify that the management system of

SECONDO MONA S.p.A.
Via Carlo del Prete, 1 - 21019 Somma Lombardo (VA) - Italy

has been found to conform to the Information Security Management System standard:

ISO/IEC 27001:2022

This certificate is valid for the following scope:

Management of IT services to support the design, production, maintenance and technical assistance of equipment for on-board systems of aircraft and military vehicles in accordance with the Statement of Applicability Version of 4 of 10.3.2025

Place and date:
Vimercate (MB), 22 April 2025

ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

[illegible]

For the issuing office:
DNV - Business Assurance
Via Energy Park, 14, - 20871 Vimercate (MB) - Italy

Claudia Baroncini
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

ACCREDITED UNIT: DNV Business Assurance Italy S.r.l., Via Energy Park, 14 - 20871 Vimercate (MB) - Italy - TEL: +39 039 68 99 905. www.dnv.it

PART-IS IMPLEMENTATION SECONDO MONA VISION

Strategic project

The Information Security Management System is a strategic project that projects the company into the future

Cost reduction

Elimination/reduction of costs related to vulnerability

Opportunity

Protection of internal processes, with related improvement

Communication

New inputs, better bidirectionality

PART-IS IMPLEMENTATION

BRICK N°1 – SAFETY MANAGEMENT SYSTEM

- Integrated SMS for every company certifications
- Safety Review Board (SRB) and Safety Action Group (SAG) in place
- SMS dedicated area in Company PLM
- Strong safety promotion (SMS logo, Company Events, contest for mascot, webinar for suppliers)
- SMS good maturity level achieved

SecondoMona
Secondo Mona
1903
Safety Management System

TRAINING FOR AERONAUTICAL SUPPLIERS IN THE SECONDO MONA SUPPLY CHAIN

WEBINAR

GROWING BETTER TOGETHER

Martedì 30 luglio 2024
Ore 10.00-11.30

INTRODUZIONE AL
SAFETY MANAGEMENT SYSTEM
Per i Fornitori della Supply Chain di Secondo Mona SpA

*La tecnologia ti fa raggiungere il cielo,
la sicurezza ti fa tornare a casa.*

PART-IS IMPLEMENTATION

BRICK N°2 – INFORMATION SECURITY SYSTEM

Information Security Management

ISO

27001

Certified

- ISO 27001 certification since 2022
- Four-levels classification of information
- Company Information Security policies in place (e.g. Clear Desk policy, Clear Screen policy, Password Management policy)
- Business Continuity Model
- Vulnerability tests
- IS good maturity level achieved

COMPANY CONFIDENTIAL

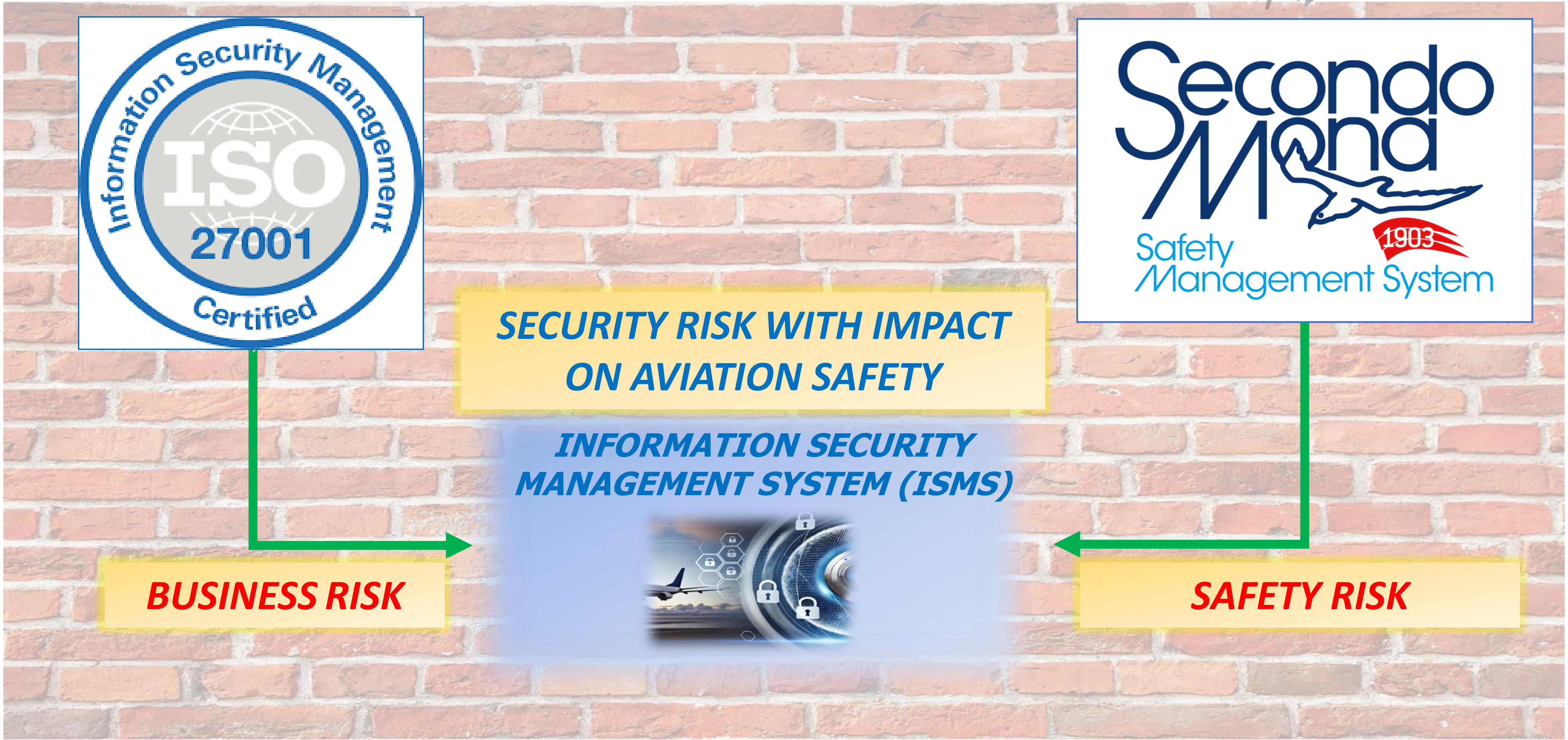
COMPANY RESTRICTED

COMPANY INTERNAL

COMPANY GENERAL USE

PART-IS IMPLEMENTATION

THE STARTING POINT: JOINING THE BRICKS



SECURITY RISK WITH IMPACT ON AVIATION SAFETY

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

BUSINESS RISK

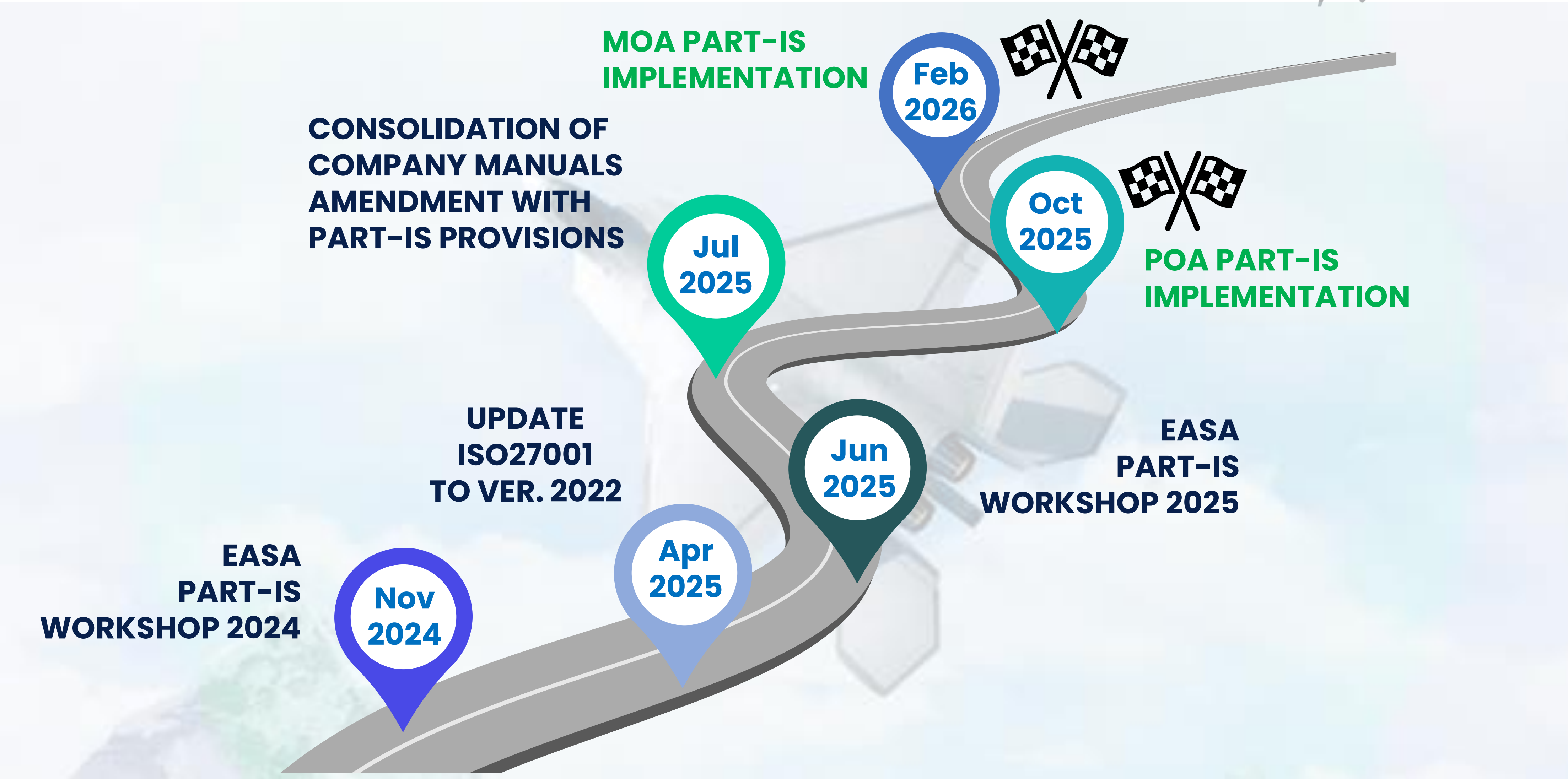
SAFETY RISK

PART-IS IMPLEMENTATION — FIRST STEP – ACTIONS AT SMS LEVEL

During Safety Management System (SMS) implementation process (started in **December 2022**), the following provisions has been introduced as **first step to implement the management** of Aviation Information Security risk:

- ICT/Cybersecurity manager nominated as member of SMS **Safety Action Group (SAG)**
- ICT/Cybersecurity section in SMS **Hazard Log**, with evaluation of hazard related to Information Security which could impact Aviation Safety.

PART-IS IMPLEMENTATION ROAD TO ISMS



Nov 2024 — EASA PART-IS WORKSHOP 2024

Apr 2025 — UPDATE ISO27001 TO VER. 2022

Jun 2025 — EASA PART-IS WORKSHOP 2025

Jul 2025 — CONSOLIDATION OF COMPANY MANUALS AMENDMENT WITH PART-IS PROVISIONS

Oct 2025 — POA PART-IS IMPLEMENTATION

Feb 2026 — MOA PART-IS IMPLEMENTATION

IMPLEMENTATION ELEMENTS

- **ISMS provisions introduced in the existing manuals framework (MOE, POE, SMM and ISM)**
- **Common system for MOA and POA (fully integrated in SMS)**
- Voluntary reporting system established for SMS extended to ISMS: use of **Hazard Events Reporting Occurrence (HERO) Form**
- Safety promotion systems implemented for SMS used also for ISMS

ISMS PROMOTION

- **Wide dissemination of Company Information Security Policy**
- **Internal communication system newsletter (ISMS news)**
- Installation of ISMS posters in production areas
- Company Safety Culture Survey
- Company events to promote SMS and ISMS principles
- **Personnel training provided to company personnel by internal trainers (CRUCIAL)**

SAFETY AND SECURITY PROMOTION - SAFETY VS SECURITY

SAFETY VS SECURITY:
TWO SIDES OF THE SAME COIN

Safety is the set of measures adopted to protect against **UNINTENDED** events, such as **human errors, incidents and damage from adverse environmental conditions.**

Security is the set of measures adopted to prevent **INTENTIONAL** acts carried out with the intent to **cause damage.**

AVIATION SAFETY: everyone's responsibility

SM Quality & Safety team

SAFETY VS SECURITY:
TWO SIDES OF THE SAME COIN

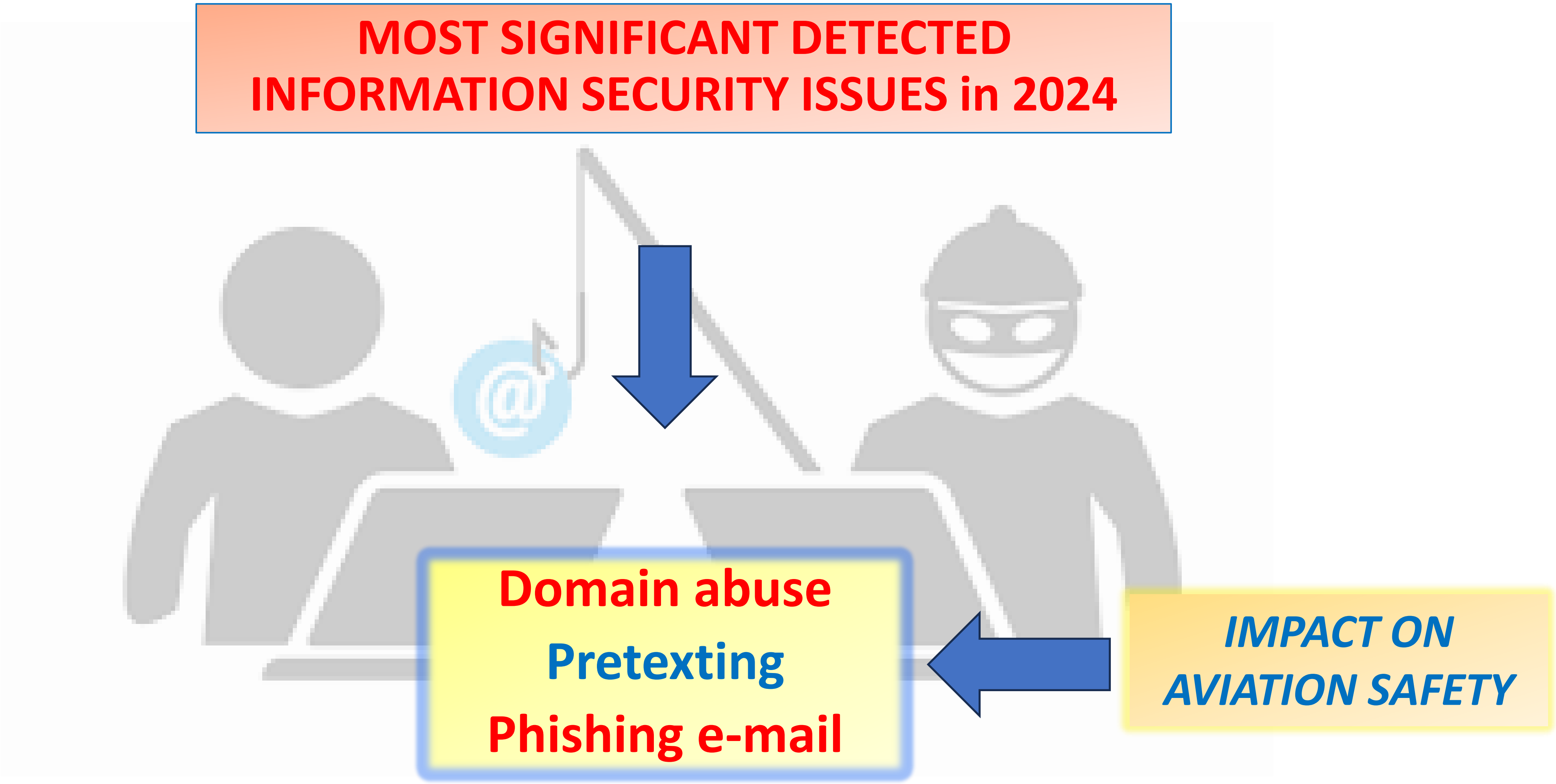
Safety is the set of measures adopted to protect against **UNINTENDED** events, such as **human errors, incidents and damage from adverse environmental conditions.**

Security is the set of measures adopted to prevent **INTENTIONAL** acts carried out with the intent to **cause damage.**

AVIATION SAFETY: everyone's responsibility

SM Quality & Safety team

OUR EXPERIENCE – SECURITY ISSUES (2024)



MOST SIGNIFICANT DETECTED INFORMATION SECURITY ISSUES in 2024

Domain abuse

Pretexting

Phishing e-mail

IMPACT ON AVIATION SAFETY

WHAT TO WORK ON MAINLY?

The main actor for mitigation action is…

THE USER

THE BEST MITIGATION BARRIER

Your data protected
Ongoing vigilance
User awareness

↓

YOU

Secondo Mona 1903

120 YEARS of History and Aerospace Technology

THANKS FOR YOUR ATTENTION

Secondo Mona S.p.A.

R.I, C.F e P.IVA 00190000125

REA Varese No. 44652

Head office and factory

Via Carlo Del Prete 1
21019 Somma Lombardo (VA) – Italy

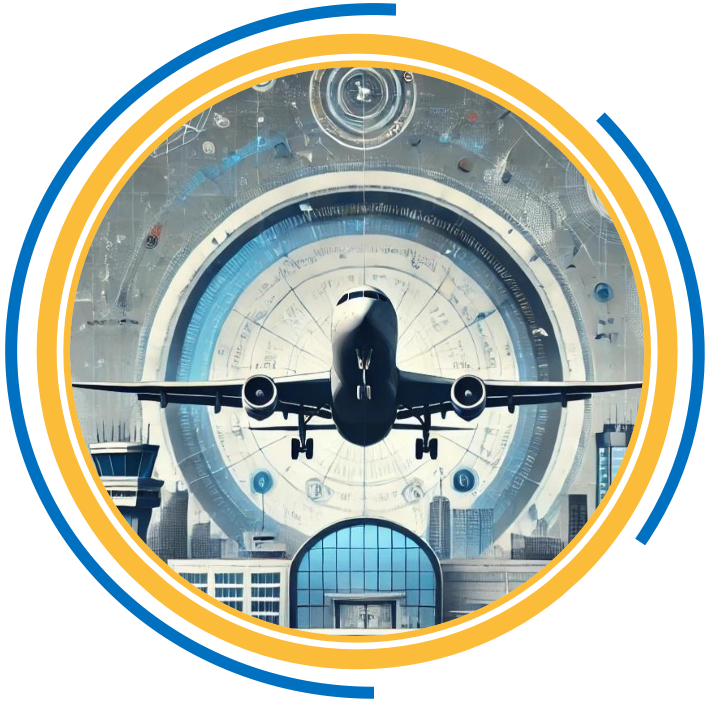
☎ +39-0331-756111

www.secondomona.com

Follow us

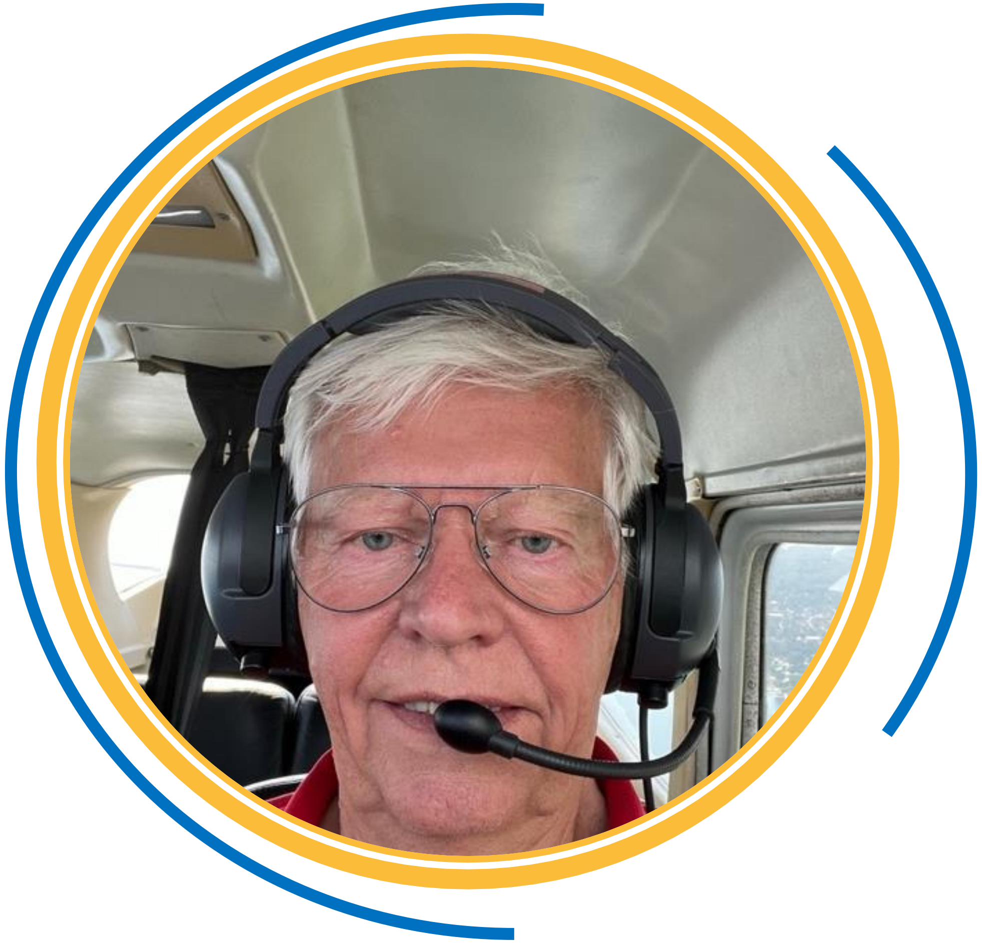
in YouTube

Proportional Implementation of Part-IS & indicators of complexity



Part-IS Implementation

Workshop 2025



Dan Banja is an experienced aviation and defense professional with over 40 years of service in the Danish Armed Forces, retiring as a Lieutenant Colonel. He holds a LAPL license with approximately 670 flight hours on Cessna 150 and 172 aircraft.

Since 2004, he has run his consultancy, Dan Flyconsult, specializing in safety management systems, project and process management, contract negotiation, and educational planning. He has served as Secretary (and since 2011, Secretary General) of the Danish Aviation Association, representing the DAA in national and international aviation forums including EASA and ECOGAS. His distinctions include Knight 1 of the Order of Dannebrog and multiple military service medals for national and international duties.

WHO I AM

Vice President ECOGAS - European Council Of General Aviation Support.

It brings together associations that unite general aviation professional: maintenance workshop, training centres, operational activities and more.

Secretary General DAA - Danish Aviation Association

Promoting commercial aviation and safeguarding the interests of its members vis-à-vis the national and international authorities and organisations, etc. and to convey contact between them and its members.

Retired army officer with PPL => LAPL.

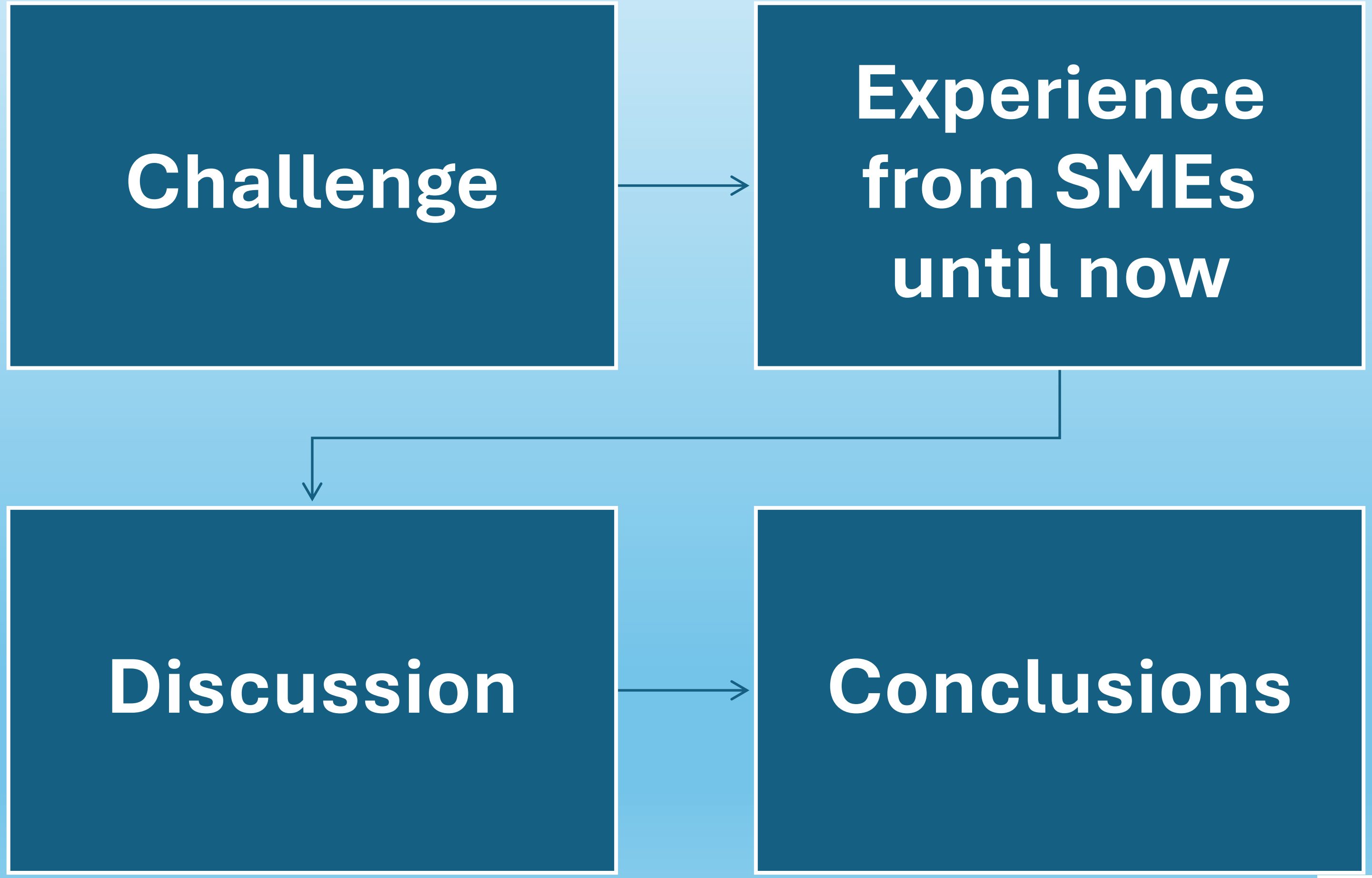
A generalist and not a specialist nor expert.

Representing the views of a large part of the GA segment, incl. IAOPA and coordinated with GA.CSTG.

ES-DAA
Erhvervsflyvningens Sammenslutning
Danish Aviation Association

ECOGAS
EUROPEAN COUNCIL OF GENERAL AVIATION SUPPORT

Part-IS Implementation Workshop 2025 – Proportional Implementation Session



Challenge

Experience from SMEs until now

Discussion

Conclusions

ES-DAA
Erhvervsflyvningens Sammenslutning
Danish Aviation Association

ECOGAS
EUROPEAN COUNCIL OF GENERAL AVIATION SUPPORT

Challenge

How to fit small and medium enterprises in Part-IS?

Experience from SMEs until now

A number of challenges have been identified following exchange with the SMEs.

Part-IS oversight approach - The guidelines to the Competent Authorities are not known to SMEs.

Elements to be assessed by the Authority needs to be communicated to the affected SMEs.

However, the list of elements needs to be made operational for SMEs.

SMEs have a limited staff and information requirements needs to reflect, what is already known to the Authority.

Discussion

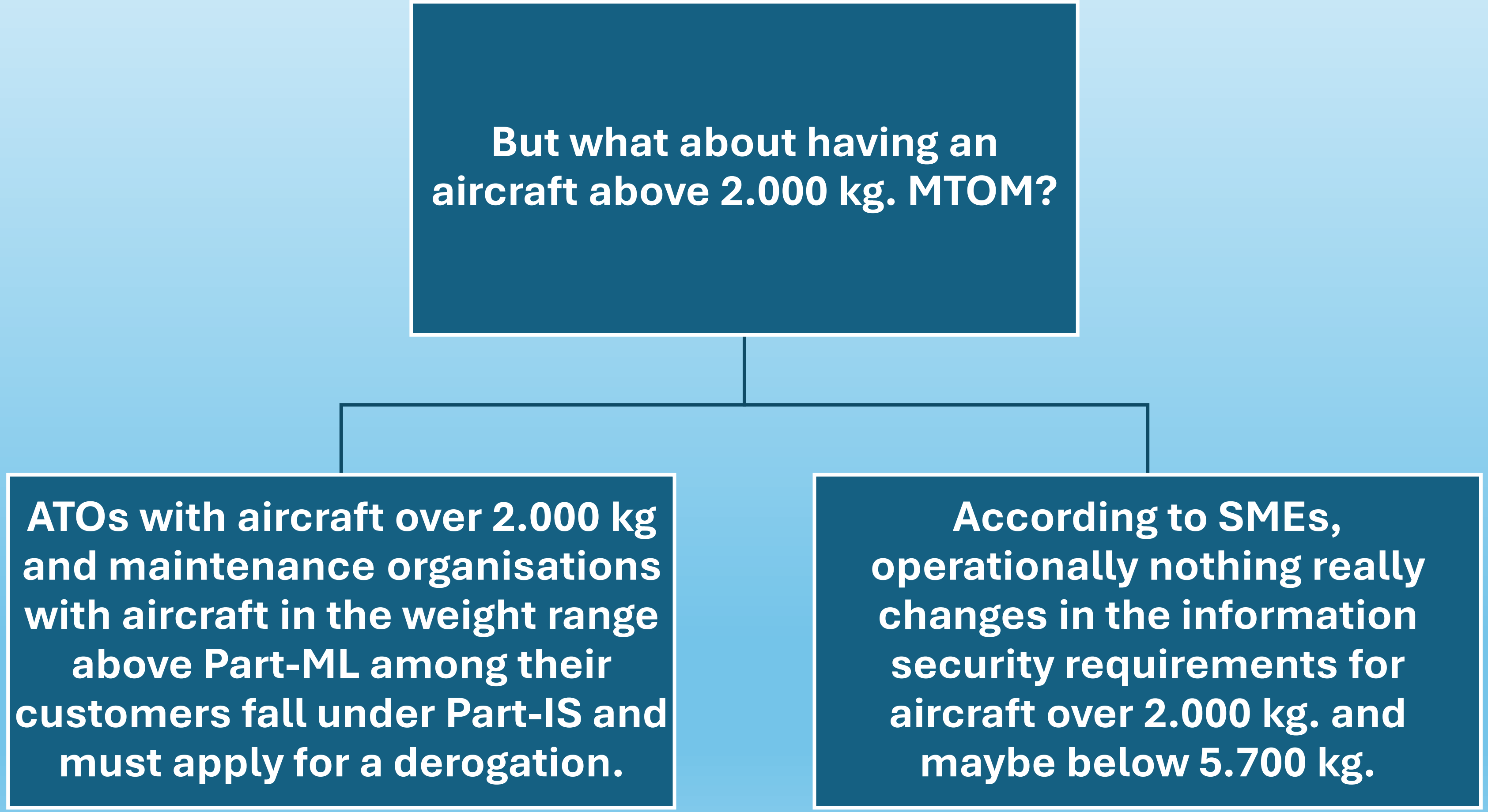
Many of the affected SMEs are not yet dealing with regulations that for them will not come into force until spring 2026.

Lessons learned are not yet available for SMEs.

Flight schools according to the ATO standard with aircraft under 2.000 kg MTOM are exempt from the provisions of Part-IS as well are Part-ML maintenance organisations.

This is a proportionate and positive decision as the risk for these organisations can be considered as low, and there are also no expected over-spill effects on the industry.

Discussion



But what about having an aircraft above 2.000 kg. MTOM?

ATOs with aircraft over 2.000 kg and maintenance organisations with aircraft in the weight range above Part-ML among their customers fall under Part-IS and must apply for a derogation.

According to SMEs, operationally nothing really changes in the information security requirements for aircraft over 2.000 kg. and maybe below 5.700 kg.

ES-DAA
Erhvervsflyvningens Sammenslutning
Danish Aviation Association

ECOGAS
EUROPEAN COUNCIL OF GENERAL AVIATION SUPPORT

Discussion – Solutions & Challenges

Derogations are offered as a mitigation measure with OR.200(e)

Development of advice for initiating a derogation process is underway in a few cases.

Applying for and maintaining the necessary derogation for SMEs demands a high level of effort and resources.

After the derogation has been accepted there is an obligation to continue monitoring and documenting the reasons for the derogation. Needs resources.

ES-DAA
Erhvervsflyvningens Sammenslutning
Danish Aviation Association

ECOGAS
EUROPEAN COUNCIL OF GENERAL AVIATION SUPPORT

Conclusions

It is early in the process to get proper lessons learnt, as the affected SMEs for the most have not yet begun looking at implementation of Part-IS.

Many SMEs are waiting for their authority to issue guidance on the implementation of Part-IS.

There is a grey zone just above the 2.000 kg., where SMEs claims that Part-IS seems not proportionate to the nature and risks associated with the different types of aircraft, operations and activities they address.

The derogation provisions can be used in such cases.

ES-DAA
Erhvervsflyvningens Sammenslutning
Danish Aviation Association

ECOGAS
EUROPEAN COUNCIL OF GENERAL AVIATION SUPPORT

Part-IS Implementation Workshop 2025 – Proportional Implementation Session

THANK YOU

ES-DAA
Erhvervsflyvningens Sammenslutning
Danish Aviation Association

ECOGAS
EUROPEAN COUNCIL OF GENERAL AVIATION SUPPORT

Tom Stewart is Director of Cyber Security at Ryanair, brings almost 20 years of experience in the aviation industry, specializing in IT and Cyber Security. Tom leads efforts to protect Europe’s largest airline network. At Ryanair, his role involves implementing a Cyber Security Strategy that aligns Cyber Security with business objectives, ensuring operational continuity and maintaining customer trust in a high-availability, high-risk environment.

AGENDA

01 Ryanair Network - Complexity

02 Ryanair Cyber Security Strategy

03 PART-IS Implementation and Progress

04 Challenges

THE RYANAIR GROUP NETWORK

RYANAIR
RYANAIR DAC
RYANAIR
RYANAIR UK
MALTA AIR
MALTA AIR
BUZZ
BUZZ
LAUDA
LAUDA EUROPE
Meet the family...
RYANAIR
HOLDINGS PLC

37 countries

over **230** airports

84 bases

over **3,600** daily flights

6 Heavy Maintenance

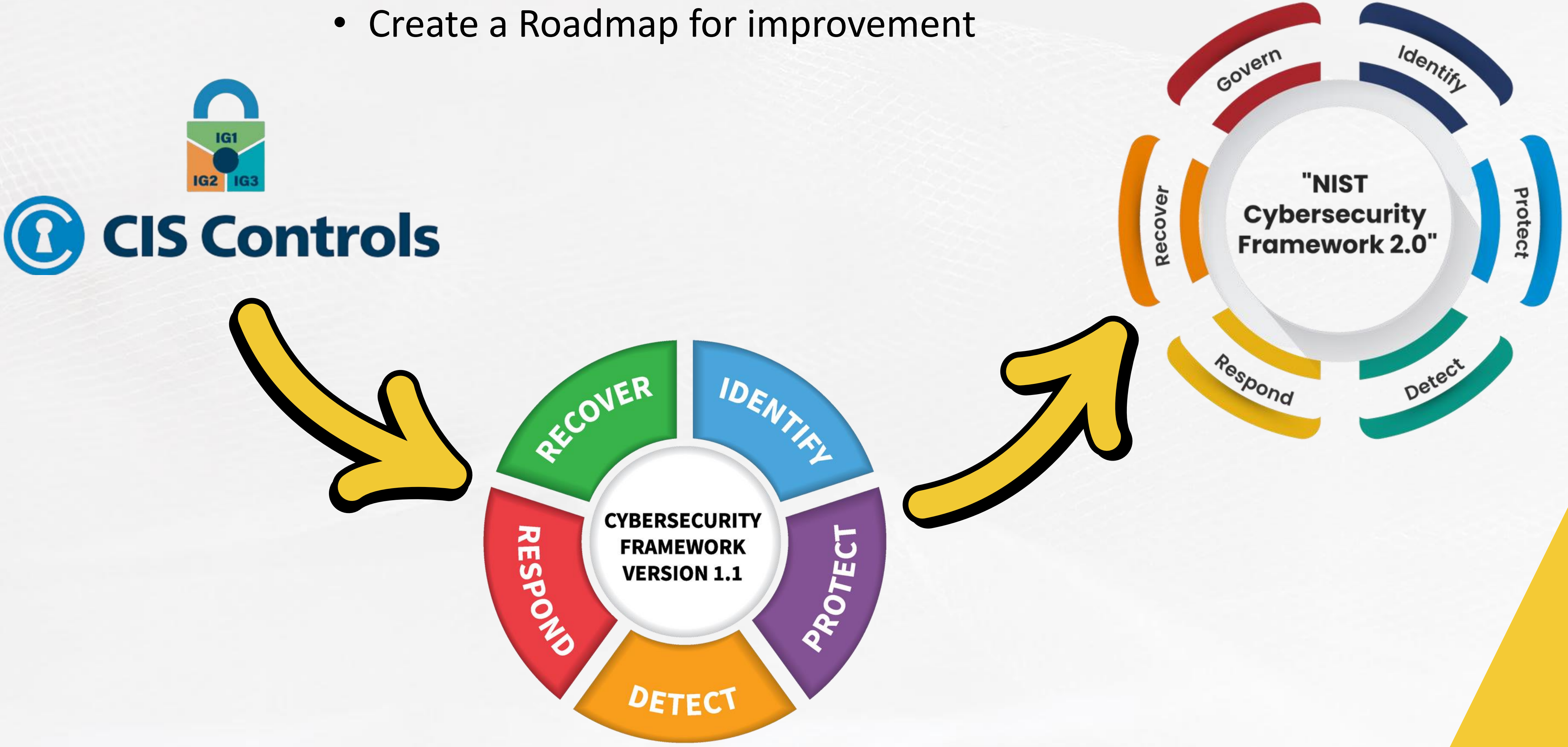
4 Training Centers

27,000+ people

RYANAIR

CYBER SECURITY STRATEGY

- Adopt Cyber Security Framework
- Review Bi-Annually - Maturity Assessment
- Create a Roadmap for improvement



IG1
IG2
IG3
CIS Controls

CYBERSECURITY FRAMEWORK VERSION 1.1
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

"NIST Cybersecurity Framework 2.0"
Govern
Identify
Protect
Detect
Respond
Recover

RYANAIR

SERVICES PORTFOLIO

Technical Security Services

- Network Security
- Endpoint Security
- Security Information and Event Management
- Vulnerability Management
- Incident Response
- Cloud Security
- Penetration Testing
- Data Protection and Encryption

Non-technical Security Services

- Risk Assessment
- Threat Intelligence
- Vendor Risk Management
- Legal and Regulatory Support
- Security Compliance and Policies
- Security Awareness and Training
- Incident Response Planning
- Security Strategy

Current PART-IS Activities

1. Defining the scope
2. Defining roles and responsibilities
3. Mapping Part-IS requirements and NIST CSF 2.0 Framework
4. Performing a gap analysis
5. Defining the structure of the ISMM

NEXT STEPS

- **RISK MANAGEMENT**

Integrating Ryanair Cybersecurity Risk Management with Safety Risk Management

- **TRIAGE**

Defining a triage process to assess if Cybersecurity incidents have potential safety impacts

- **EVENTS & INCIDENTS**

Integration of Cybersecurity events and incidents with Safety reporting tools

- **ISMM**

Preparing the first iteration of ISMM

- **TRAINING**

Preparing additional training material and arranging sessions for staff in scope

- **ASSET MANAGEMENT**

Implementing specific tagging for assets and applications in scope

RYANAIR

CHALLENGES

Complexity of regulatory requirements

The intricate nature of PART-IS regulations requires significant expertise and understanding, often leading to confusion and misinterpretation among airline compliance teams.

Need for cross-departmental collaboration

Effective cyber security requires input and cooperation across various departments, yet siloed operational structures often hinder collaborative efforts.

Establishing a cyber security culture

Building a proactive organizational culture around cyber security involves not just training but embedding security principles into every layer of the airine's operations.

Staff training and awareness

As the backbone of any cyber security implementation, training staff to recognize and respond to threats is vital, however achieving this across various departments can be administratively burdensome.

Legacy Systems

Many airlines rely on outdated technology which can create vulnerabilities and hinder the implementation of contemporary cyber security measures as stipulated by EASA regulations.

When does a Cyber Risk become a Safety Risk

How much cyber vulnerability is acceptable before it poses an unacceptable threat to human safety, operational integrity, or environmental impact? Understanding this boundary is essential for setting risk thresholds, designing safeguards, and ensuring accountability across both IT and safety-critical domain.

QUESTIONS

Mario Lenitz is a Quality Manager at Austro Control, overseeing compliance monitoring for the “Luftfahrtagentur” (LFA) in Austria. He is also leading changes to prepare LFA for Part-IS oversight.

Mario is a communications engineer with nearly 25 years of experience gained also in consulting, IT and banking. He is an accredited ISO/IEC 27001 auditor for information security management systems.

TLP clear

Proportional Implementation of Part-IS & indicators of complexity

25.06.2025

Mario Lenitz, Austro Control – Member of Part-IS TF

EASA
European Union Aviation Safety Agency

eRules

PART-IS
(IR/DR + AMC/GM)

austro CONTROL

Is this the truth?

NO!!

Many organisations are exemped or derogated

Part IS is not applicable to:

Production organisatio
holding an approva

Private operators of other th
complex motor-powered aircr

Organisation designing UAS in the "specific" category when not required to hold a DOA approval.

eoretical

pen”

y ICAO Annex 6

isations approved under bilateral agreements

What about the rest?

IS.I/D.OR.200 Information security management system (ISMS)

d) The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.I.OR.200(a) **shall correspond to the nature and complexity of its activities, based on an assessment of the information security risks inherent to those activities**, and may be integrated within other existing management systems already implemented by the organisation.

Complexity criteria in the Safety Rules – Authority Requirements

e. g. AMC2 145.B.305(b) Oversight programme

SPECIFIC NATURE AND COMPLEXITY OF THE ORGANISATION

When determining the oversight programme, including the product audits, the competent authority should consider in particular the following elements, as applicable:

(1) the effectiveness of the organisation’s management system in identifying and addressing non-compliances and safety hazards;

(2) the implementation by the organisation of any industry standards that are directly relevant to the organisation’s activities subject to this Regulation;

(3) the procedure applied to amend the scope of changes not requiring prior approval;

(4) any specific procedures implemented by the organisation that are related to any alternative means of compliance used;

(5) the number of approved locations and the activities performed at each location;

(6) the number and type of any subcontractors that perform maintenance tasks; and

(7) the volume of activity for each A, B, C and D class rating, as applicable.

Not working for Part-IS !!

Complexity criteria in the Safety Rules – Organisation Requirements

e. g. AMC1 ORO.GEN.200(b) Management system

SIZE, NATURE AND COMPLEXITY OF THE ACTIVITY

(a) An operator should be considered as complex when it has a workforce of more than 20 full time equivalents (FTEs) involved in the activity subject to Regulation (EC) No 216/2008 and its Implementing Rules.

(b) Operators with up to 20 FTEs involved in the activity subject to Regulation (EC) No 216/2008 and its Implementing Rules may also be considered complex based on an assessment of the following factors:

(1) in terms of complexity, the extent and scope of contracted activities subject to the approval;

(2) in terms of risk criteria, the extent of the following:

(i) operations requiring a specific approval;

(ii) high-risk commercial specialised operations;

(iii) operations with different types of aircraft used; and

(iv) operations in challenging environment (offshore, mountainous area, etc.).

Not working for Part-IS !!

Complexity criteria for Information security are different

The information security risk does not only depend on the size of the organisation, but on their complexity regarding Information Security

large

small

simple

complex

How could we assist these organisations to implement a **„Right Sized ISMS“**

Building the right-sized ISMS

Proportionality aspects for Part-IS implementation in relation to organisational complexity and safety relevance

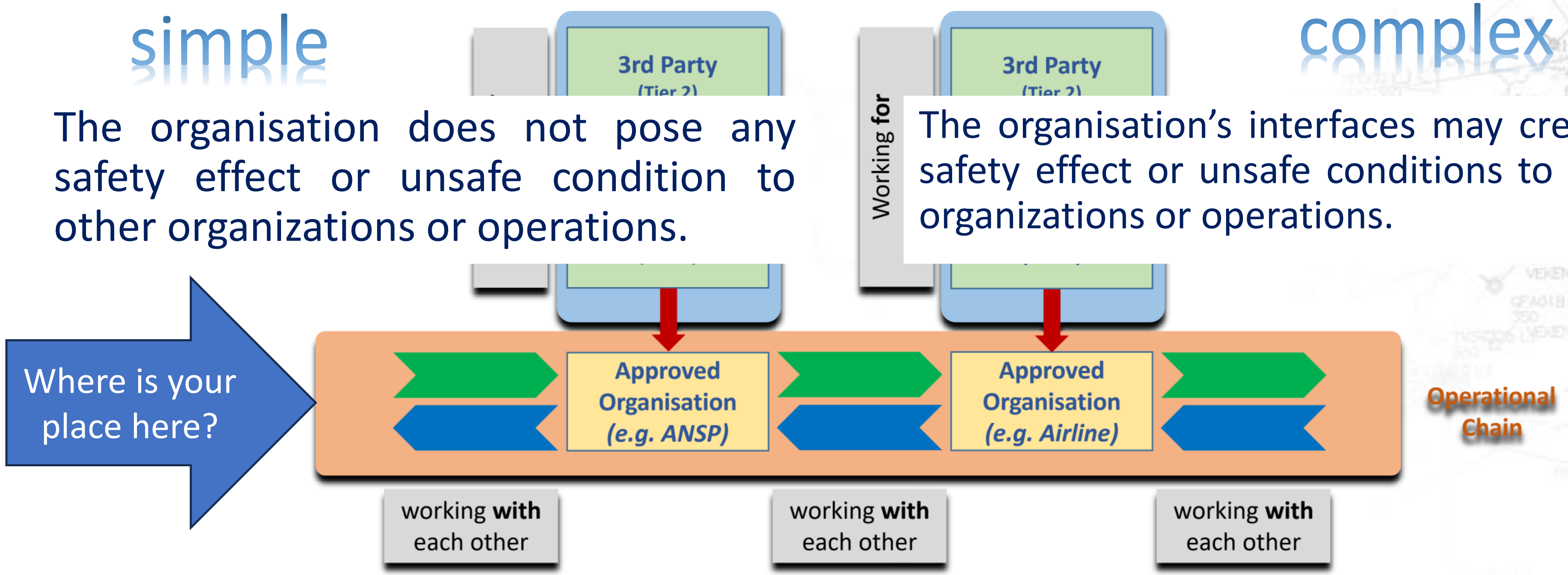
1. **SAFETY IMPACT** - Where the organisation is placed in the functional chain and the number and safety relevance of interfacing organisations/stakeholders.
2. **ORGANIZATIONAL COMPLEXITY** – The size of the organisation and complexity of the organisational structure and processes (e.g. number of staff, departments, hierarchical layers, process complexity)
3. **ICT-COMPLEXITY** - The complexity of the Information and Communication Technology (ICT) systems and data used by the organisation and their connection to external parties.

Specific guidance for each aspect – individual applicability

Proportionality considerations

Organisation role in the functional chain and number and criticality of interfacing organisations/stakeholders

The organisation's position in the functional chain *(= propagation to safety effect to itself and their stakeholders*) and its overall contribution to the safety of related functional processes are key indicators of complexity.



The organisation does not pose any safety effect or unsafe condition to other organizations or operations.

The organisation’s interfaces may create a safety effect or unsafe conditions to other organizations or operations.

Proportionality considerations

Complexity of the organisational structure, hierarchies and processes

The complexity of an organisation's structure—typically determined by the number of staff, hierarchical layers, number of processes and their interdependences—directly influences the level of internal coordination required and the extent to which information exchange needs to be formalised and proceduralised.

simple

The organisations is characterised by a combination of limited number of staff, few hierarchical layers and straight forward processes.

complex

organisations is characterised by a combination of large number of staff, hierarchical layers and a high number of interconnected processes and interfaces.

Proportionality considerations

Complexity of the ICT systems and data used by the organisation

The complexity of the information and communication technology systems and data used by the organisation and their connection to external parties directly influences the level of customisation and tailoring required for risk management and incident detection, response and recovery.

simple

The organisations is characterised by a combination of usage of few ICT tools and utilisation of standard ICT products in a basic, commercial of-the-shelf, ICT-architecture.

complex

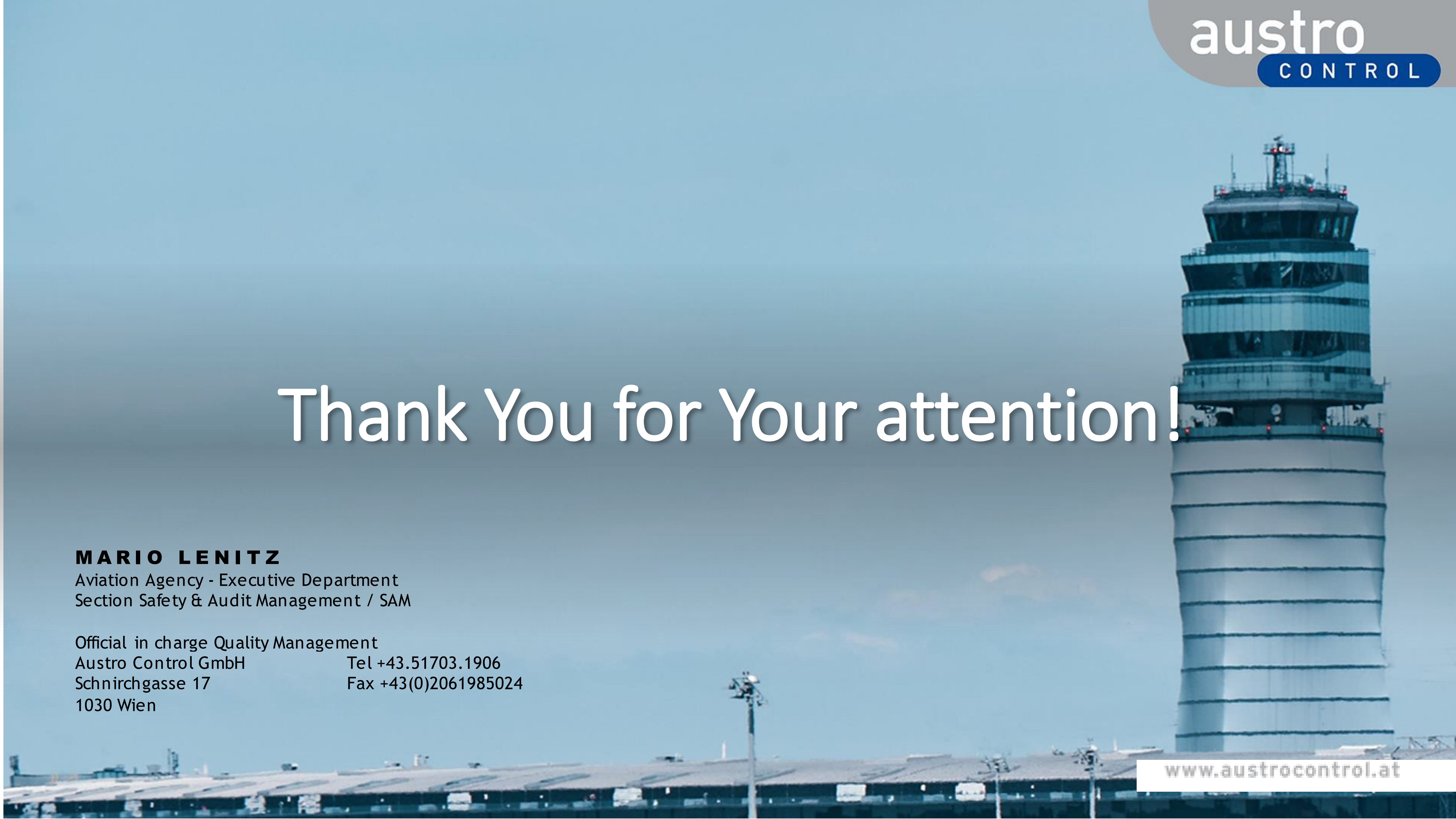
organisations is characterised by a combination of usage of several and diverse ICT tools, amongst which bespoke ICT solutions and architectures.

Possible proportionality (self)-assessment of our sample organisations

Design your ISMS after assessment
with the necessary depth and breadth from each aspect

Safety impact	simple	complex	complex	complex
Organisation complexity	complex	complex	simple	simple
ICT complexity	simple	complex	simple	complex

NOTE: The complexity classification criteria are not an input to the organisation’s risk assessment.



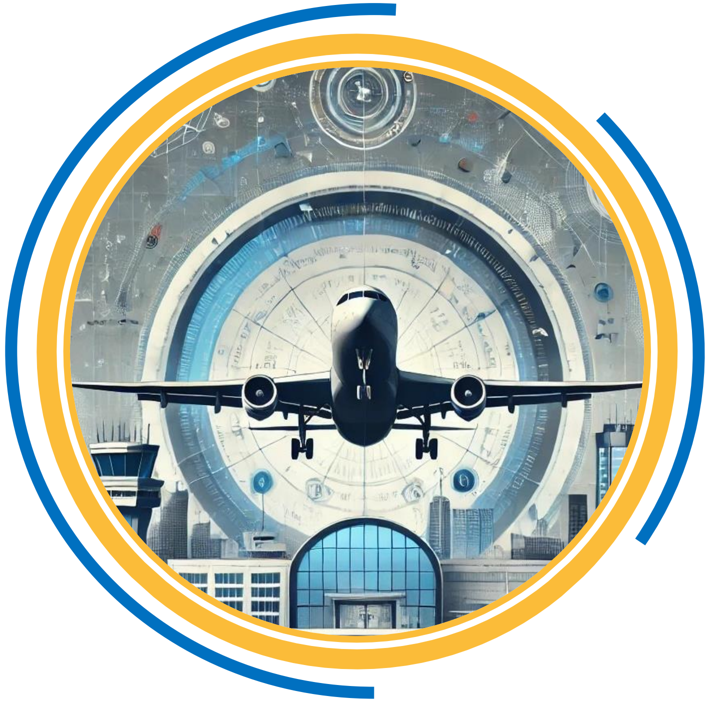
Thank You for Your attention!

MARIO LENITZ
Aviation Agency - Executive Department
Section Safety & Audit Management / SAM

Official in charge Quality Management
Austro Control GmbH Tel +43.51703.1906
Schnirchgasse 17 Fax +43(0)2061985024
1030 Wien

www.austrocontrol.at

Aviation product certification and Part-IS



Part-IS Implementation

Workshop 2025

Nicolas Durandeau - After having spent 13 years in the aerospace industry (5AFRAN, AIRBUS and THALES) designing embedded systems, Nicolas joined EASA 10 years ago.

He occupied first the position of avionics and cybersecurity expert. He is now Senior expert in Cybersecurity in the Certification Directorate in charge of coordinating the certification activities for all type of flying products (ranging from drone to large aeroplane)

EASA
European Union Aviation Safety Agency

Aviation Product Certification and Part-IS

Nicolas Durandeau
Borja García-Blanco Castro

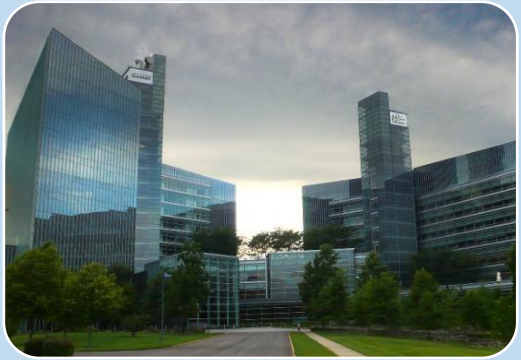
Aviation Cybersecurity Certification Experts
EASA Certification Directorate

Part-IS Implementation Workshop 2025 – 25 June 2025

Your safety is our mission.

An Agency of the European Union

Making EU aviation cyber resilient



Products (Aircrafts, Engines, …) ED Decision 2020/006/R

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

✓

Organisations (People, Processes)

- **Part-IS** Regulations published in October 2022 and February 2023
- AMC/GM published on 12 July 2023

✓

Information Sharing

- Create a community to
  - Share knowledge
  - Perform Analysis
  - Collaborate
  - Reinforce the system

Capacity building & Research

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

Content

How Part 21 – Product certification can benefit from Part-IS?

How Part-IS can benefit from Part 21 – Product certification?

EASA
European Union Aviation Safety Agency

Part IS – Part 21 Interaction

How Product Certification can benefit from Part-IS?

Your safety is our mission.

An Agency of the European Union

Basic regulation (effective July 2018)

- Article 4 (d): […] the Agency and the Member States shall:
  - *[…] take into account interdependencies between the different domains of aviation safety, and between aviation safety, cyber security and other technical domains of aviation regulation; […]*

- ***ANNEX II: Essential requirements for airworthiness***
  - *1.3.5: Design precautions must be taken to minimise the hazards to the aircraft and occupants from reasonably probable threats, including information security threats, both **inside** and **external** to the aircraft, including protecting against the possibility of a significant failure in, or disruption of, any non-installed equipment.*

CS Cybersecurity requirements: Summary

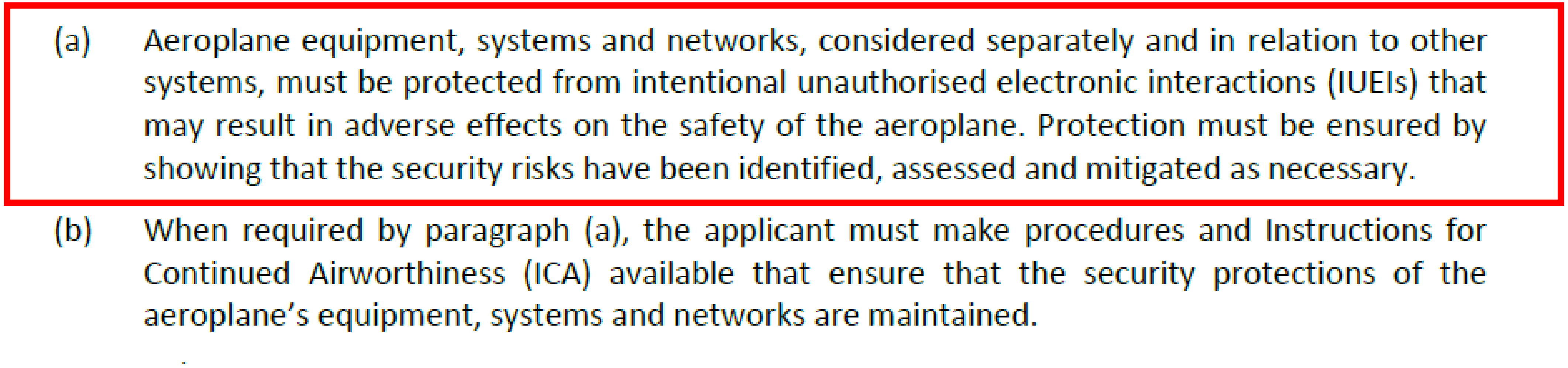
Type	CS 25 amdt 25	CS 23 Class4	CS 29 amdt 8	CS 27 amdt 7	CS-E amdt 6	CS-P amdt 2	CS-APU Amdt 1	CS-ETSO Amdt 15

Req	1319
	H25.6
		GM
		2500(b)
			1319
			A29.5
				1319
				A27.5
					20(d)
					25(c)(13)
					50(l)
						40(c)(13)
						230(g)
							30(c)(13)
							90(d)
								Subpart A
								§2.6

AMC	AMC 20-42							

CS Requirement for design before operation

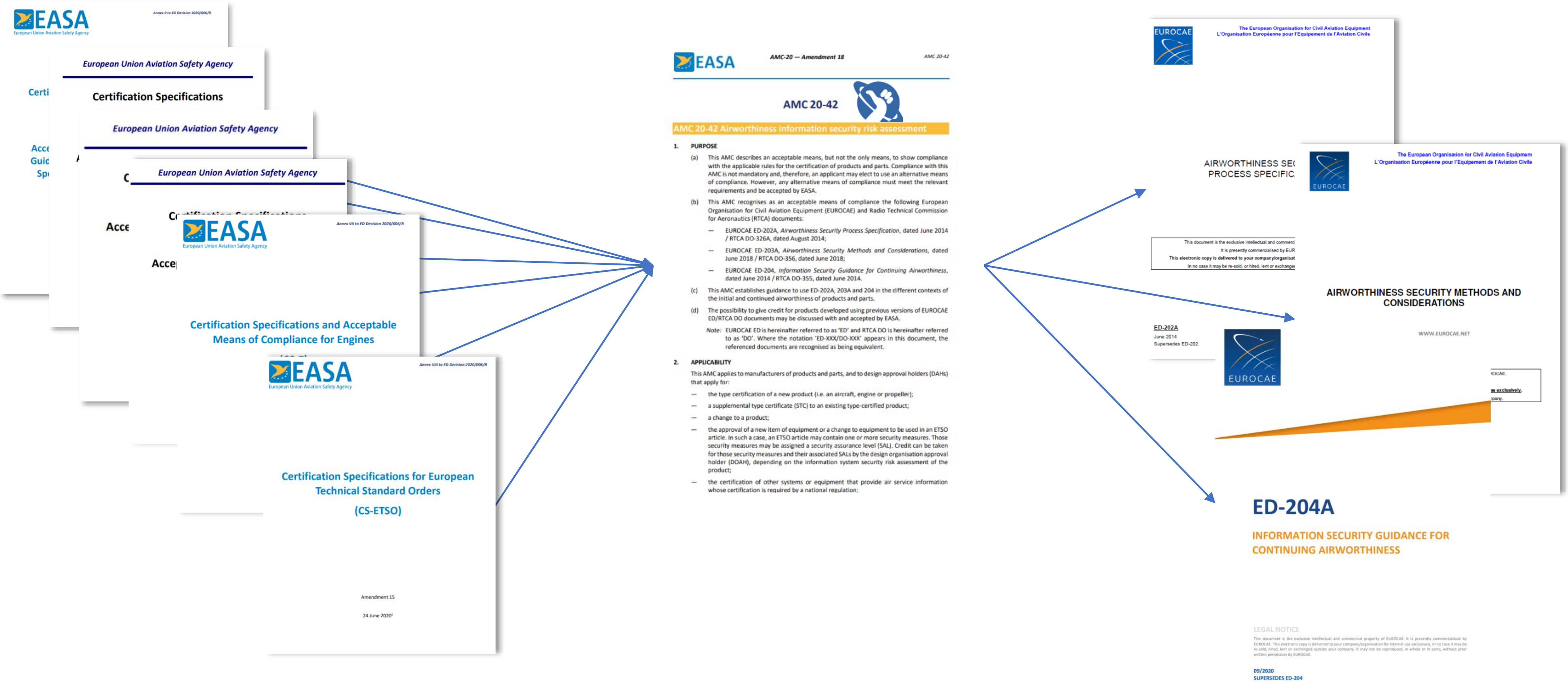
→ Example requirement CS 2X.1319:



(a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.

(b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained.

CS Cybersecurity requirements and AMC



Annex II to ED Decision 2020/006/R

European Union Aviation Safety Agency

Certi

Acce
Guid
Spe

European Union Aviation Safety Agency

Certification Specifications

European Union Aviation Safety Agency

European Union Aviation Safety Agency

Acce

Acce

Annex VII to ED Decision 2020/006/R

European Union Aviation Safety Agency

Certification Specifications and Acceptable Means of Compliance for Engines

Annex VIII to ED Decision 2020/006/R

European Union Aviation Safety Agency

Certification Specifications for European Technical Standard Orders

(CS-ETSO)

Amendment 15

24 June 2020

AMC-20 — Amendment 18

AMC 20-42

AMC 20-42

AMC 20-42 Airworthiness information security risk assessment

1. PURPOSE

(a) This AMC describes an acceptable means, but not the only means, to show compliance with the applicable rules for the certification of products and parts. Compliance with this AMC is not mandatory and, therefore, an applicant may elect to use an alternative means of compliance. However, any alternative means of compliance must meet the relevant requirements and be accepted by EASA.

(b) This AMC recognises as an acceptable means of compliance the following European Organisation for Civil Aviation Equipment (EUROCAE) and Radio Technical Commission for Aeronautics (RTCA) documents:

— EUROCAE ED-202A, *Airworthiness Security Process Specification*, dated June 2014 / RTCA DO-326A, dated August 2014;

— EUROCAE ED-203A, *Airworthiness Security Methods and Considerations*, dated June 2018 / RTCA DO-356, dated June 2018;

— EUROCAE ED-204, *Information Security Guidance for Continuing Airworthiness*, dated June 2014 / RTCA DO-355, dated June 2014.

(c) This AMC establishes guidance to use ED-202A, 203A and 204 in the different contexts of the initial and continued airworthiness of products and parts.

(d) The possibility to give credit for products developed using previous versions of EUROCAE ED/RTCA DO documents may be discussed with and accepted by EASA.

Note: EUROCAE ED is hereinafter referred to as 'ED' and RTCA DO is hereinafter referred to as 'DO'. Where the notation 'ED-XXX/DO-XXX' appears in this document, the referenced documents are recognised as being equivalent.

2. APPLICABILITY

This AMC applies to manufacturers of products and parts, and to design approval holders (DAHs) that apply for:

— the type certification of a new product (i.e. an aircraft, engine or propeller);

— a supplemental type certificate (STC) to an existing type-certified product;

— a change to a product;

— the approval of a new item of equipment or a change to equipment to be used in an ETSO article. In such a case, an ETSO article may contain one or more security measures. Those security measures may be assigned a security assurance level (SAL). Credit can be taken for those security measures and their associated SALs by the design organisation approval holder (DOAH), depending on the information system security risk assessment of the product;

— the certification of other systems or equipment that provide air service information whose certification is required by a national regulation;

EUROCAE

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

AIRWORTHINESS SEC
PROCESS SPECIFIC

This document is the exclusive intellectual and commerci
It is presently commercialised by EUR
This electronic copy is delivered to your company/organisat
In no case it may be re-sold, or hired, lent or exchange

ED-202A
June 2014
Supersedes ED-202

EUROCAE

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

AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS

WWW.EUROCAE.NET

OCAE.
e exclusively.
pany.

ED-204A

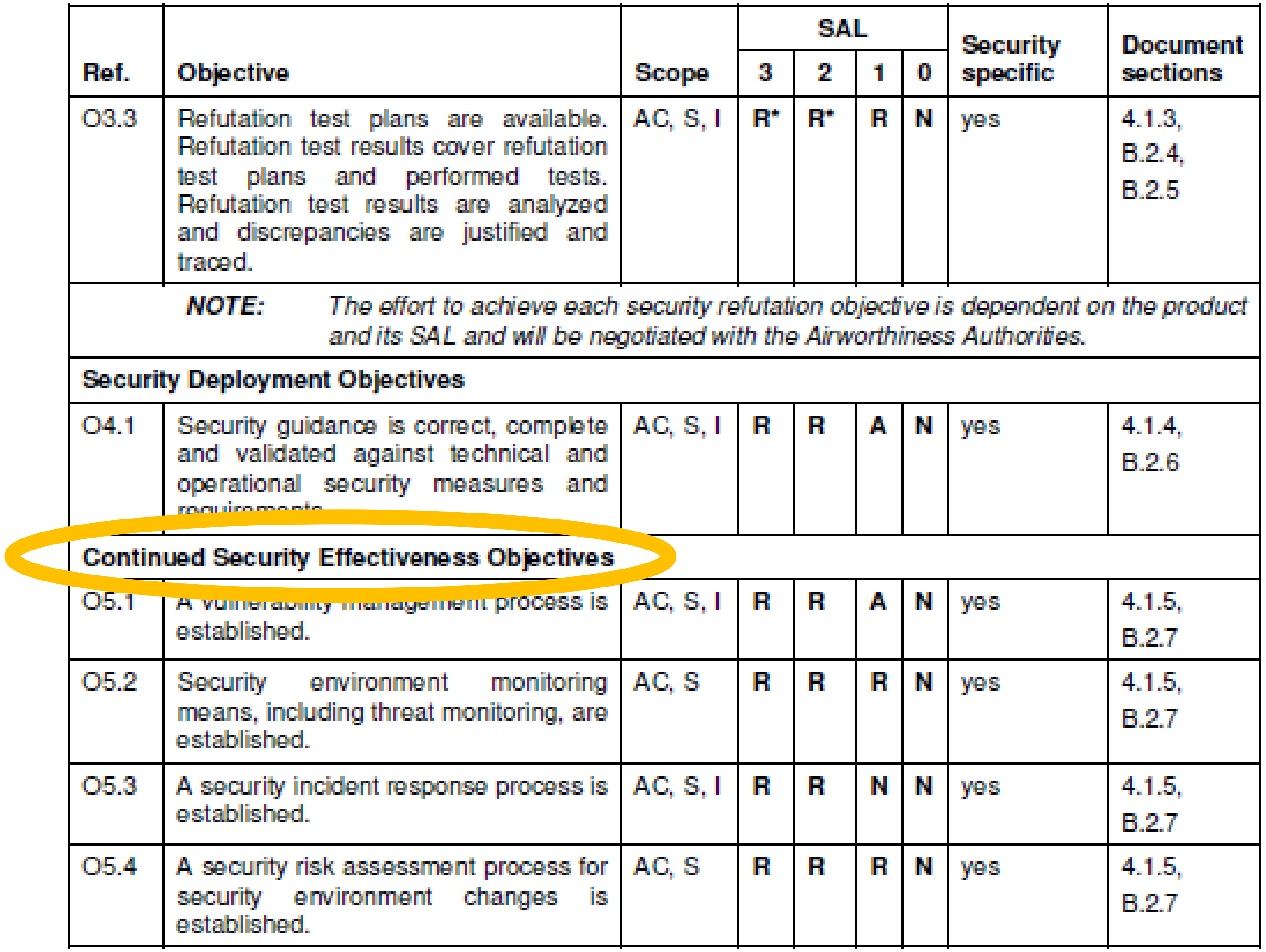
INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

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

Security Assurance Objectives – Appendix A ED 203A

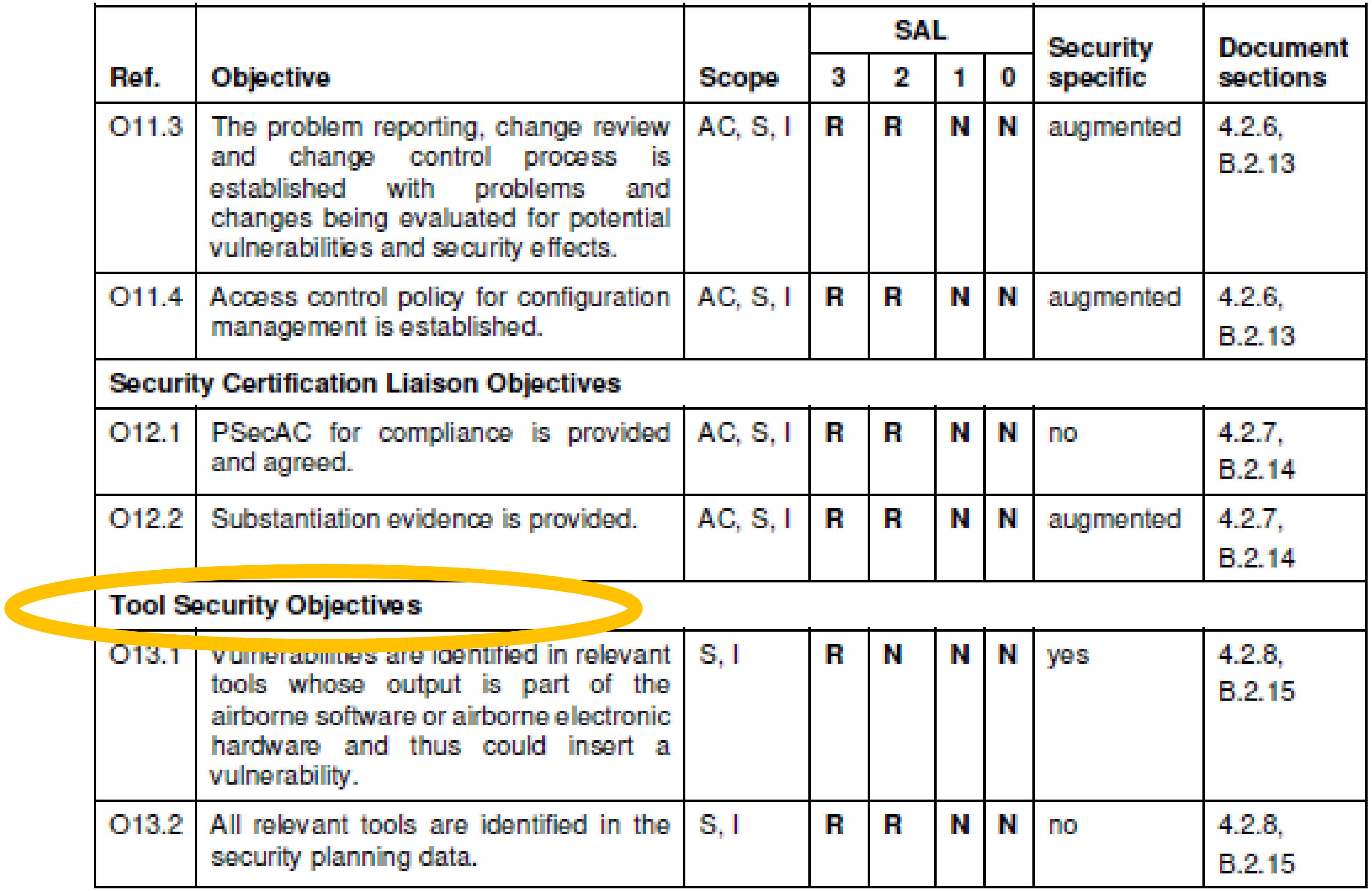


Ref.	Objective	Scope	SAL				Security specific	Document sections
			3	2	1	0		
O3.3	Refutation test plans are available. Refutation test results cover refutation test plans and performed tests. Refutation test results are analyzed and discrepancies are justified and traced.	AC, S, I	R*	R*	R	N	yes	4.1.3, B.2.4, B.2.5
	NOTE: *The effort to achieve each security refutation objective is dependent on the product and its SAL and will be negotiated with the Airworthiness Authorities.*							
Security Deployment Objectives								
O4.1	Security guidance is correct, complete and validated against technical and operational security measures and requirements.	AC, S, I	R	R	A	N	yes	4.1.4, B.2.6
Continued Security Effectiveness Objectives								
O5.1	A vulnerability management process is established.	AC, S, I	R	R	A	N	yes	4.1.5, B.2.7
O5.2	Security environment monitoring means, including threat monitoring, are established.	AC, S	R	R	R	N	yes	4.1.5, B.2.7
O5.3	A security incident response process is established.	AC, S, I	R	R	N	N	yes	4.1.5, B.2.7
O5.4	A security risk assessment process for security environment changes is established.	AC, S	R	R	R	N	yes	4.1.5, B.2.7

- → Organisational Risk assessment required by Part-IS may lead to implement security measures on elements in scope such as:
  - → vulnerability management process (may cover O5.1)
  - → Incident management process (may cover O5.3)

Credits - EUROCAE ED-203A

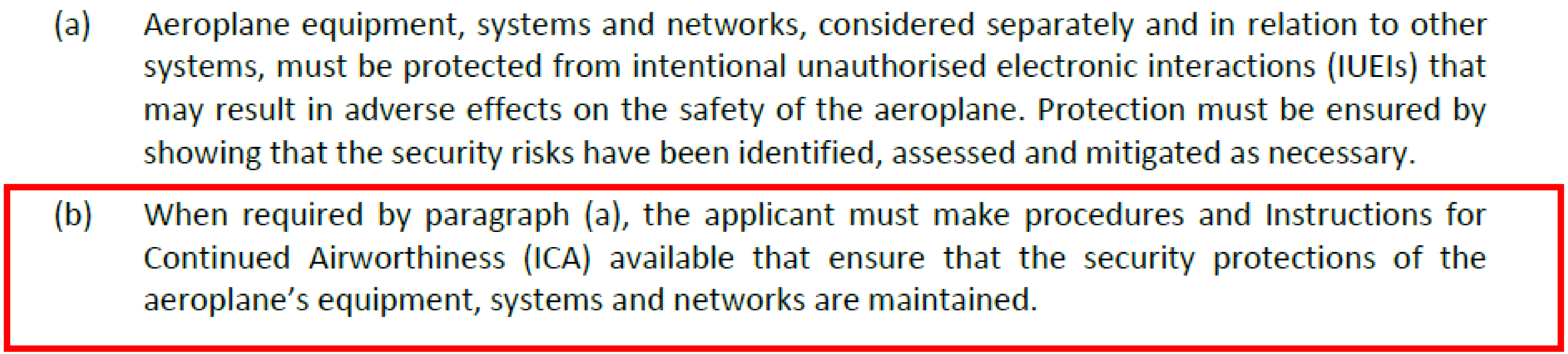
Security Assurance Objectives – Appendix A ED 203A



Ref.	Objective	Scope	SAL				Security specific	Document sections
			3	2	1	0		
O11.3	The problem reporting, change review and change control process is established with problems and changes being evaluated for potential vulnerabilities and security effects.	AC, S, I	R	R	N	N	augmented	4.2.6, B.2.13
O11.4	Access control policy for configuration management is established.	AC, S, I	R	R	N	N	augmented	4.2.6, B.2.13
Security Certification Liaison Objectives								
O12.1	PSecAC for compliance is provided and agreed.	AC, S, I	R	R	N	N	no	4.2.7, B.2.14
O12.2	Substantiation evidence is provided.	AC, S, I	R	R	N	N	augmented	4.2.7, B.2.14
Tool Security Objectives								
O13.1	Vulnerabilities are identified in relevant tools whose output is part of the airborne software or airborne electronic hardware and thus could insert a vulnerability.	S, I	R	N	N	N	yes	4.2.8, B.2.15
O13.2	All relevant tools are identified in the security planning data.	S, I	R	R	N	N	no	4.2.8, B.2.15

CS Instructions for continued Airworthiness

→ Example requirement CS 2X.1319:

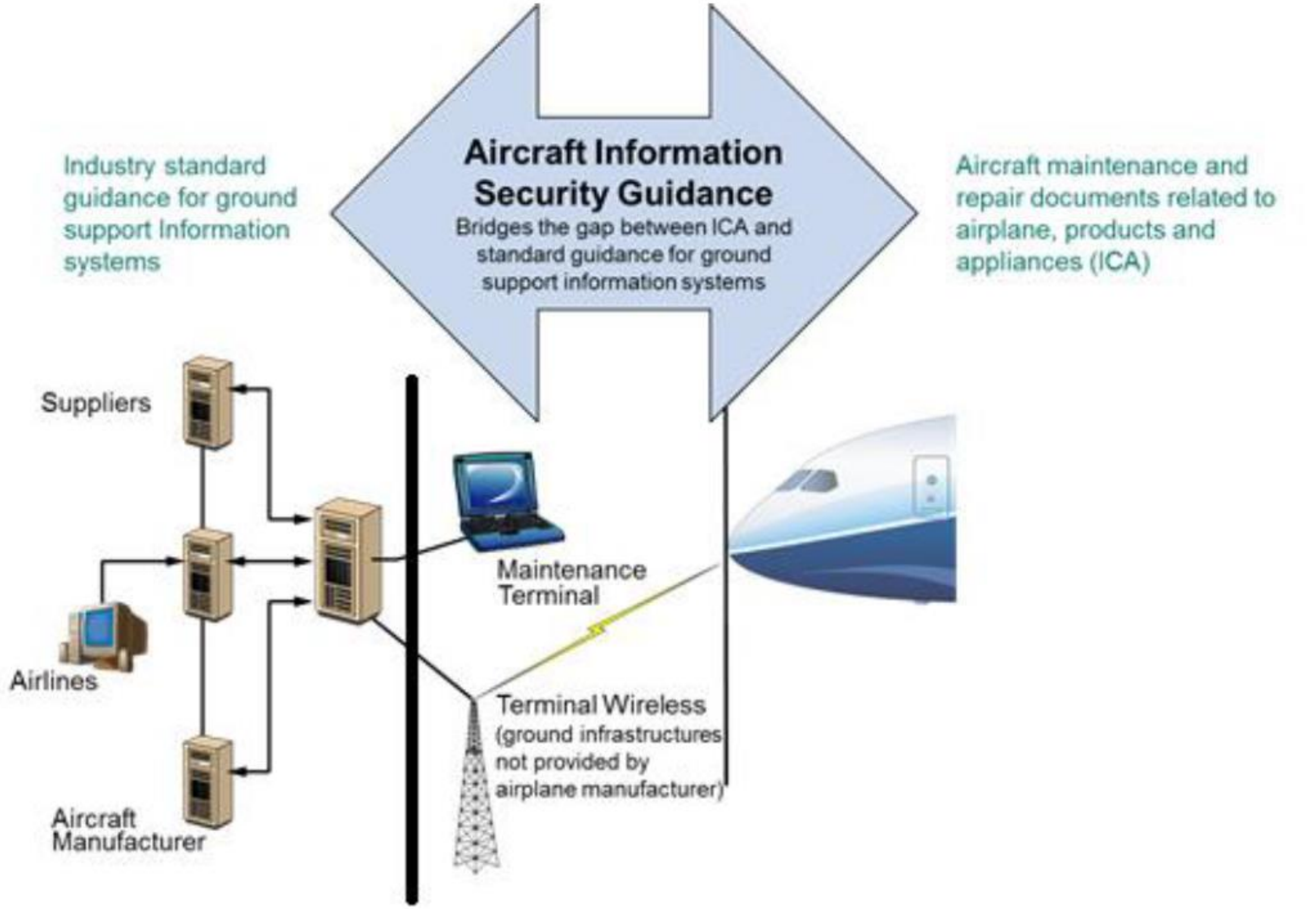


(a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.

(b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained.

ED 204A – Information Security Guidance for Continuing Airworthiness

- It provides guidance to following stages of the product life cycle:
  - Operation
  - Support
  - Maintenance
  - Administration
  - Decommissioning


Industry standard guidance for ground support Information systems
Aircraft Information Security Guidance
Bridges the gap between ICA and standard guidance for ground support information systems
Aircraft maintenance and repair documents related to airplane, products and appliances (ICA)
Suppliers
Airlines
Aircraft Manufacturer
Maintenance Terminal
Terminal Wireless (ground infrastructures not provided by airplane manufacturer)

Credits - EUROCAE ED-204A

ED 204A – Example for Ground support Equipment

- Example of recommended operational security measure for GSE:
  - Equipment Security and Operations Management
  - Access Control
  - Usage
  - Storage
  - Incident management
  - Lifecycle management
  - Decommissioning

- Design Approval Holder may require to have those measures implemented by the operator (recommended or applied ICA)

Credits - EUROCAE ED-204A

How Product Certification benefits from Part IS?

Part IS Requirements and processes can be used to show certain level of compliance during product certification.

→ Security Assurance Objectives (ED 203A)

→ Design Approval Holder (DAH) and/or Operator Responsibilities (ED 204A)

EASA

European Union Aviation Safety Agency

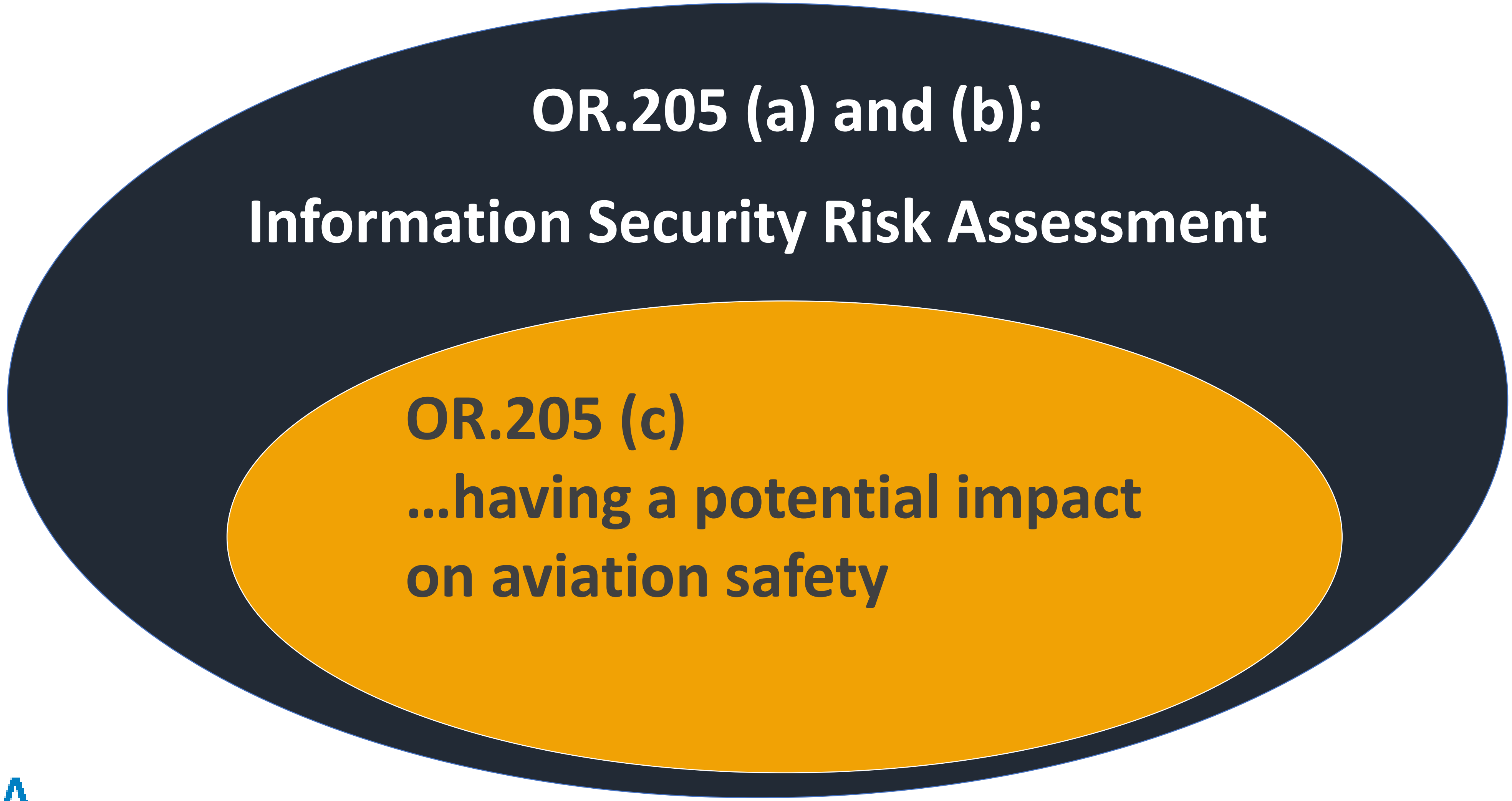
Part IS – Part 21 Interaction

How Part-IS can benefit from Product Certification?

Your safety is our mission.

An Agency of the European Union

Creating Input for the ISMS Scope Definition



OR.205 (a) and (b):

Information Security Risk Assessment

OR.205 (c)
…having a potential impact
on aviation safety

OR.205 – Elements and Interfaces

IS.OR.205 Information security risk assessment

(a) The organisation shall identify all its elements which could be exposed to information security risks. That shall include:

(1) the organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;

(2) the equipment, systems, data and information that contribute to the functioning of the elements listed in point (1).

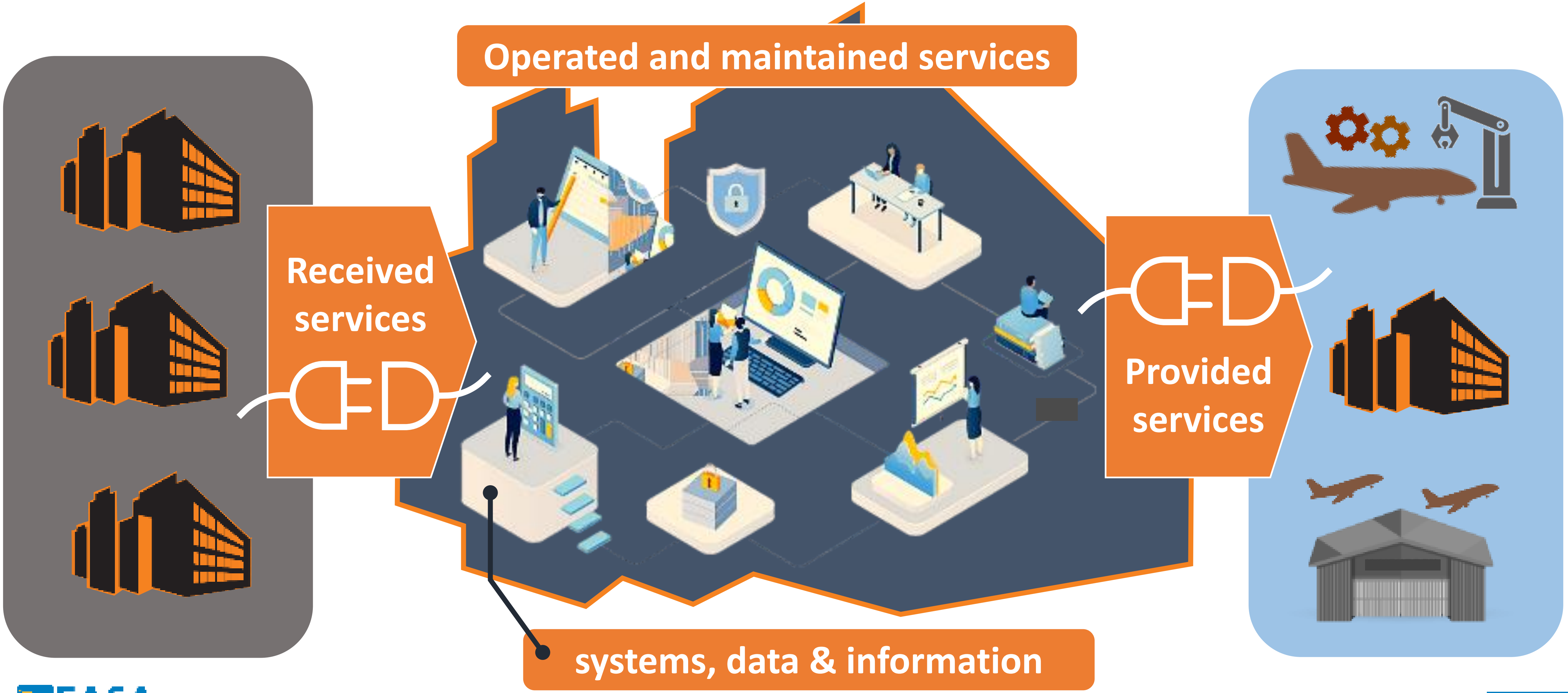
(b) The organisation shall identify the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.

OR.205 – Risk Assessment mutual comparison

→ **OR.205(c):** For the identified elements and interfaces, identify the information security risks with **potential impact on aviation safety**

- **Establish a predefined classification of risks levels**, based on:
  - Potential of occurrence of the threat scenario
  - Severity of safety consequences
- **For each identified risk:**
  - Assign a risk level (per the predefined classification)
    - → NOTE: To facilitate the mutual comparability of risks assessments, the assignment of the risk level shall take into account relevant information acquired in coordination with the interfaced organisations.
  - Associate the risk to the related element or interface.
  - Establish whether the risk is acceptable or must be treated (per IS.OR.210)

Part-IS Interfaced Organisations



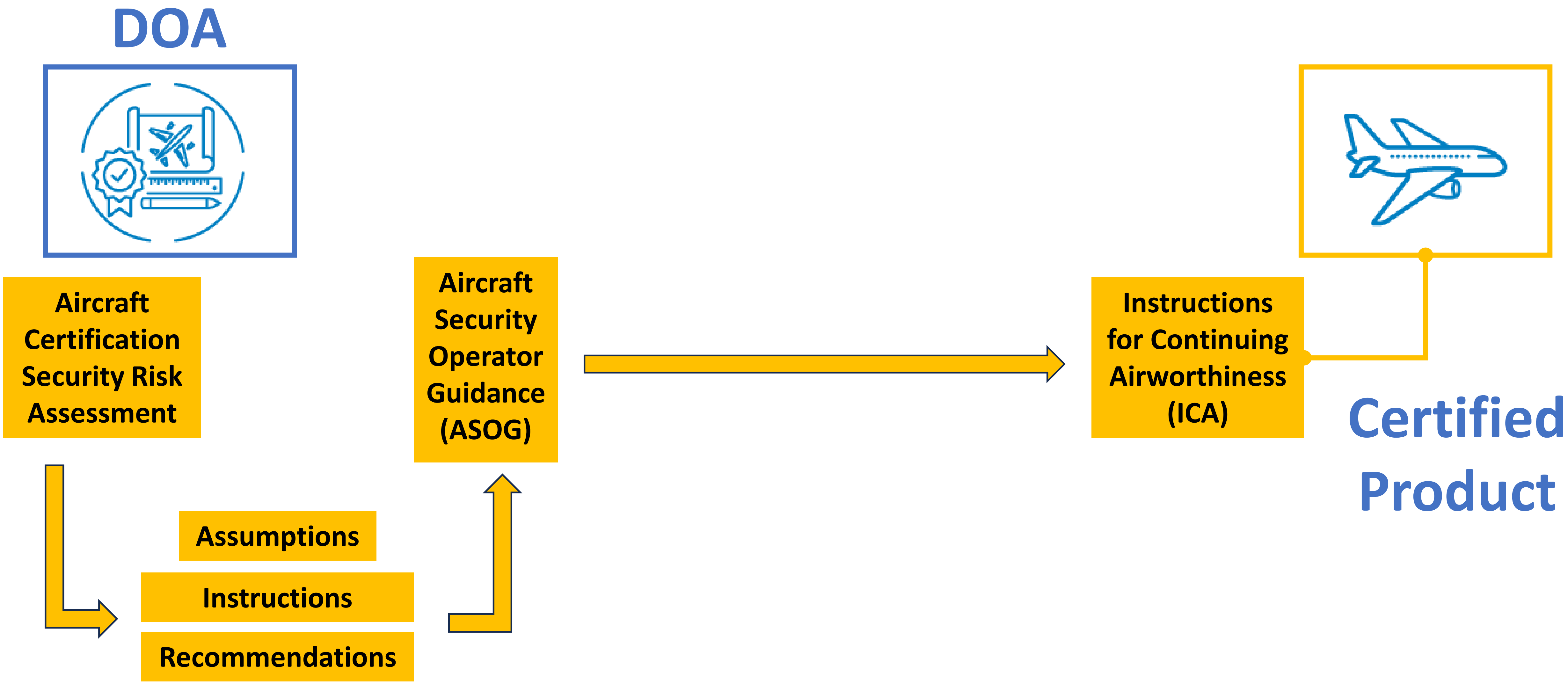
Operated and maintained services

Received services

Provided services

systems, data & information

Certified Product <u>designed</u> by Part-IS Organisation



DOA

Aircraft Certification Security Risk Assessment

Assumptions

Instructions

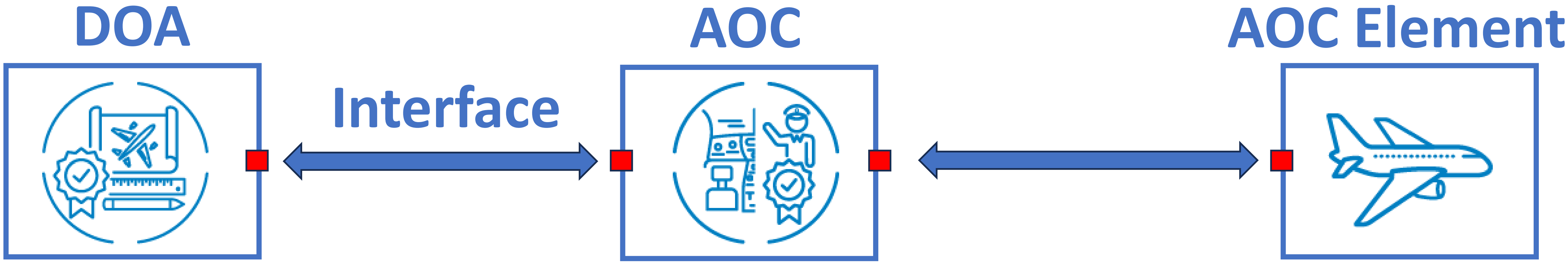
Recommendations

Aircraft Security Operator Guidance (ASOG)

Instructions for Continuing Airworthiness (ICA)

Certified Product

Interfaces and Risk Sharing



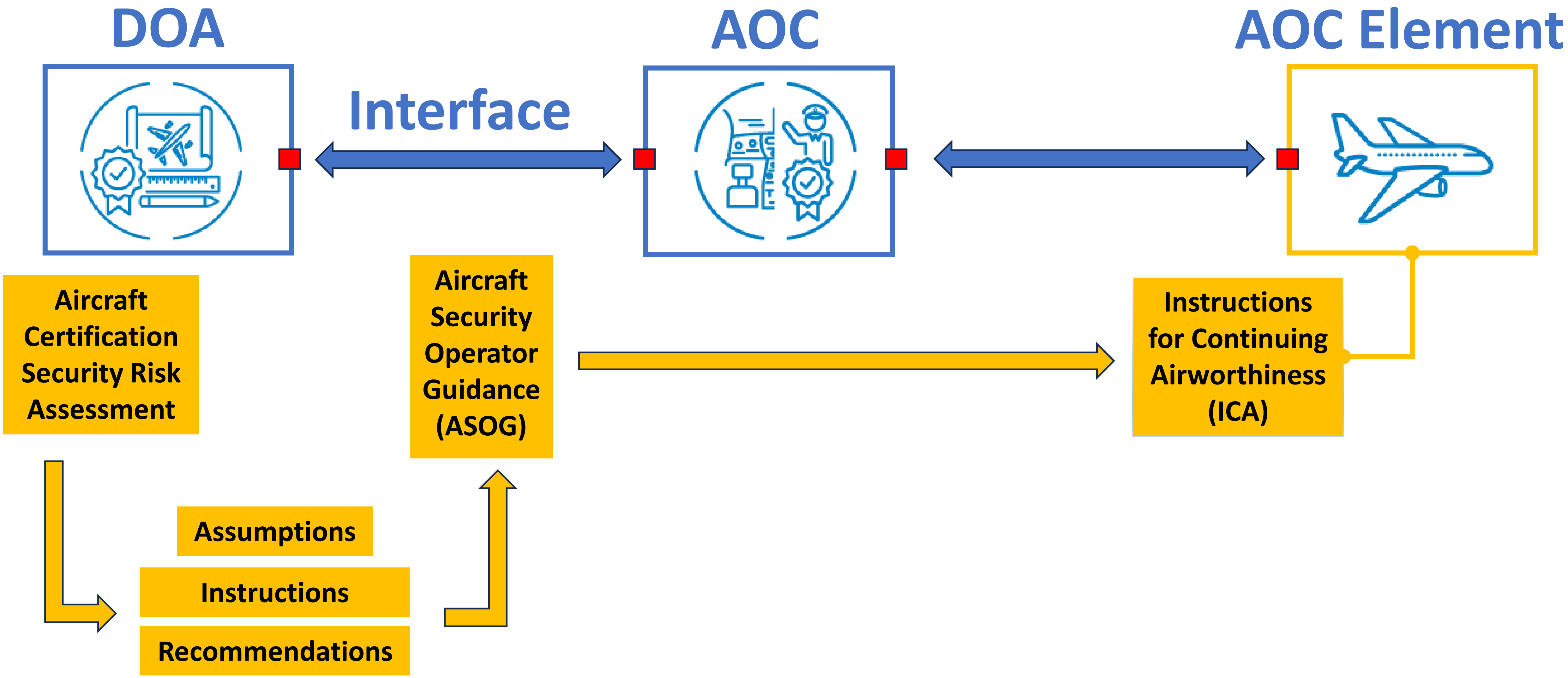
OR.205 (b)

The organisation shall identify the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.

OR.210 (b)

The organisation shall also inform organisations with which it has an interface in accordance with point IS.I.OR.205(b) of any risk shared between both organisations

Certified Product operated by Part-IS Organisation



DOA

Interface

AOC

AOC Element

Aircraft Certification Security Risk Assessment

Assumptions

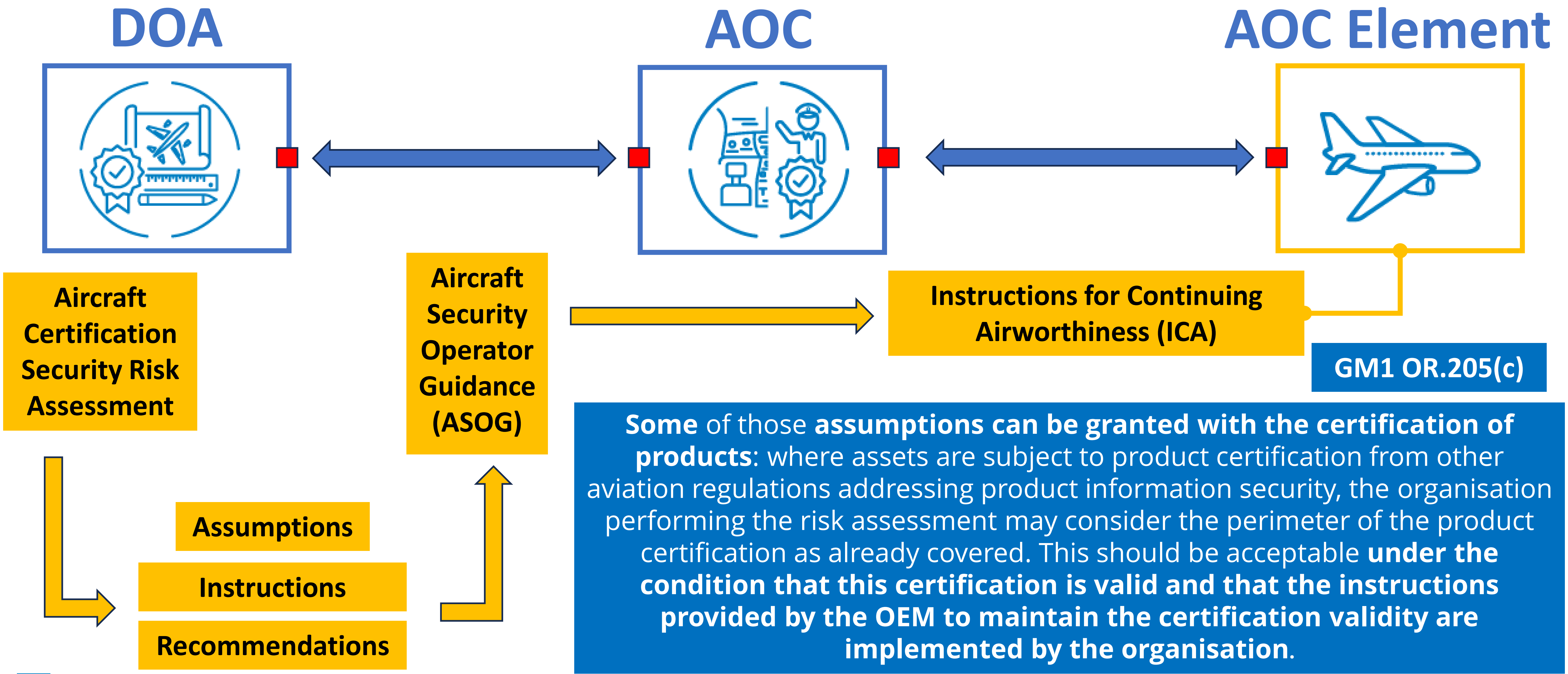
Instructions

Recommendations

Aircraft Security Operator Guidance (ASOG)

Instructions for Continuing Airworthiness (ICA)

Product Certification Assumptions



DOA

AOC

AOC Element

Aircraft Certification Security Risk Assessment

Assumptions

Instructions

Recommendations

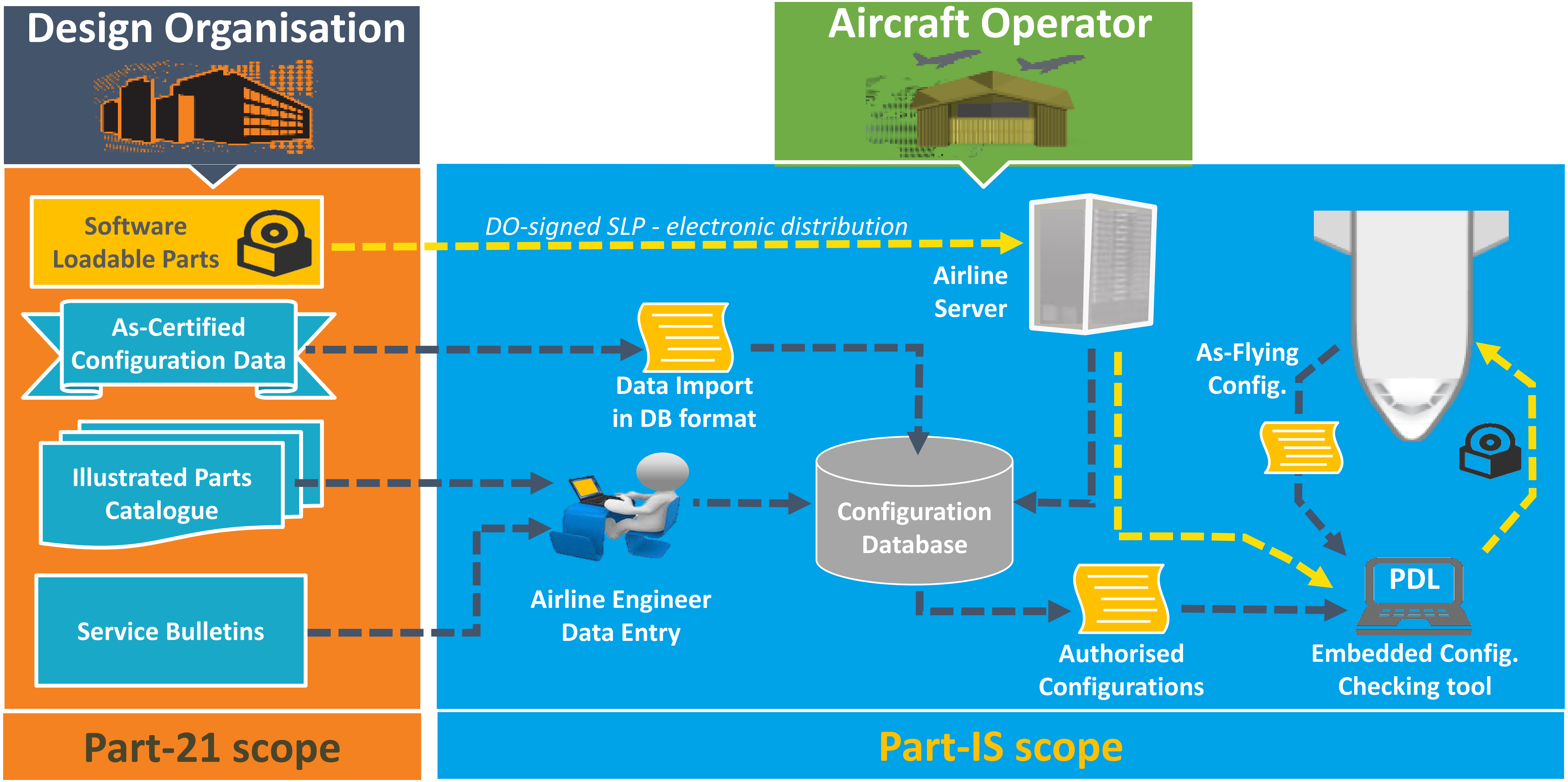
Aircraft Security Operator Guidance (ASOG)

Instructions for Continuing Airworthiness (ICA)

GM1 OR.205(c)

Some of those **assumptions can be granted with the certification of products**: where assets are subject to product certification from other aviation regulations addressing product information security, the organisation performing the risk assessment may consider the perimeter of the product certification as already covered. This should be acceptable **under the condition that this certification is valid and that the instructions provided by the OEM to maintain the certification validity are implemented by the organisation**.

Interface between Part-21 Continuing Airworthiness and Part-IS



Design Organisation

Software Loadable Parts

As-Certified Configuration Data

Illustrated Parts Catalogue

Service Bulletins

Aircraft Operator

DO-signed SLP - electronic distribution

Airline Server

Data Import in DB format

Airline Engineer Data Entry

Configuration Database

As-Flying Config.

Authorised Configurations

PDL

Embedded Config. Checking tool

Part-21 scope

Part-IS scope

How Part IS benefits from Product Certification ?

- **Information Security Risk is shared** among all stakeholders (e.g Design Approval Holder <-> Operator) and Part-IS deals with Risk Sharing and Interfaces (OR.205 & OR.210)

  - **Assumptions** considered for the product design (Security Risk Assessment) are maintained by user Organisations (e.g. AOC, CAMO) through Part-IS compliance

  - Information Security aspects contained in the **Recommendations and Instructions (ICA)** issued during product certification are maintained /exchanged by user Organisations (e.g. AOC, CAMO) through Part-IS compliance

EASA

European Union Aviation Safety Agency

Thank you!

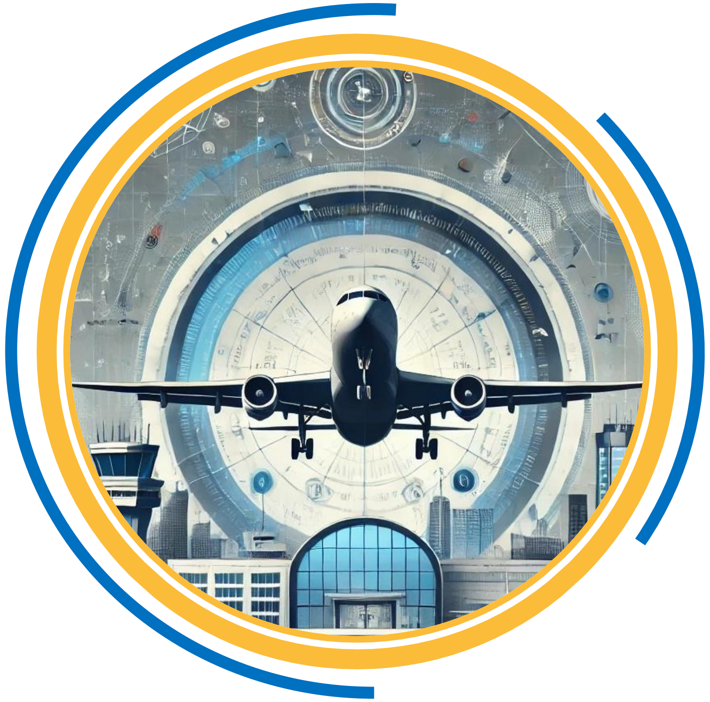
easa.europa.eu/connect

f in @

Your safety is our mission.

An Agency of the European Union

Enhancing CTI & Information Sharing for Part-IS compliance



Part-IS Implementation

Workshop 2025

EASA

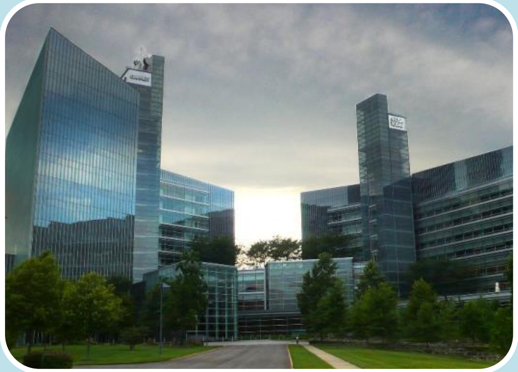
Gerry Ngu is a Senior Expert for Cybersecurity in Aviation, with over 20 years of experience at EASA in various roles, including in the Safety and Certification domain.

Over the past 9 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.

Part-IS Implementation Workshop 2025

1. Introduction to CTI
2. What type of CTI exist?
3. Why is CTI important for aviation?
4. How CTI supports Part-IS compliance?
5. How info sharing between org works best?
6. Useful considerations for CTI
7. Major take-aways

Making EU aviation cyber resilient



Products (Aircrafts, Engines, UAS …)

- Transition from case by case approach to mandatory on all products.
- 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

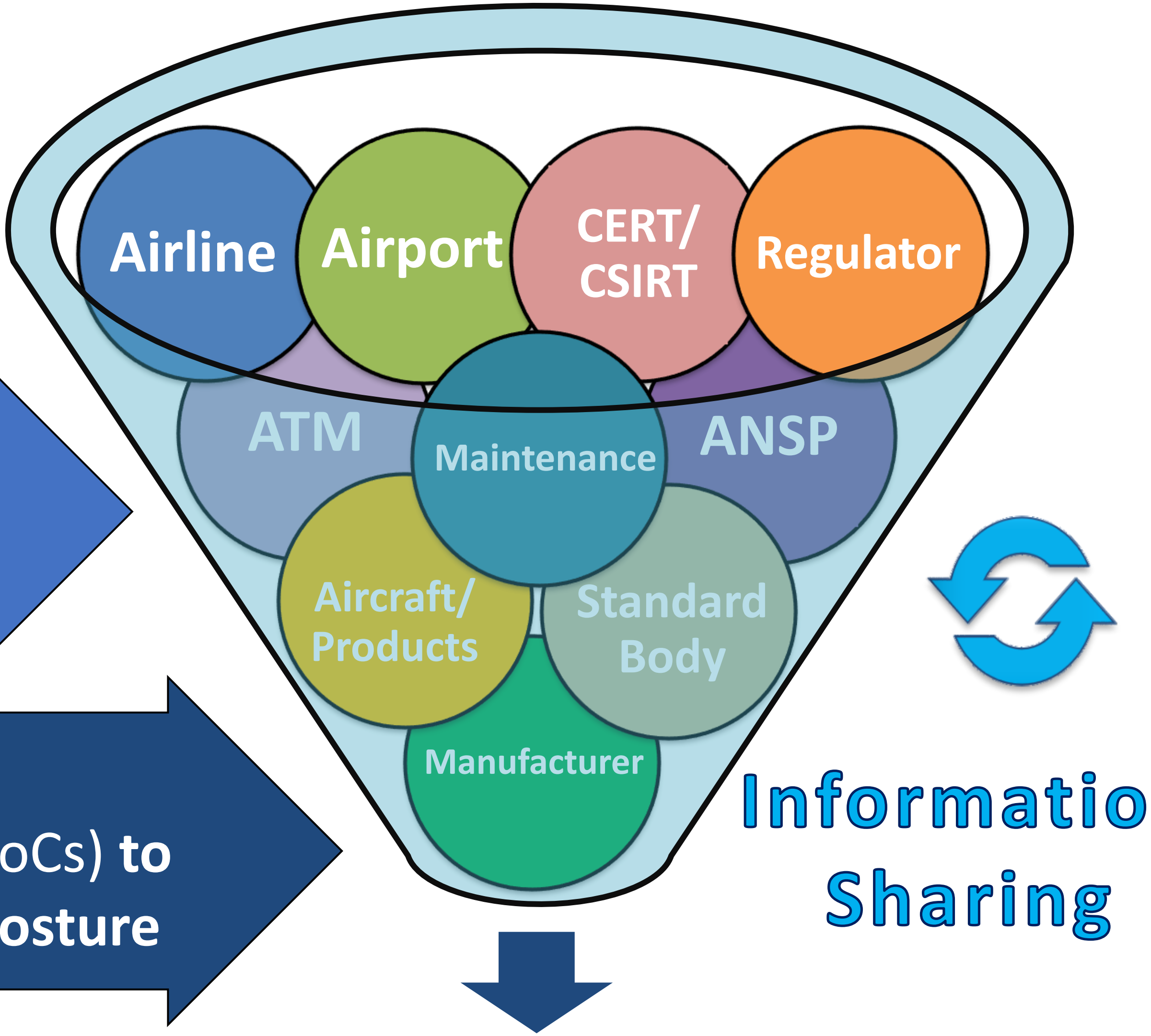
EASA

Cyber Threat Intelligence & Information Sharing

Sharing
IS caring

CTI: systematic collection, analysis & sharing of information on threats that may impact aviation safety, security & operations

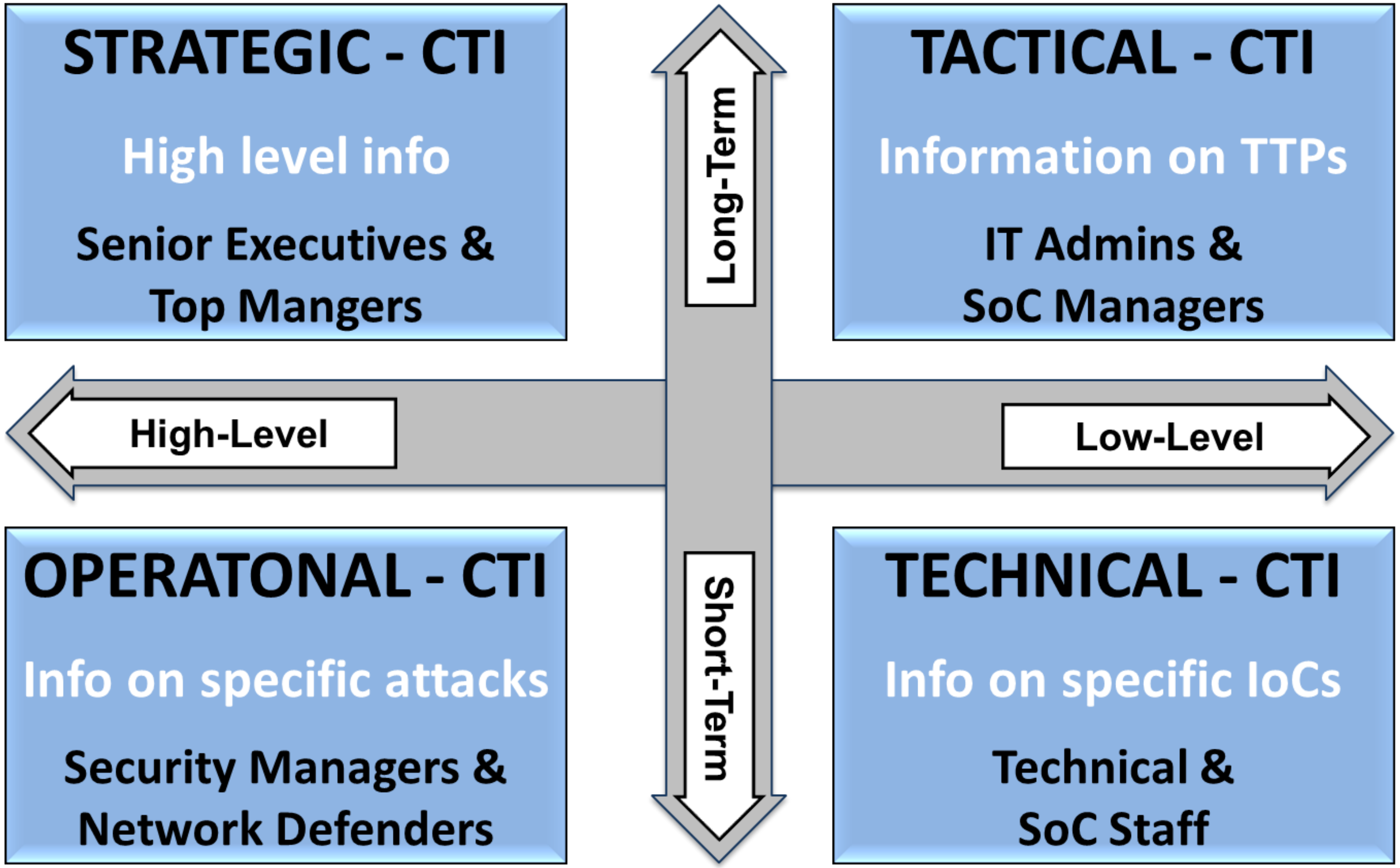
Info Sharing: organisations exchanging threat information (attack methods, vulnerabilities & IoCs) **to enhance their collective information security posture**



Information
Sharing

Resilience of the Aviation ECO-System

Cyber Threat Intelligence types



STRATEGIC - CTI

High level info

Senior Executives & Top Mangers

TACTICAL - CTI

Information on TTPs

IT Admins & SoC Managers

OPERATONAL - CTI

Info on specific attacks

Security Managers & Network Defenders

TECHNICAL - CTI

Info on specific IoCs

Technical & SoC Staff

Strategic CTI: overview of the aviation’s threat landscape

Tactical CTI: details on threat actors & attack vectors. How to build defense strategy to mitigate attacks

Technical CTI: evidence of an attack. Create base for analysts (reported IP addresses, phishing content, malware samples, fraudulent URLs)

Operational CTI: knowledge about attacks (motive, timing, how the attack was carried out)

CTI in the Aviation sector 1/2

Why is CTI important for Aviation?

- Protects critical systems (ATM, avionics, maintenance equipment)
- Anticipates evolving threats
- Enables informed risk management
- Strengthens incident response capabilities
- Supports regulatory compliance (e.g. EASA Part-IS, NIS-2, EU reg 376.

Who contributes to CTI in Aviation?

- Airlines & airports
- Air Navigation Service Providers (ANSPs)
- Manufacturers (OEMs, MROs)
- Suppliers & IT providers
- National CERTs/CSIRTs
- Law enforcement & intelligence agencies
- EASA/ECCSA, ECTL/EATM-CERT, ENISA, CERT-EU, ISACs…

CTI in the Aviation sector 2/2

What are the key CTI sources?

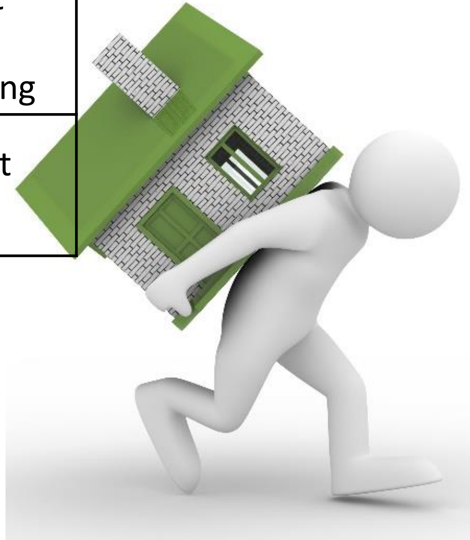
- Vulnerability databases (CVE, NVD, VulnDB, ExploitDB)
- Malware analysis reports
- Incident reports (internal & external)
- Intelligence feeds (open-source & private)
- Industry sharing platforms (ISACs, CERTs, ECCSA, EATM-CERT…)

What are the main CTI outputs?

- Threat reports & advisories (internal & external)
- IoC (Indicators of Compromise) lists
- TTP (Tactics, Techniques, Procedures) profiles
- Risk scoring & impact analysis
- Defensive recommendations (if needed)

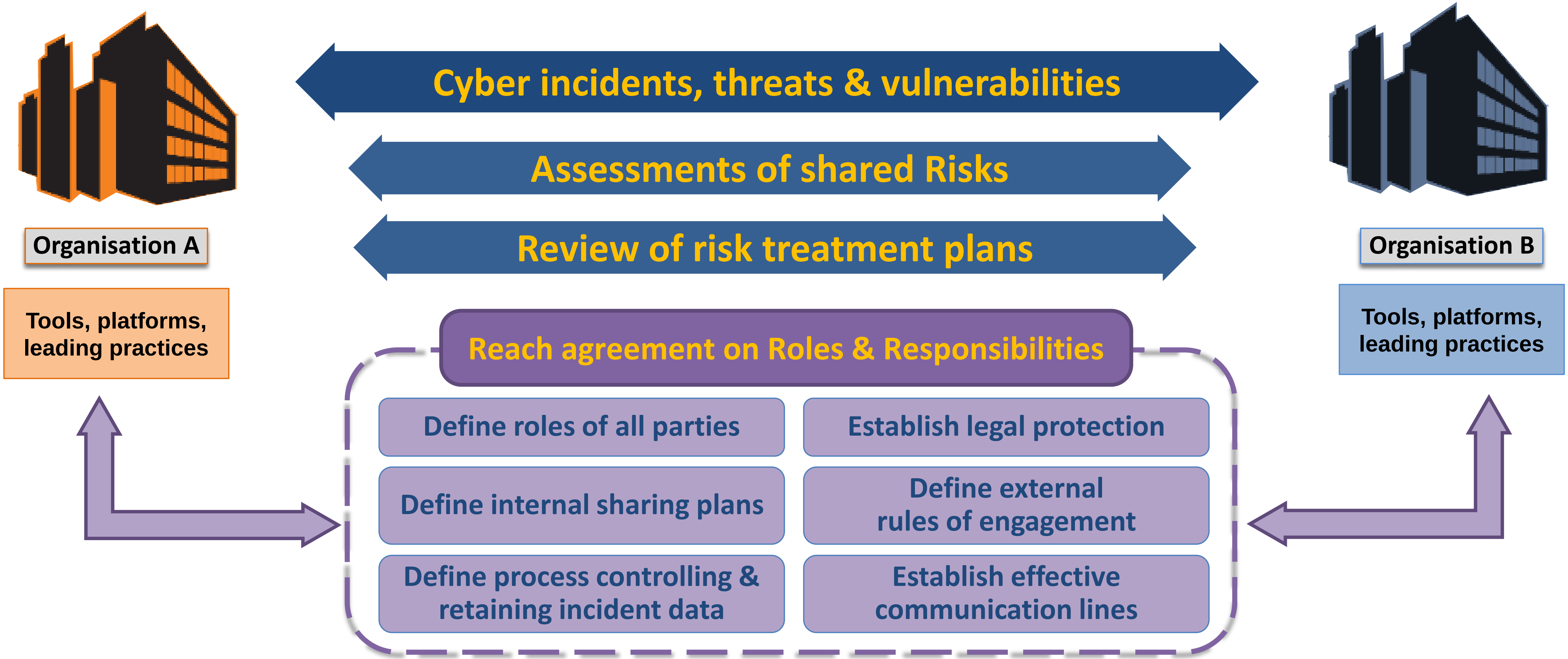
How CTI supports Part-IS compliance?

Part-IS requirement	How CTI supports Part-IS requirement	Relevant AMC/GM
OR.200- ISMS General requirements	Informs all ISMS elements via AMCs/GMs that encourage threat-based management	**AMC1 IS.OR.200(a)(2)** - Threat identification should be informed by external sources **GM1 IS.OR.200(a)** - recommended CTI sources (ECCSA, CERTs)
OR.205- Risk assessment	Enhances risk assessment quality by introducing real-world threat vectors	**AMC1 IS.OR.205(a)** - Risk assessment should consider threat intel sources **GM1 IS.OR.205(a)** - Encourages using external CTI feeds
OR.215- Performance monitoring & improvement	Feeds into monitoring trends and ISMS maturity	**AMC1 IS.OR.215(a)** - Use of incident trends and threat intelligence in ISMS improvement
OR.220- Event management	Improves detection and response planning via IOC/TTP knowledge	**AMC1 IS.OR.220(a)** - CTI enhances detection of threats and planning of responses **GM1 IS.OR.220(a)** - Use of known threat indicators
OR.225- Awareness & training	Enhances relevance of training using actual threat scenarios	**AMC1 IS.OR.225(a)** - Awareness should reflect current threat landscape **GM1 IS.OR.225(a)** - Suggests using threat intel to tailor training
OR.230- External reporting scheme	Provides context to minor anomalies & reportable threats (TTPs linked to aviation-specific APTs)	**GM1 IS.OR.230(a) -** Events must be reported when significant and context; CTI helps assess significance & context



CTI plays key role in meeting proactive & risk-based requirements under Part-IS

Sharing information between organisations 2/2



Cyber incidents, threats & vulnerabilities

Assessments of shared Risks

Review of risk treatment plans

Organisation A

Tools, platforms, leading practices

Organisation B

Tools, platforms, leading practices

Reach agreement on Roles & Responsibilities

- Define roles of all parties
- Establish legal protection
- Define internal sharing plans
- Define external rules of engagement
- Define process controlling & retaining incident data
- Establish effective communication lines

Organisation CTI capability = Build on own CTI capability + [Trust third party capability]

Traffic Light Protocol (TLP) & severity

Traffic Light Protocol (TLP) description	
TLP:RED	**NOT for disclosure, restricted ONLY to participant** Information may not be shared with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed
TLP:AMBER+STRICT	**Limited disclosure, restricted ONLY to participants' OWN organisation** Information may only be shared with members of their own organisation Information shared ONLY within their OWN organisation
TLP:AMBER	**Limited disclosure, restricted OWN organisation & its clients** Recipients can only spread this on a need-to-know basis within their organisation and its clients
TLP:GREEN	**Limited disclosure, restricted to the community** Information may be shared with peers and partner organisations within their sector or community, but not via publicly accessible channels
TLP:CLEAR (WHITE)	**Disclosure is not limited** Information may be distributed without restriction and is subject to standard copyright rules

Severity description		
	HIGH	Attack exhibiting a high level of preparation, resources and/or skills (E.g. highly targeted spear-phishing attack against well-identified individuals, use of 0-days, advanced anti-detection techniques or massive infrastructure for disruption, etc.)
	MEDIUM	Attack leveraging moderate resources and/or skills (E.g. large spear-phishing attacks, criminal malware with the latest delivery mechanisms or anti-detection features, etc.)
	LOW	Attack using basic resources and/or skills (E.g. general mass malware, common attack techniques, opportunistic defacements, etc.)

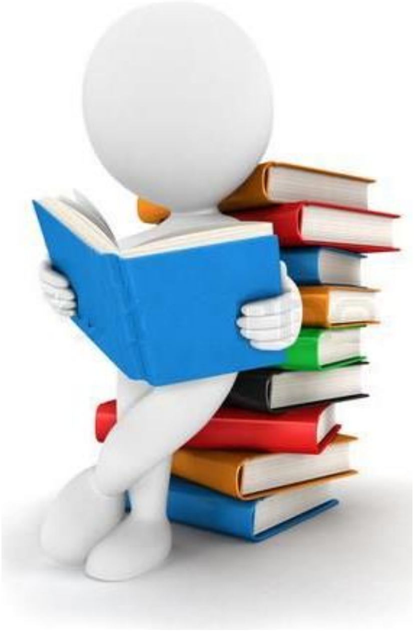
EASA

Source reliability & information credibility

Source Reliability Table		
A	Completely Reliable	No doubt about the source. History of complete reliability
B	Usually reliable	History of mostly valid information
C	Fairly reliable	Provided valid information in the past
D	Not usually reliable	Significant doubts. Provided valid information in the past
E	Unreliable	History of invalid information
F	Reliability cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable

Information Credibility Table		
1	Confirmed by other sources	Logical in itself; Consistent with other information on the subject
2	Probably True (NC)	Logical in itself; consistent with other information on the subject
3	Possibly True (NC)	Reasonably logical in itself; agrees with other information on the subject
4	Doubtful (NC)	Possible but not logical; no other information on the subject
5	Improbable (NC)	Not logical in itself; contradicted by other information on the subject
6	Truth cannot be judged	No basis exists for evaluating the validity of the information
(NC) = Not Confirmed information		

Major take-aways



Cyber Threat Intelligence is a useful enabler for effective compliance with EASA Part-IS

CTI strengthens: threat identification, risk-based decision-making & incident preparedness

CTI supports AMC/GM expectations: for proactive monitoring, awareness & continuous ISMS improvement

Incorporating CTI ensures aviation organisations: stay resilient, informed & regulation-ready in a dynamic threat landscape

Contact us at:

CyberSec@easa.europa.eu

Gerry.Ngu@easa.europa.eu

Join our Community:

easa.europa.eu/connect

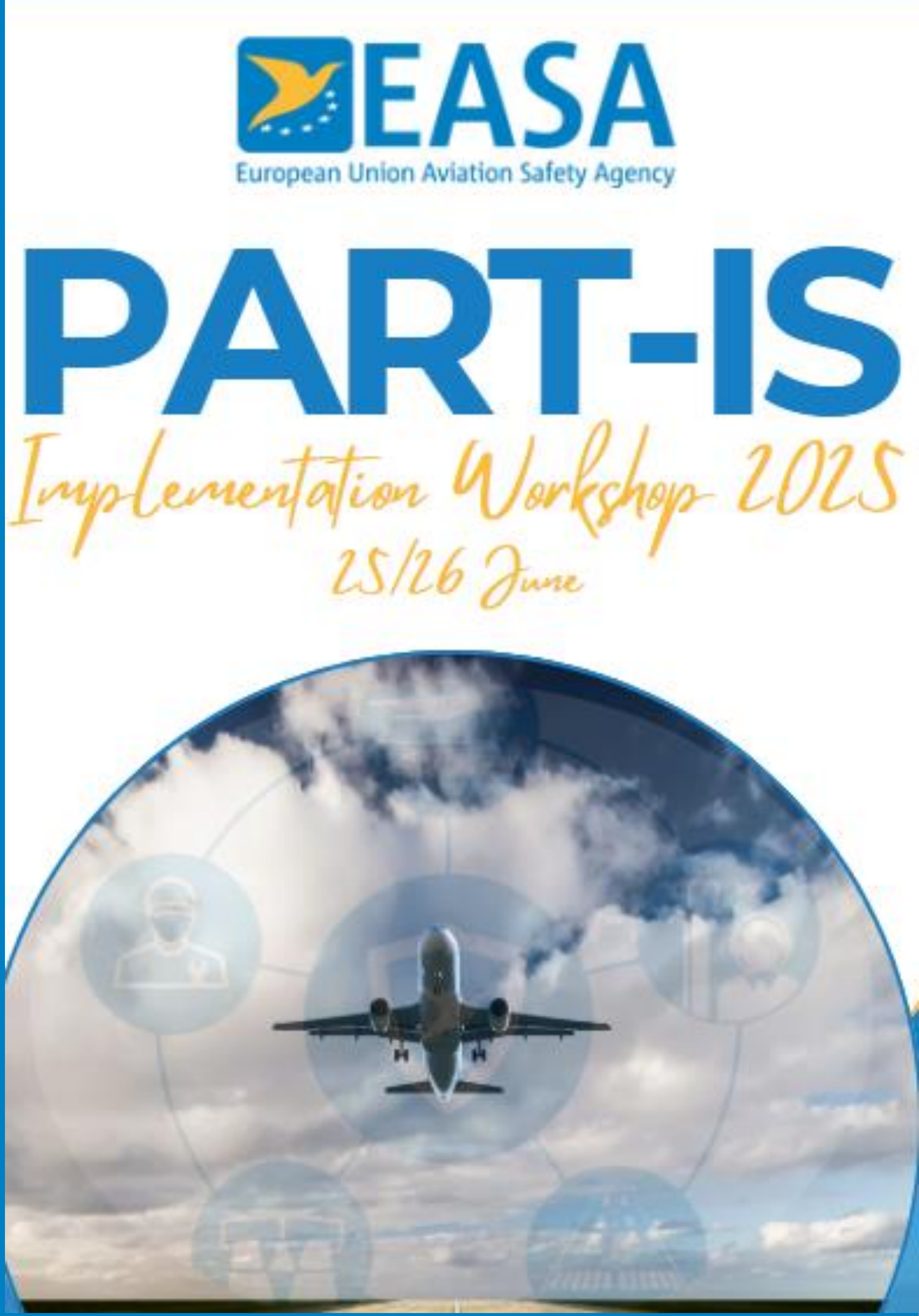
Your safety is our mission.

An Agency of the European Union

EASA
European Union Aviation Safety Agency

Part-IS Implementation Workshop 2025

Conclusions – Day 1


EASA
European Union Aviation Safety Agency
PART-IS
Implementation Workshop 2025
25/26 June

Part-IS Workshop agenda – Day 2

Part-IS Task Force outcomes - Implementation tools and guidance

This session will provide an overview of the available tools and guidance as well as the harmonisation activities carried of by the Part-IS Task Force.

Part-IS Task Force Representatives from Member States (Spain, Austria)

Oversight Approach – Overview and Q&A

This session will provide an overview of the oversight approach by the applicability date

EASA

Mapping of EU cybersecurity rules applicable to the aviation sector (Part-IS, NIS2 and AVSEC)

This session will present the progress of the comparison exercise conducted under the Aviation Cybersecurity Subgroup between requirements stemming from Part-IS and other applicable EU cybersecurity legislation for aviation entities (NIS2 and AVSEC)

European Commission (DG MOVE, DG CNECT) Irish Aviation Authority, Federal Office for Information Security (BSI)

Q&A

Part-IS Guidance Material (GM) update

The update that took place in the latest iteration of the Guidance Material of Part-IS will be presented

EASA

Meet the experts sessions (on-site only)

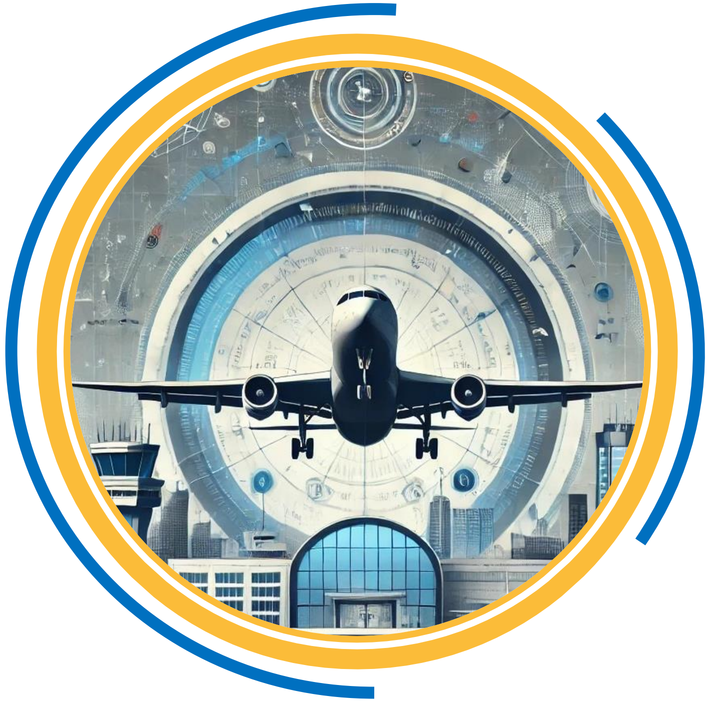
Participants will have the opportunity to exchange in 10min slots with EASA experts on-site on selected topics

Q&A

EASA

See you tomorrow!

Thanks for being with us virtually and in presence



Part-IS Implementation

Workshop 2025