# Part-IS CAFE #3

## Part IS Info Meeting

30.09.2025

TLP Clear

# Was ist das Part IS CAFE?
# Warum machen wir das Meeting?

- Schnellere Information der Organisationen
- Allgemeine Verfügbarkeit von Dokumenten
- Standardisierung

- Implementierung für alle Betriebe per Gesetz bis 16.10.2025 (POA, DOA, Aerodrome) bzw. 22.2.2026 (der Rest)
- Anforderungen in Part IS sind ein neues Territorium, weil KEINE klassische „Safety Regulation
- Vorgehensweise nicht klar erkennbar (Unsicherheiten in der Umsetzung)

# Wie soll das Part IS Café ablaufen?

Dauer ca. 2 Stunden

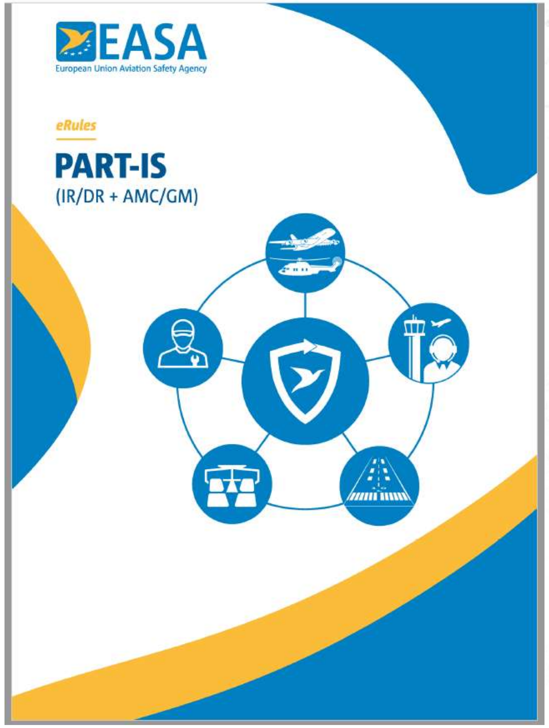
Ablauf:

- Kurze Einleitung zum Format
- Info´s von ACG an Betriebe
- Fragen der Betriebe

Fragen bitte via Chat stellen, wir übernehmen sie in eine Liste, sofern sie nicht sofort beantwortet werden können. Diese werden dann in den folgenden Cafés beantwortet.

Erklärung zum Set-Up:
Die Inspektor:innen und Prüfer:innen wurden ebenso eingeladen, um einen gleichen Wissensstand für alle Beteiligte zu erzeugen. Obwohl wir in bislang 5 eintägigen Trainings einen Großteil unserer Kolleg:innen erreichen konnten, sind viele dieser Informationen dieses Café für die Kolleg:innen auch neu. Vor Allem, da einige Informationen, auch auf Europäischer Ebene, sehr aktuell sind. Deshalb konnten sie bisher auch nicht vollinhaltlich Auskunft zum Thema geben. **Wir bitten um Verständnis!**

# Generelle Informationen zu Part-IS



EASA

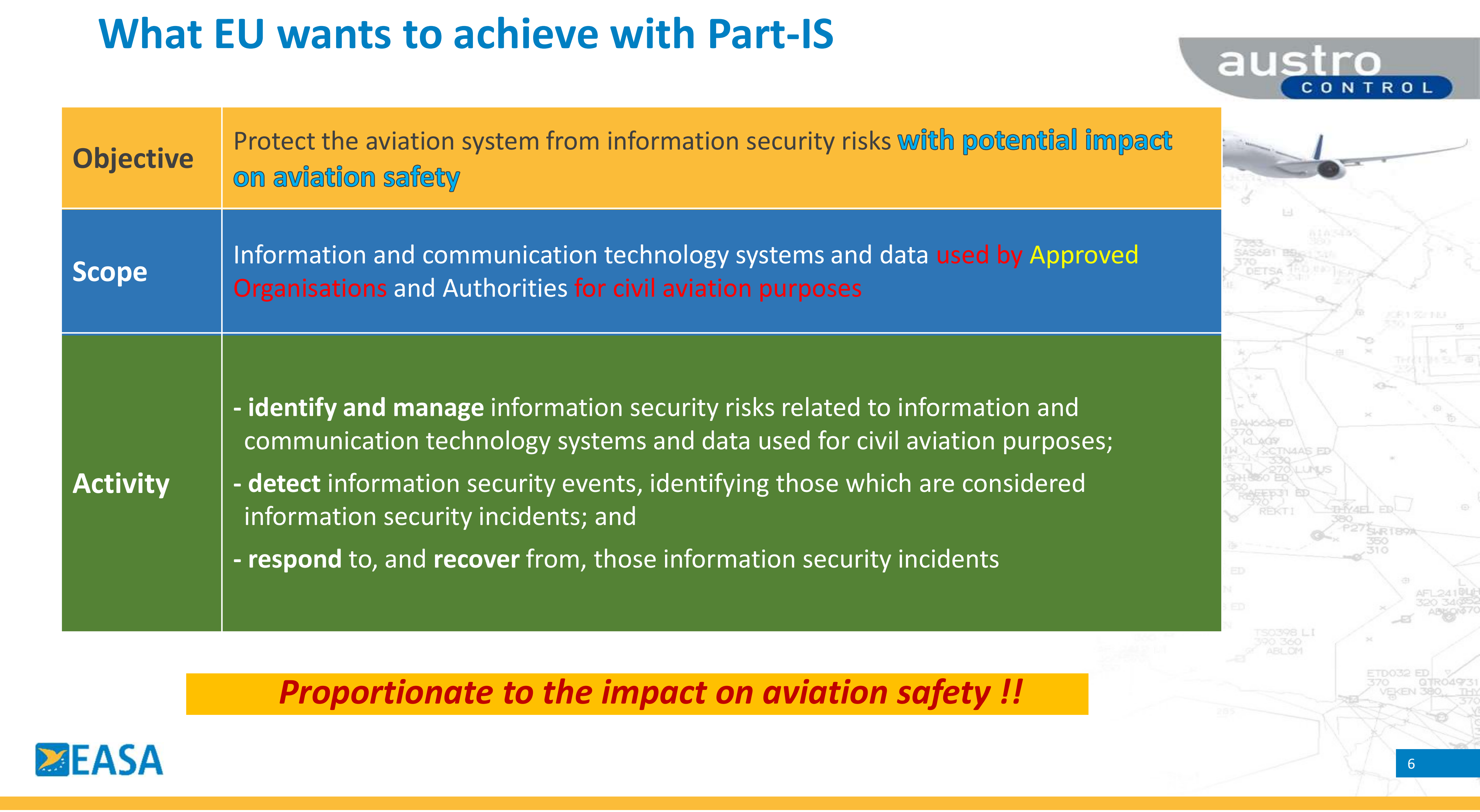
European Union Aviation Safety Agency

eRules

PART-IS

(IR/DR + AMC/GM)

Part-IS-Café – 30.09.2025



# What EU wants to achieve with Part-IS

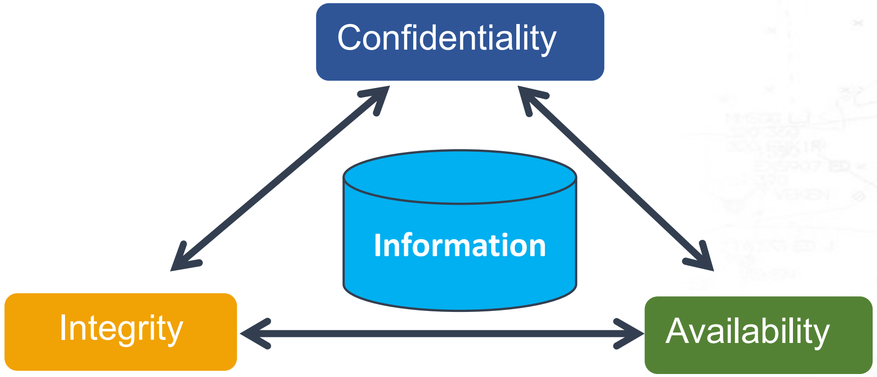
| | |
|---|---|
| **Objective** | Protect the aviation system from information security risks **with potential impact on aviation safety** |
| **Scope** | Information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes |
| **Activity** | - **identify and manage** information security risks related to information and communication technology systems and data used for civil aviation purposes;<br>- **detect** information security events, identifying those which are considered information security incidents; and<br>- **respond** to, and **recover** from, those information security incidents |

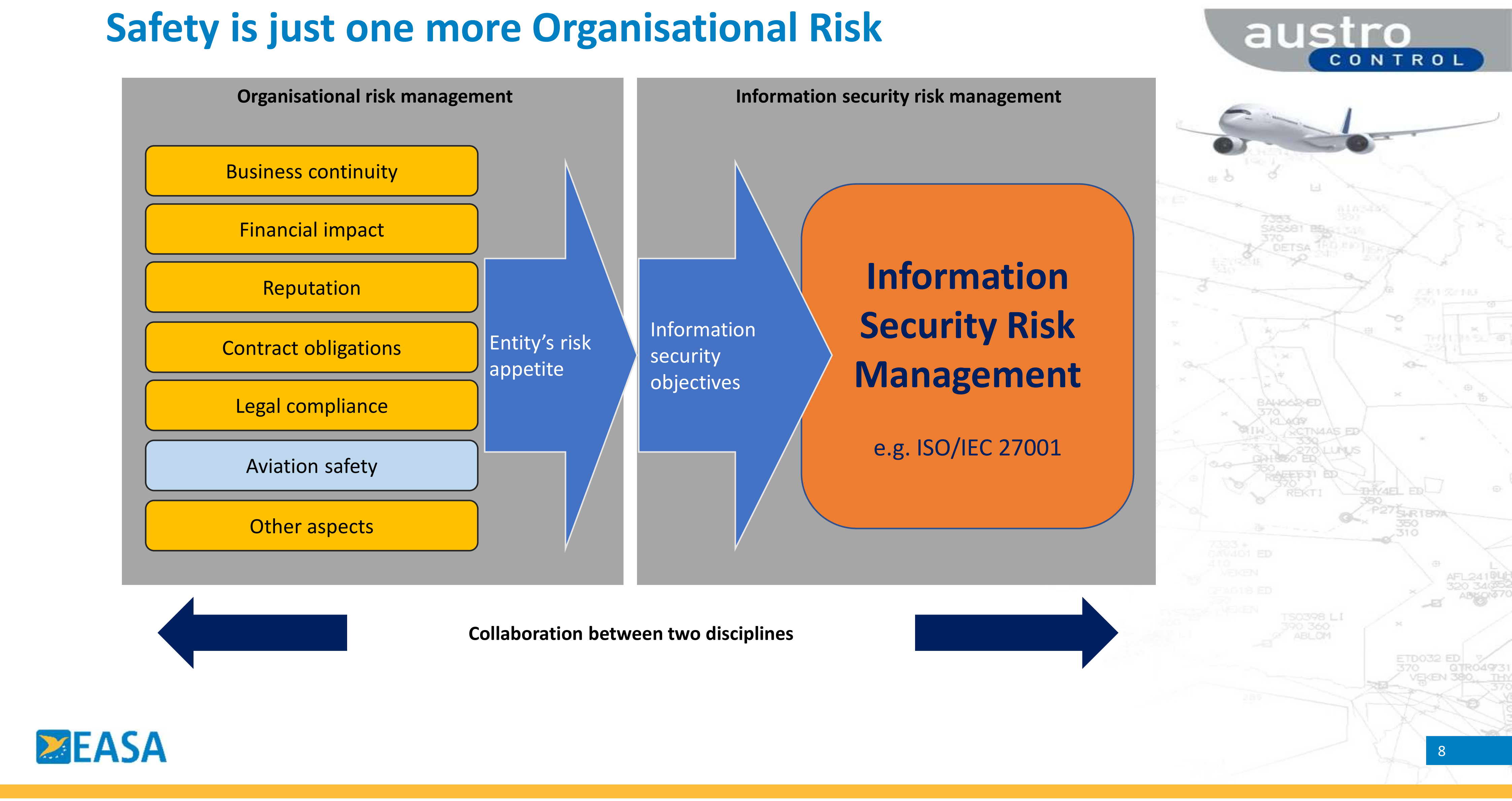
***Proportionate to the impact on aviation safety !!***

# What is an ISMS ?

## What is Information Security Management?

- ISO 27001 states that ***Information Security Management*** *is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their*
  - ***Confidentiality,***
  - ***Integrity,*** *and*
  - ***Availability***.





# Safety is just one more Organisational Risk

**Organisational risk management**

- Business continuity
- Financial impact
- Reputation
- Contract obligations
- Legal compliance
- Aviation safety
- Other aspects

Entity's risk appetite

**Information security risk management**

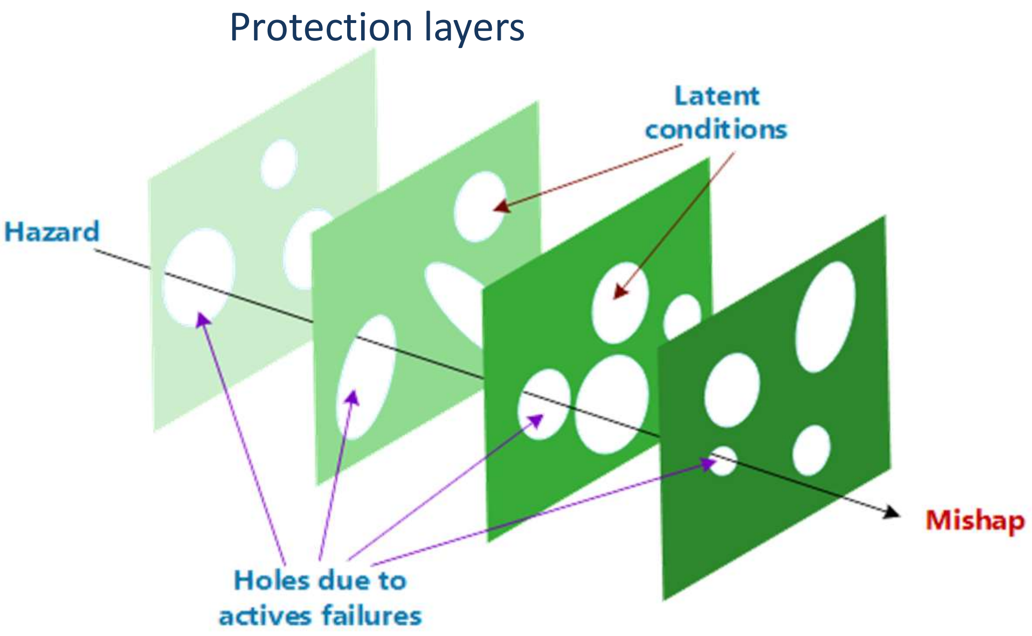
Information security objectives

**Information Security Risk Management**

e.g. ISO/IEC 27001

**Collaboration between two disciplines**

# The cultural bias in aviation



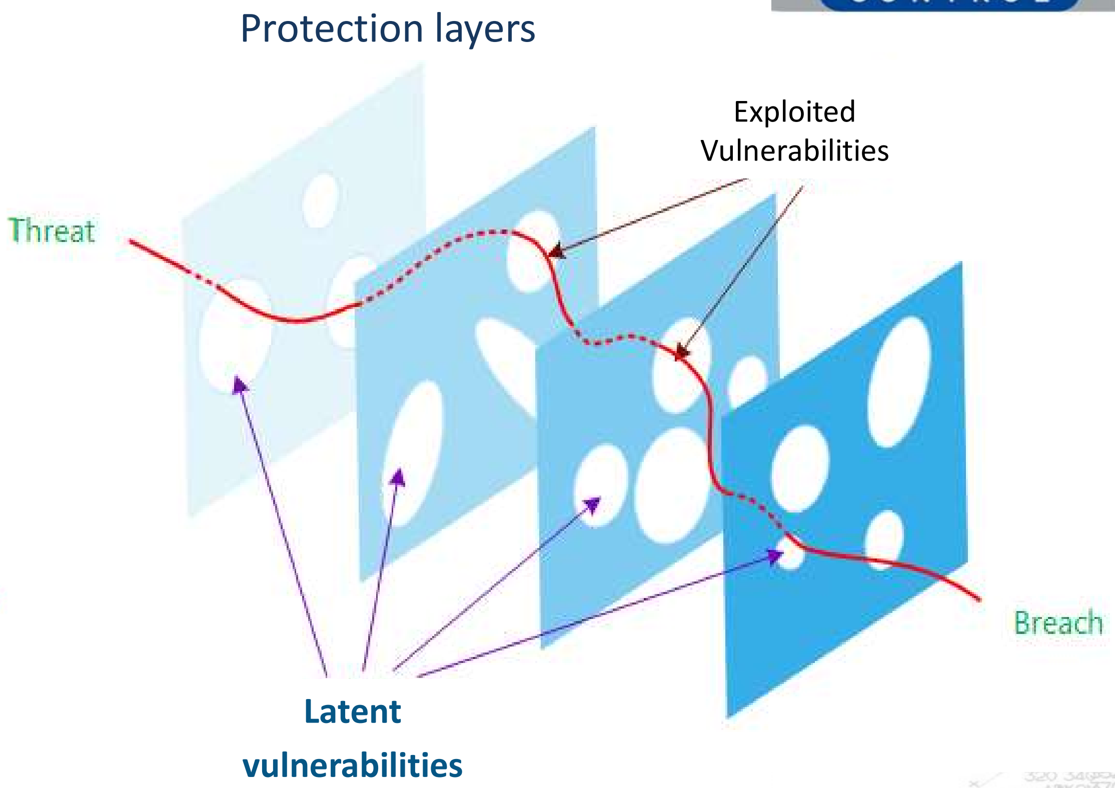
Protection layers

Latent conditions

Hazard

Mishap

Holes due to actives failures



Protection layers

Exploited Vulnerabilities

Threat

Breach

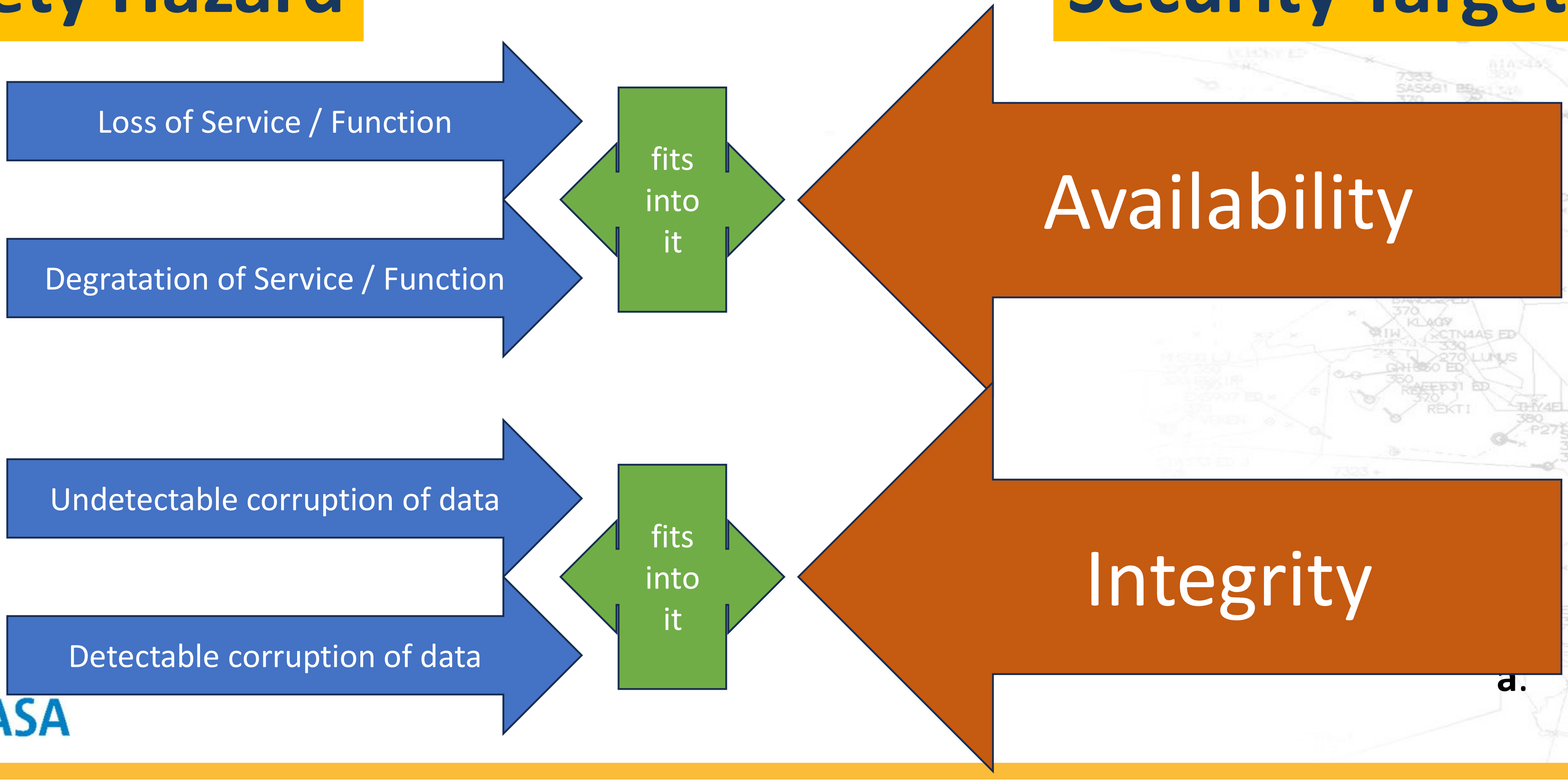
Latent vulnerabilities

**Safety** **versus** **Security**

# Safety ~~versus~~ and Security – Example (ANS)

## Safety Hazard

## Security Target



Loss of Service / Function

Degratation of Service / Function

fits into it

Availability

Undetectable corruption of data

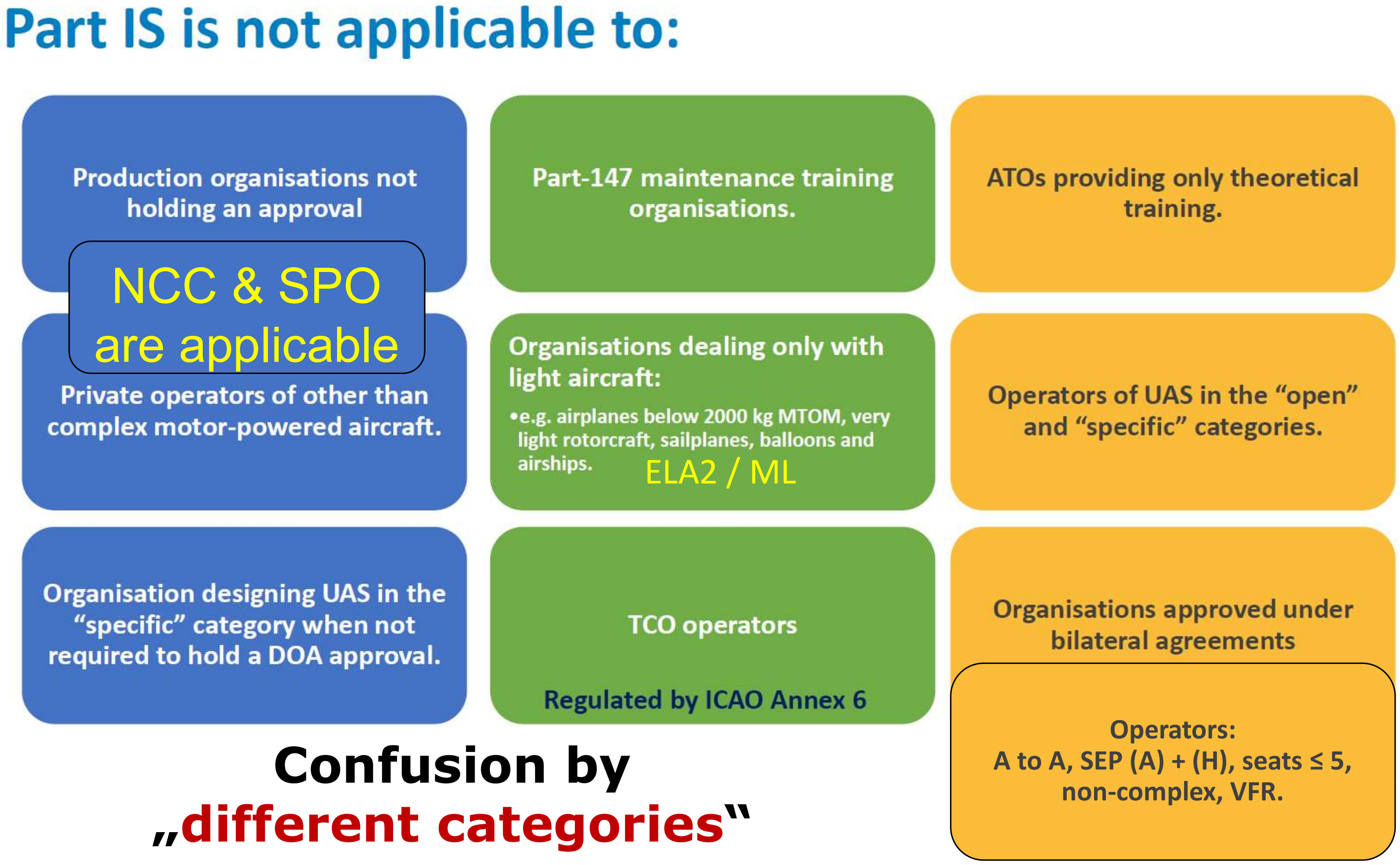
Detectable corruption of data

fits into it

Integrity

a.

# Applicability



## Part IS is not applicable to:

Production organisations not holding an approval

Part-147 maintenance training organisations.

ATOs providing only theoretical training.

NCC & SPO are applicable

Private operators of other than complex motor-powered aircraft.

Organisations dealing only with light aircraft:

- e.g. airplanes below 2000 kg MTOM, very light rotorcraft, sailplanes, balloons and airships.

ELA2 / ML

Operators of UAS in the “open” and “specific” categories.

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

TCO operators

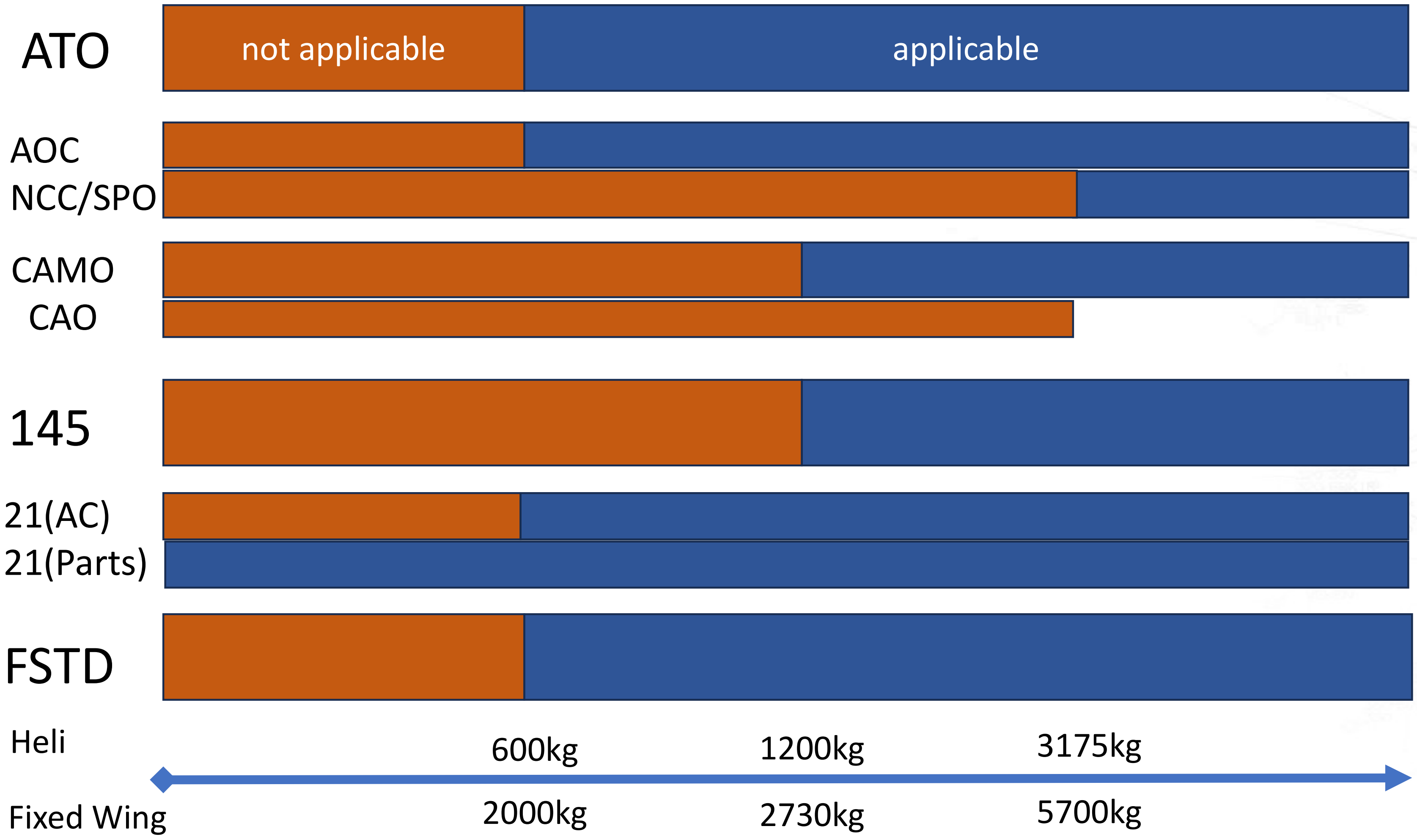
Regulated by ICAO Annex 6

Organisations approved under bilateral agreements

Operators:
A to A, SEP (A) + (H), seats ≤ 5, non-complex, VFR.

**Confusion by „different categories“**

# Applicability – based on MTOM



ATO

not applicable

applicable

AOC

NCC/SPO

CAMO

CAO

145

21(AC)

21(Parts)

FSTD

Heli

600kg

1200kg

3175kg

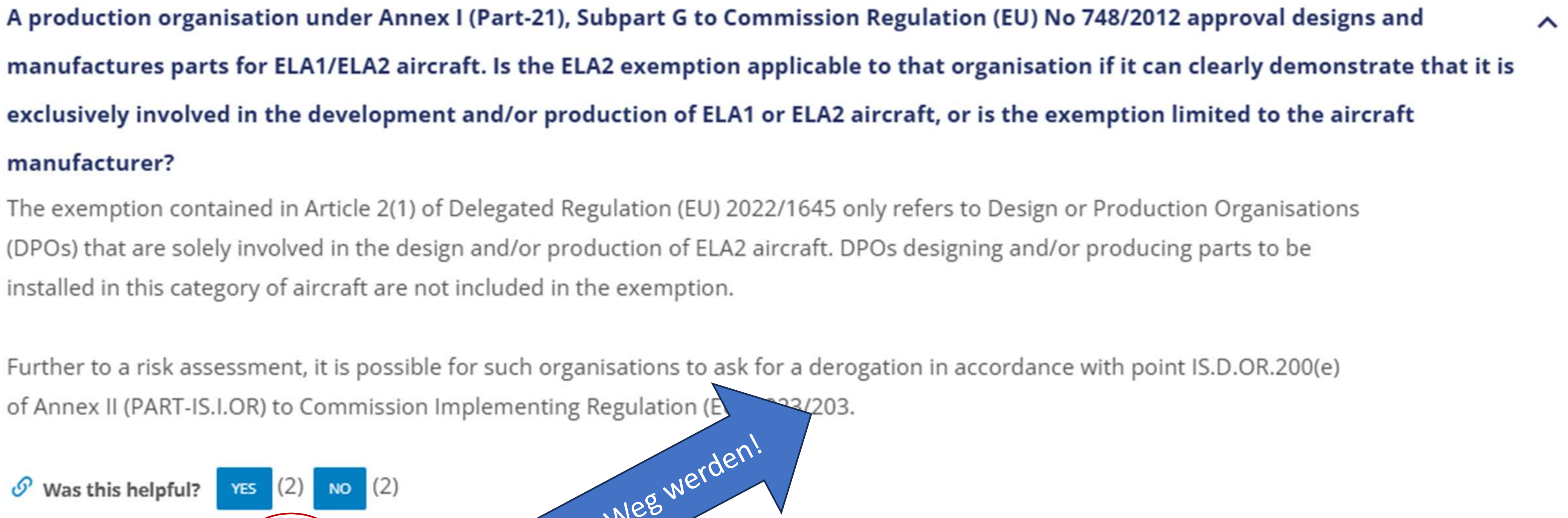
Fixed Wing

2000kg

2730kg

5700kg

# Applicability EASA FAQ



**A production organisation under Annex I (Part-21), Subpart G to Commission Regulation (EU) No 748/2012 approval designs and manufactures parts for ELA1/ELA2 aircraft. Is the ELA2 exemption applicable to that organisation if it can clearly demonstrate that it is exclusively involved in the development and/or production of ELA1 or ELA2 aircraft, or is the exemption limited to the aircraft manufacturer?**

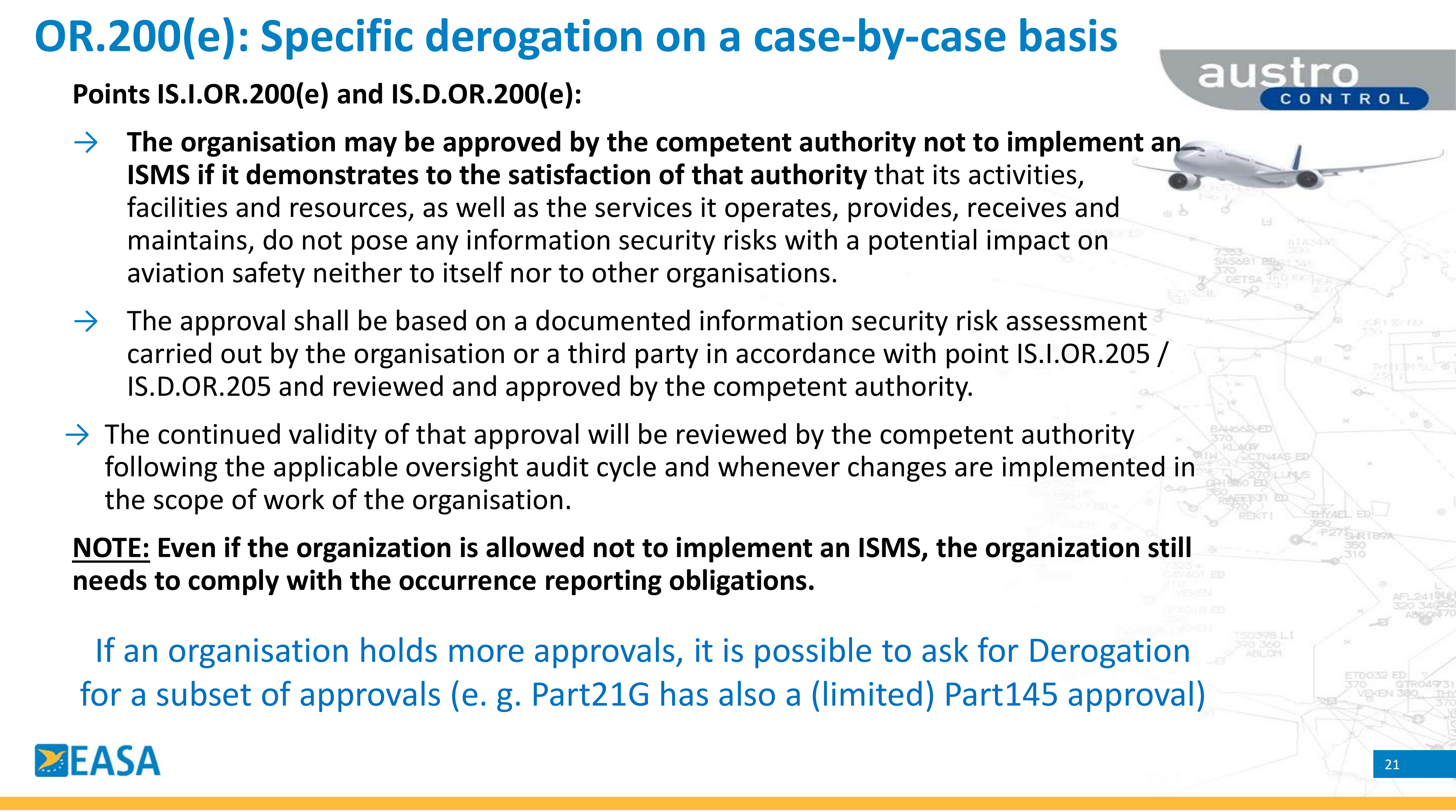
The exemption contained in Article 2(1) of Delegated Regulation (EU) 2022/1645 only refers to Design or Production Organisations (DPOs) that are solely involved in the design and/or production of ELA2 aircraft. DPOs designing and/or producing parts to be installed in this category of aircraft are not included in the exemption.

Further to a risk assessment, it is possible for such organisations to ask for a derogation in accordance with point IS.D.OR.200(e) of Annex II (PART-IS.I.OR) to Commission Implementing Regulation (E[illegible]23/203.

Das sollte unser Weg werden!

# Derogation process accoding IS.D/I.OR.200 (e)

Part-IS-Café – 26.08.2025



# OR.200(e): Specific derogation on a case-by-case basis

**Points IS.I.OR.200(e) and IS.D.OR.200(e):**

→ **The organisation may be approved by the competent authority not to implement an ISMS if it demonstrates to the satisfaction of that authority** that its activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with a potential impact on aviation safety neither to itself nor to other organisations.

→ The approval shall be based on a documented information security risk assessment carried out by the organisation or a third party in accordance with point IS.I.OR.205 / IS.D.OR.205 and reviewed and approved by the competent authority.

→ The continued validity of that approval will be reviewed by the competent authority following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.

**NOTE: Even if the organization is allowed not to implement an ISMS, the organization still needs to comply with the occurrence reporting obligations.**

If an organisation holds more approvals, it is possible to ask for Derogation for a subset of approvals (e. g. Part21G has also a (limited) Part145 approval)

# How the process works

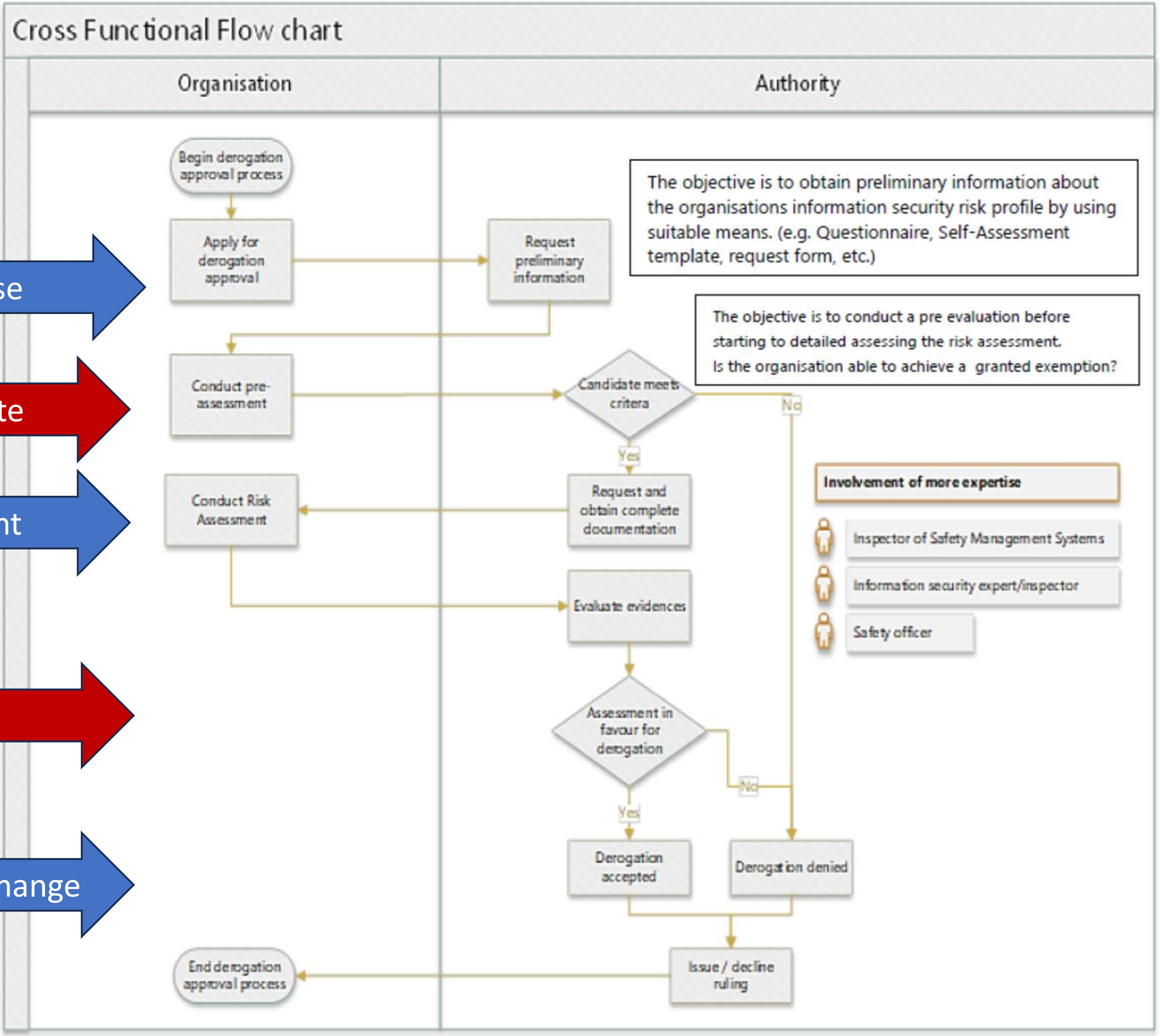
Pre-assessement phase

Authority accepts applicant as canditate

Detailed Risk Assessment

Authority decides on derogation

Re-assessment required for each change


Cross Functional Flow chart
Organisation
Authority
Begin derogation approval process
Apply for derogation approval
Request preliminary information
Conduct pre-assessment
Candidate meets critera
No
Yes
Conduct Risk Assessment
Request and obtain complete documentation
Involvement of more expertise
Inspector of Safety Management Systems
Information security expert/inspector
Safety officer
Evaluate evidences
Assessment in favour for derogation
No
Yes
Derogation accepted
Derogation denied
Issue / decline ruling
End derogation approval process

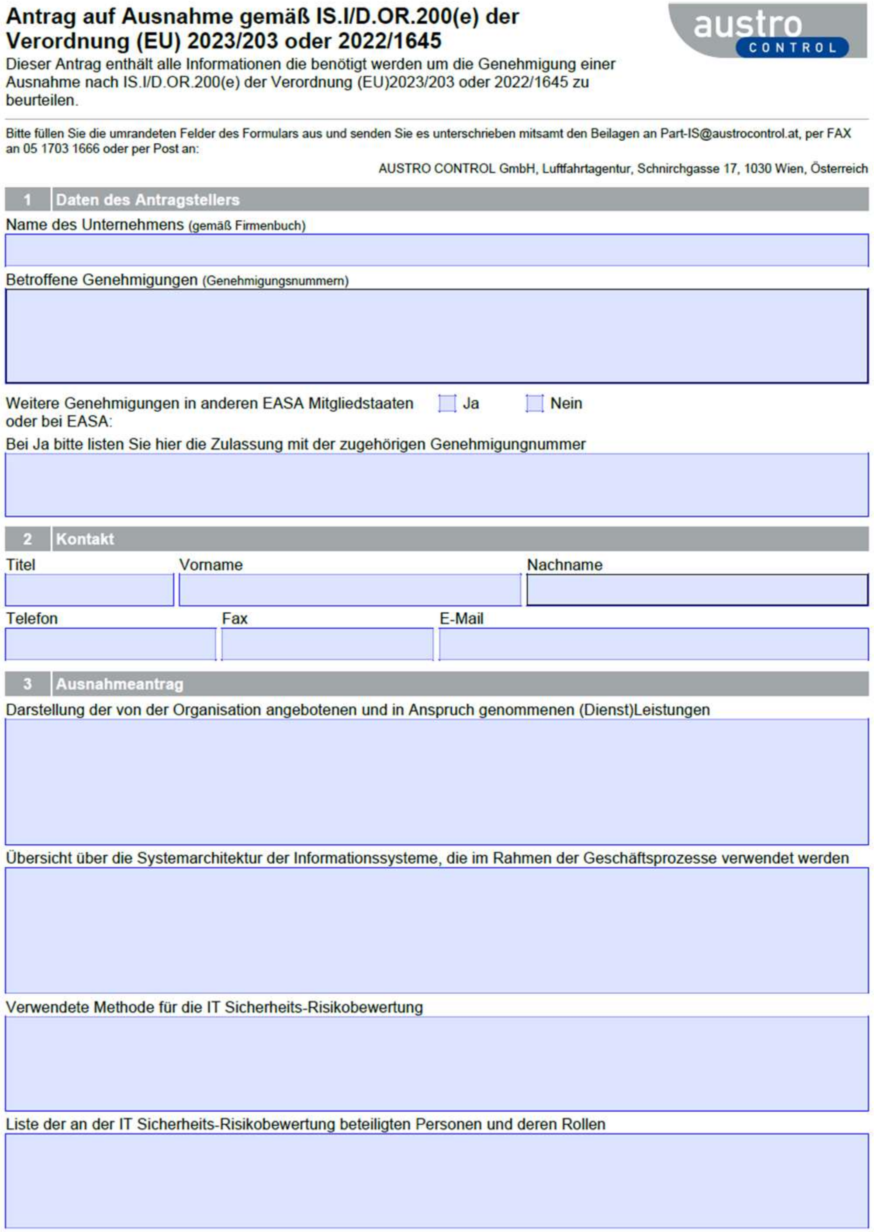
The objective is to obtain preliminary information about the organisations information security risk profile by using suitable means. (e.g. Questionnaire, Self-Assessment template, request form, etc.)

The objective is to conduct a pre evaluation before starting to detailed assessing the risk assessment.
Is the organisation able to achieve a granted exemption?

# Antragstellung

## Schritte zum Antrag

- *Internes Erst-Assessment ob die Kriterien erfüllt werden können (z. B. durch CMF)*
- *Antrag (FO_LFA_ALG_007) ausfüllen und versenden (**Part-IS@austrocontrol.at**).*
- *Falls seitens der ACG positiv bewertet:*
    - *vollständige Risikobewertung durchführen*
    - *Nachweise erbringen, wie die nicht zu derogierenden Anforderungen erfüllt werden (Notiz in Block 5)*
    - *Nachweis, dass das genehmigte Änderungsverfahren die Überwachung der Einhaltung der Derogationsbedingungen bei Änderungen abbildet.*



**Antrag auf Ausnahme gemäß IS.I/D.OR.200(e) der Verordnung (EU) 2023/203 oder 2022/1645**

Dieser Antrag enthält alle Informationen die benötigt werden um die Genehmigung einer Ausnahme nach IS.I/D.OR.200(e) der Verordnung (EU)2023/203 oder 2022/1645 zu beurteilen.

Bitte füllen Sie die umrandeten Felder des Formulars aus und senden Sie es unterschrieben mitsamt den Beilagen an Part-IS@austrocontrol.at, per FAX an 05 1703 1666 oder per Post an:

AUSTRO CONTROL GmbH, Luftfahrtagentur, Schnirchgasse 17, 1030 Wien, Österreich

**1 Daten des Antragstellers**

Name des Unternehmens (gemäß Firmenbuch)

Betroffene Genehmigungen (Genehmigungsnummern)

Weitere Genehmigungen in anderen EASA Mitgliedstaaten oder bei EASA: □ Ja □ Nein

Bei Ja bitte listen Sie hier die Zulassung mit der zugehörigen Genehmigungnummer

**2 Kontakt**

Titel Vorname Nachname

Telefon Fax E-Mail

**3 Ausnahmeantrag**

Darstellung der von der Organisation angebotenen und in Anspruch genommenen (Dienst)Leistungen

Übersicht über die Systemarchitektur der Informationssysteme, die im Rahmen der Geschäftsprozesse verwendet werden

Verwendete Methode für die IT Sicherheits-Risikobewertung

Liste der an der IT Sicherheits-Risikobewertung beteiligten Personen und deren Rollen

# Manual approval & Change management procedure

Part-IS-Café – 30.09.2025

## IS.I/D.OR.250 Information Security Management Manual (ISMM)

- **OR.250(a):** Provide the authority an ISMM and associated manuals/procedures with:
  - Statement by Acc.Manager or Head of Design that the organisation will always comply with Part-IS and the ISMM.
  - Titles, names, duties, accountabilities, responsibilities and authorities of:
    - Nominated person(s)
    - Compliance monitoring person(s)
    - Common Responsible Person, if applicable
    - Key persons for implementation of the ISMS
  - Organisational Chart with chains of accountability of persons mentioned above.
  - The Information Security Policy
  - Number and categories of staff, and the system to plan their availability
  - The description of the internal reporting scheme
  - **Procedures on how the organisation complies with part-IS**
  - Details of currently approved AltMoC’s

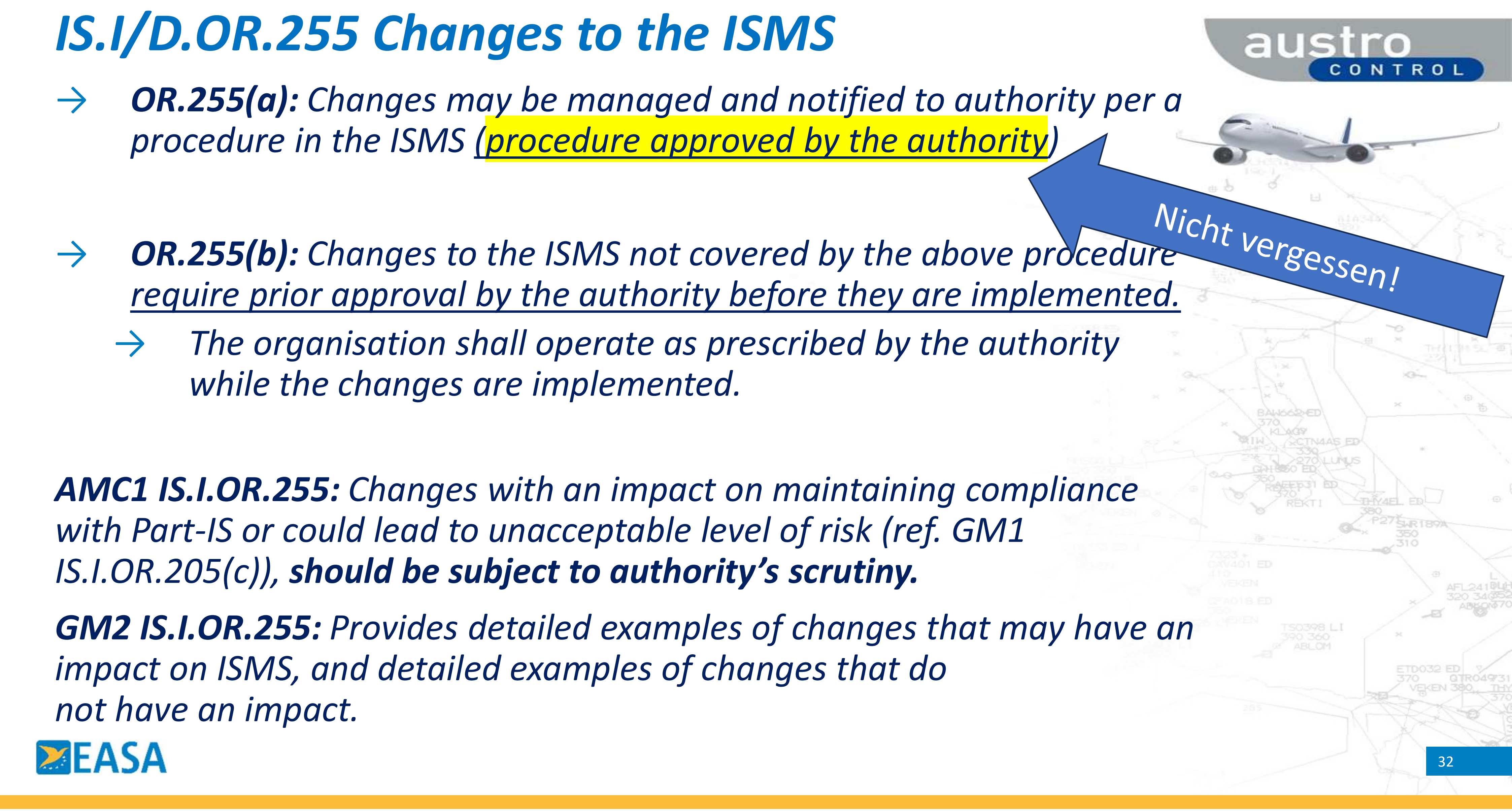
# *IS.I/D.OR.250 Information Security Management Manual (ISMM)*

- ***OR.250(b) and (c):***
  - *Initial issue of ISMM shall be approved and copy retained by authority*
  - *Amendments to the ISMM to be managed per a procedure established by the organisation. Otherwise, they shall be approved by the authority*
  - *Copy of any amendments to be provided to the authority*

- ***OR.250(d):** The ISMM may be integrated with other expositions or manuals (with clear cross-references about what portions correspond to the requirements of Part-IS)*

# IS.I/D.OR.250 Information Security Management Manual (ISMM) – upcoming Rule Change!

- **OR.250(b) and (c):**
  - *(b) The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority. An approval shall not be required for declared organisations. The ISMM shall be amended as necessary to remain an up-to-date description of the ISMS of the organisation. A copy of any amendments to the ISMM shall be provided to the competent authority.*
  - *Amendments to the ISMM shall be managed in a procedure established by the organisation. Any amendments that are not included within the scope of that procedure and any amendments related to the changes referred to in point IS.I.OR.255(b), shall be approved by the competent authority. An approval shall not be required for declared organisations.*



# *IS.I/D.OR.255 Changes to the ISMS*

- → ***OR.255(a):*** *Changes may be managed and notified to authority per a procedure in the ISMS (procedure approved by the authority)*

Nicht vergessen!

- → ***OR.255(b):*** *Changes to the ISMS not covered by the above procedure require prior approval by the authority before they are implemented.*
  - → *The organisation shall operate as prescribed by the authority while the changes are implemented.*

***AMC1 IS.I.OR.255:*** *Changes with an impact on maintaining compliance with Part-IS or could lead to unacceptable level of risk (ref. GM1 IS.I.OR.205(c)),* ***should be subject to authority's scrutiny.***

***GM2 IS.I.OR.255:*** *Provides detailed examples of changes that may have an impact on ISMS, and detailed examples of changes that do not have an impact.*

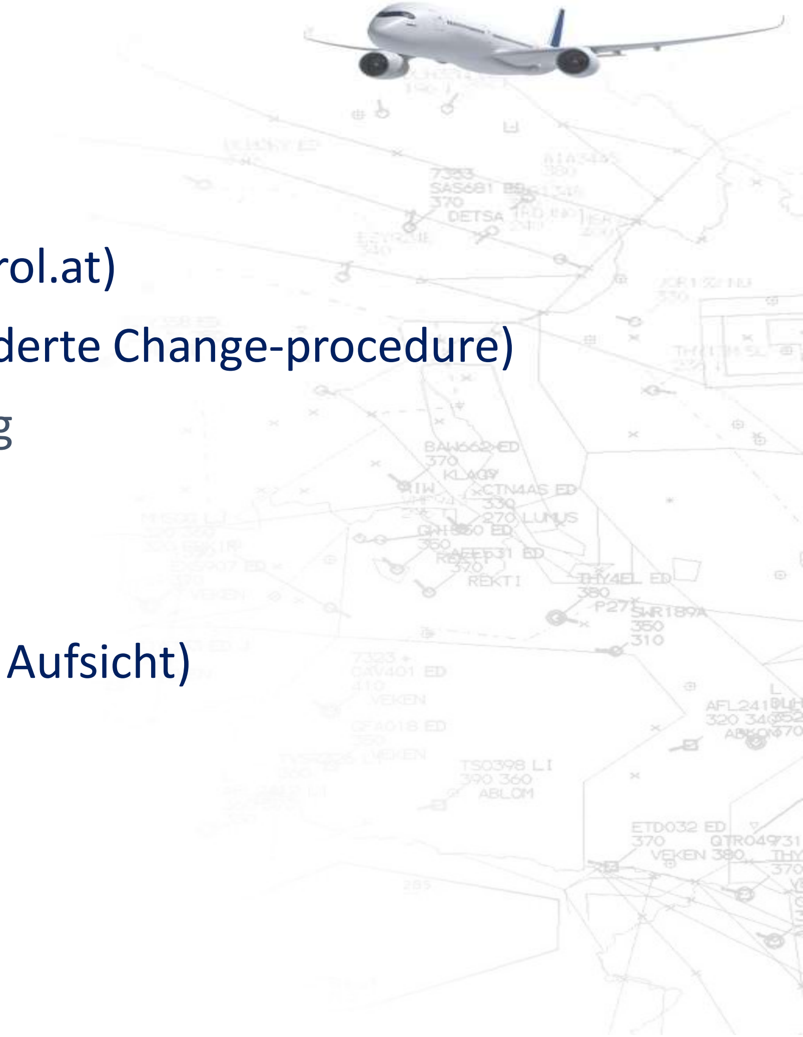
# IS.I/D.OR.255 Changes to the ISMS
# - upcoming Rule Change!

→ **OR.255(a):** *Changes to the ISMS may be managed and notified to the competent authority in a procedure developed by the organisation. That procedure shall be approved by the competent authority, except for declared organisations.*

→ **OR.255(b):** *With regard to changes to the ISMS not covered by the procedure referred to in point (a), the organisation shall apply for and obtain an approval issued by the competent authority, except for declared organisations, for which an approval is not required.*

**D. h. dass für „Declared Organisations“ Part-IS weiterhin anwendbar ist, es müssen Handbuch und Change-Procedure nicht mehr genehmigt sein!**

# Part IS



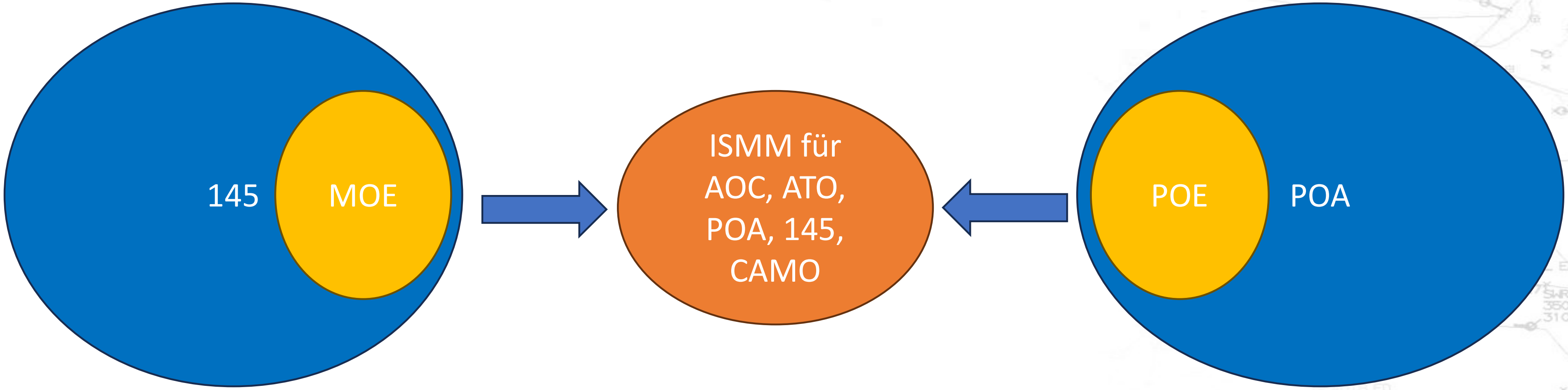
Wie leite ich die Genehmigung ein?

1. Antrag auf Genehmigung des ISMM (Part-IS@austrocontrol.at)
2. ISMS-Handbuch mit ggf. Beilagen übermitteln (z. B. geänderte Change-procedure)
3. Handbuch Review und Rückfragen bis genehmigungsfähig
4. Ausstellung der Handbuch Genehmigung
5. Umsetzung der Implementierung
6. Festlegen eines Audit Termins (im Rahmen der normalen Aufsicht)

# Informationen für Antragstellung

Variante 1: Die Übergreifende

Ein Antrag auf Genehmigung des ISMM für mehrere Zulassungen (Bedingung: gemeinsames Managementsystem) und Ausstellung eines einzigen Bescheides



Verrechnung: 1 x sonstige Änderung in Sinne des Antragstellers+ Zeit

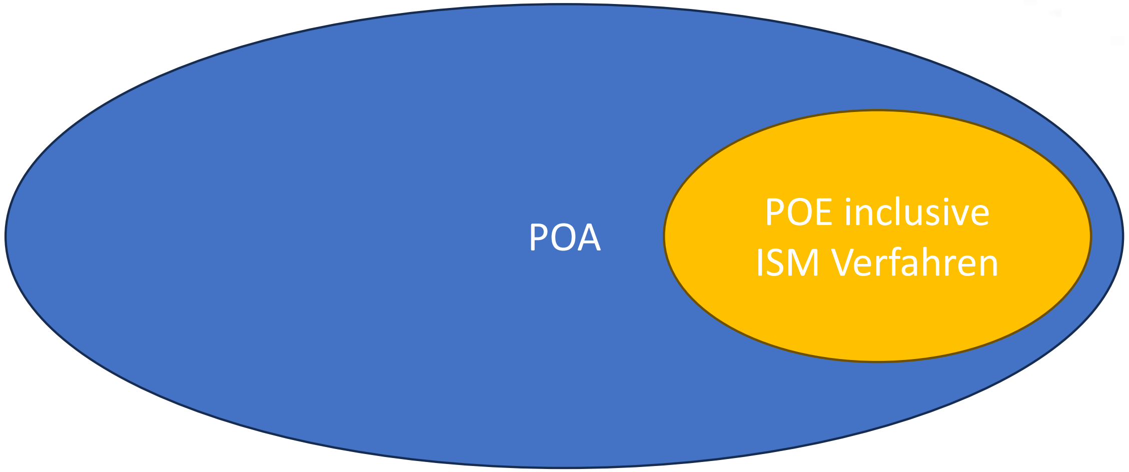
Genehmigung mit einem Bescheid für alle angeführten Zulassungen

# Informationen für Antragstellung

Variante 2: Die Einzelne

Ein Antrag für Änderung eines Handbuchs für eine Zulassung

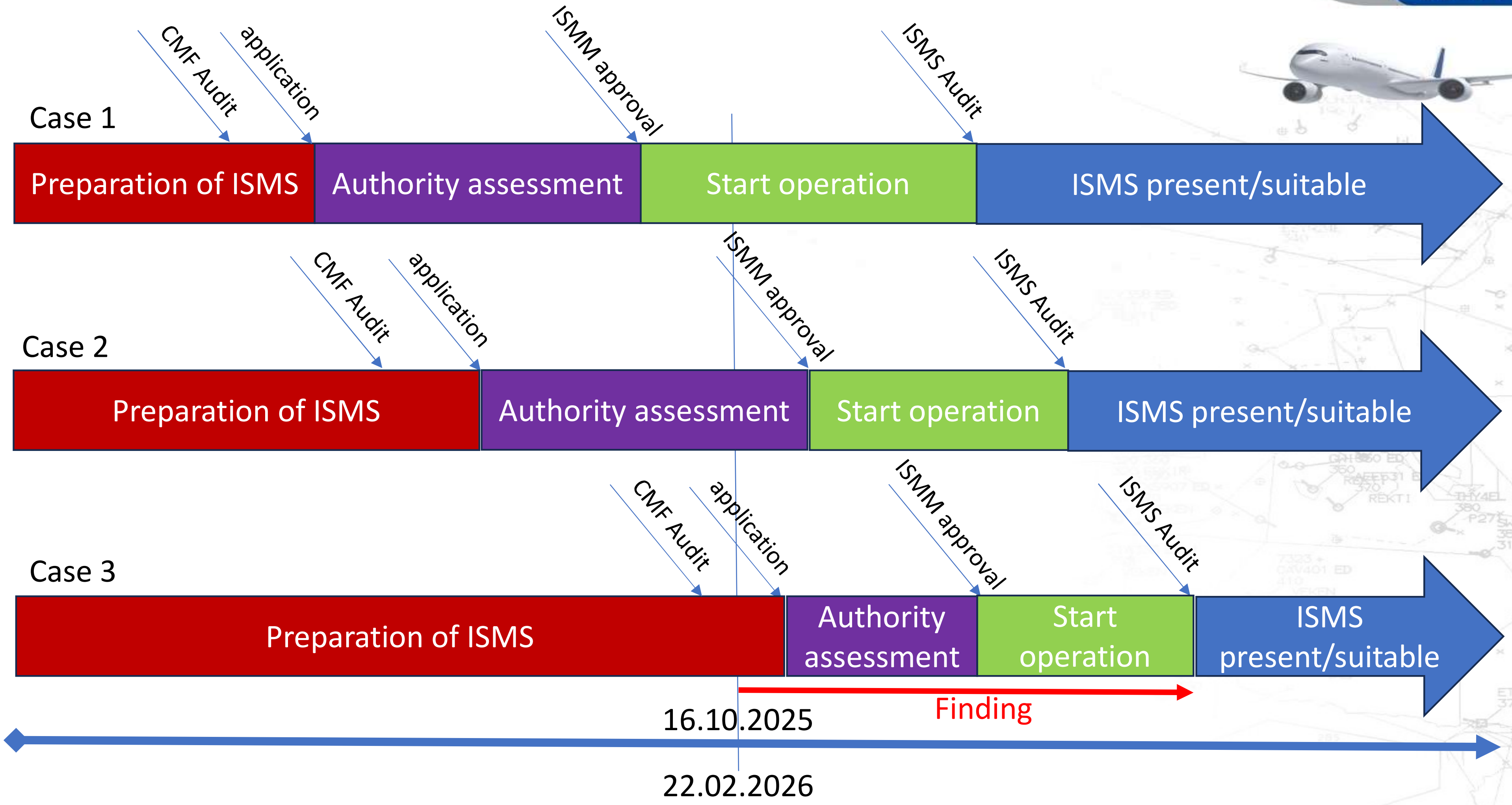
(Option: nur 1 Bescheid bei mehreren Anträgen)



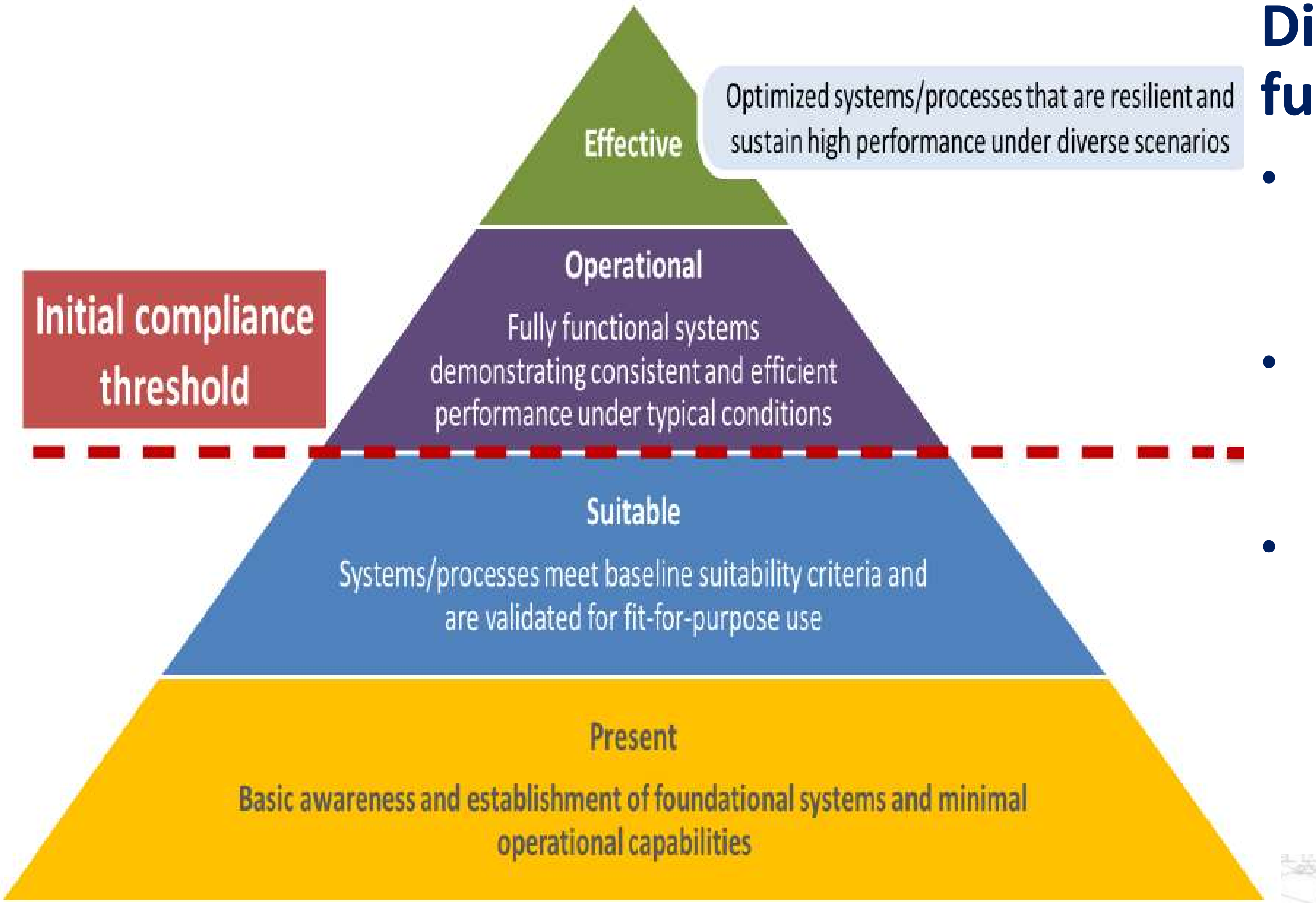
Verrechnung: Änderung der Zulassung + Zeit

Ein Unternehmen kann mehrere unabhängige Anträge stellen.

# Cases related to applicbility date



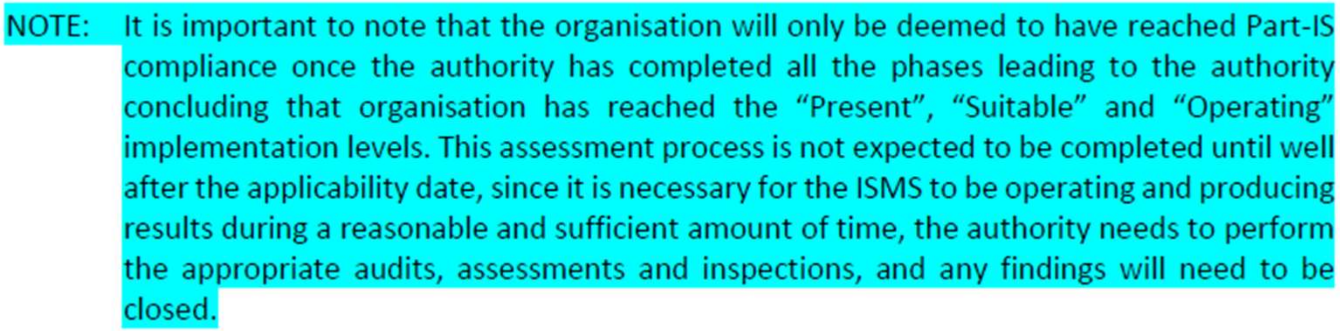
# How to show Compliance to Part-IS


Effective
Optimized systems/processes that are resilient and sustain high performance under diverse scenarios
Operational
Fully functional systems demonstrating consistent and efficient performance under typical conditions
Initial compliance threshold
Suitable
Systems/processes meet baseline suitability criteria and are validated for fit-for-purpose use
Present
Basic awareness and establishment of foundational systems and minimal operational capabilities

## Different needs for different functions

- The internal Compliance Monitoring Function needs to assess compliance also to Part-IS.
- Compliance to Part-IS needs to be shown to the authority to get the initial approval of the ISMM.
- The authority needs supporting tools to assess compliance during the approval process

# Actual amendments to GM „Part-IS oversight approach“



NOTE: It is important to note that the organisation will only be deemed to have reached Part-IS compliance once the authority has completed all the phases leading to the authority concluding that organisation has reached the “Present”, “Suitable” and “Operating” implementation levels. This assessment process is not expected to be completed until well after the applicability date, since it is necessary for the ISMS to be operating and producing results during a reasonable and sufficient amount of time, the authority needs to perform the appropriate audits, assessments and inspections, and any findings will need to be closed.

NOTE: the amended text is highlighted in turquoise.

Part-IS Implementation Task Force

Guidelines

Part-IS oversight approach

Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS[1]

Part-IS TF G-03 rev. 1

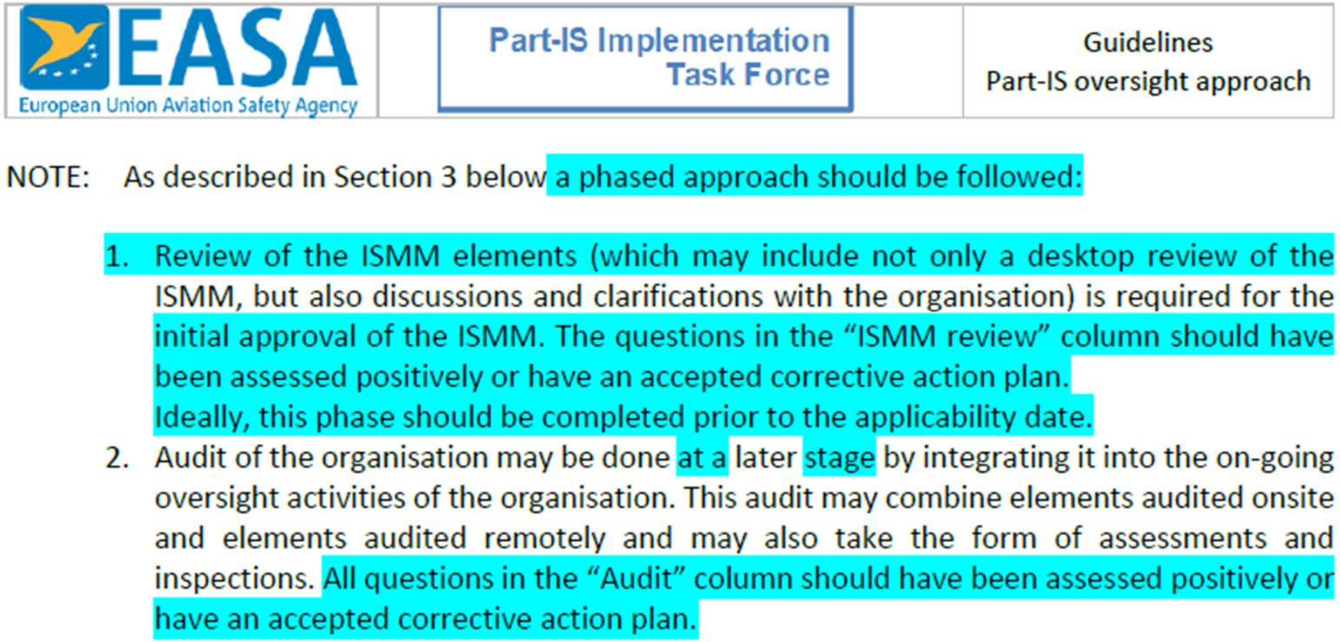
August 2025

“This document has been developed by the Part-IS Implementation Task Force, a collaborative effort of EASA States civil aviation authorities. The Task Force has worked with great care to produce a comprehensive set of guidelines aimed at ensuring a harmonised implementation of Part-IS across Member States. This initiative is part of the ongoing commitment to maintain high standards of aviation safety throughout the European Union.”

[1] A set of rules contained in Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 and in Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down requirements for the management of information security risks with a potential impact on aviation safety for aviation organisations and authorities across the entire aviation domain.

TE.GEN.00400-008 © European Union Aviation Safety Agency. All rights reserved. ISO9001 Certified. Proprietary document. Copies are not controlled. Confirm revision status through the EASA-Internet/Intranet.

Page 1 of 23

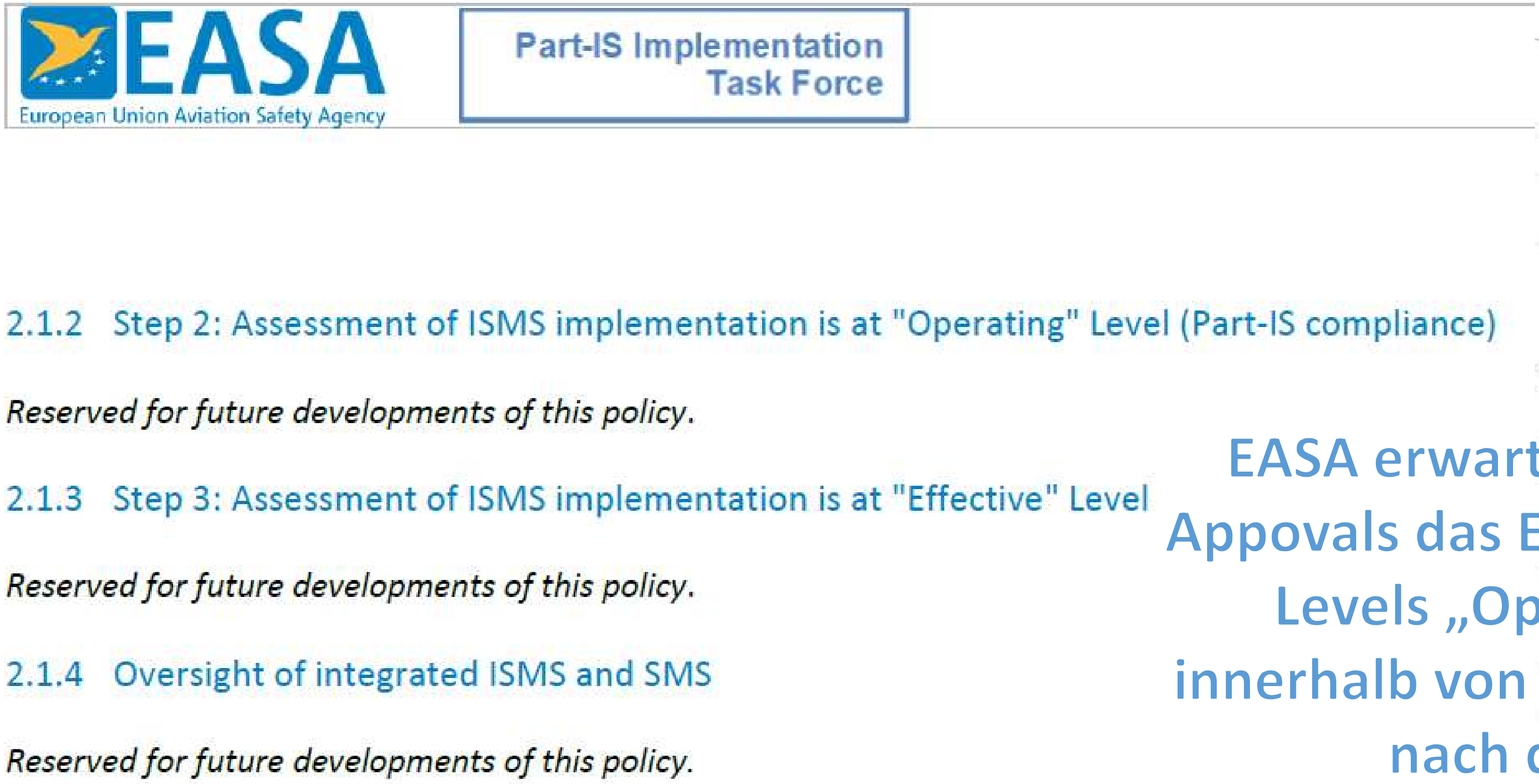


| EASA European Union Aviation Safety Agency | Part-IS Implementation Task Force | Guidelines<br>Part-IS oversight approach |
|---|---|---|

NOTE: As described in Section 3 below a phased approach should be followed:

1. Review of the ISMM elements (which may include not only a desktop review of the ISMM, but also discussions and clarifications with the organisation) is required for the initial approval of the ISMM. The questions in the “ISMM review” column should have been assessed positively or have an accepted corrective action plan.
   Ideally, this phase should be completed prior to the applicability date.
2. Audit of the organisation may be done at a later stage by integrating it into the on-going oversight activities of the organisation. This audit may combine elements audited onsite and elements audited remotely and may also take the form of assessments and inspections. All questions in the “Audit” column should have been assessed positively or have an accepted corrective action plan.

# Wie geht es weiter?



EASA European Union Aviation Safety Agency

Part-IS Implementation Task Force

### 2.1.2 Step 2: Assessment of ISMS implementation is at "Operating" Level (Part-IS compliance)

*Reserved for future developments of this policy.*

### 2.1.3 Step 3: Assessment of ISMS implementation is at "Effective" Level

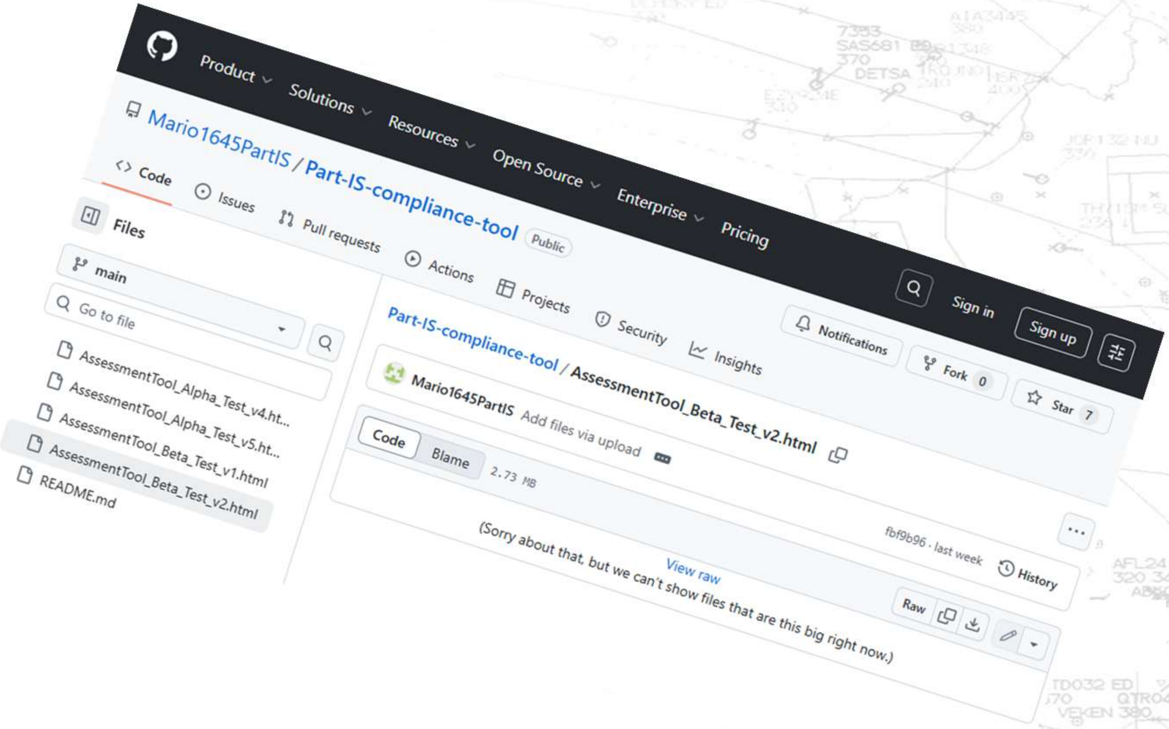
*Reserved for future developments of this policy.*

### 2.1.4 Oversight of integrated ISMS and SMS

*Reserved for future developments of this policy.*

EASA erwartet für ihre Appovals das Erreichen des Levels „Operating“ innerhalb von **18 Monaten** nach dem Anwendbarkeitsdatum

# Tools & Guidance



Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

Mario1645PartIS / Part-IS-compliance-tool Public

Notifications Fork 0 Star 7

Code Issues Pull requests Actions Projects Security Insights

Files

main

Go to file

AssessmentTool_Alpha_Test_v4.ht...

AssessmentTool_Alpha_Test_v5.ht...

AssessmentTool_Beta_Test_v1.html

AssessmentTool_Beta_Test_v2.html

README.md

Part-IS-compliance-tool / AssessmentTool_Beta_Test_v2.html

Mario1645PartIS Add files via upload

fbf9b96 · last week History

Code Blame 2.73 MB

Raw

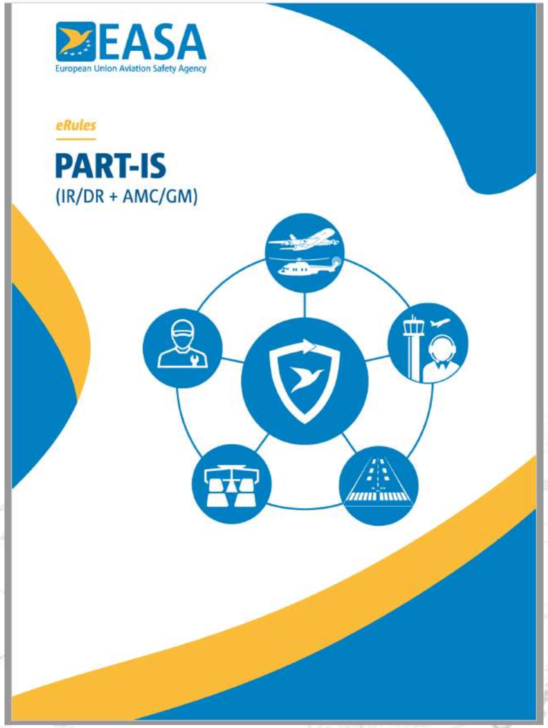
View raw

(Sorry about that, but we can't show files that are this big right now.)

Part-IS-Café – 29.07.2025

# How to support?

## Bring the rule and the assessment criteria together

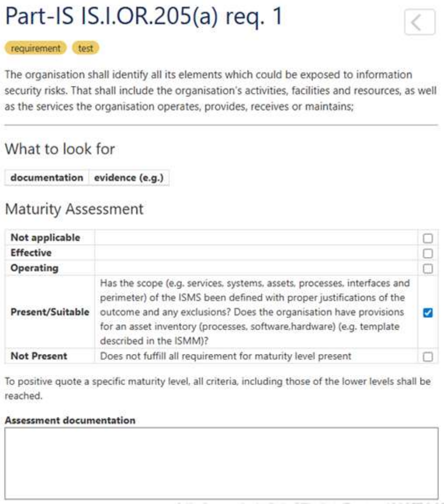

EASA

European Union Aviation Safety Agency

*eRules*

**PART-IS**

(IR/DR + AMC/GM)


Part-IS IS.I.OR.205(a) req. 1

The organisation shall identify all its elements which could be exposed to information security risks. That shall include the organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;

What to look for

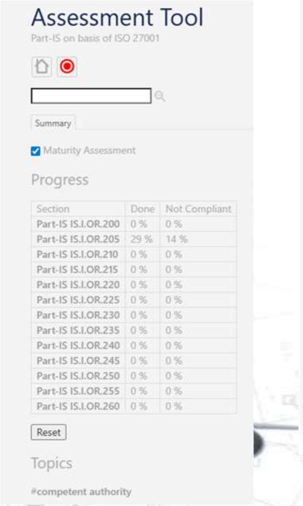
| documentation | evidence (e.g.) |
|---|---|

Maturity Assessment

| | | |
|---|---|---|
| **Not applicable** | | ☐ |
| **Effective** | | ☐ |
| **Operating** | | ☐ |
| **Present/Suitable** | Has the scope (e.g. services, systems, assets, processes, interfaces and perimeter) of the ISMS been defined with proper justifications of the outcome and any exclusions? Does the organisation have provisions for an asset inventory (processes, software,hardware) (e.g. template described in the ISMM)? | ☑ |
| **Not Present** | Does not fuffill all requirement for maturity level present | ☐ |

To positive quote a specific maturity level, all criteria, including those of the lower levels shall be reached.

**Assessment documentation**


Assessment Tool

Part-IS on basis of ISO 27001

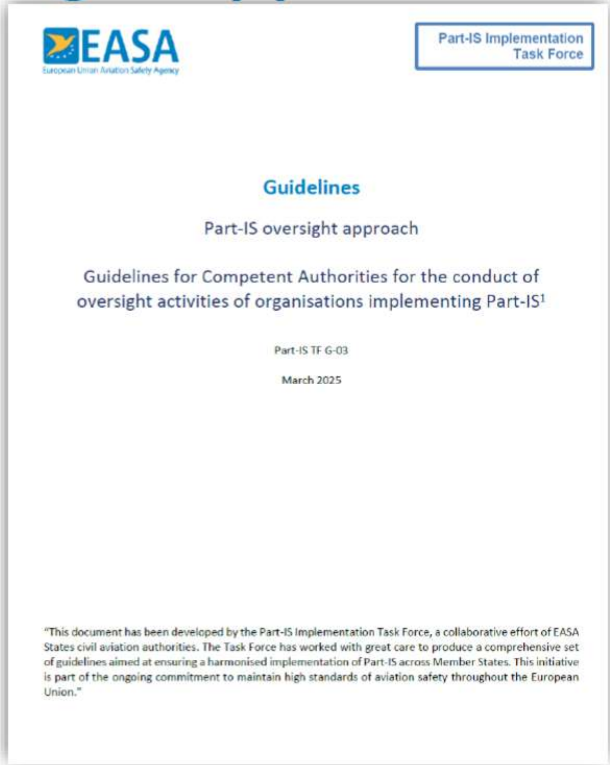
☑ Maturity Assessment

Progress

| Section | Done | Not Compliant |
|---|---|---|
| Part-IS IS.I.OR.200 | 0 % | 0 % |
| Part-IS IS.I.OR.205 | 29 % | 14 % |
| Part-IS IS.I.OR.210 | 0 % | 0 % |
| Part-IS IS.I.OR.215 | 0 % | 0 % |
| Part-IS IS.I.OR.220 | 0 % | 0 % |
| Part-IS IS.I.OR.225 | 0 % | 0 % |
| Part-IS IS.I.OR.230 | 0 % | 0 % |
| Part-IS IS.I.OR.235 | 0 % | 0 % |
| Part-IS IS.I.OR.240 | 0 % | 0 % |
| Part-IS IS.I.OR.245 | 0 % | 0 % |
| Part-IS IS.I.OR.250 | 0 % | 0 % |
| Part-IS IS.I.OR.255 | 0 % | 0 % |
| Part-IS IS.I.OR.260 | 0 % | 0 % |

Topics

#competent authority


EASA

European Union Aviation Safety Agency

Part-IS Implementation Task Force

**Guidelines**

Part-IS oversight approach

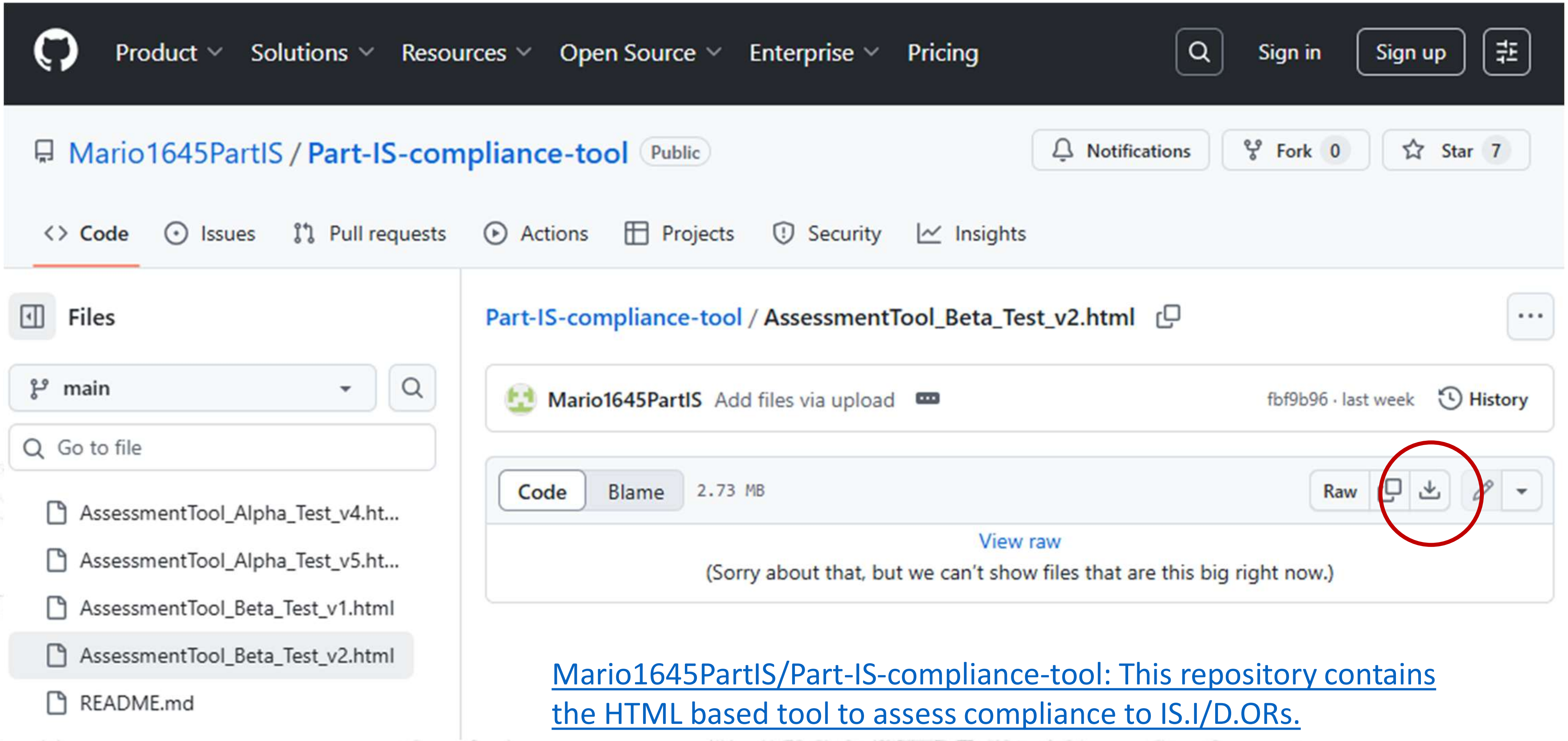
Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS[1]

Part-IS TF G-03

March 2025

"This document has been developed by the Part-IS Implementation Task Force, a collaborative effort of EASA States civil aviation authorities. The Task Force has worked with great care to produce a comprehensive set of guidelines aimed at ensuring a harmonised implementation of Part-IS across Member States. This initiative is part of the ongoing commitment to maintain high standards of aviation safety throughout the European Union."

# Where to get it?



Mario1645PartIS / Part-IS-compliance-tool Public

Part-IS-compliance-tool / AssessmentTool_Beta_Test_v2.html

Mario1645PartIS Add files via upload fbf9b96 · last week

2.73 MB

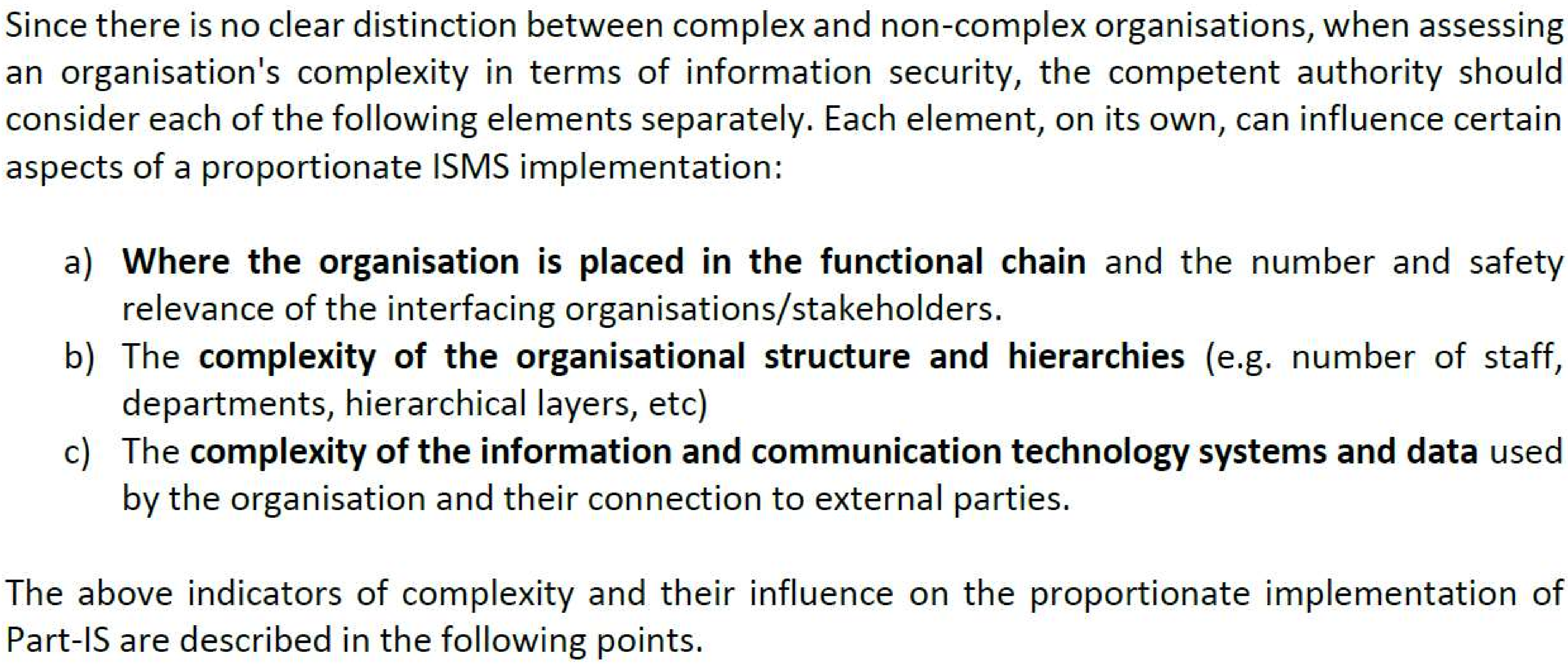
View raw

(Sorry about that, but we can't show files that are this big right now.)

- AssessmentTool_Alpha_Test_v4.ht...
- AssessmentTool_Alpha_Test_v5.ht...
- AssessmentTool_Beta_Test_v1.html
- AssessmentTool_Beta_Test_v2.html
- README.md

Mario1645PartIS/Part-IS-compliance-tool: This repository contains the HTML based tool to assess compliance to IS.I/D.ORs.

# Proportionality criteria –in the new GM

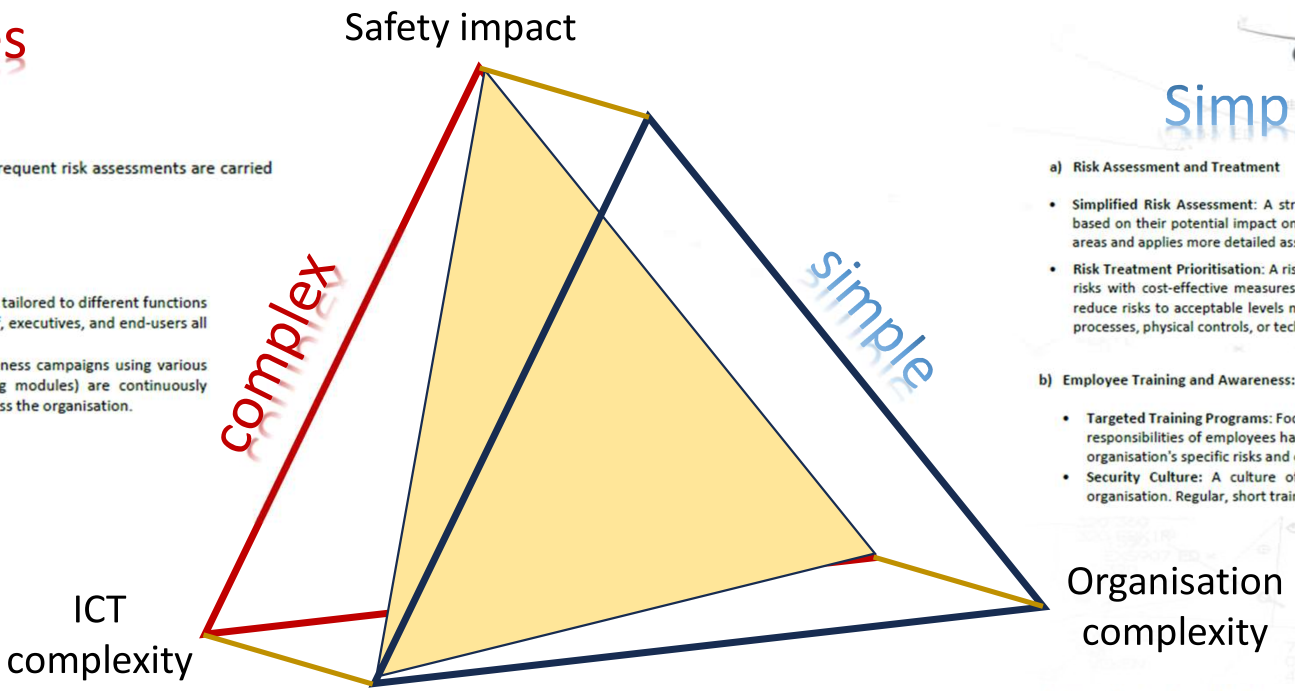


Since there is no clear distinction between complex and non-complex organisations, when assessing an organisation's complexity in terms of information security, the competent authority should consider each of the following elements separately. Each element, on its own, can influence certain aspects of a proportionate ISMS implementation:

a) **Where the organisation is placed in the functional chain** and the number and safety relevance of the interfacing organisations/stakeholders.
b) The **complexity of the organisational structure and hierarchies** (e.g. number of staff, departments, hierarchical layers, etc)
c) The **complexity of the information and communication technology systems and data** used by the organisation and their connection to external parties.

The above indicators of complexity and their influence on the proportionate implementation of Part-IS are described in the following points.

# Possible proportionality (self)-assessment of an organisation



## Complex - samples

a) Risk Assessment and Treatment

- **Detailed Risk Assessments:** Detailed and often more frequent risk assessments are carried out.

d) Comprehensive Training and Awareness Programs:

- **Role-Based Training**: Extensive role-based training programs tailored to different functions within the organisation is implemented. For example, IT staff, executives, and end-users all have different levels of training specific to their roles.
- **Continuous Security Awareness Campaigns**: Security awareness campaigns using various methods (e.g., phishing simulations, workshops, e-learning modules) are continuously deployed to keep security top-of-mind for all employees across the organisation.

a) Advanced Security Technologies

- **Integration of Advanced Security Tools**: Security technologies like Security Information and Event Management (SIEM), Data Loss Prevention (DLP), and Endpoint Detection and Response (EDR) systems should be utilised to help manage the scale and complexity of monitoring, detecting, and responding to security incidents across the organisation.
- **Automated Threat Intelligence**: Automated threat intelligence platforms should be implemented to enable real-time threat detection and response across the broad threat surface.

## Simple - samples

a) Risk Assessment and Treatment

- **Simplified Risk Assessment**: A streamlined risk assessment process that prioritises risks based on their potential impact on safety is used. The assessment focuses on high-impact areas and applies more detailed assessments only where and if necessary.
- **Risk Treatment Prioritisation**: A risk treatment plan that prioritises addressing high-impact risks with cost-effective measures is adopted. In such cases, cost-effective controls that reduce risks to acceptable levels may be used. These controls can often leverage existing processes, physical controls, or technology.

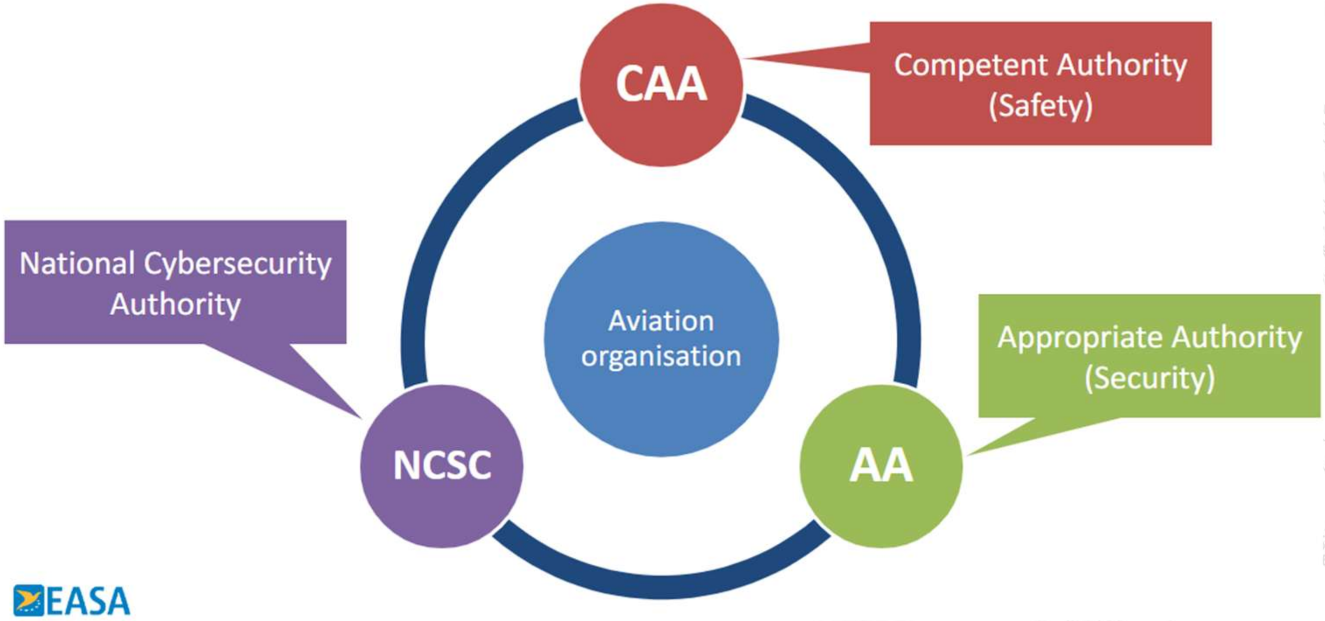
b) Employee Training and Awareness:

- **Targeted Training Programs**: Focused training programs that target the specific roles and responsibilities of employees has been provided. The training should be relevant to the organisation's specific risks and operational context.
- **Security Culture:** A culture of security awareness is encouraged throughout the organisation. Regular, short training sessions and awareness campaigns are conducted.

a) Use of Standards and Tools

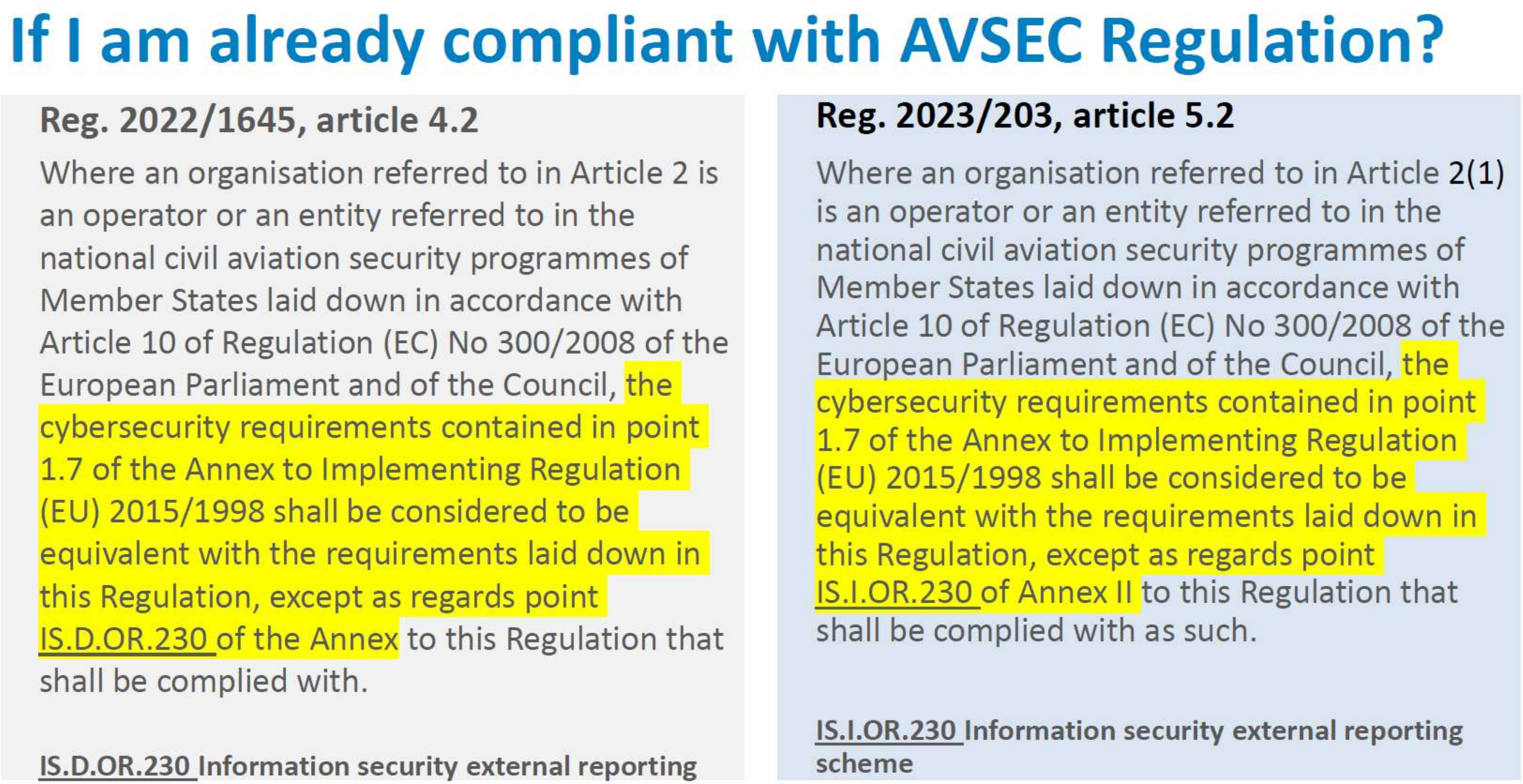
- **Leverage ISO/IEC 27001 Controls**: Usage of the ISO/IEC 27001 Annex A controls as a checklist to ensure all critical areas are covered while reducing the effort of designing controls from scratch. In such cases the Part-IS vs. ISO/IEC 27001 comparison guide shall be referenced to ensure that Part-IS specifics have been correctly addressed.
- **Simplified Incident Management:** A basic incident management process that allows for quick identification, reporting, and response to security incidents is adopted. Lessons learned from incidents should be anyhow integrated into the ISMS for continuous improvement.
- **Automated Tools**: Automated tools for monitoring, logging, and managing security incidents are used in order to reduce manual effort while maintaining continuous compliance.

# Part-IS interplay with other regulations


CAA
Competent Authority (Safety)
National Cybersecurity Authority
Aviation organisation
Appropriate Authority (Security)
NCSC
AA
EASA

Part-IS-Café – 30.09.2025

# AVSEC



## If I am already compliant with AVSEC Regulation?

**Reg. 2022/1645, article 4.2**

Where an organisation referred to in Article 2 is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 of the European Parliament and of the Council, the cybersecurity requirements contained in point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998 shall be considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.D.OR.230 of the Annex to this Regulation that shall be complied with.

**IS.D.OR.230 Information security external reporting**

**Reg. 2023/203, article 5.2**

Where an organisation referred to in Article 2(1) is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 of the European Parliament and of the Council, the cybersecurity requirements contained in point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998 shall be considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.I.OR.230 of Annex II to this Regulation that shall be complied with as such.

**IS.I.OR.230 Information security external reporting scheme**

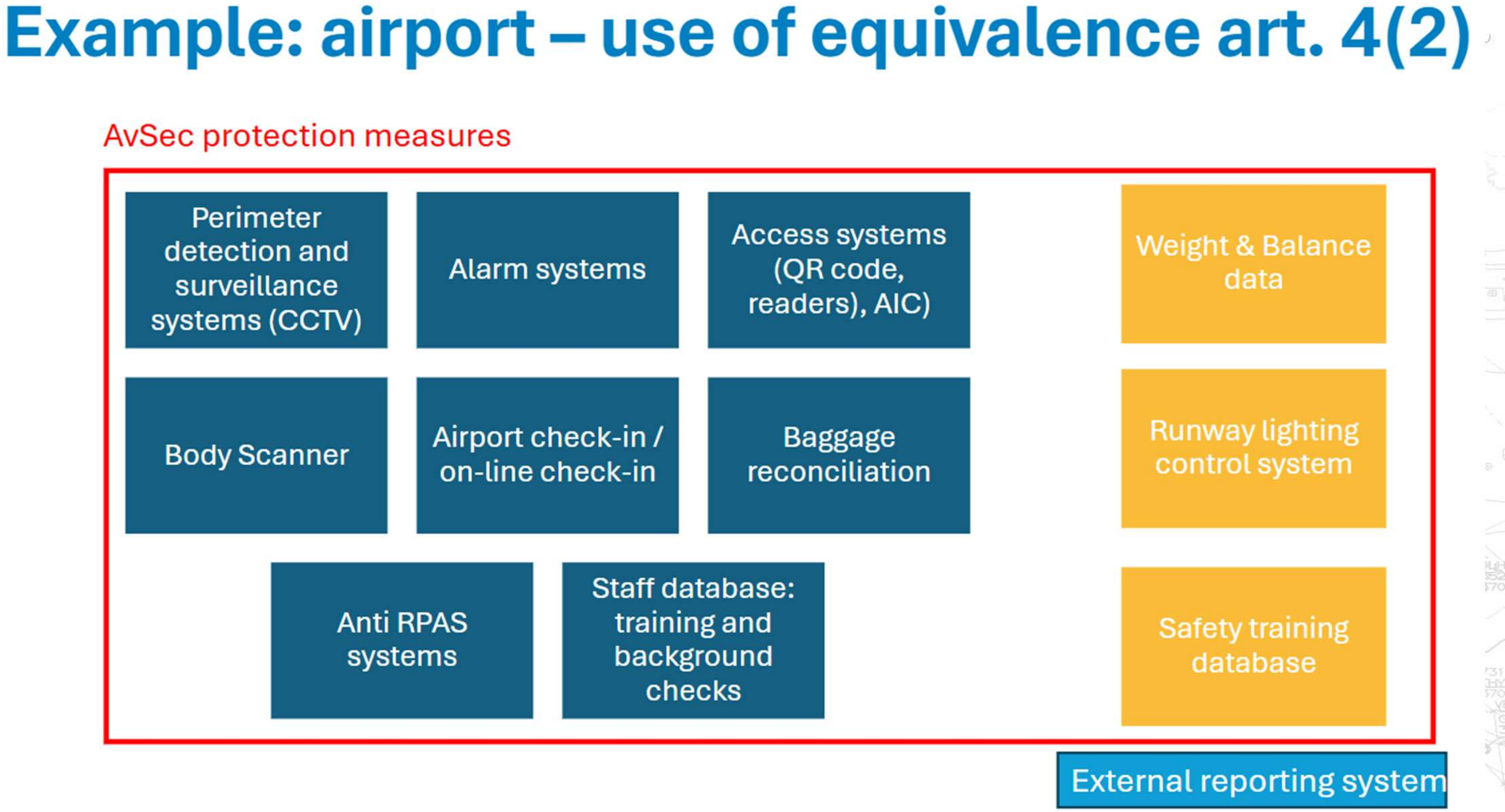
**Automatik? → AVSEC ersetzt Part-IS, aber wie?**

# Rahmenbedigungen – AVSEC

## GM1 Article 5(2) — Requirements arising from other Union legislation

Notwithstanding the equivalence between the provisions in Regulation (EU) 2023/203 and the cybersecurity requirements contained in point 1.7 of the Annex to Regulation (EU) 2015/1998, in order to ensure effective management of safety consequences by leveraging the requirements of Regulation (EU) 2015/1998, organisations need to consider the differences in the scope of the rules in terms of which elements are covered under the two different regulatory frameworks.

# AVSEC – latest development



## Example: airport – use of equivalence art. 4(2)

AvSec protection measures

- Perimeter detection and surveillance systems (CCTV)
- Alarm systems
- Access systems (QR code, readers), AIC)
- Body Scanner
- Airport check-in / on-line check-in
- Baggage reconciliation
- Anti RPAS systems
- Staff database: training and background checks
- Weight & Balance data
- Runway lighting control system
- Safety training database

External reporting system

# AVSEC – EASA FAQ

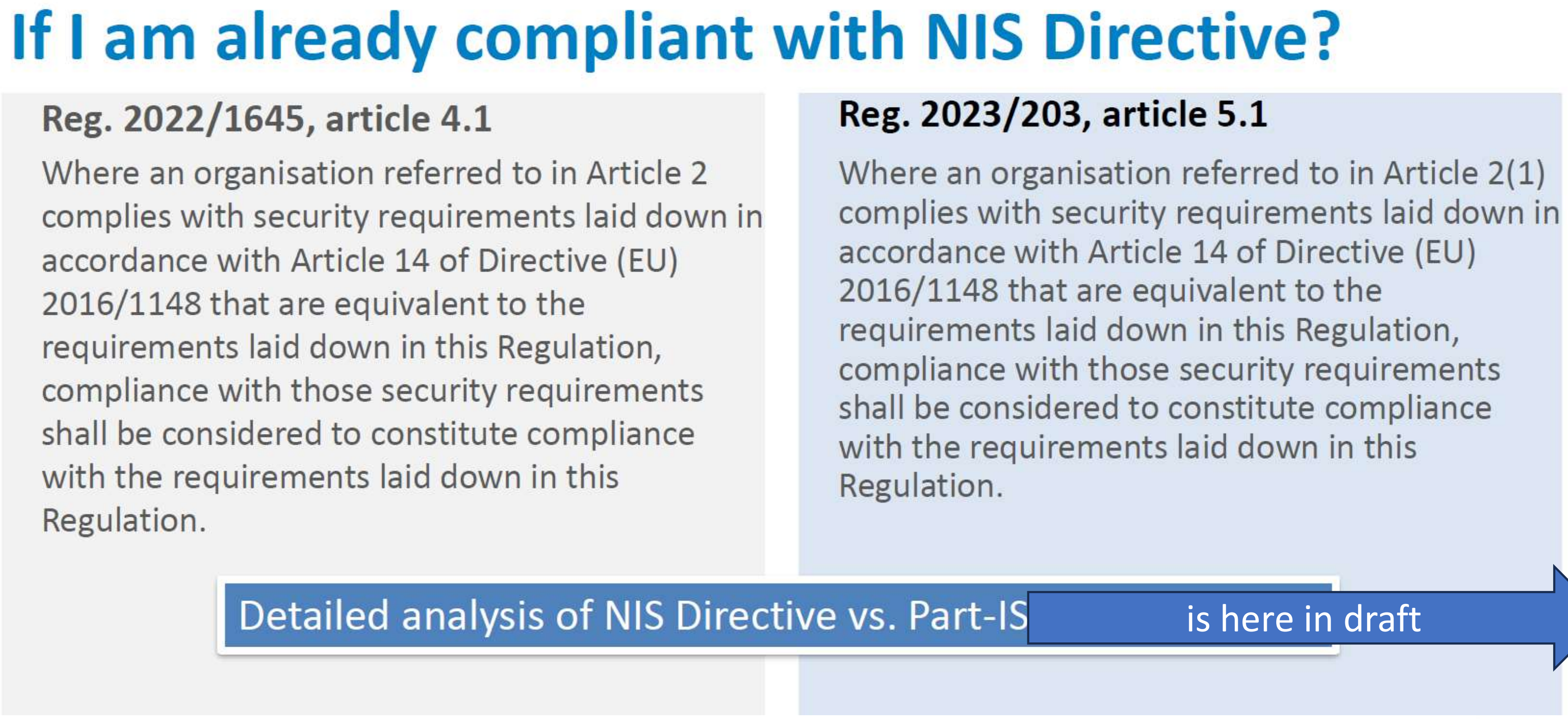
## In words of EASA ...

- **My organisation is an operator or entity referred to in the national civi programmes of Member States laid down in accordance with Article 10 of Reg , 2008 and complies with the cybersecurity requirements of point 1.7 of ementing Regulation (EU) 2015/1998. As a consequence, is the organisation ly compliant with Part-IS?**

- No, as required by Article 4(2) of Delegated R /1645 and Article 5(2) of Implementing Regulation (EU) 2023/20 those requirements, point IS.OR.230 needs to be complied with in order to ha with the requirements stemming from Part-IS. Compliance with Part-IS will b mpetent authority that is identified in Article 6 of the Implementing Regulatio e Delegated Regulation.

The limit is NOT the AOC approval! If CAMO a/o ATO are strongly integrated, the scope of the AVSEC program may be extended to other related approvals.

# NIS2



## If I am already compliant with NIS Directive?

**Reg. 2022/1645, article 4.1**

Where an organisation referred to in Article 2 complies with security requirements laid down in accordance with Article 14 of Directive (EU) 2016/1148 that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation.

**Reg. 2023/203, article 5.1**

Where an organisation referred to in Article 2(1) complies with security requirements laid down in accordance with Article 14 of Directive (EU) 2016/1148 that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation.

Detailed analysis of NIS Directive vs. Part-IS is here in draft

Mapping of EU cybersecurity rules applicable to the aviation sector

*Disclaimer:*

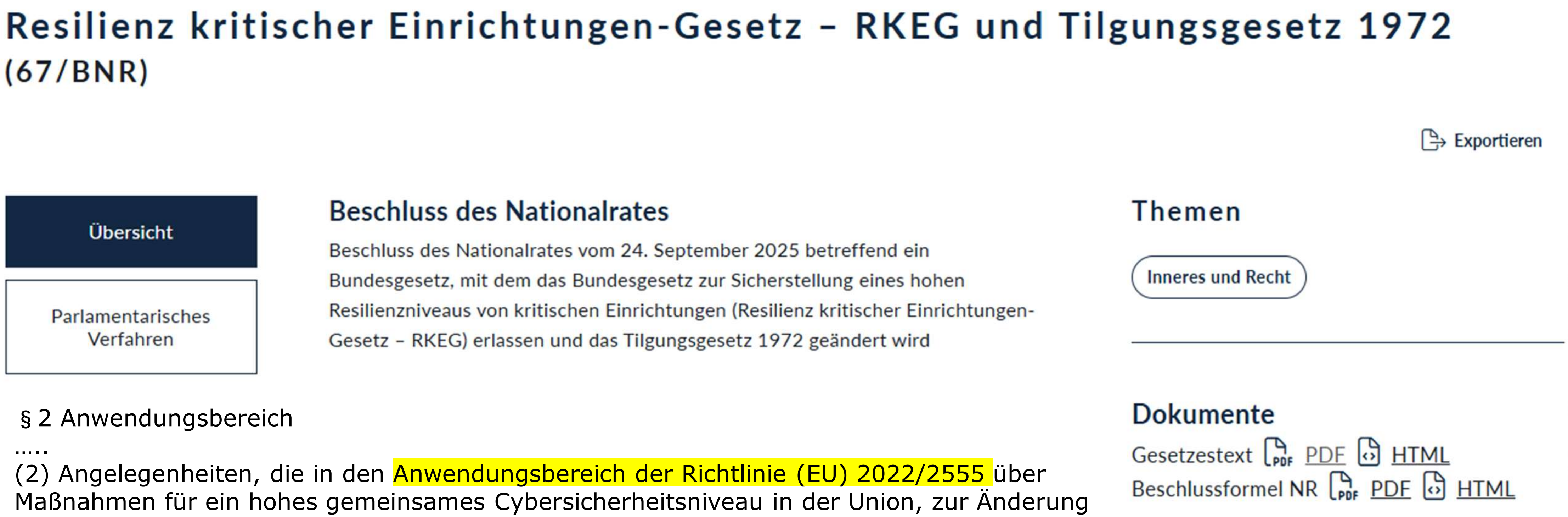
*This is a draft document, which is shared for feedback from stakeholders. It has not been discussed or agreed by the NIS Cooperation Group*

| | |
|---|---|
| Document Title: | Mapping of EU cybersecurity rules applicable to the aviation sector |
| Version: | Dv1 |
| Status: | Draft for consultation |
| Date: | 26/05/2025 |

NIS COOPERATION GROUP

**Workgroup between DG Move and DG Connect since September 2023.**

# Rahmenbedigungen – NIS-2 – RKEG



## Resilienz kritischer Einrichtungen-Gesetz – RKEG und Tilgungsgesetz 1972 (67/BNR)

Exportieren

### Beschluss des Nationalrates

Beschluss des Nationalrates vom 24. September 2025 betreffend ein Bundesgesetz, mit dem das Bundesgesetz zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz – RKEG) erlassen und das Tilgungsgesetz 1972 geändert wird

### Themen

Inneres und Recht

### Dokumente

Gesetzestext PDF HTML
Beschlussformel NR PDF HTML

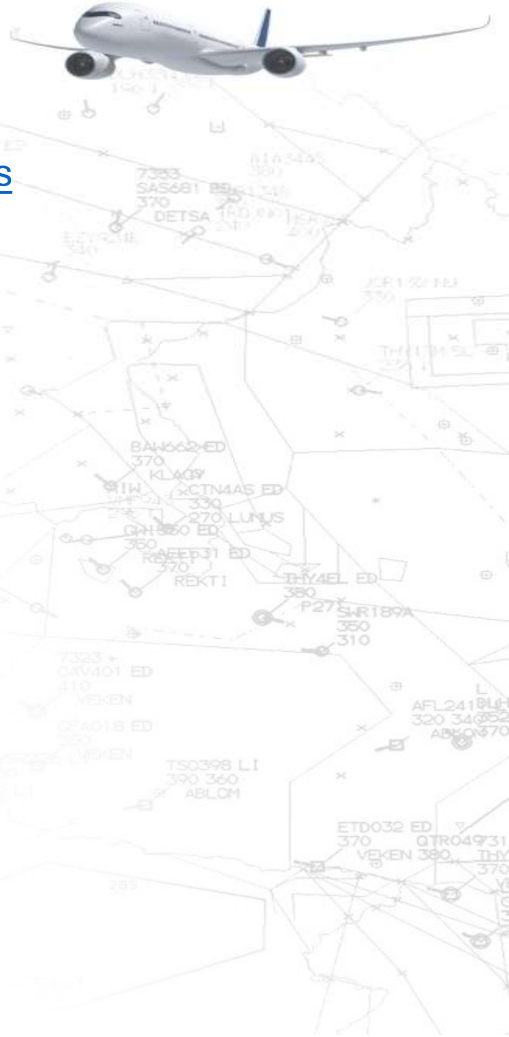
§ 2 Anwendungsbereich

…..

(2) Angelegenheiten, die in den Anwendungsbereich der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. Nr. L 333 vom 27.12.2022 S. 80, (im Folgenden: NIS-2-RL) fallen, bleiben von diesem Bundesgesetz unberührt.

**Achtung ! – RKEG is KEINE Umsetzung von NIS-2**

# Part IS



## IS Task Force Dokumente:

https://www.easa.europa.eu/community/topics/part-implementation-task-force-deliverables

EASA FAQ:

https://www.easa.europa.eu/en/the-agency/faqs/information-security-part

FOCA Info Page:

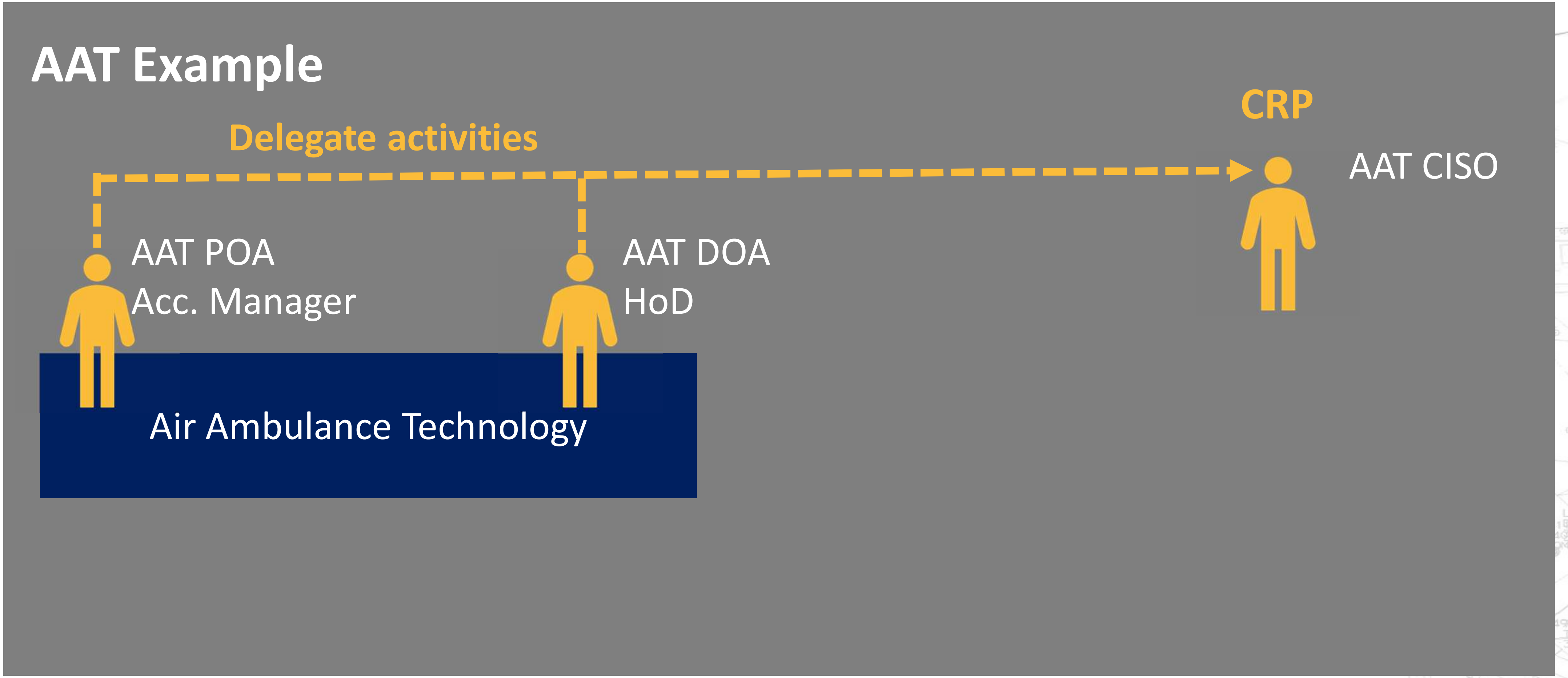
https://www.bazl.admin.ch/bazl/en/home/flugbetrieb/security-measures/cybersecurity/part-is.html

## ACG page:

Austro Control GmbH - Part-IS

# Fragen der Organisationen

# Example – CRP for POA & DOA



AAT Example

CRP

Delegate activities

AAT CISO

AAT POA
Acc. Manager

AAT DOA
HoD

Air Ambulance Technology