TLP White

Part IS Info Meeting

Part IS CAFE

Part-IS CAFE

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

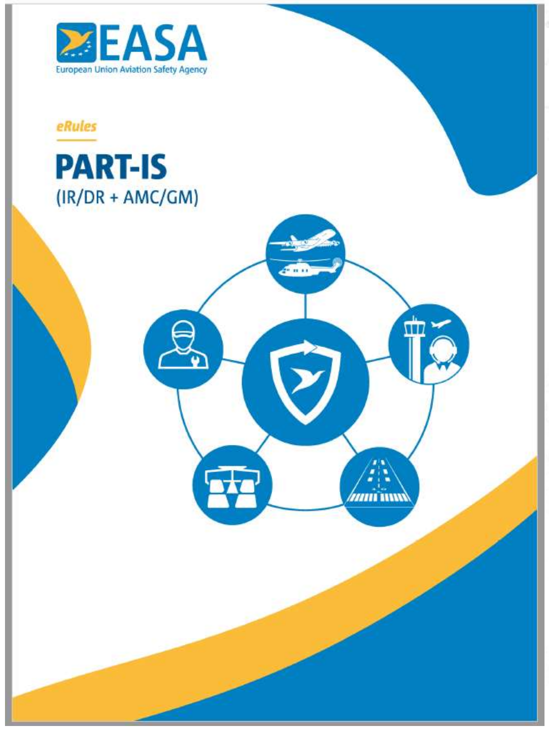
Ablauf:

- 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.

<u>Erklärung zum Set-Up:</u>
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



Part-IS-Café – 29.07.2025

Making EU aviation cyber resilient

Products

Cyber obejetives included in certification processes for all products

Aviation Organisations (People, Processes)

Part-IS regulatory package in force, applicable by 2026

Information Sharing - Collaborate to Reinforce the system

ECCSA to share knowledge

NoCA to analysis events

Capacity building & Research

For a competent and well aware workforce

To understand the future Threat Landscape

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; - **detect** information security events, identifying those which are considered information security incidents; and - **respond** to, and **recover** from, those information security incidents

Proportionate to the impact on aviation safety !!

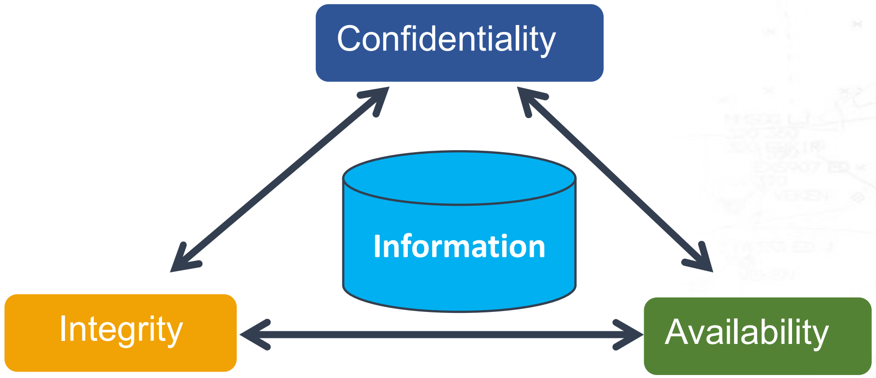
EASA

Jetzt geht es um Informationssicherheit !

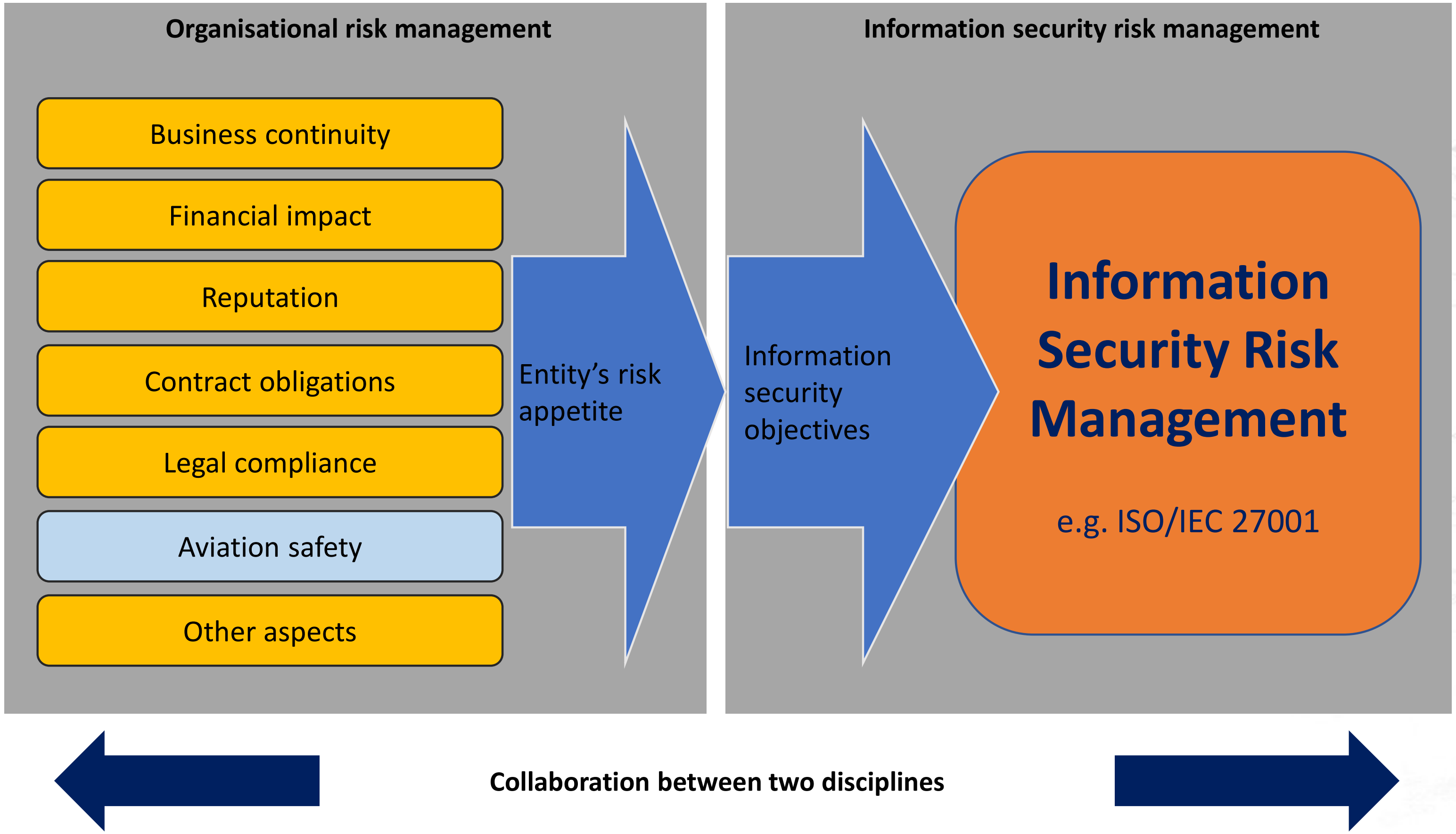
What is an ISMS ?

What is Information Security Management?

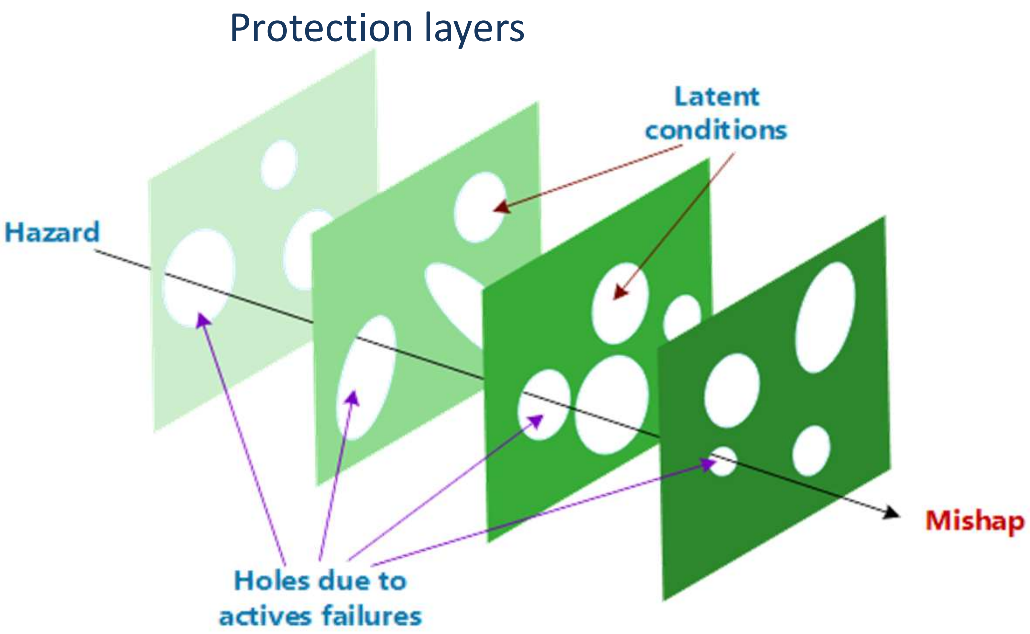
- ISO 27001 states that ***Information Security Management** is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their*
  - *Confidentiality,*
  - *Integrity, and*
  - *Availability.*

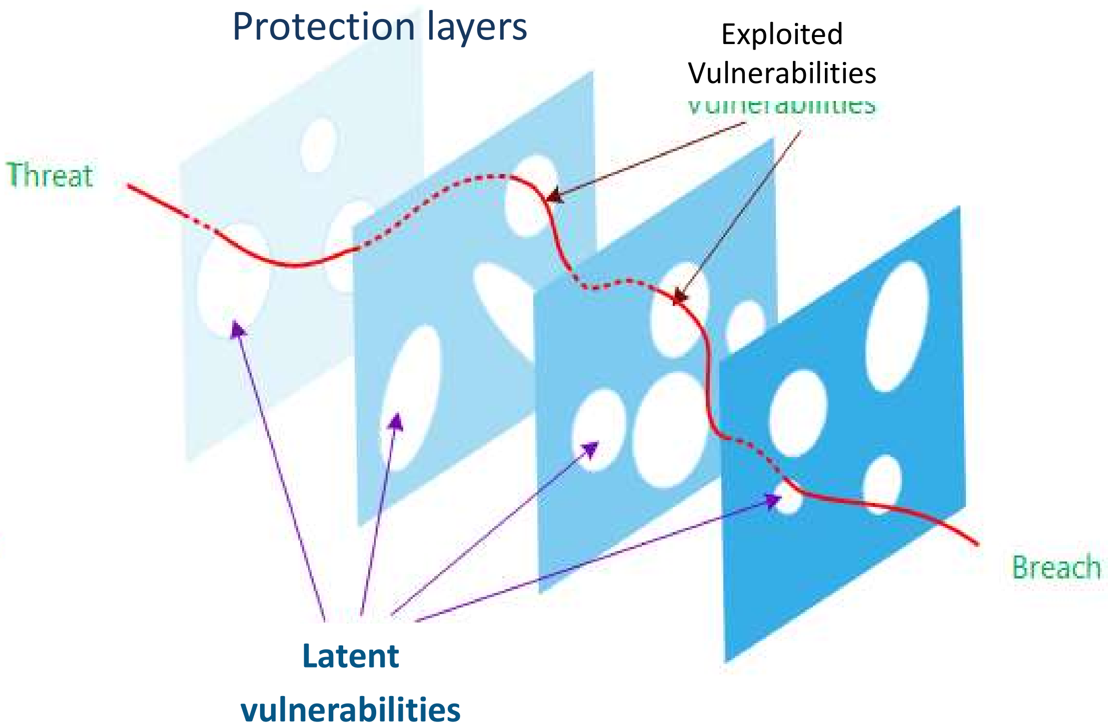


Safety is just one more Organisational Risk



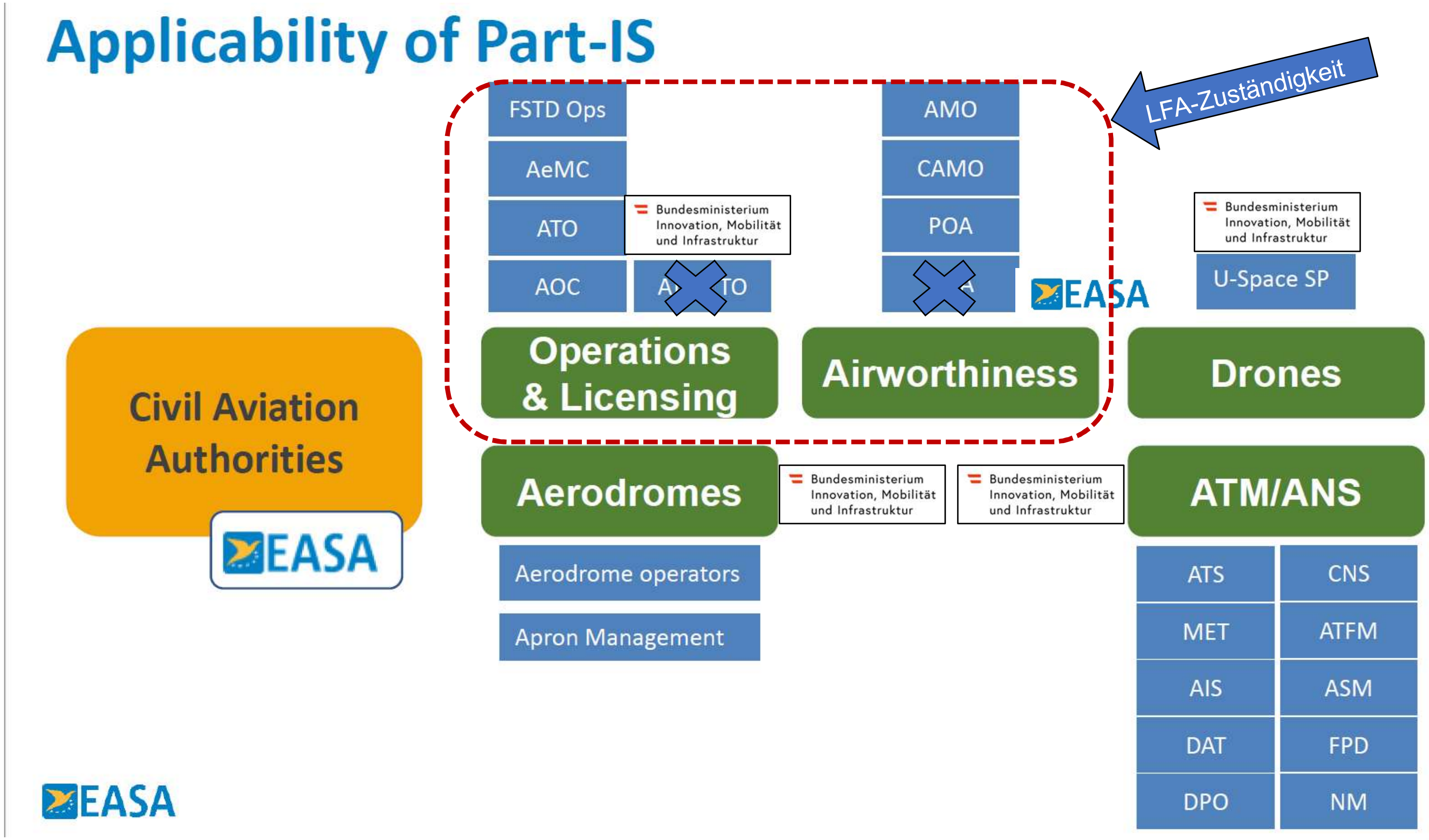
The cultural bias in aviation





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

Rahmenbedigungen – Anwendbarkeit



Part-IS ist die erste „cross-domain" IR

Applicability

Part IS is not applicable to:

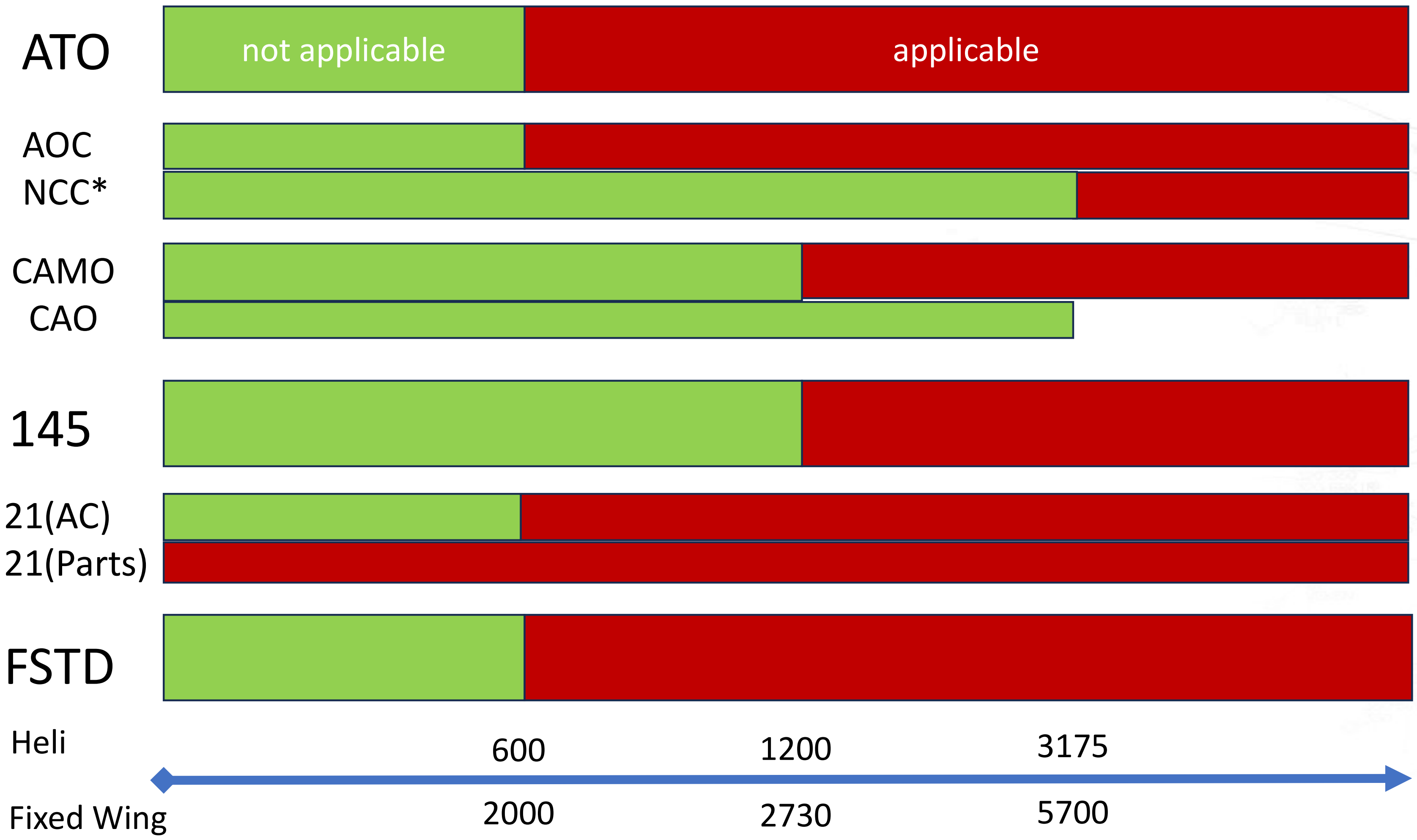
Production organisations not holding an approval	Part-147 maintenance training organisations.	ATOs providing only theoretical training.
Private operators of other than complex motor-powered aircraft.	Organisations dealing only with light aircraft: •e.g. airplanes below 2000 kg MTOM, very light rotorcraft, 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

NCC & SPO are applicable

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

Confusion by „different cetegories"

Applicability – based on MTOW



* plus special exmptions for specific operations

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

Part-IS-Café – 29.07.2025

Derogation IS.OR.200(e)

Unbeschadet der Meldepflichten gemäß der Verordnung (EU) Nr. 376/2014 des Europäischen Parlaments und des Rates und der Anforderungen von Punkt IS.I/D.OR.200(a)(13) ***kann die zuständige Behörde der Organisation die Genehmigung erteilen****, die unter den Buchstaben a bis d genannten und die diesbezüglichen in den Punkten IS.I/D.OR.205 bis IS.I/D.OR.260 enthaltenen Anforderungen* ***nicht umzusetzen****, wenn diese* ***zur Zufriedenheit der Behörde nachweist****, dass ihre Tätigkeiten, Einrichtungen und Ressourcen sowie die von ihr betriebenen,* ***angebotenen, erhaltenen und aufrechterhaltenen Dienste keine Informations-sicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit weder für ihre eigene noch für andere Organisationen darstellen****.* *Voraussetzung für die Genehmigung ist eine dokumentierte Bewertung des Informationssicherheitsrisikos, die von der Organisation oder einem Dritten nach Punkt IS.D.OR.205 durchgeführt und von ihrer zuständigen Behörde überprüft und genehmigt wurde.*

Die Aufrechterhaltung der Gültigkeit dieser Genehmigung wird von der zuständigen Behörde nach dem geltenden Auditzyklus für die Aufsicht und immer dann überprüft, wenn Änderungen im Tätigkeitsumfang der Organisation vorgenommen werden.

Adobe Acrobat Document

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 toimplement 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)

Guideline from July 2024

Key objectives for the development

- harmonise the process for organisations to apply for derogations and their assessment and approval by Competent Authorities in all Member States, while ensuring continuous monitoring to maintain the validity of the supporting evidence
- The assessment criteria include the organisation's exposure to the aviation landscape, safety contribution and processes
- Already established risk assessment methodology as a mandatory part of the SMS of the organisation should be used to address information security risks

The updated GM of Part-IS is now published | EASA community

EASA
European Union Aviation Safety Agency

Part-IS Implementation Task Force

Guidelines

Implementation guidelines for Part-IS* - IS.I/D.OR.200 (e)

Part-IS TF G-02

July 2024

"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."

* 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.

Page 1 of 11

How the process works

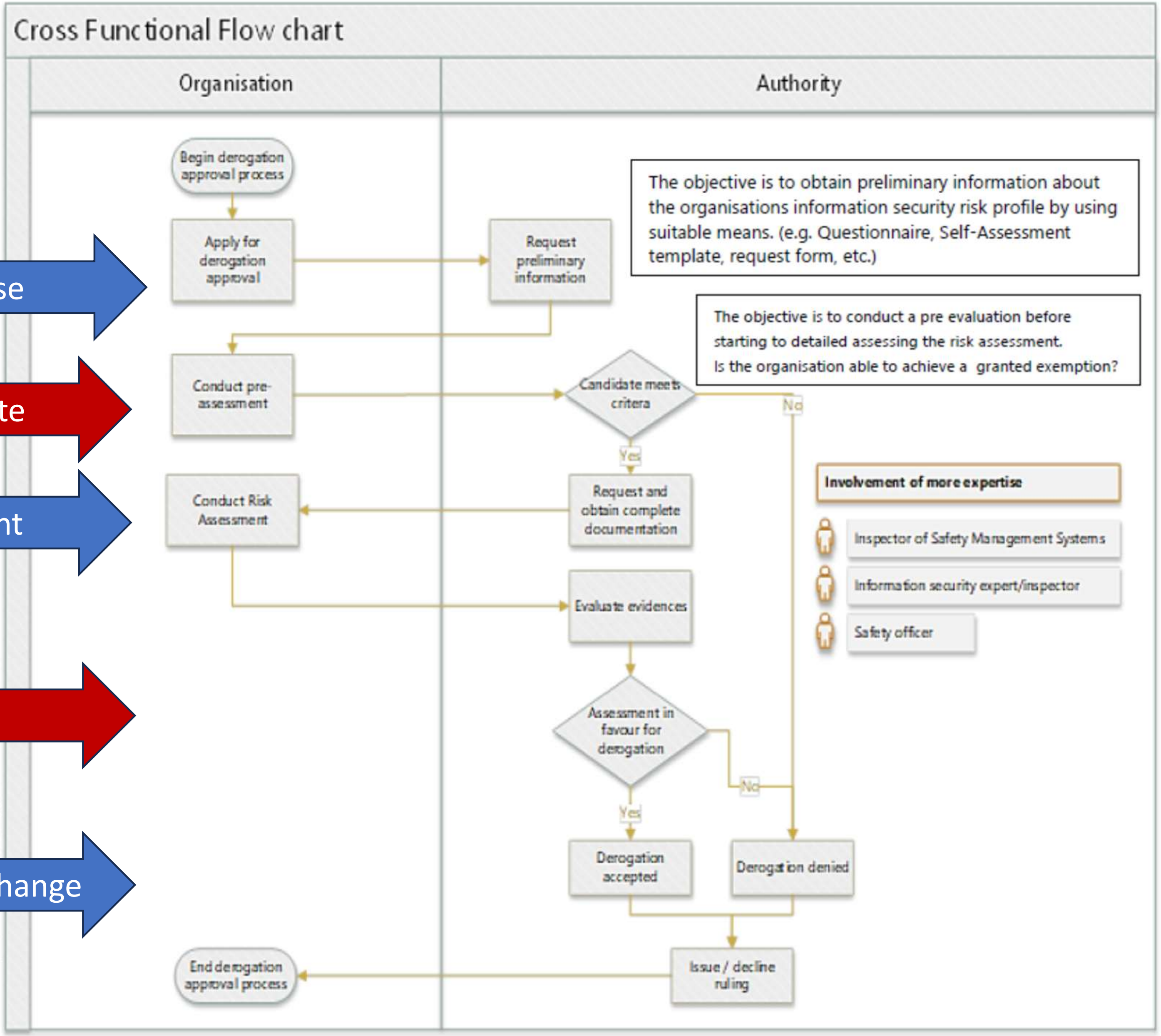
Pre-assessement phase

Authority accepts applicant as canditate

Detailed Risk Assessment

Authority decides on derogation

Re-assessment required for each change



Herausforderungen - Changes

Scope – Änderungen, Änderungen von LFZ

- *Bei jeder Änderung des Scopes ist zu prüfen, ob die Anwendbarkeit (weiter) gegeben ist.*
- *Änderungen, die eine neue Anwendbarkeit nach sich ziehen* ***sind erst dann zu genehmigen****, sobald die* ***Compliance zu Part-IS nachgewiesen*** *ist.*
- *Jede Scope-Änderung muss ein Update des verpflichtenden IS-Risk-Assessments beinhalten und durch den Inspektor geprüft werden.*

Änderungen im Falle einer Derogation (IS.OR.200(e))

- *Bei jeder Änderung ist durch die Organisation mittels IS-Risk-Assessment nachzuweisen, dass die Bedingungen für die Derogation weiter bestehen.*
- *Das genehmigte Verfahren zur „changes without prior approval" muss eine Eigenbewertung des IS-Risk-Assessments beinhalten. Diese ist verpflichtend mit dem Change an die Behörde zu senden ➔ Prüfung durch die Behörde.*

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

GM1 IS.I/D.OR.200(e)

Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for a derogation by the competent authority

Some examples of organisations that may consider asking for a derogation might include:

- An air operator that performs non-high-risk commercial specialised operations (SPO) with non-complex aircraft, if the nature of the operations justifies the grounds for a derogation.
- An air operator that operates ELA2 aircraft as defined in Article 1(2)(j) of Regulation (EU) No 748/2012 with the exception of one aircraft that is operated in predefined operational conditions or under certain operational limitations.
- A maintenance organisation approved under Part-145 dealing only with maintenance of components or maintenance activities that do not contribute to ensuring the structural integrity of the aircraft nor any major safety-related functionalities — for instance, undertaking activities such as washing, removing coatings, painting, etc.

AMC1 IS.I/D.OR.200(e)

Organisations should follow AMC1 IS.I/D.OR.205(a) and AMC1 IS.I/D.OR.205(b) to perform the required information security risk assessment to seek the approval of the derogation. is deemed satisfactory for a derogation to be granted.

Organisations that would like to have the risk assessment performed by a third party should consider the requirements for contracting information security management activities (IS.I/D.OR.235)

Derogation IS.OR.200 (e) how to

Wo wäre es wahrscheinlich, dass eine Derogation Erfolg hat ?

- *AtoB operator, die alle sonstigen Kriterien für die Nichtanwendbarkeit nach Art. 2 (c) (ii) fallen.*
- *SPO operator (non high risk), die alle sonstigen Kriterien für die Nichtanwendbarkeit nach Art. 2 (c) (ii)+(iii) fallen.*
- *POA für Parts und Components, ohne Einfluss auf die Luftfahrzeugstruktur oder sicherheitsrelevante Funktion (z. B. Aufkleber, Stoffe, einfaches Interior) <- Achtung" „Cabin Safety"*
- *Wartungsbetrieb für Parts und Components, ohne Einfluss auf die Luftfahrzeugstruktur oder sicherheitsrelevante Funktion (z. B. einfaches Interior, Reinigung, einfaches Equipment)*
- *Operator oder ATO, die einzelne „non ELA2-aircraft" betreiben, wenn Risiko mit ELA2 äquivalent. (DA52 vs. DA62)*
- *Wartungsbetriebe oder CAMOs, die einzelne „non ELA2-aircraft" im Scope haben, die „nahe" an ELA2 sind. (DA52 vs. DA62)*

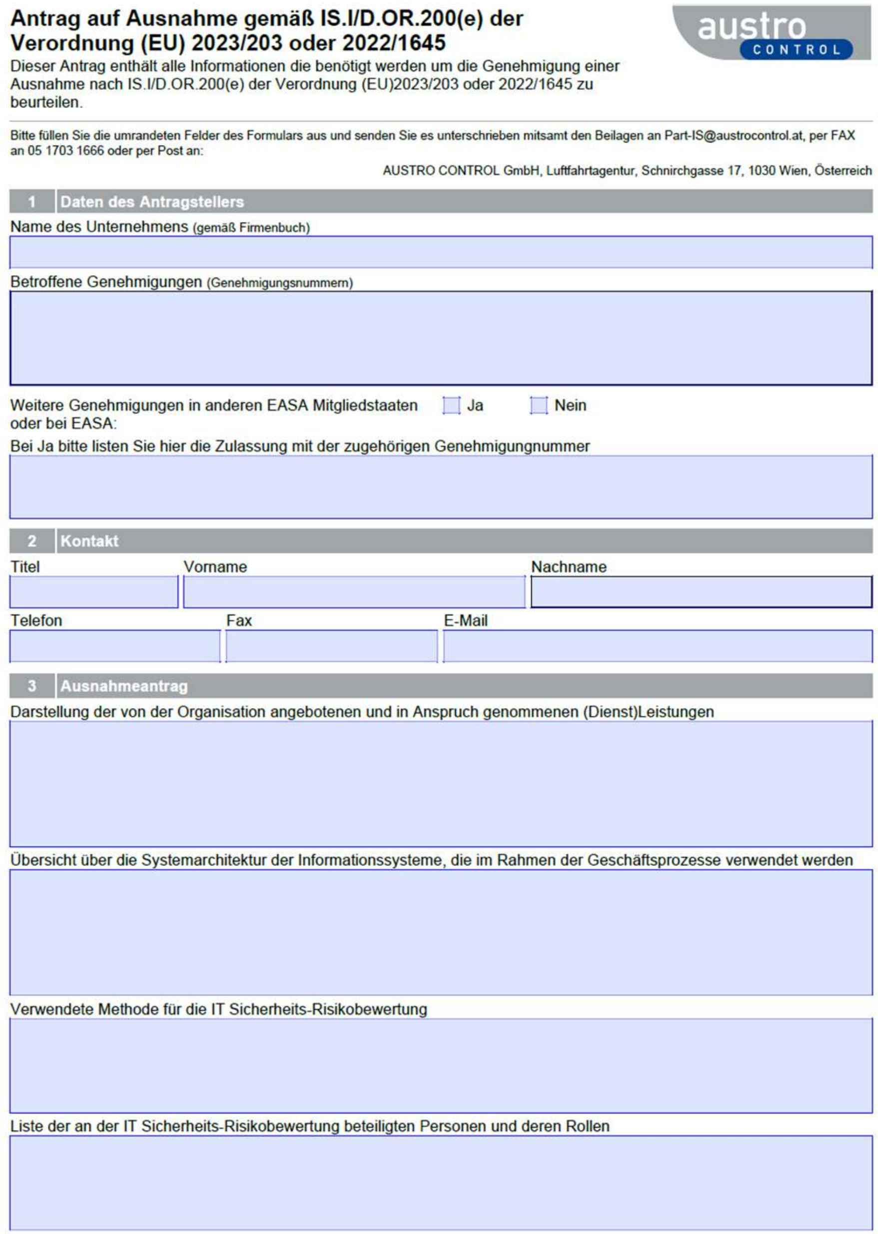
Adobe Acrobat Document

GM BAZL

Antragstellung

Schritte zum Antrag

- *Internes Erst-Assessment ob die Kriterien erfüllt werden können (z. B. durch CMF)*
- *Antrag (FO_LFA_AIR_xxx) 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 Derogations-bedingungen 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 – 29.07.2025

Part-IS requirements:

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*

30

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 <u>(with clear cross-references about what portions correspond to the requirements of Part-IS)</u>*

31

Zusammenwirken IS-Security und Safety – neues GM

Ein SMS für viele Appro-vals ?

Ein ISMS für viele Approvals ?

Ein gemeinsames ISMS macht dann Sinn, wenn auch das SMS eine gemeinsame Basis hat

Wie gehen wir als Behörde vor

Keine Übergangsfrist! - Was sagt das Guidance Material

- *Part-IS ist mit Stichtag **22. Februar 2026** (15. Oktober 2025 für POA) für die anwendbaren Organisationen gültig.*
- *Das Handbuch (ggf. die Change procedure) sollte bis dahin genehmigt sein.*

PSOE maturity approach

Table of Contents

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

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.

Page 12 of 22

Part IS

Wie leite ich die Implementierung ein?

1. Antrag auf Genehmigung des ISMM
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)

Relevanz für „suitable“ bzw. „operating“

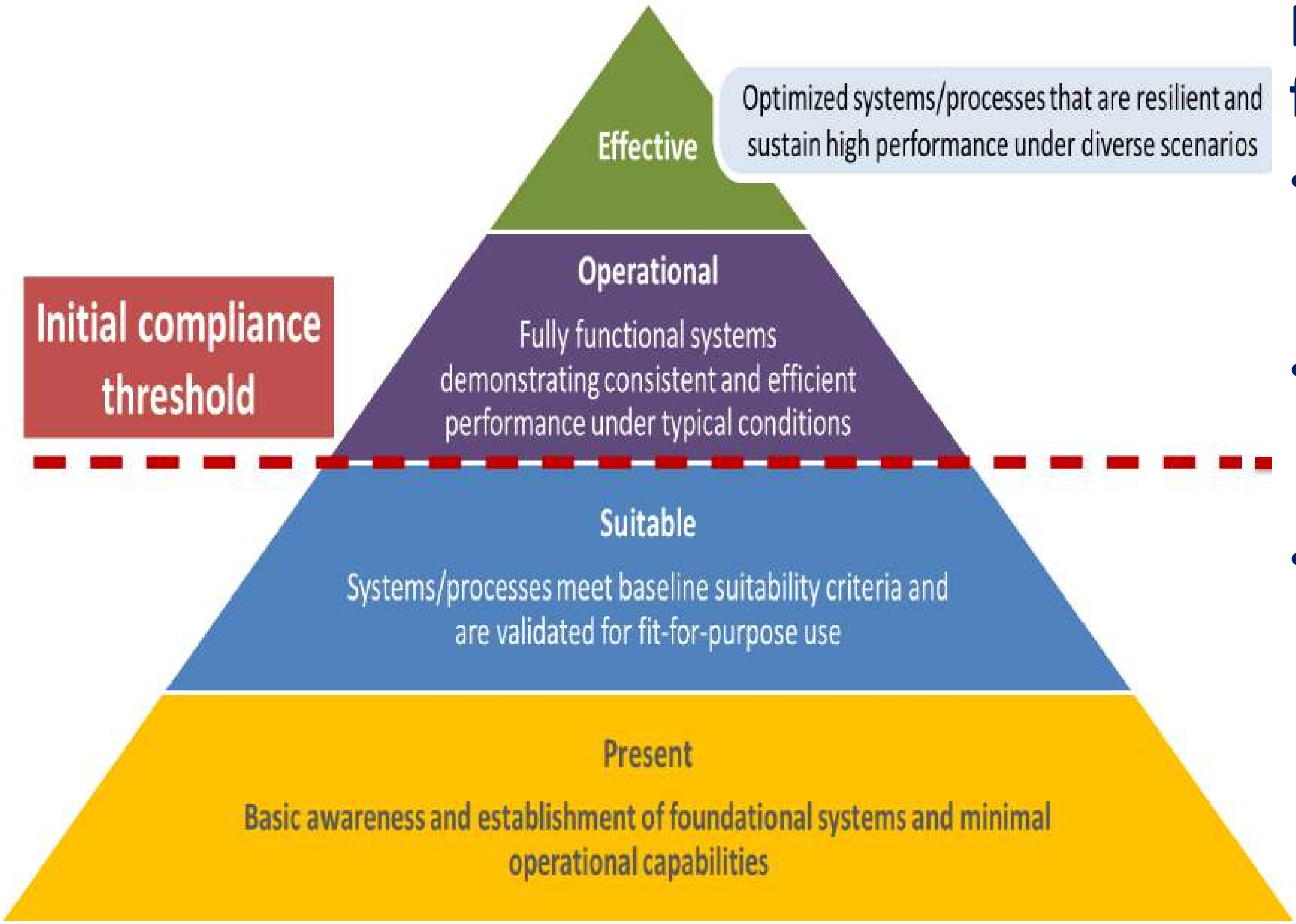
Table 1: Requirements relevance in the ISMS Foundation and Operational stages

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

Microsoft Excel-Arbeitsblatt

Tabelle aus GM als Excel

How to show Compliance to Part-IS



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“

"Operating" level corresponds to the "ISMS operation" elements indicated in the table above. This is the level that should be reached for the organisation to be considered as Part-IS compliant.

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.

The "Effective" level corresponds to the subsequent "continuous improvement" that should be

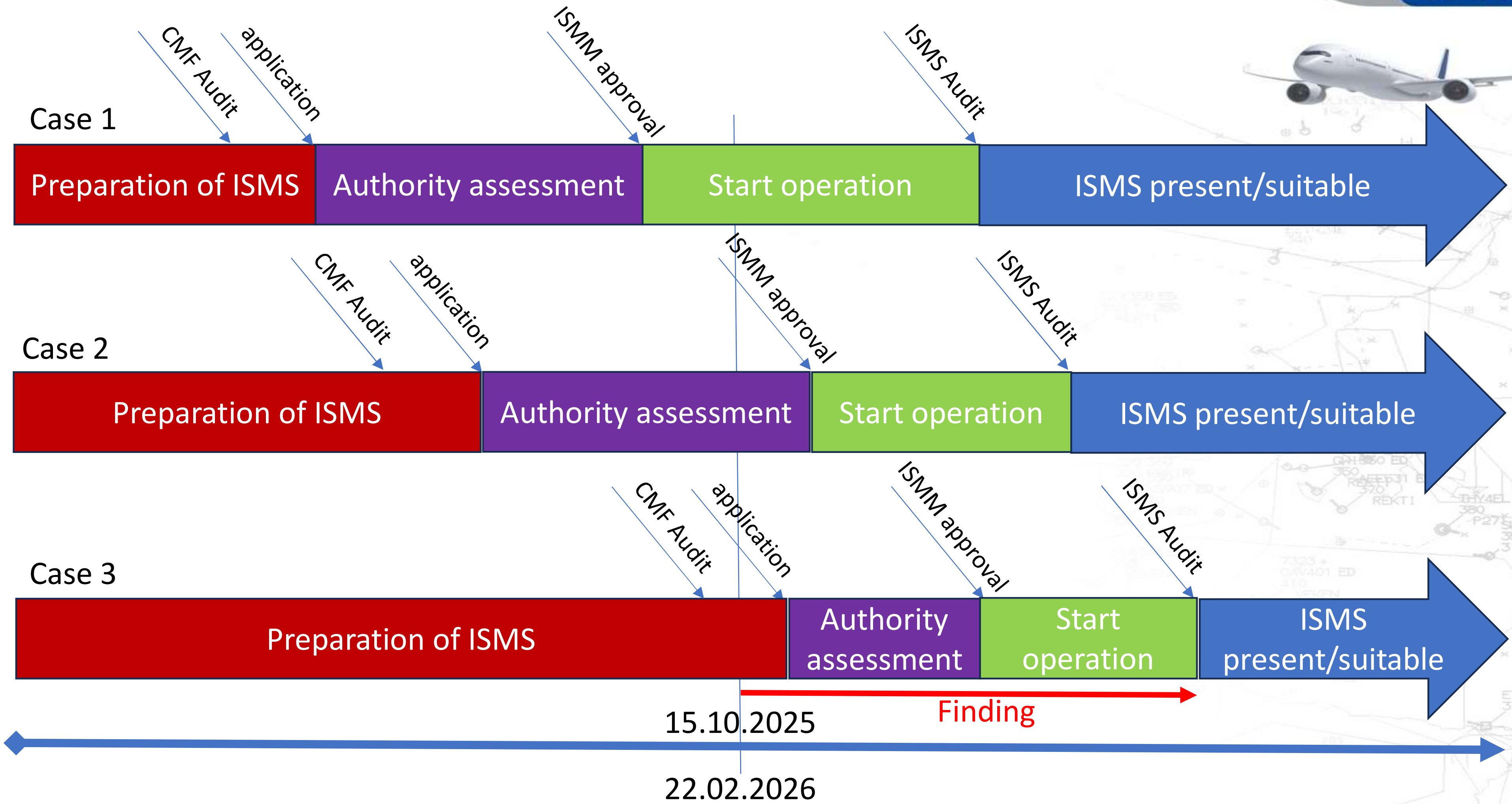
If disagreement of TF-members to be notified by 25th Aug.

Implementation Task Force	Guidelines 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~~, while~~. 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.

Cases related to applicbility date



Wie geht es weiter?

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

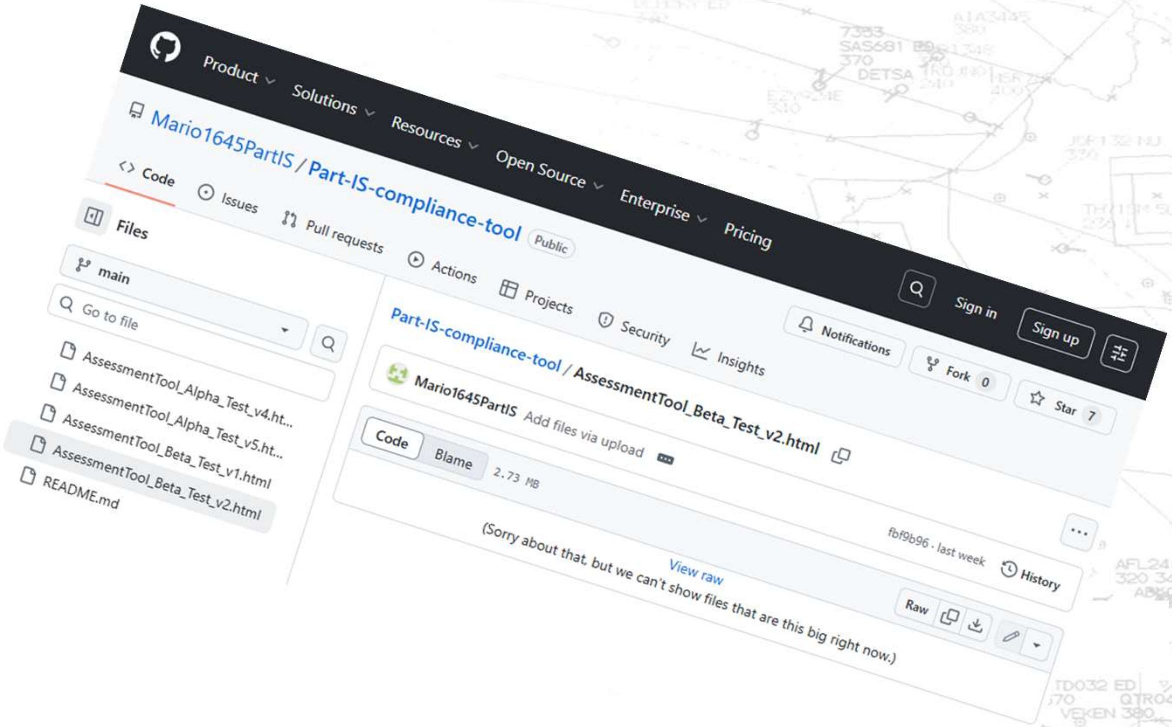
Reserved for future developments of this policy.

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

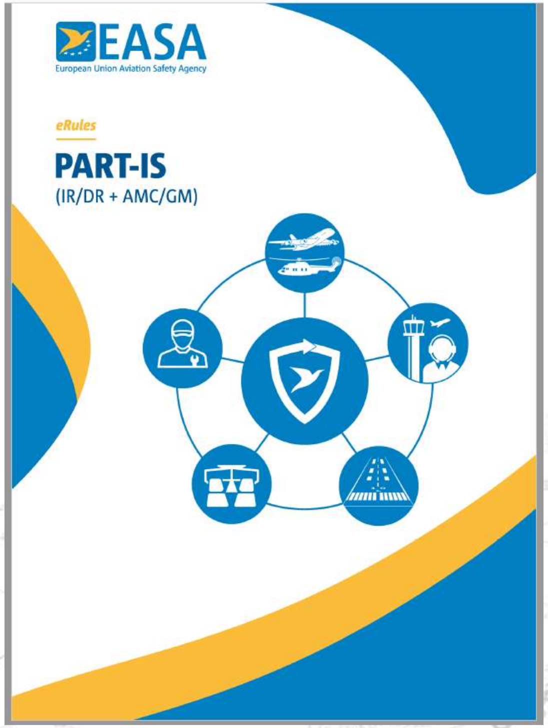
Tools & Guidance

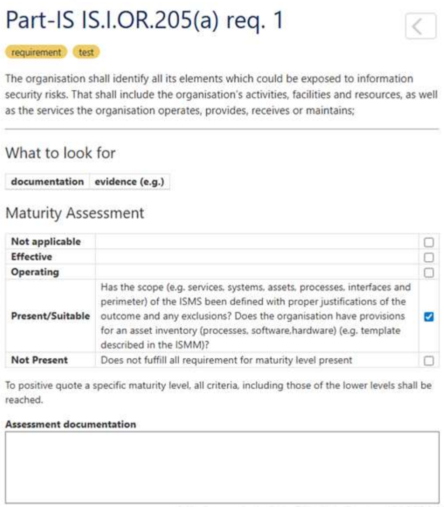


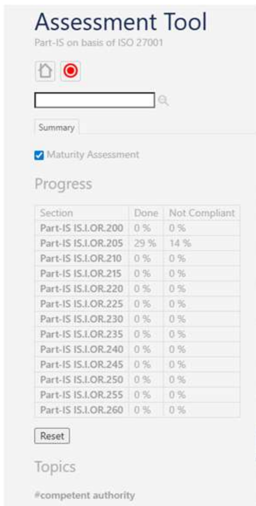
Part-IS-Café – 29.07.2025

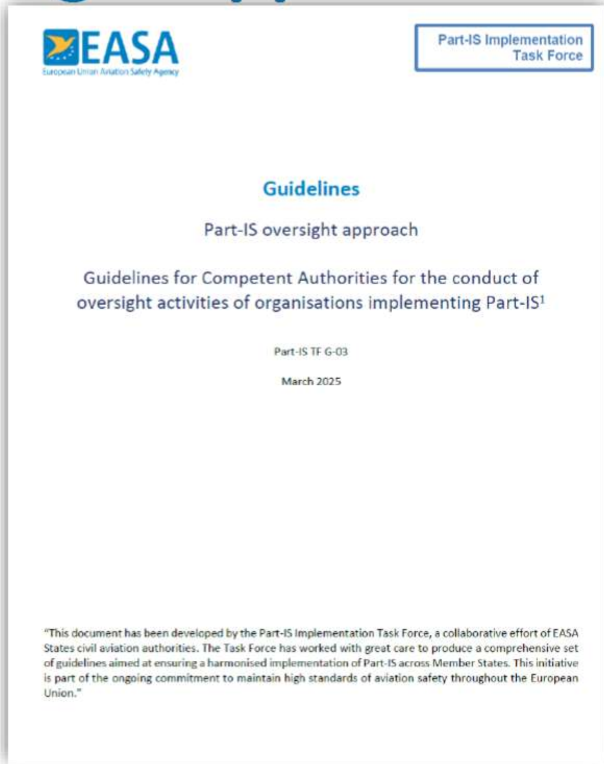
How to support?

Bring the rule and the assessment criteria together

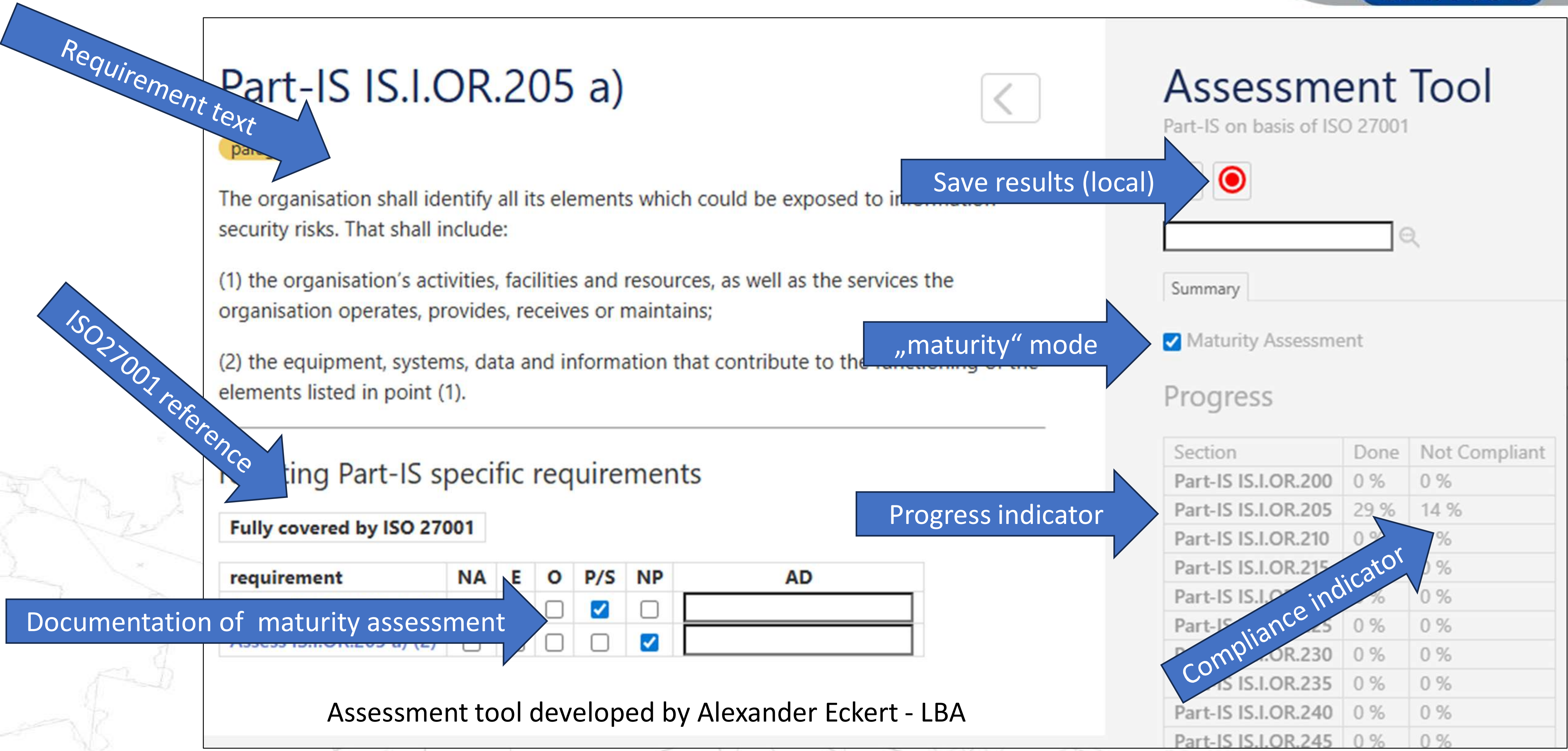








Assessment tool – Maturity assessment



Assessment tool developed by Alexander Eckert - LBA

Assessment tool – Maturity assessment - detail

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

requirement test

Requirement text

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	☐

From EASA-GM

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

Assessment documentation

Place for evidence

austro

Assessment Tool

Part-IS on basis of ISO 27001

Save results (local)

Summary

☑ Maturity Assessment

„maturity“ mode

Progress

Progress & Compliance indicator

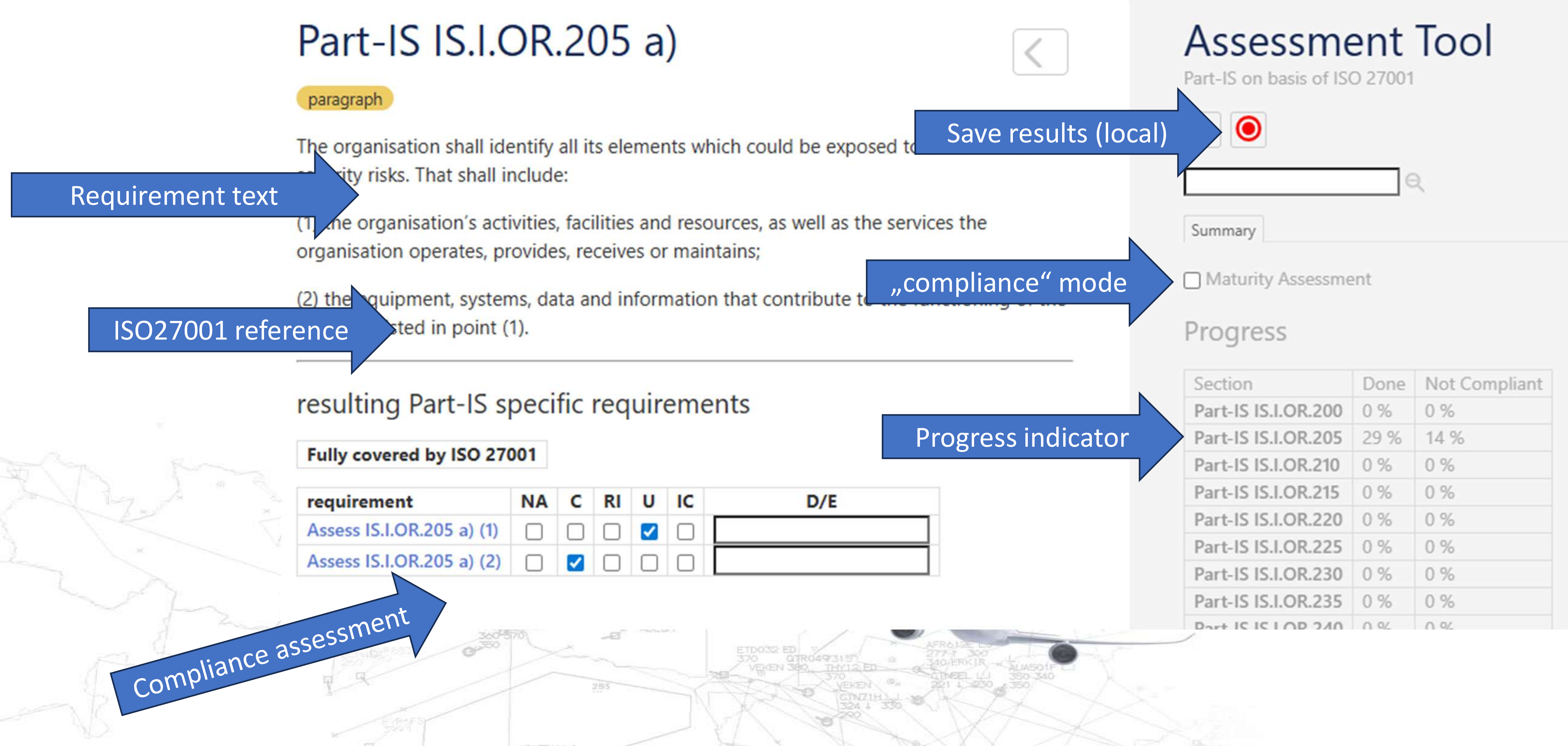
Section	Done	Not Compliant
Part-IS IS.I.OR.200	0 %	0 %
Part-IS IS.I.OR.205	29 %	14 %
Part-IS IS.I.OR.210	0 %	0 %
Part-IS IS.I.OR.215	0 %	0 %
Part-IS IS.I.OR.220	0 %	0 %
Part-IS IS.I.OR.225	0 %	0 %
Part-IS IS.I.OR.230	0 %	0 %
Part-IS IS.I.OR.235	0 %	0 %
Part-IS IS.I.OR.240	0 %	0 %
Part-IS IS.I.OR.245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

Reset

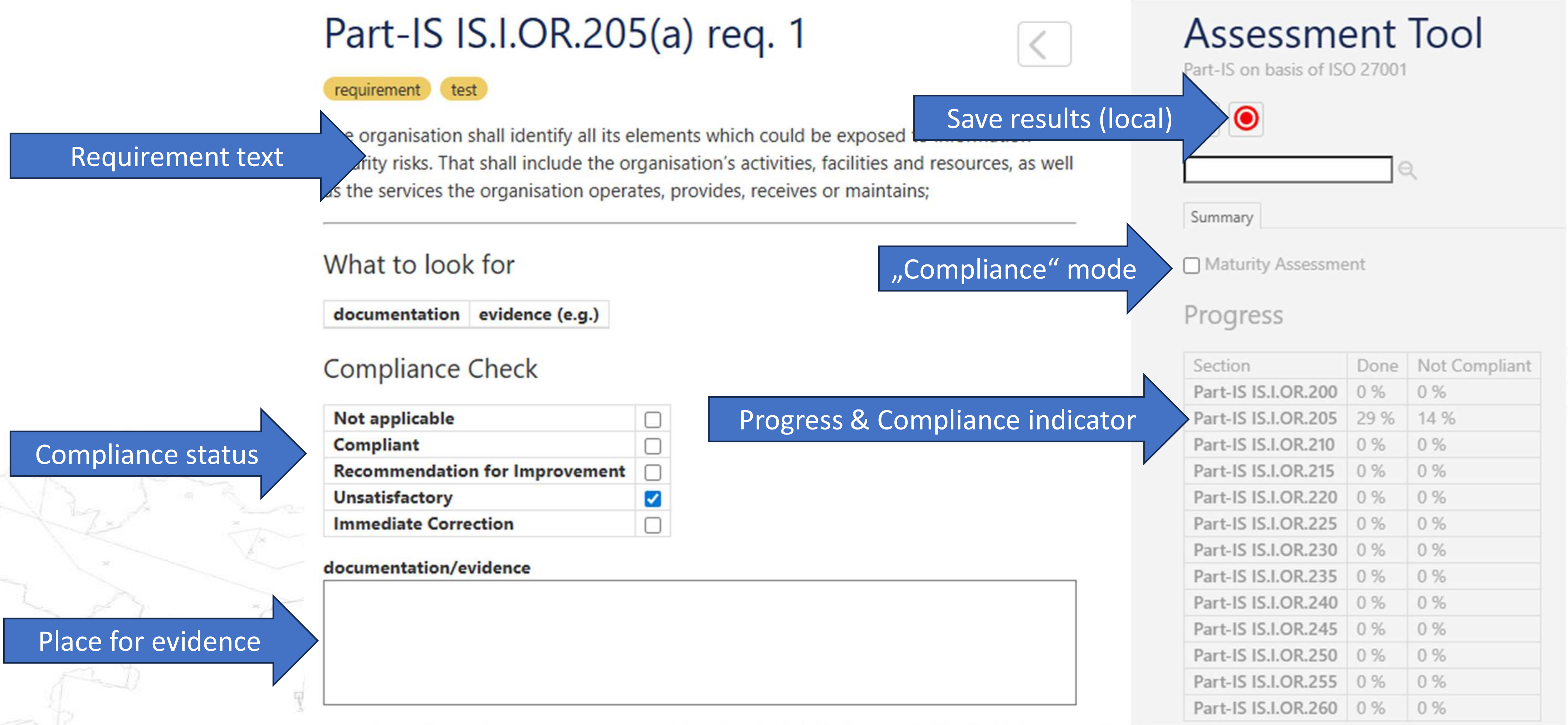
Topics

#competent authority

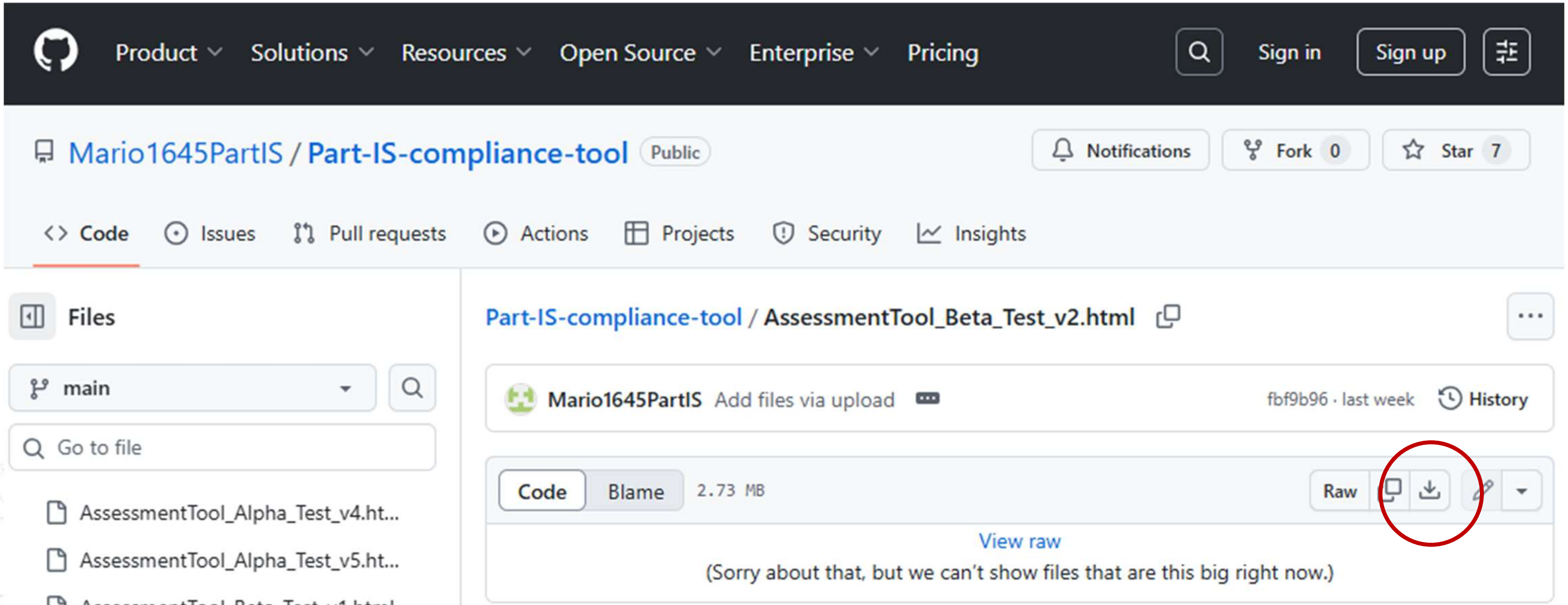
Assessment tool - – Compliance Check



Assessment tool detail – Compliance Check



Where to get it?

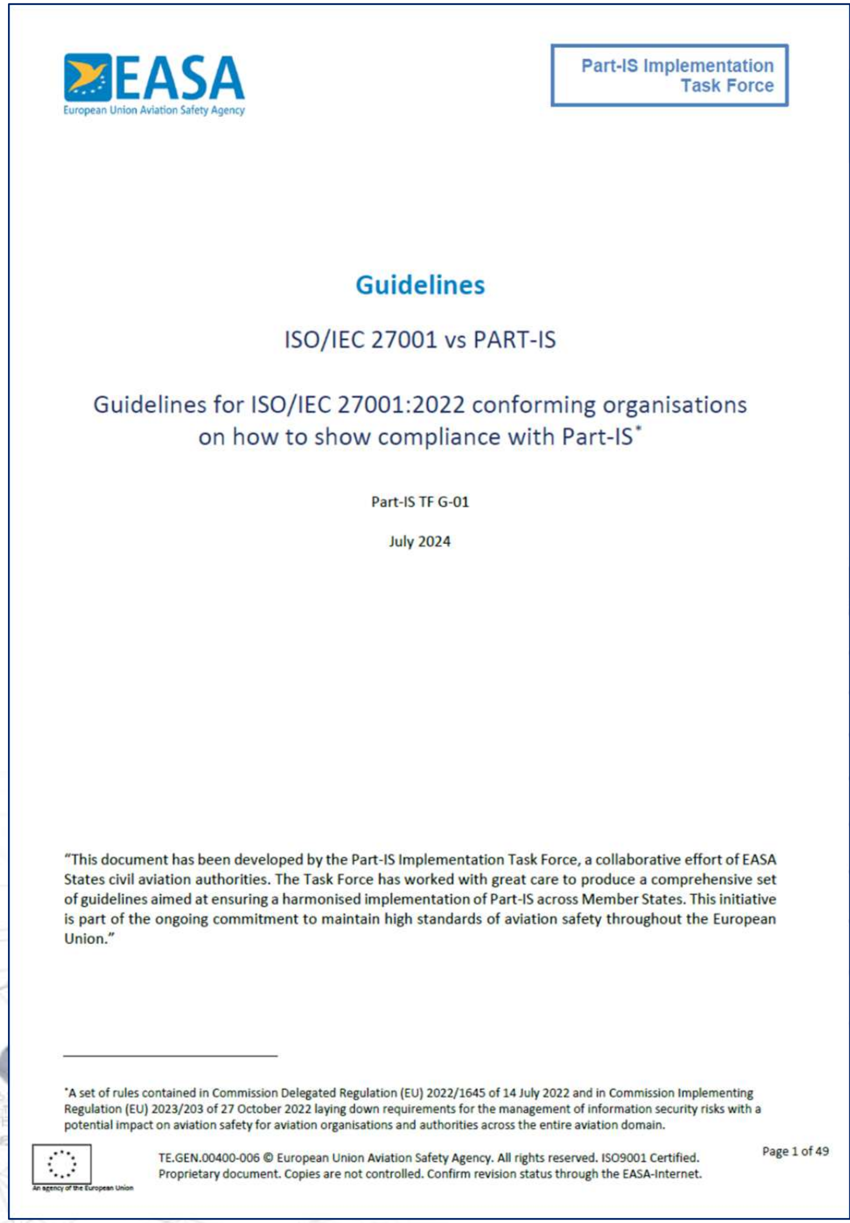


[Mario1645PartIS/Part-IS-compliance-tool: This repository contains the HTML based tool to assess compliance to IS.I/D.ORs.]

ISO27001 Guideline

Key objectives for the development

- Initial focus on **industry stakeholders**, as they need the guidance first.
- Focus on **ISO/IEC 27001:2022** as certificates based on ISO/IEC 27001:2013 are not valid after October 2025
- No ISO27001 certificate is necessary to use the guideline. The ISMS shall be in conformity with the standard
- **All** IS.OR-Requirements are covered.
- final version published in July 2024 to allow industry to transpose their existing ISMS into Part-IS compliance.
- The Guideline does not only reflect IS27001, but also similarities between the "safety-rules" and Part-IS. The similarities are labeled domain per domain.
- Readable also for "ISMS-personal" with less knowledge of aviation safety rules (e. g. consultants).


EASA
European Union Aviation Safety Agency

Part-IS Implementation
Task Force

Guidelines

ISO/IEC 27001 vs PART-IS

Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS*

Part-IS TF G-01

July 2024

"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."

*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.

An agency of the European Union

TE.GEN.00400-006 © European Union Aviation Safety Agency. All rights reserved. ISO9001 Certified.
Proprietary document. Copies are not controlled. Confirm revision status through the EASA-Internet.

Page 1 of 49

How to use the guideline

Rule text (same for „I“ and „D“)

Mapping to controls of ISO27001:2022 - Annex I

Explanation of ISO27001:2022 mapping

Mapping to similar requirements of „safety rules“

Implementation guidance

2.1 Example on IS.OR.235 (a) Contracting of ISM activities

The unmodified requirement of Part-IS

Requirement

a) `The organisation shall ensure that when contracting any part of the activities referred to in point IS.I.OR.200 to other organisations, the contracted activities comply with the requirements of this Regulation and the contracted organisation works under its oversight. The organisation shall ensure that the risks associated with the contracted activities are appropriately managed.

The ISO/IEC 27001 counterpart to the requirement

b) ISO/IEC 27001 mapping

A5.19 Information security in supplier relationships

A5.21 Managing information security in the information and communication technology (ICT) supply chain

A5.22 Monitoring, review and change management of supplier services

The reason for a specific Part-IS guidance

Part-IS particularity

ISO/IEC 27001 controls A5.19, A5.21 and A5.29 may cover this requirement. The difference in the requirements of IS.OR.235 is, that it is limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, ….).

In addition, all “domain specific” implementation rules (e.g. ORO.AOC.110, ORA.GEN.205, CAMO.A.205, 145.A.205, 21.A.139 (d) (1), 21.A.239 (d) (3), ATM/ANS.OR.B.020, ATCO.OR.C.005, ADR.OR.D.010,) of Reg. (EU) 2018/1139 require procedures to deal with contracted activities in a wider scope, where information security should be integrated.

The add-on guidance

Guidance for Part-IS implementation

The difference in the requirements of IS.OR.235 is, that it is limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, ….). The controls in ISO/IEC 27001 do not exclude those kinds of services, but sometimes it will not be in the focus of the organisation.

Therefore, there is no need to establish an independent system for those contractors mentioned IS.OR.235 (a). The list of suppliers should be reviewed to ensure, that the suppliers providing the services mentioned in IS.OR.235 are covered.

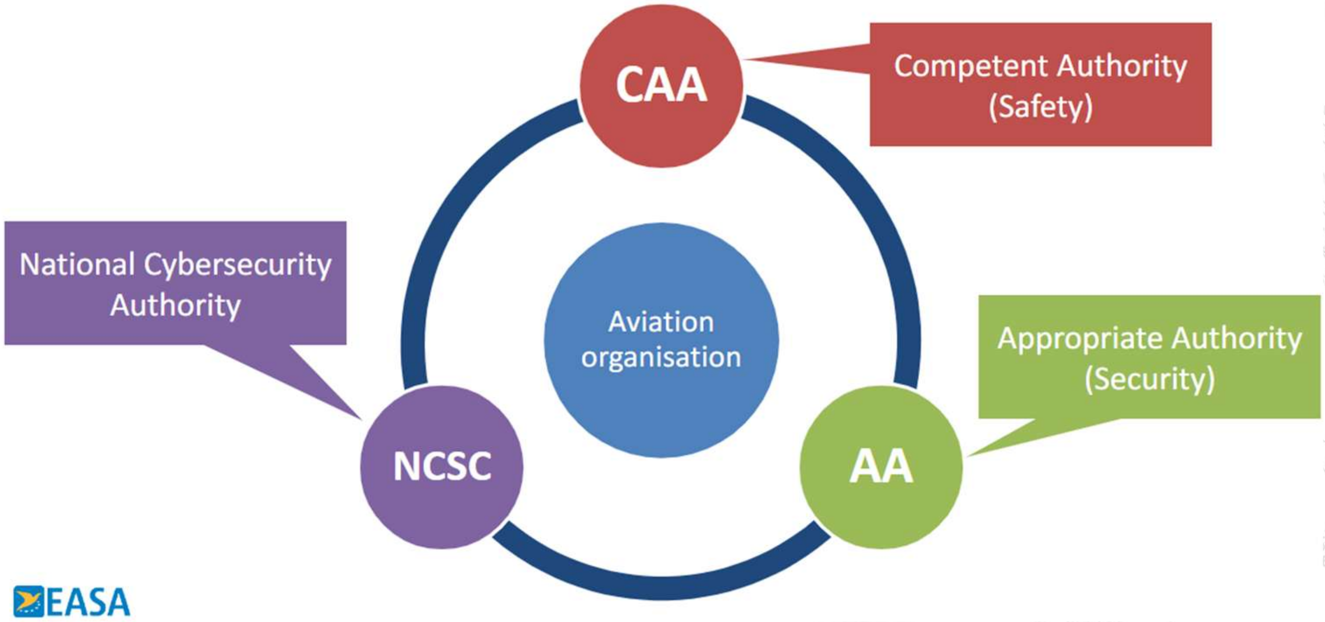
Proportionality criteria – same in new GM

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.

Part-IS interplay with other regulations



Part-IS-Café – 29.07.2025

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?

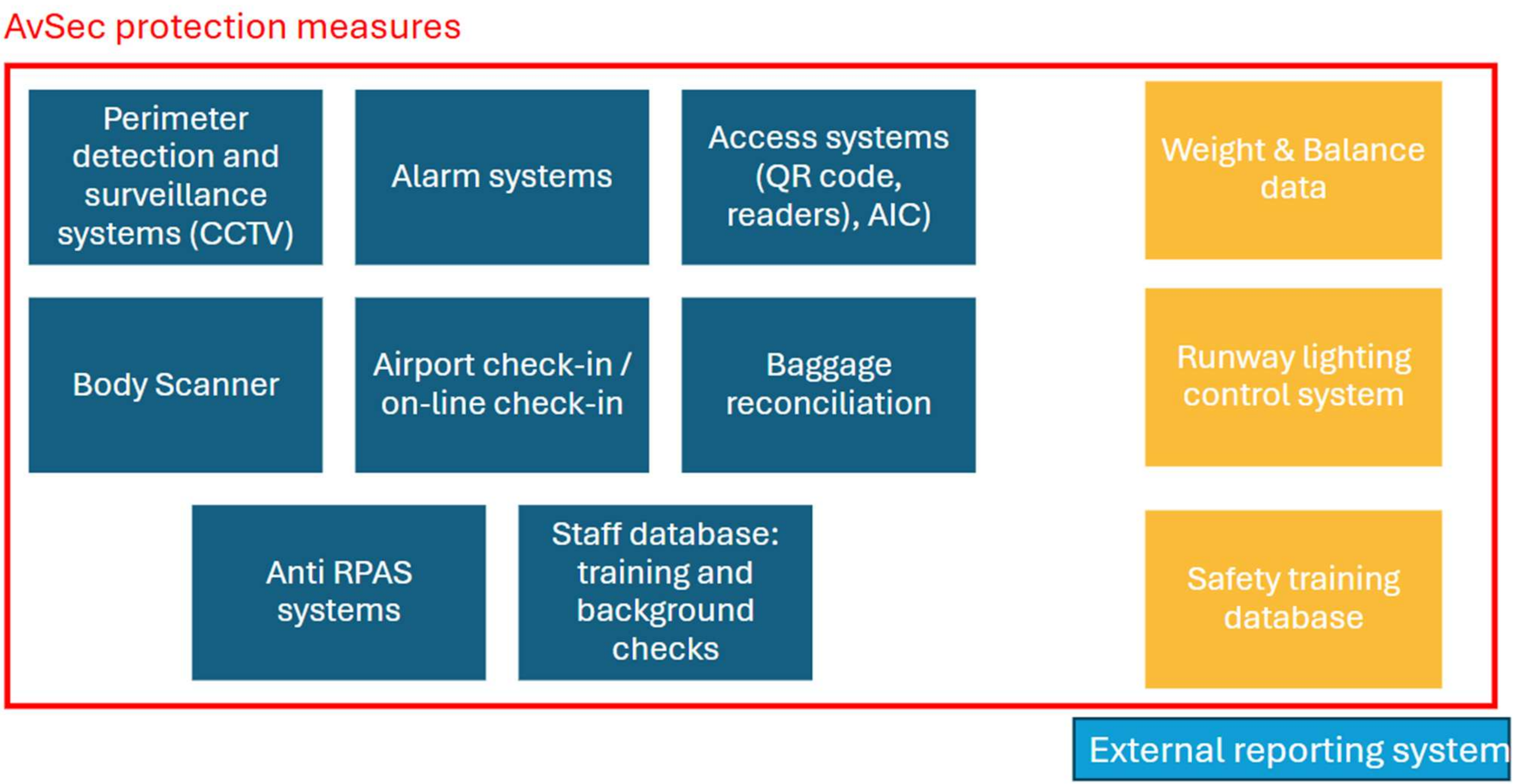
Rahmenbedigungen – AVSEC – neues GM

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 – latest development

In words of EASA ...

- The legal equivalence stated in art. 4(2) should be [illegible]pply only to the systems identified in the organisations security[illegible]hey are also in the scope of Part-IS.
- Should an AOC-holder want to only f[illegible] requirements to protect its systems, nothing prevents them [illegible]ope (perimeter of applicability) of the system that they have in pl[illegible] order to also cover safety elements. Moreover, compliance [illegible]0 has to be ensured.
- ~~Alternatively, the [illegible]hority may agree to replace compliance with AvSec by complian[illegible]ents contained in the other EU or national legislation (e.g. Part-IS)~~ [illegible]t happen in Austria!

- [illegible]T the AOC approval! If CAMO a/o ATO are strongly integrated, the [illegible] the AVSEC program may be extended to other related approvals.

Discussions with BMIMI in progress

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

Workgroup between DG Move and DG Connect since September 2023.

Rahmenbedigungen – NIS2 – neues GM

GM1 Article 5(1) — Requirements arising from other Union legislation

Pursuant to Article 44 of Directive (EU) 2022/2555 (the NIS 2 Directive), the previous Directive (EU) 2016/1148 (the NIS Directive) was repealed with effect from 18 October 2024. In accordance with the NIS 2 Directive, references to the repealed Directive shall be construed as references to Directive (EU) 2022/2555 and shall be read in accordance with the correlation table set out in Annex III. In accordance with this table, references to Article 14 of Directive (EU) 2016/1148 shall be now read as references to Article 21 and Article 23 of Directive (EU) 2022/2555. For an exact correlation, please refer to Annex III to Directive (EU) 2022/2555. For legal certainty, the equivalence of any requirements should be assessed against the requirements of the national legislation transposing Directive (EU) 2022/2555. When assessing the equivalence established between the requirements laid down in Regulation (EU) 2023/203 and Directive (EU) 2022/2555, organisations should consider the following:

— The equivalence between Regulation (EU) 2023/203 and Directive (EU) 2022/2555 requirements should be assessed in terms of which requirements can be deemed as equivalent.

— Possible differences in the perimeter of applicability of the rules, in particular as regards the elements that are within the scope under the two different frameworks.

NISG 2023 -> 2026?

Part-IS wurde auf europäischer Ebene nicht angenommen!

NISG kommt voraussichtlich erst 2026

§ 27. Ausnahmen von Verpflichtungen für wesentli[...] oder wichtige Einrichtungen aufgrund sektorspe[...] Rechtsakte der Europäischen Union

(1) Sofern wesentliche oder wi[...] sektorspezifischen Rechtsakten der Eu[...] zur Cybersicherheit (oder de[...] nationalen Umsetzungsrechtsakten) unterliegen,

1. gemäß welcher die[...] Einri[...]tungen entweder eigene Risikomanagemen[...] ergreifen oder erhebliche Cybersi[...]älle melden müssen;
2. die entsprechenden [...]ungen in ihrer Wirkung den in diese[...]sgesetz festgelegten Verpflichtungen (§[...] zumindest gleichw[...] sind und
3. der Bundesminister für Inneres die [...]eichw[...]tigkeit dieser Vorschriften und der[...] E[...]n[...]g in einer Verordnung festgestellt ha[...]

gelten diese sektorsp[...]ifi[...]n Bestimmungen anstelle der in diesem [...]n[...]es[...]setz [...]geregelten Bestimmungen.

a) Luftverkehr	Luftfahrtunternehmen im Sinne des Art. 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit i[...] Zivilluftfahrt und zur Aufhebung der [...]erordnun[...] (EG) Nr. 2320/2002, ABl. L 97 vom 9.4.[...] S. 72, [...] gewerblichen Zwecken eing[...]z[...]
	Flughafenl[...]tungsorga[...] § 3 Z 2 Bundesgese[...]r die [...]est[...]g[...]ng von Flughafenentgelten (Flughafenen[...]gel[...]gesetz – FEG), BGBl. I Nr. 41/2012, Flughäfen im Sinne des § 3 Z 1 FEG, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU, ABl. L 348 vom 20.12.2013, S. 1 angeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
	Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Art. 2 Z 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums ("Rahmenverordnung"), ABl. L 96 vom 31.3.2004 S. 1 bereitstellen
b)	Infrastrukturbetreiber im Sinne des Art. 3 Z 2 der

Equivalence with Part-IS -> tbd.

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

Fragestunde für CAMO