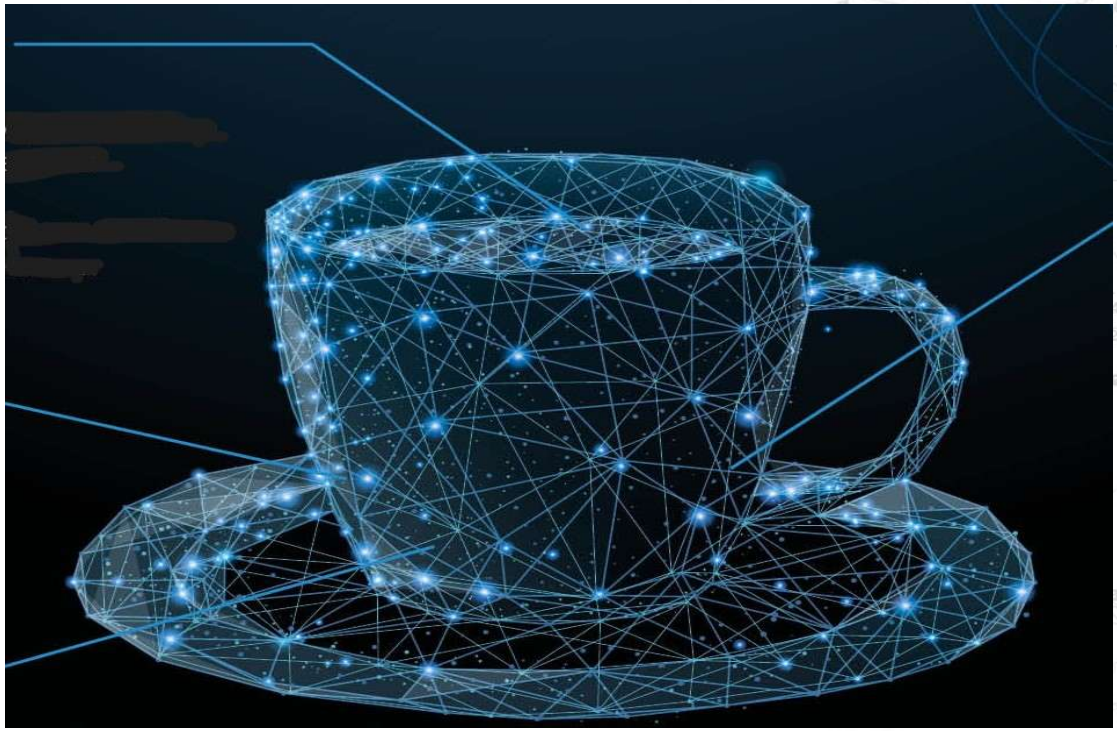
Part-IS CAFE #2

Part IS Info Meeting

26.08.2025



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

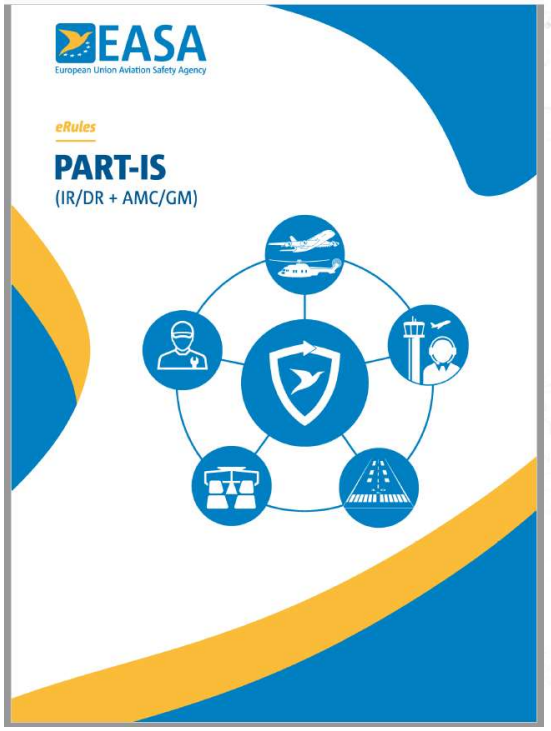
Ablauf:

- 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



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

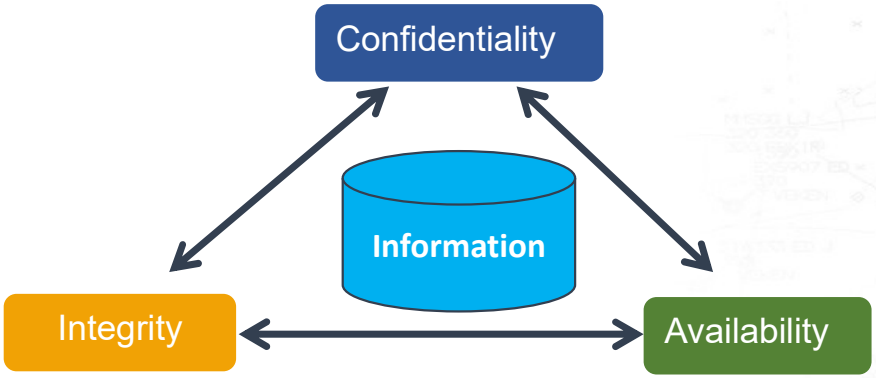
Proportionate to the impact on aviation safety !!

Jetzt geht es um Informationssicherheit !

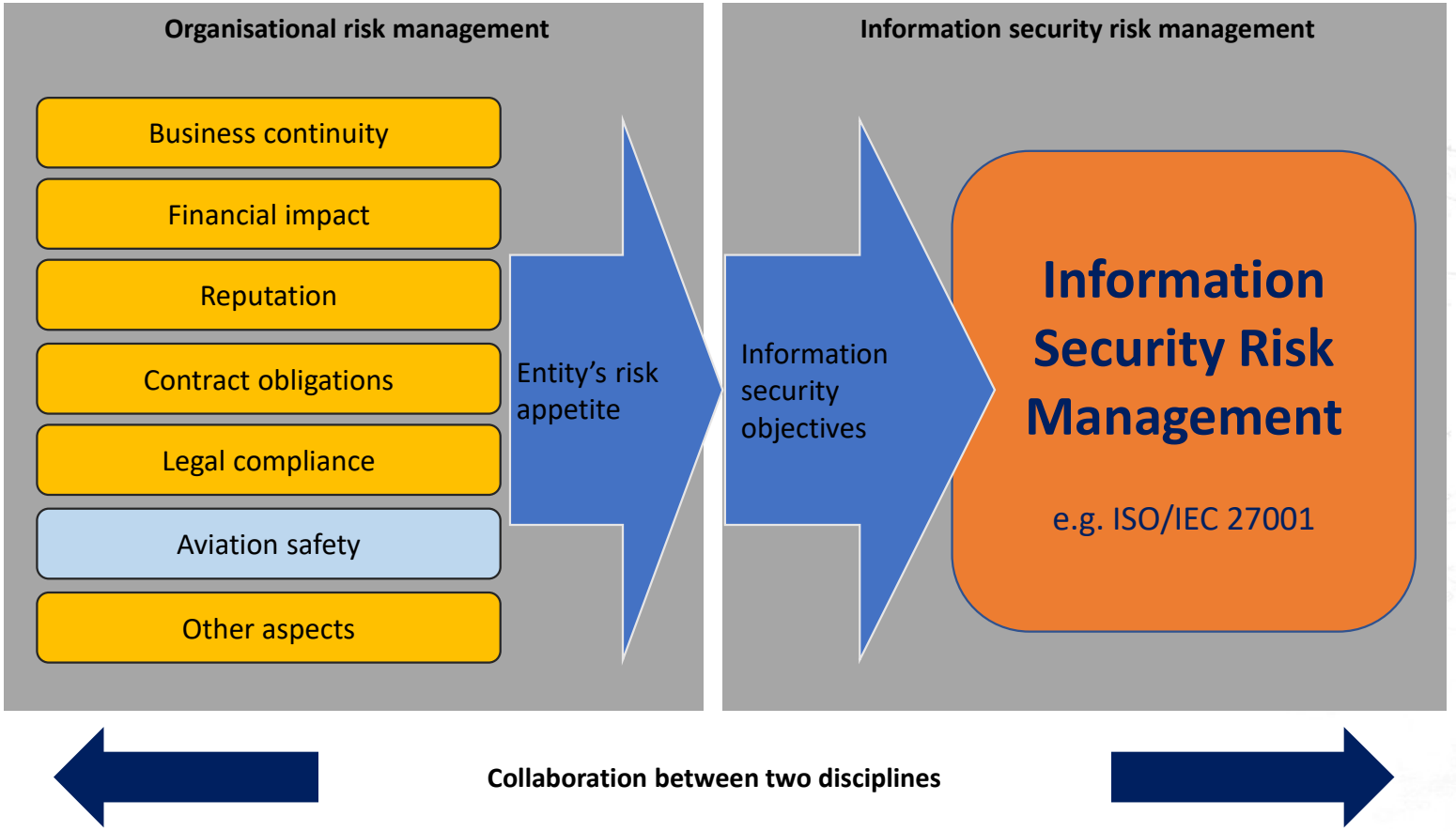
What is an ISMS ?

What is Information Security Management?

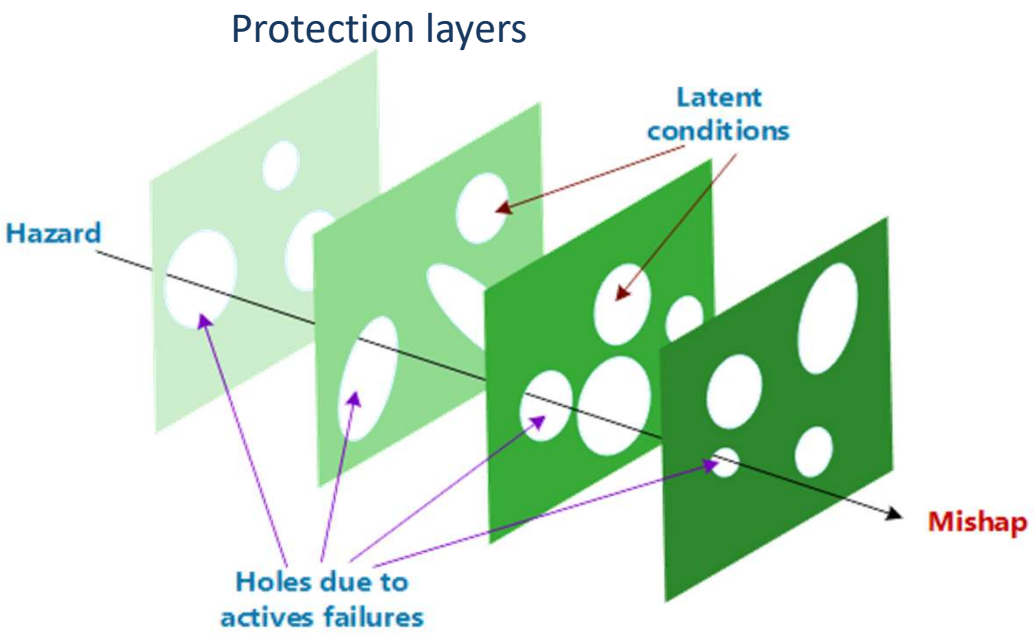
- ISO 27001 states that ***Information Security Management*** *is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their*
  - *Confidentiality,*
  - *Integrity, and*
  - *Availability.*

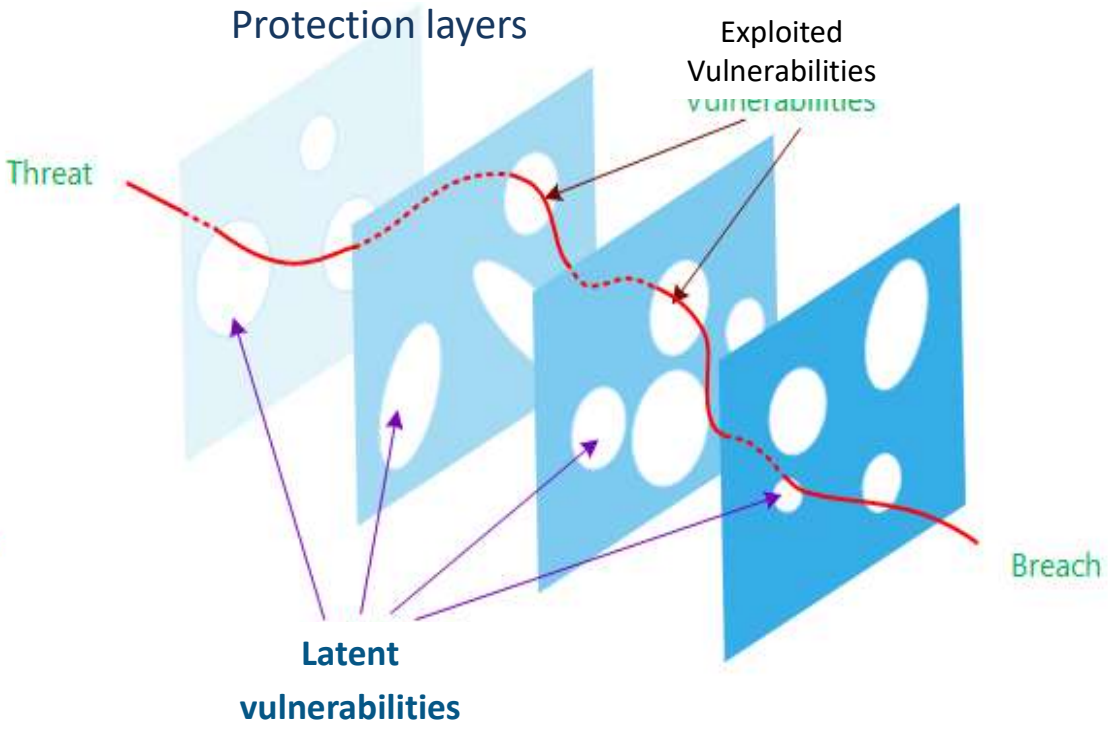


Safety is just one more Organisational Risk



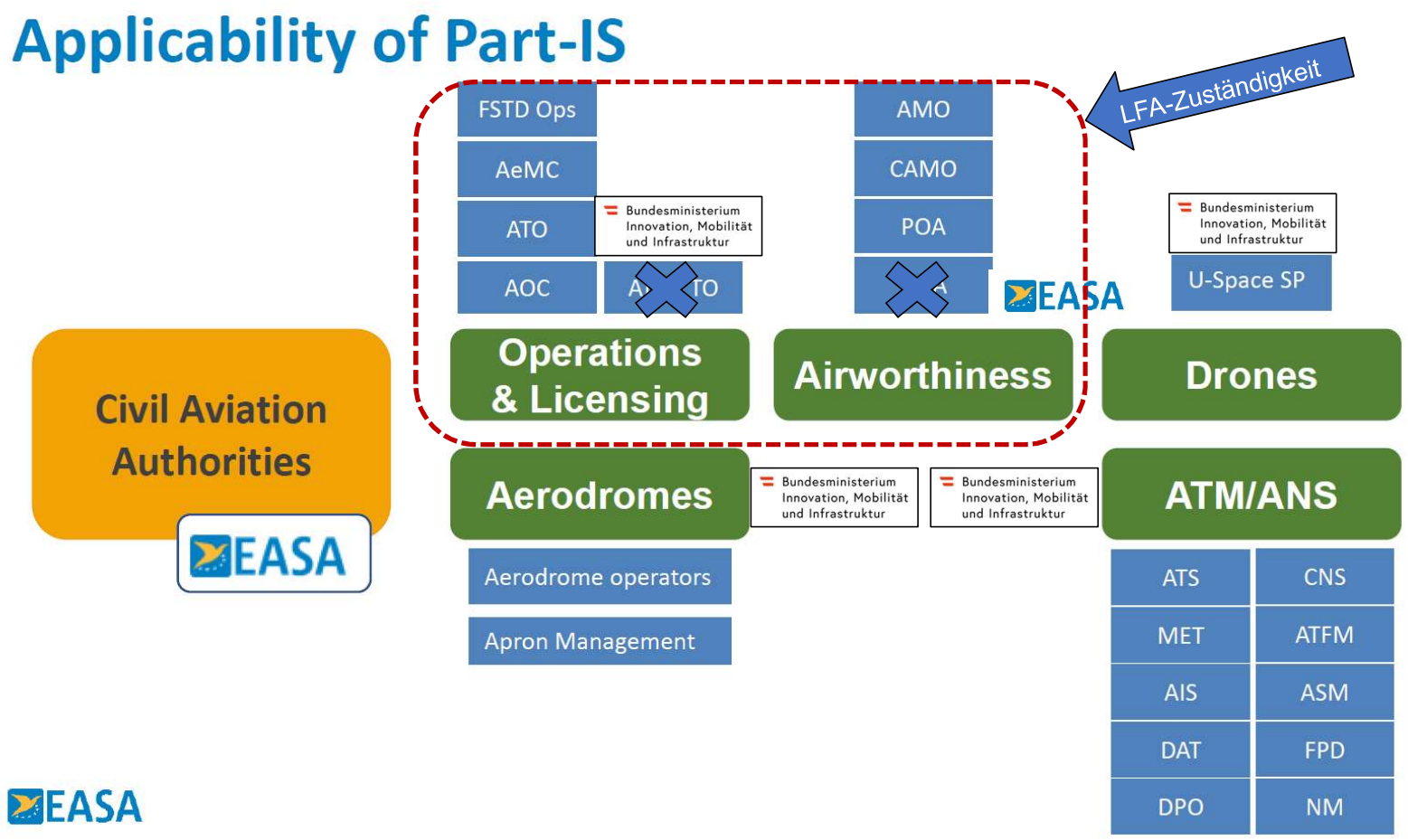
The cultural bias in aviation





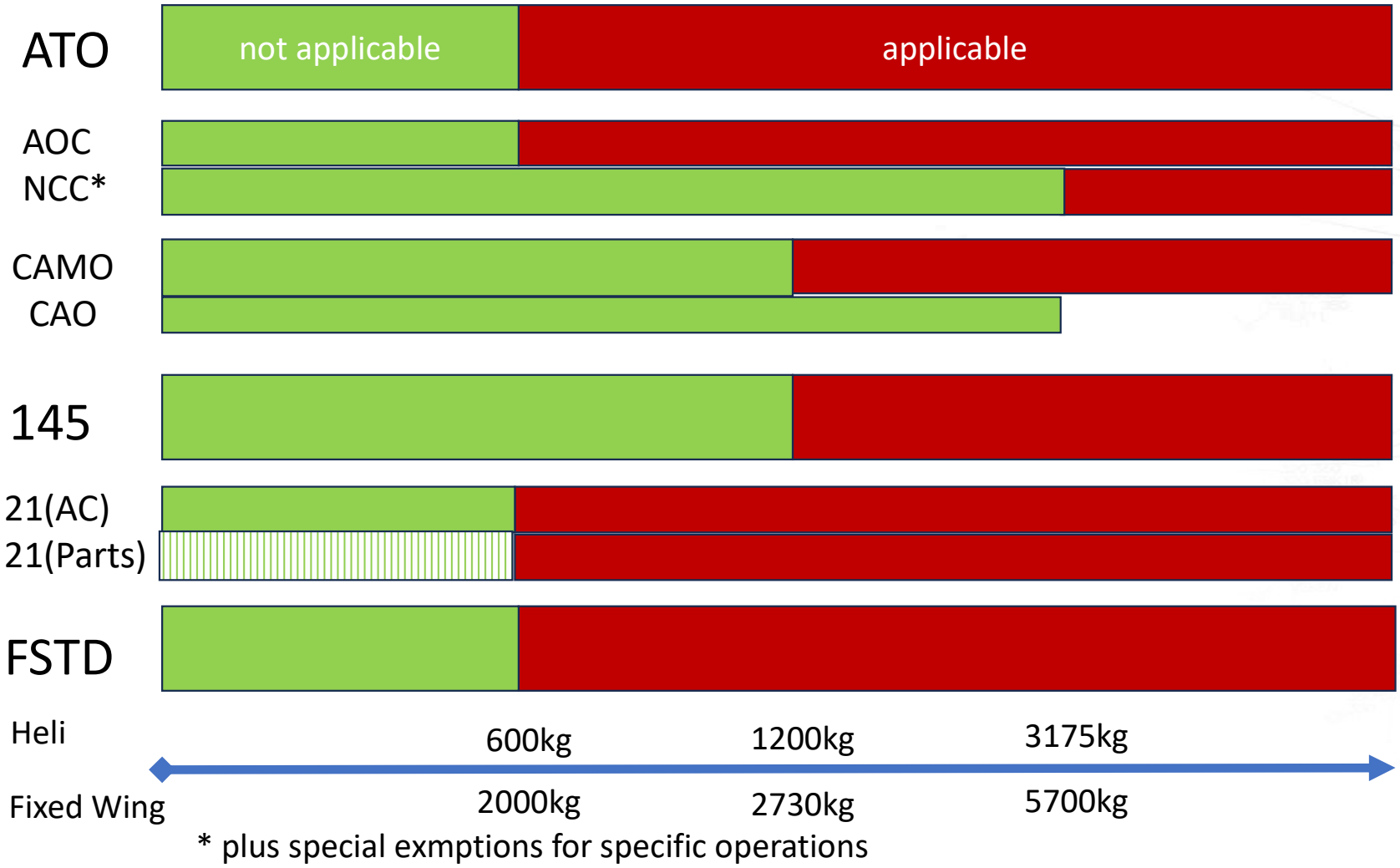
Safety **vs.** **Security**

Rahmenbedigungen – Anwendbarkeit



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

Applicability – based on MTOM



* plus special exmptions for specific operations

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

Part-IS-Café – 26.08.2025

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 Informationssicherheitsrisiken 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 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.

<u>NOTE:</u> 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)

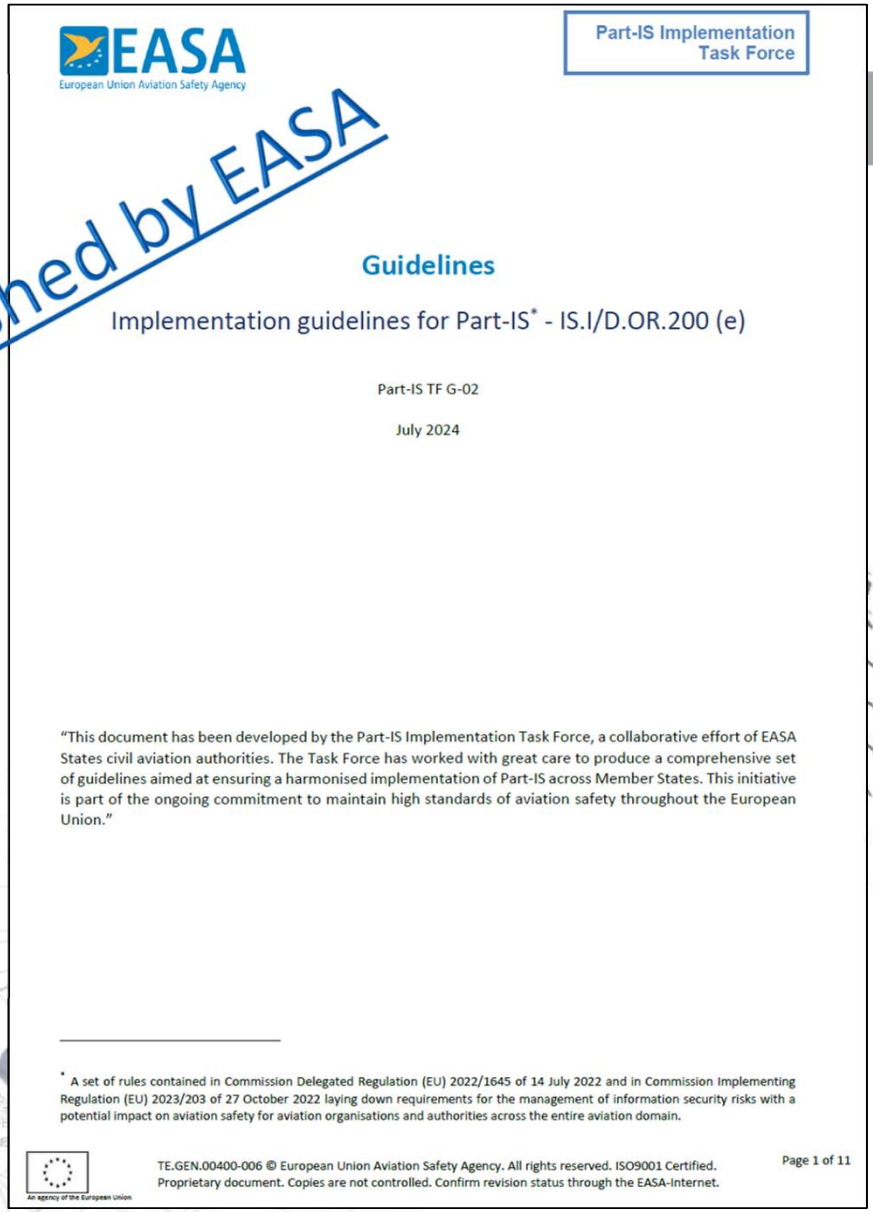
Guideline from July 2024

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 by EASA

[ED Decision 2025/014/R - Regular update of the AMC & GM to Regulations (EU) 2022/1645 and 2023/203 | AMC & GM to Part-IS.D.OR — Issue 1, Amendment 1 | AMC & GM to Part-IS.I.OR — Issue 1, Amendment 1 | EASA]



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.

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 11

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) in AT

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

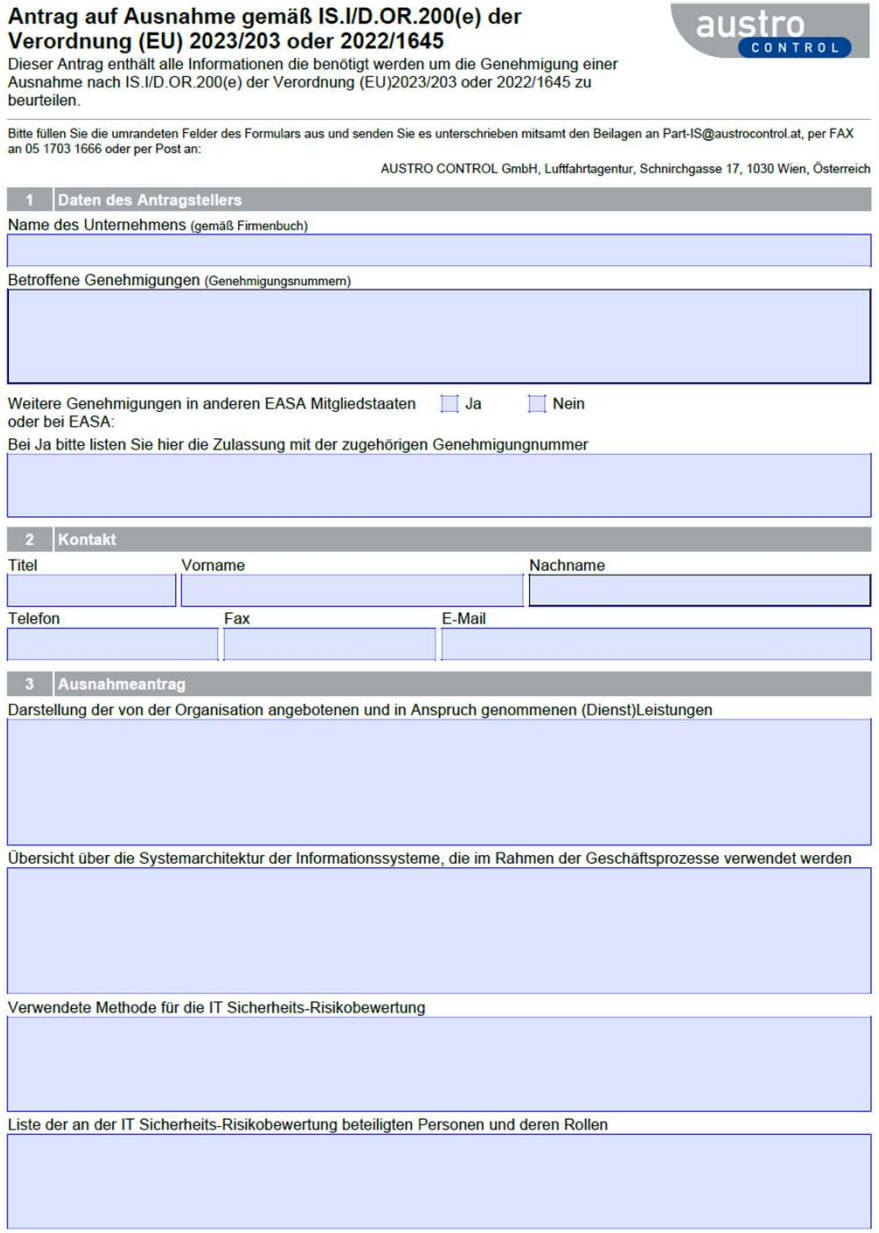
GM BAZL

Nationale Kriterien in finaler Abstimmung

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 Derogations-bedingungen bei Änderungen abbildet.*



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

austro CONTROL

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 ☐ Ja ☐ Nein
oder bei EASA:

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 – 26.08.2025

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*

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)*

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

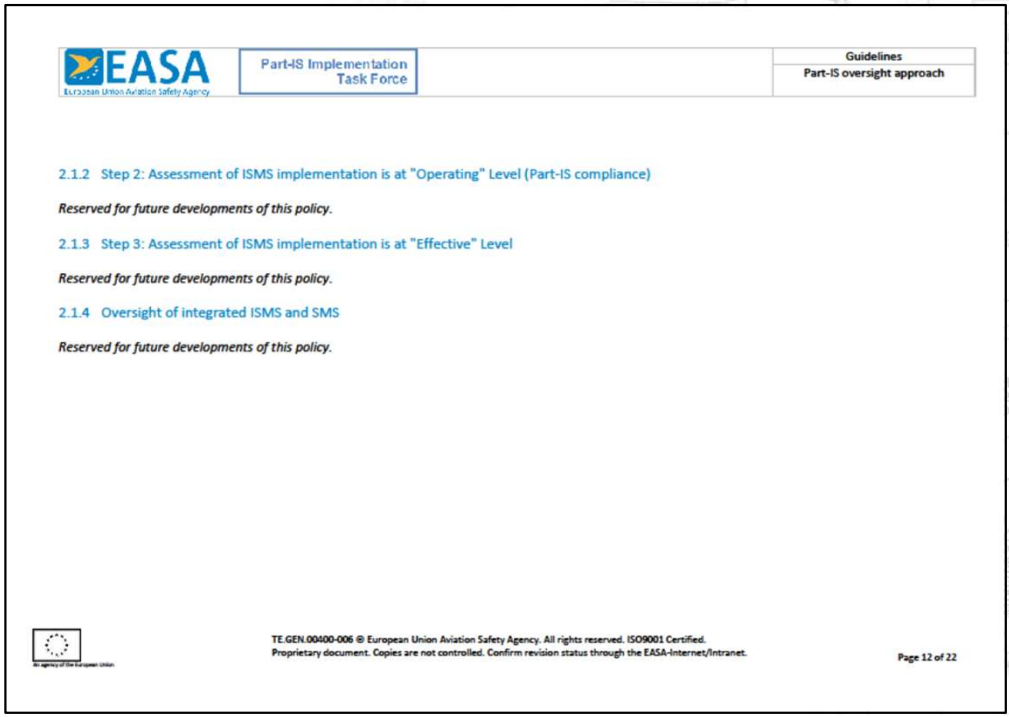
Wie gehen wir als Behörde vor

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 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.

Part IS

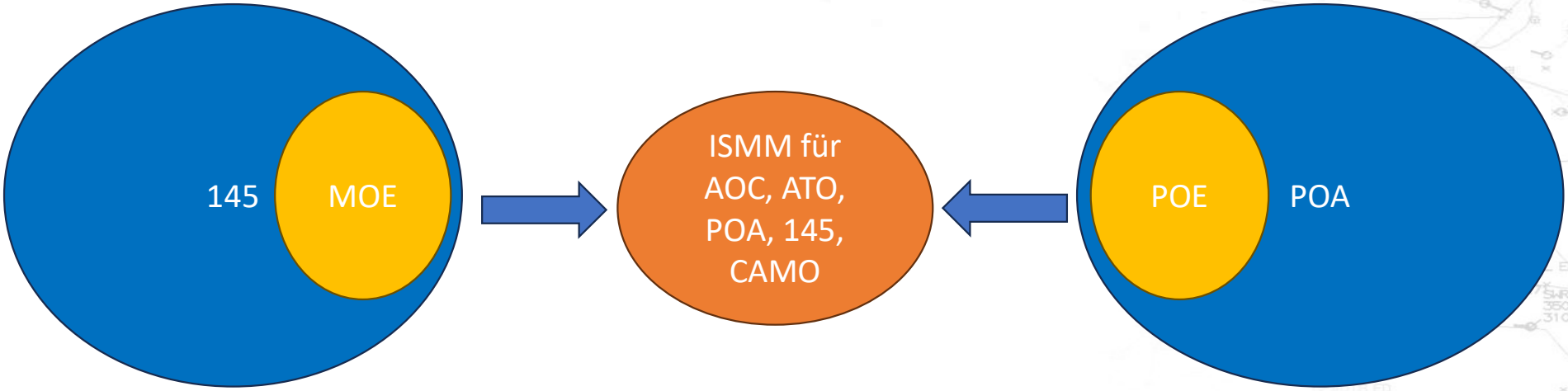
Wie leite ich die Genehmigung ein?

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

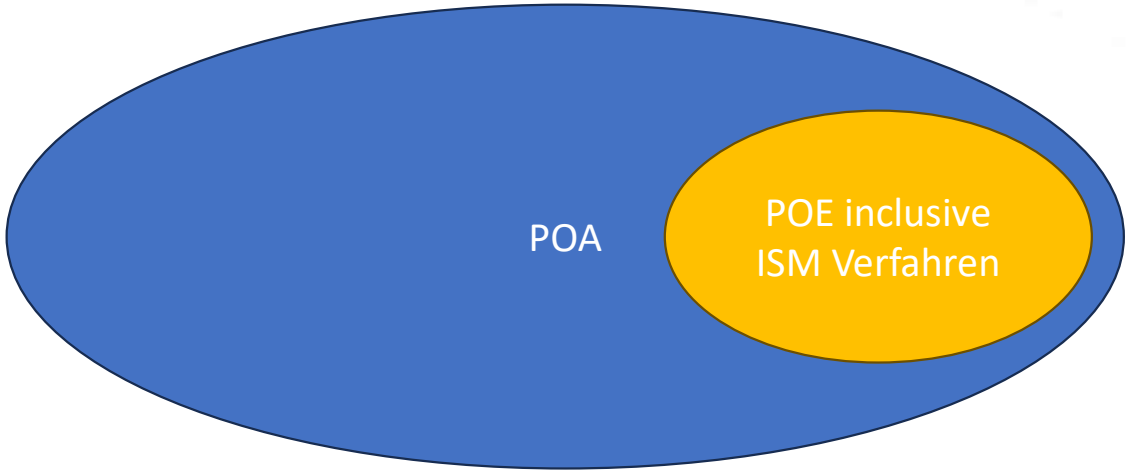
Genehmigung mit einem Bescheid für alle angeführten Zulassungen

Informationen für Antragstellung

Variante 2: Die Einzelne

Ein Antrag für Änderung eines Handbuchs für eine Zulassung

(Option: nur 1 Bescheid bei mehreren Anträgen)



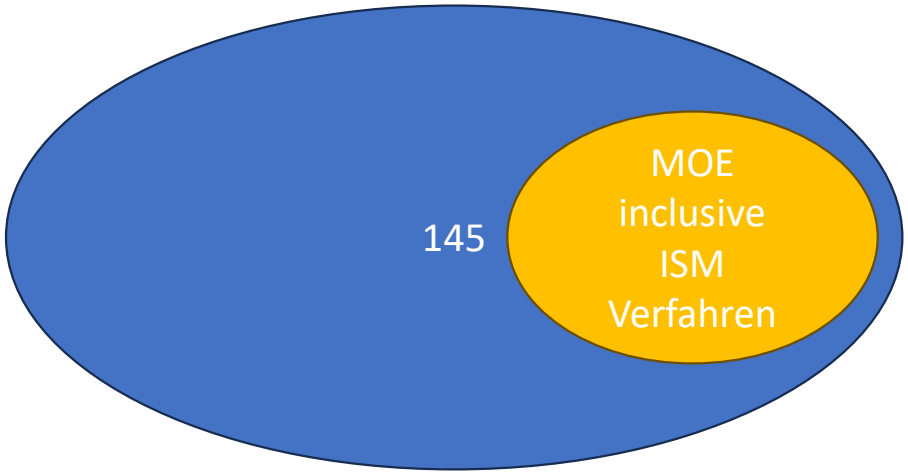
Verrechnung: Änderung der Zulassung + Zeit

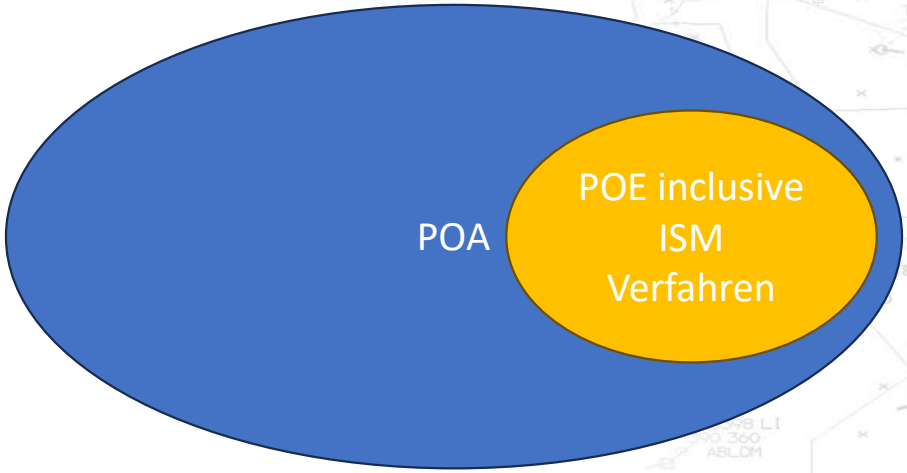
Ein Unternehmen kann mehrere unabhängige Anträge stellen.

Informationen für Antragstellung

Variante 3: Die Gemeinsame

Ein Antrag für alle Änderungen in den Handbüchern für die bestehenden Zulassungen.





Verrechnung: jeweilige Änderung der Zulassung + Zeit

Part-IS requirements:

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)*

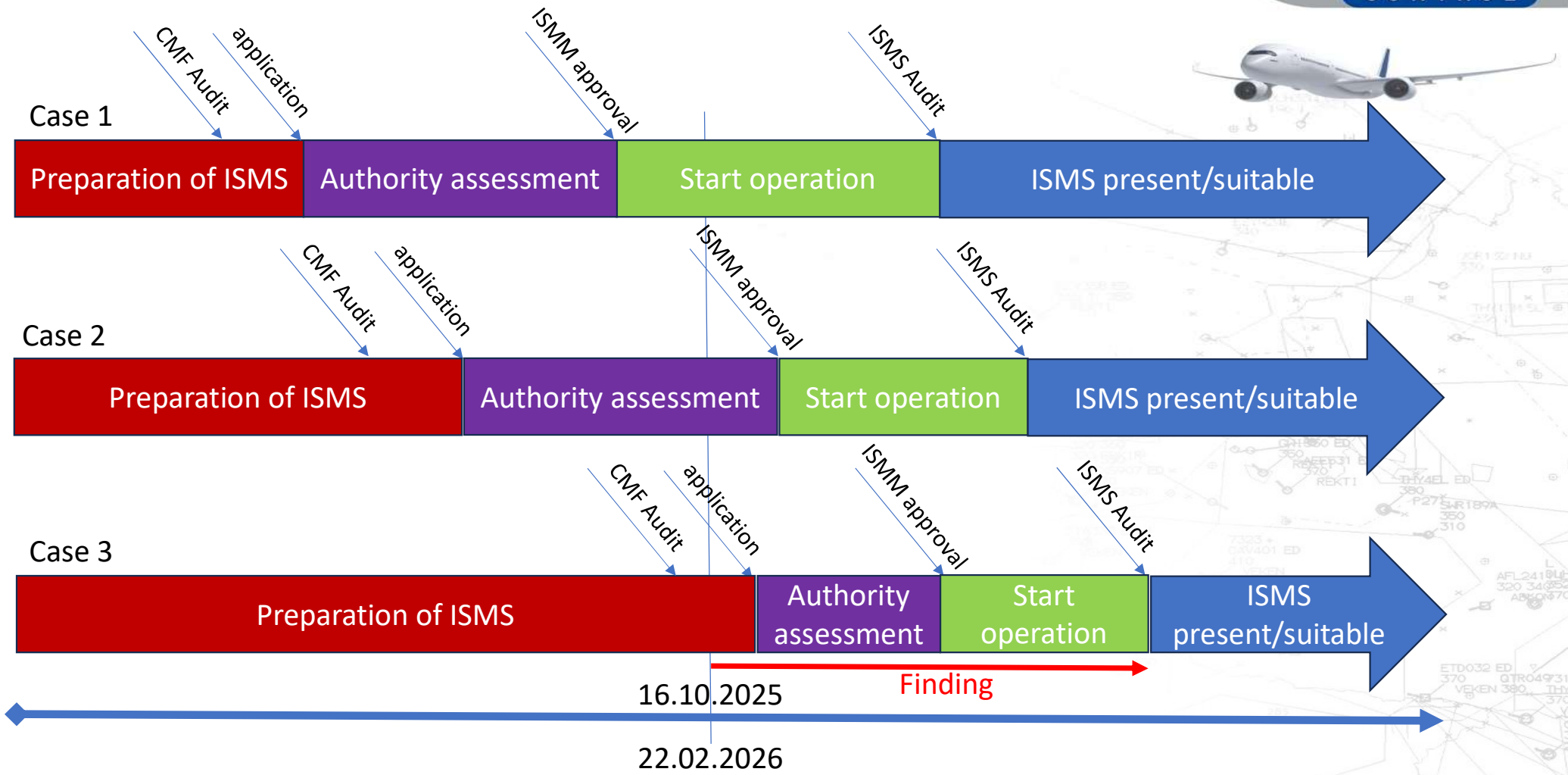
- **OR.255(b):** *Changes to the ISMS not covered by the above procedure require prior approval by the authority before they are implemented.*
  - *The organisation shall operate as prescribed by the authority while the changes are implemented.*

Nicht vergessen!

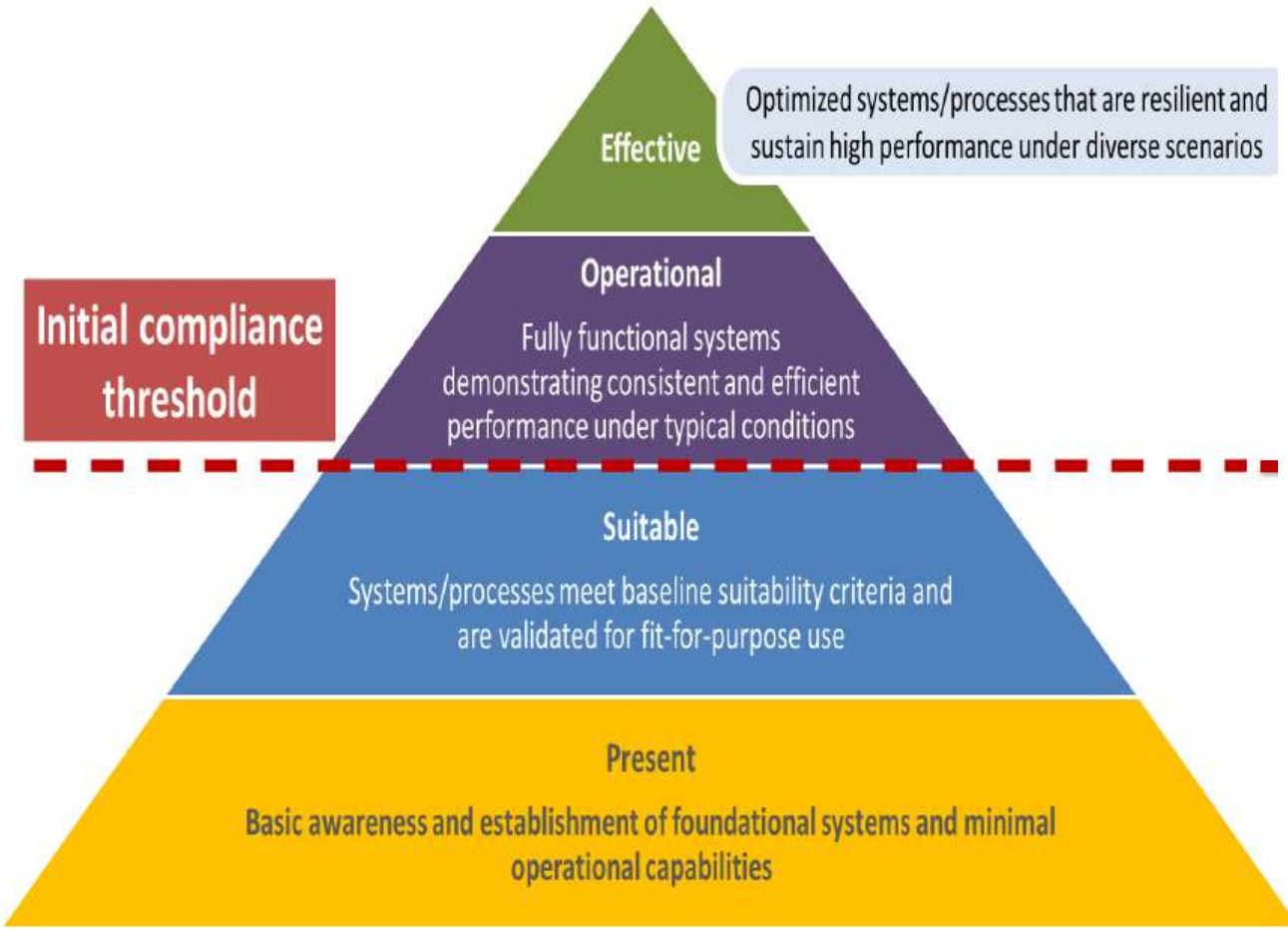
AMC1 IS.I.OR.255: *Changes with an impact on maintaining compliance with Part-IS or could lead to unacceptable level of risk (ref. GM1 IS.I.OR.205(c)),* ***should be subject to authority's scrutiny.***

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.*

Cases related to applicbility date



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·


EASA

Guidelines

Part-IS oversight approach

Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS!

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.¶

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.

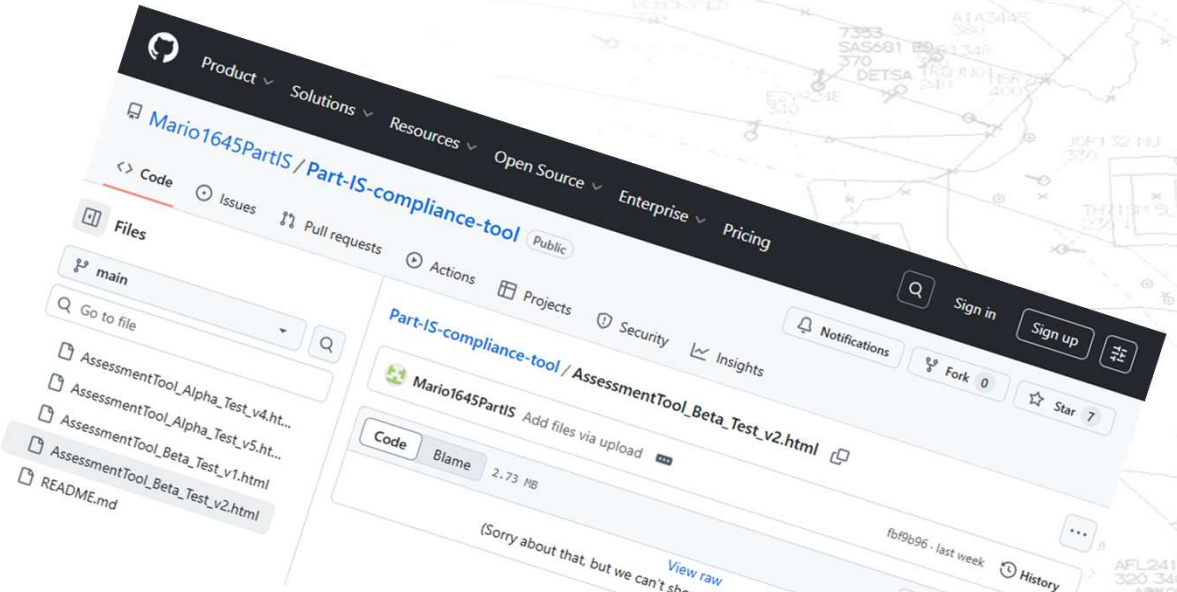
2.1.4 Oversight of integrated ISMS and SMS

Reserved for future developments of this policy.

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

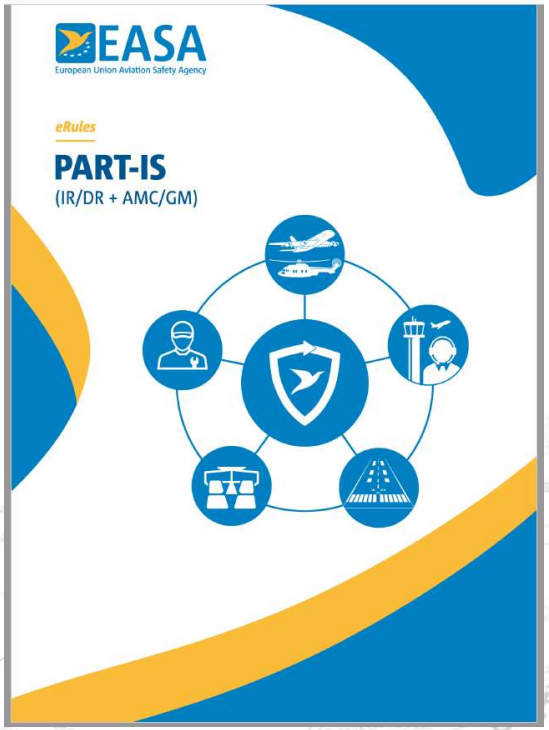
Tools & Guidance

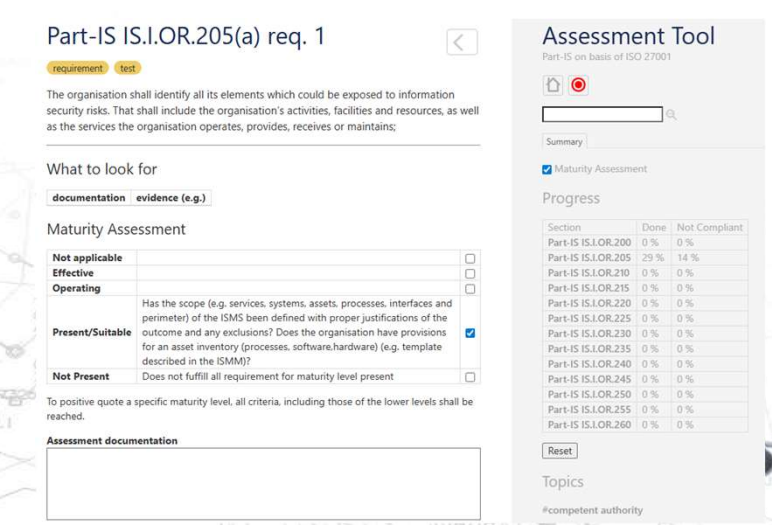
Part-IS-Café – 29.07.2025

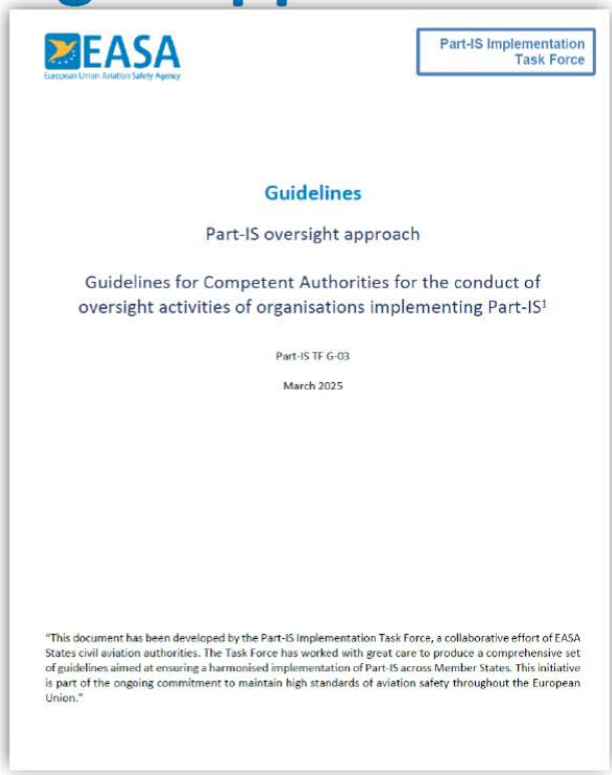


How to support?

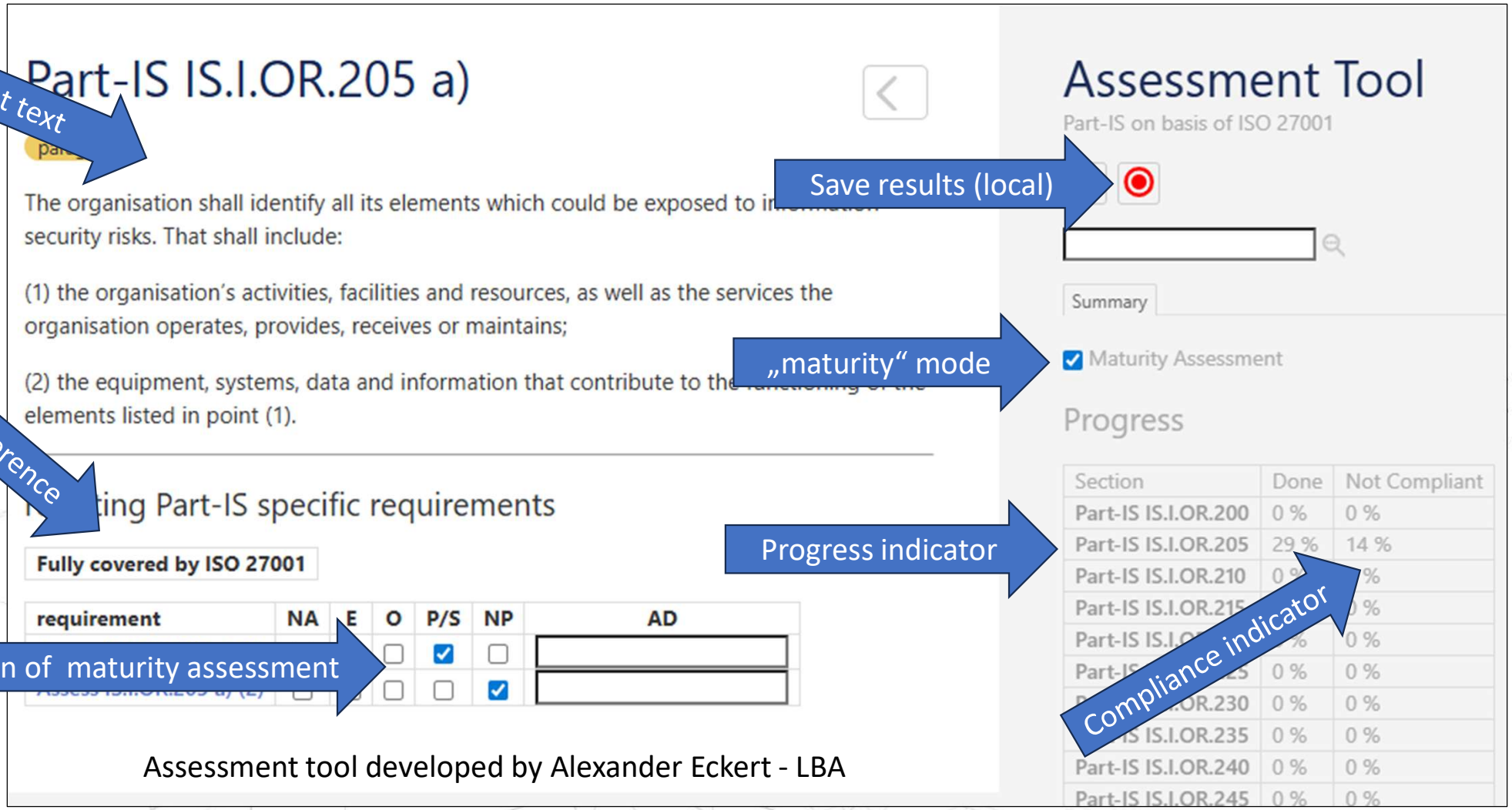
Bring the rule and the assessment criteria together





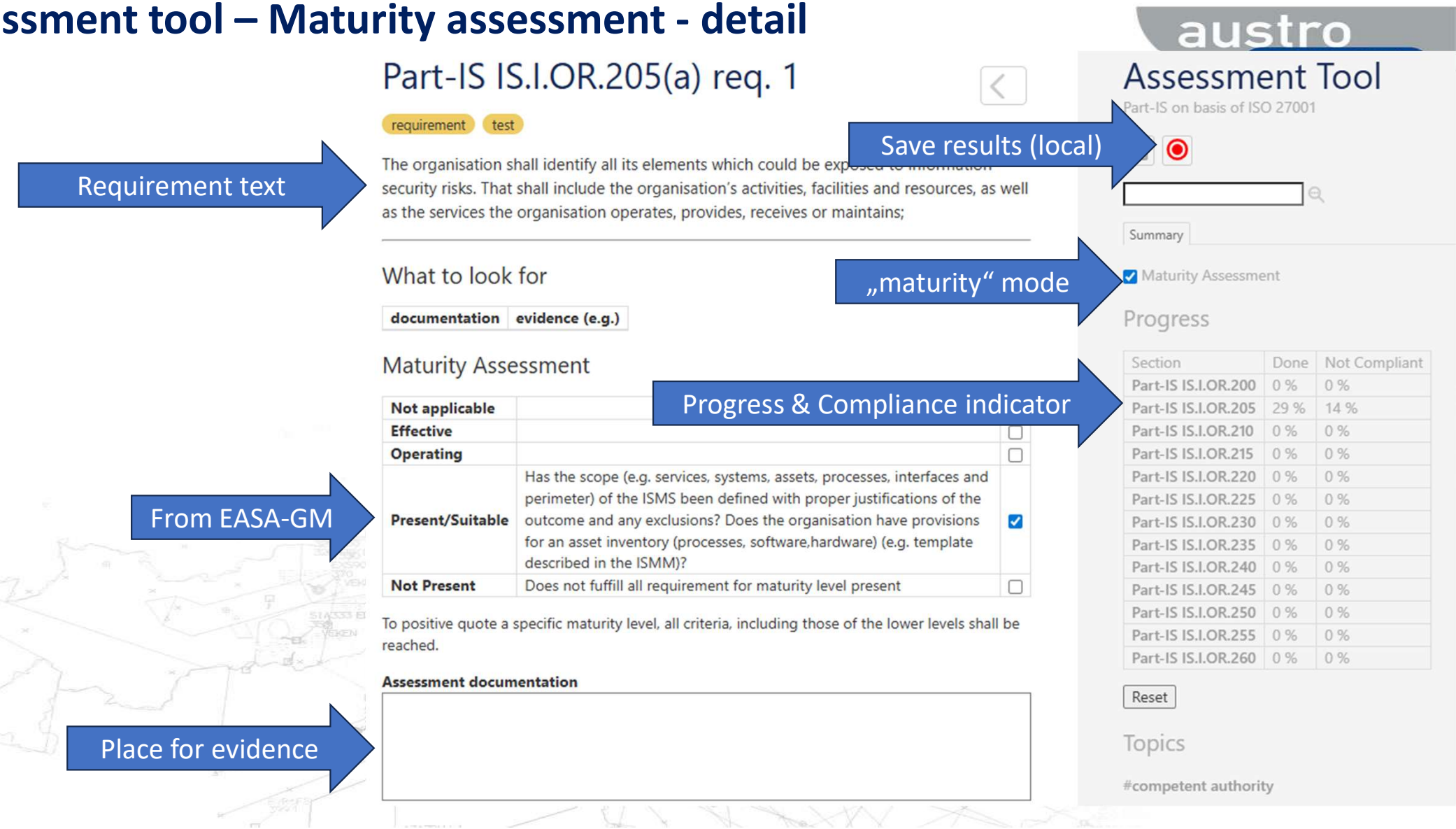


Assessment tool – Maturity assessment

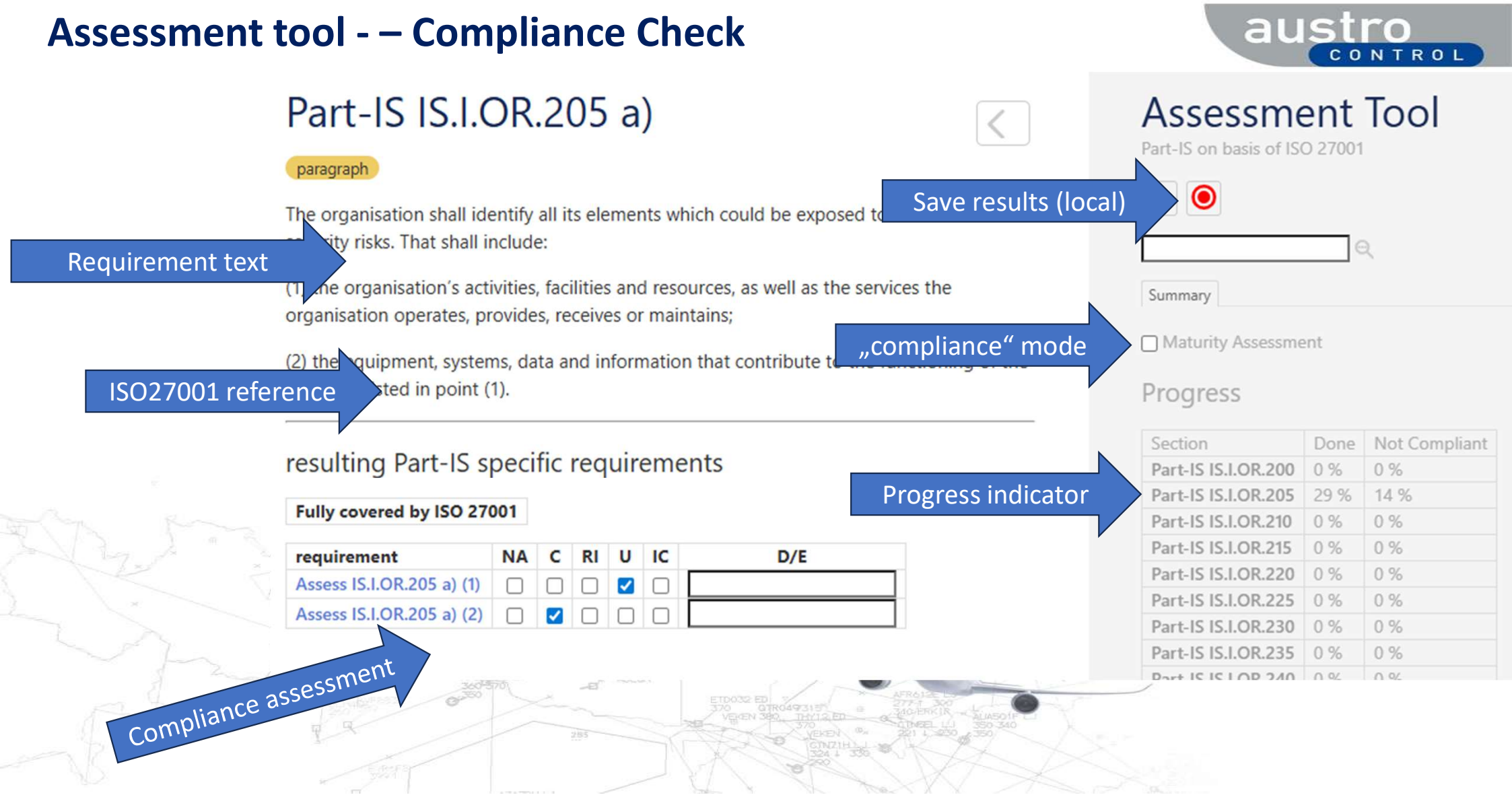


Assessment tool developed by Alexander Eckert - LBA

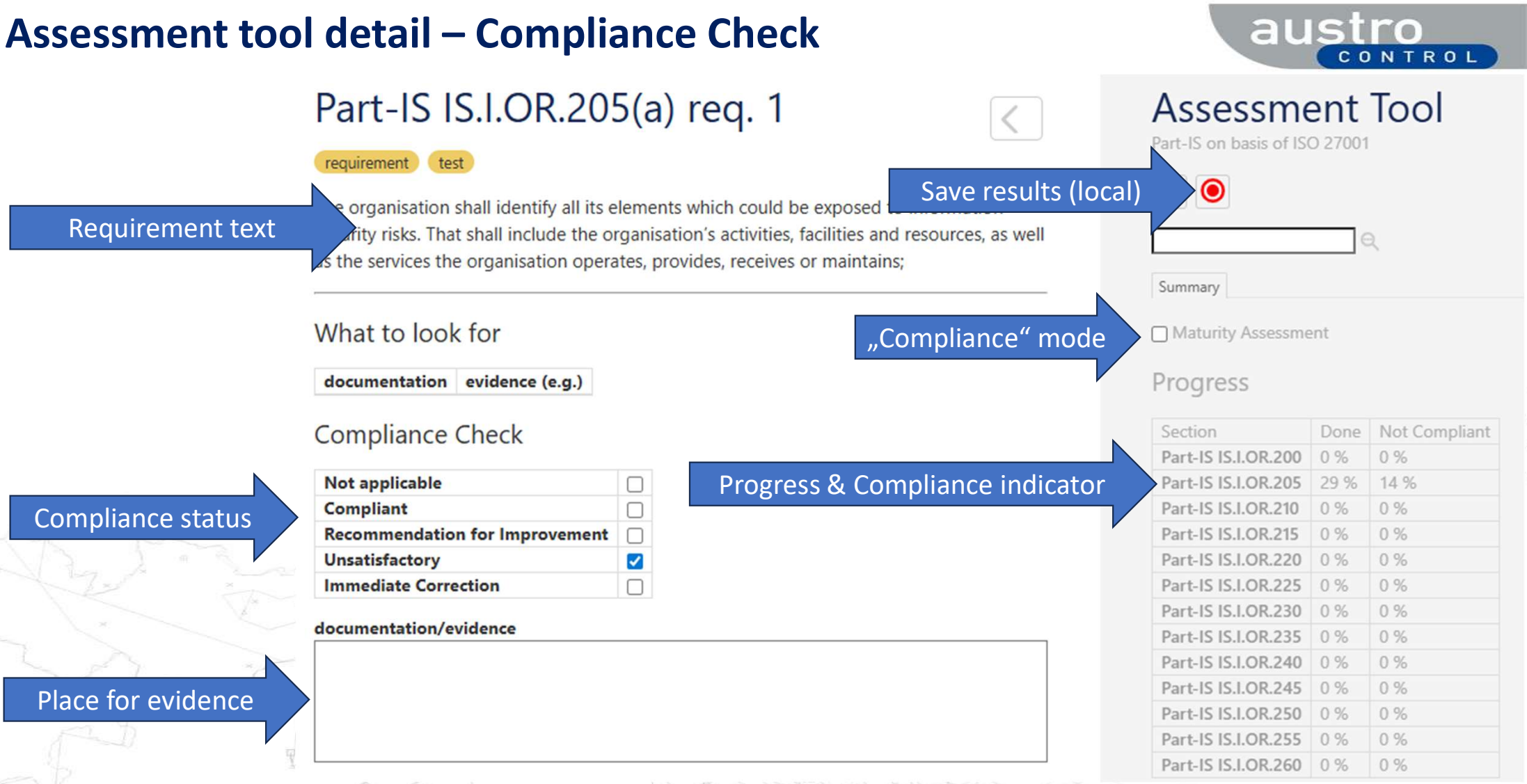
Assessment tool – Maturity assessment - detail



Assessment tool - – Compliance Check



Assessment tool detail – Compliance Check



Requirement text

Save results (local)

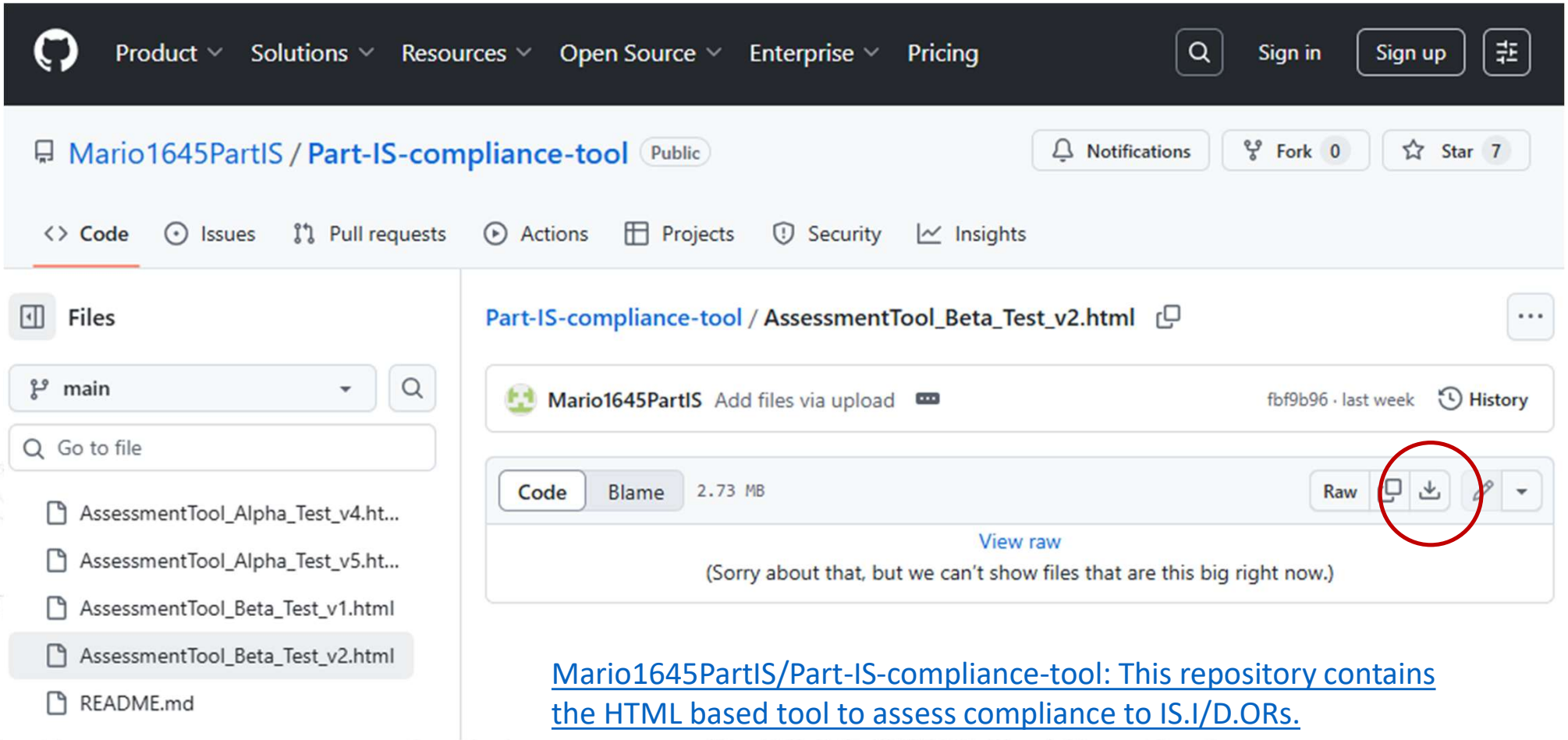
„Compliance“ mode

Progress & Compliance indicator

Compliance status

Place for evidence

Where to get it?

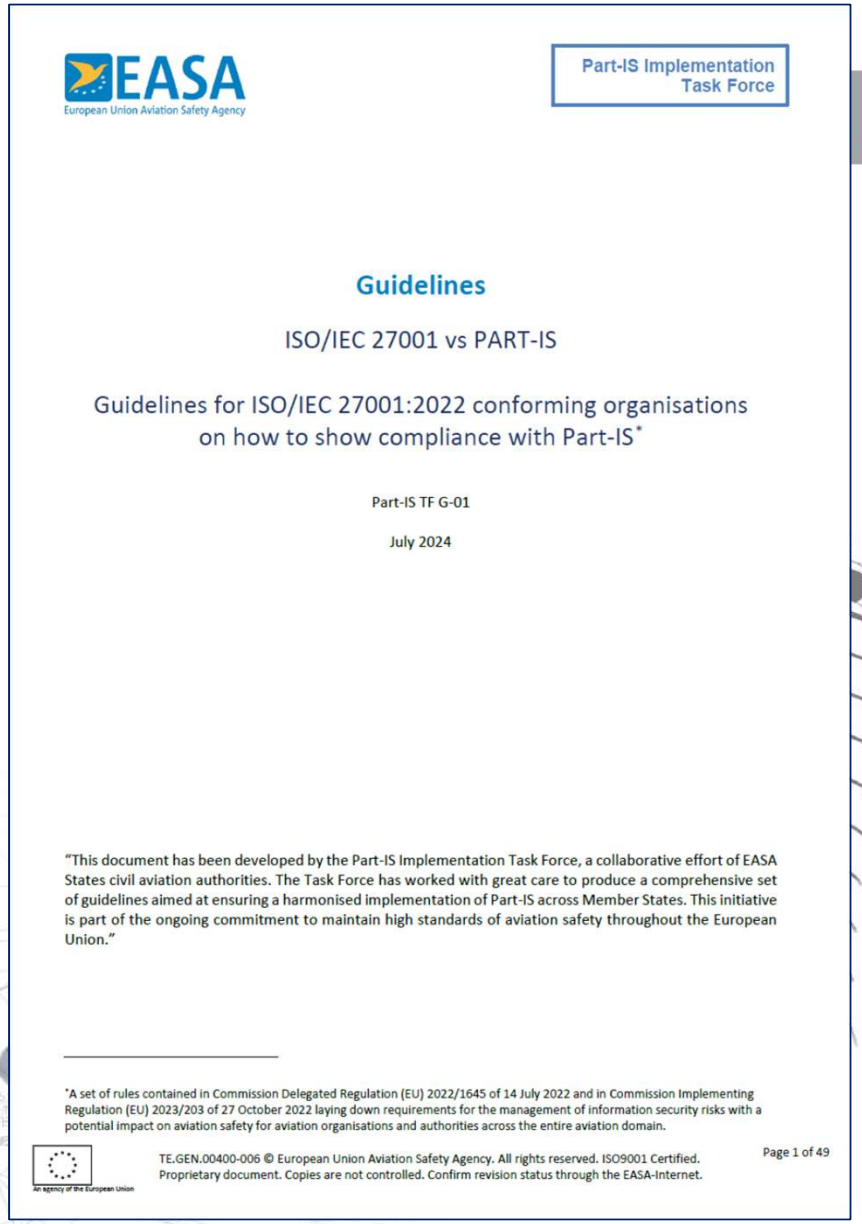


[Mario1645PartIS/Part-IS-compliance-tool: This repository contains the HTML based tool to assess compliance to IS.I/D.ORs.]

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.

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

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