

Part-IS Implementation

Workshop 2025

Cologne, June 25 - 26



Your safety is our mission.

Welcome to Day 2!

Thanks for being with us virtually and in presence



Part-IS Implementation Workshop

Part-IS Workshop agenda – Day 1

Opening speech - Introduction to the event

Welcoming you to our workshop

EASA

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

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

EASA, Lufthansa Cargo AG, SECONDO MONA

Proportional Implementation of Part-IS & indicators of complexity

This session will cover the proportionality elements of Part-IS implementation by describing the indicators of complexity that can be used to assess the implementation effort needed

EASA, Ryanair, ECOGAS

Q&A

Aviation product certification and Part-IS

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

EASA

Enhancing CTI & Information Sharing for Part-IS compliance

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

EASA

Meet the experts sessions (on-site only)

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

Q&A

EASA

Part-IS Workshop agenda – Day 2

Part-IS Task Force outcomes - Implementation tools and guidance

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

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

Oversight Approach – Overview and Q&A

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

EASA

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

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

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

Q&A

Part-IS Guidance Material (GM) update

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

EASA

Meet the experts sessions (on-site only)

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

Q&A

EASA

Part-IS Task Force outcomes - Implementation tools and guidance



Part-IS Implementation Workshop 2025



Hortensia Caballero is the Project Manager for EASA Part-IS implementation at AESA. She leads Spain's PART-IS regulation rollout and chairs the PART-IS Task Force with EASA and EU NAAs. She has recently been appointed as NATO CIVIL expert in Cybersecurity.

Hortensia has over 15 years of international experience in air traffic management, civil aviation security, and Cybersecurity, where she managed air traffic controller licenses and worked as an aviation safety oversight inspector and instructor in the NAA.



AGENCIA ESTATAL
DE SEGURIDAD AÉREA

PART-IS TASK FORCE

Progress update



Image created with AI

Part-IS TF Members



Kick off ---2023

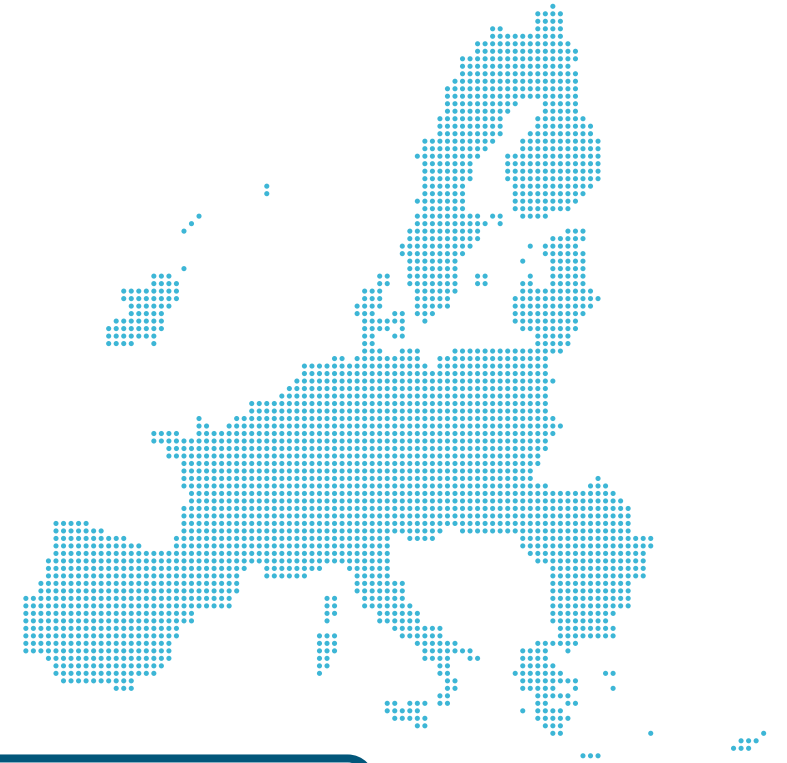
2025

2026



28 Competent Authorities

European Commission, EASA
and ENISA



Diversity of expertise, knowledge and perspective



Enhanced cooperation framework



Authority Collaboration

Monthly meetings between National Aviation Authorities



Policy clarifications

Discussion and clarification on building common understanding



Information sharing

Sharing experience about the practical implementation of REG and update the information of the related EU or ICAO WGs



Consistent approach

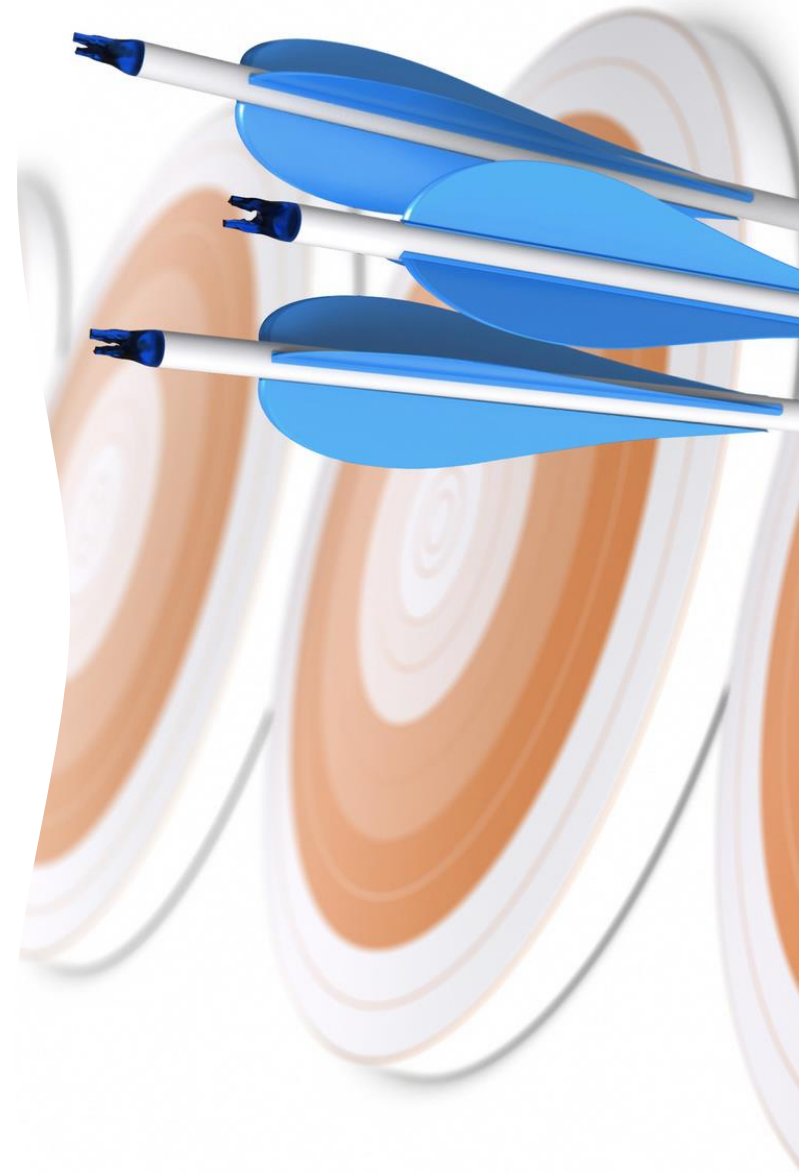
Proportionate and standardised oversight approach across Member States



Key achievements

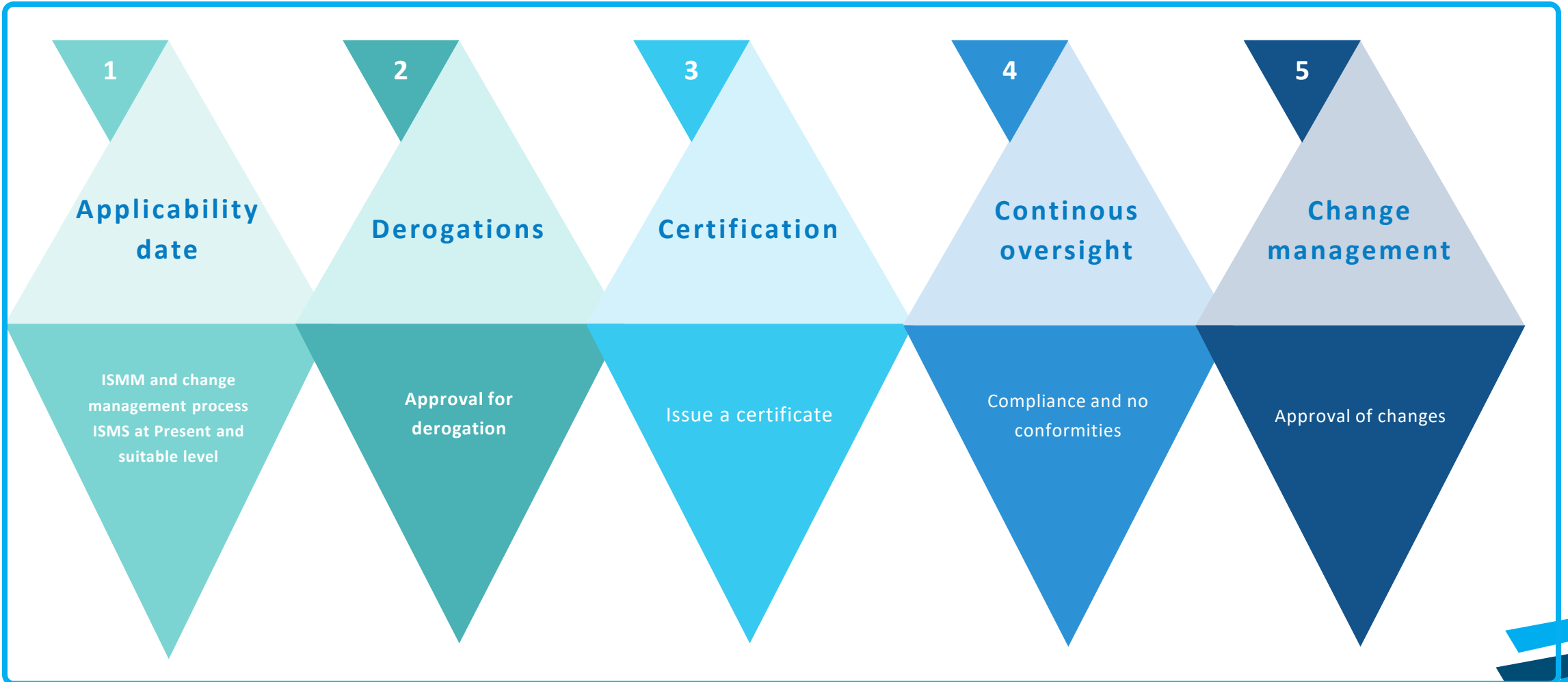
Publication of Guidance material

- 1 — **Guidelines for ISO/IE 27001:2022**
Document to support organisations with existing ISMS conforming to ISO/IEC 27001:2022 to integrate Part-IS into their existing ISMS
- 2 — **Implementation guidelines for derogation**
Standard process for organisations to apply for derogations and their assessment and approval by Competent Authorities
- 3 — **PART-IS oversight approach**
Framework for Competent authorities and aviation organisations to standardise and ensure implementation of REG EASA PART-IS



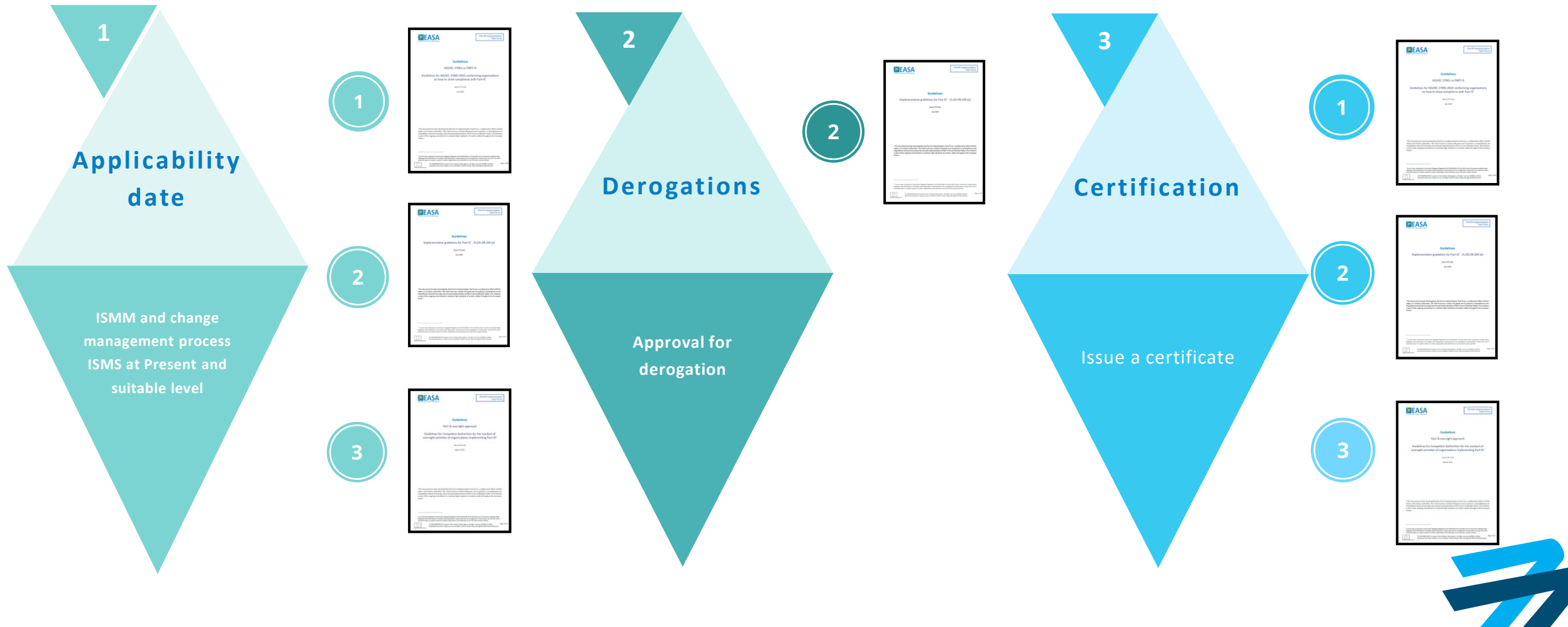
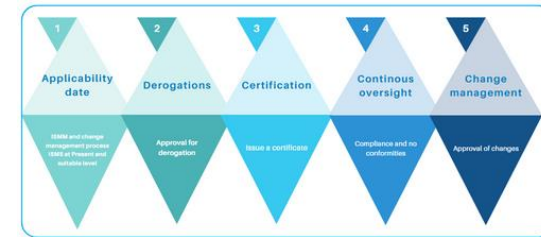
Key achievements

CAA key processes



Key achievements

CAA key processes



Main development initiatives



Progress Assessment Tool

Fostering the deployment of an assessment tool to monitor the organisation's compliance with PART-IS requirements



Policy Clarifications

Addressing policy queries to anticipate issues and discuss a harmonised understanding



NAA Inspector Training

PART-IS training objectives for performing oversight activities
Adopted EASA Train the Trainers for CAAs

All the achievements and initiatives address immediate needs while building long-term capacity. Each component strengthens the overall supervision framework.





Persistent Challenges

Harmonisation efforts

Slightly different approaches to requirements may exist across authorities. Harmonisation efforts and coordination continue to address these discrepancies

Regulatory Framework Integration

Part-IS must align with other aviation regulations. Complexity increases with multiple overlapping requirements

Limited resources

Specialised cybersecurity with potential impact on safety oversight requires expertise. Authorities can face staffing and training constraints





Next steps

Organisations prepare for the applicability date using published guidance

Authorities may adopt the initial oversight approach published

Further development of PART-IS oversight approach

Description of ISMS implementation at operating maturity level
by end 2025

Integration of Mapping of EU cybersecurity rules applicable to
aviation sector

Facilitate aviation sector to comply with EU legislation

Sharing experiences in the implementation phase to address the
issues identified appropriately

Collaboration mechanisms between Competent Authorities





PART-IS TASK FORCE



Building a resilient aviation cybersecurity ecosystem



@AesaSpain



www.seguridadaerea.gob.es



AESA





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

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

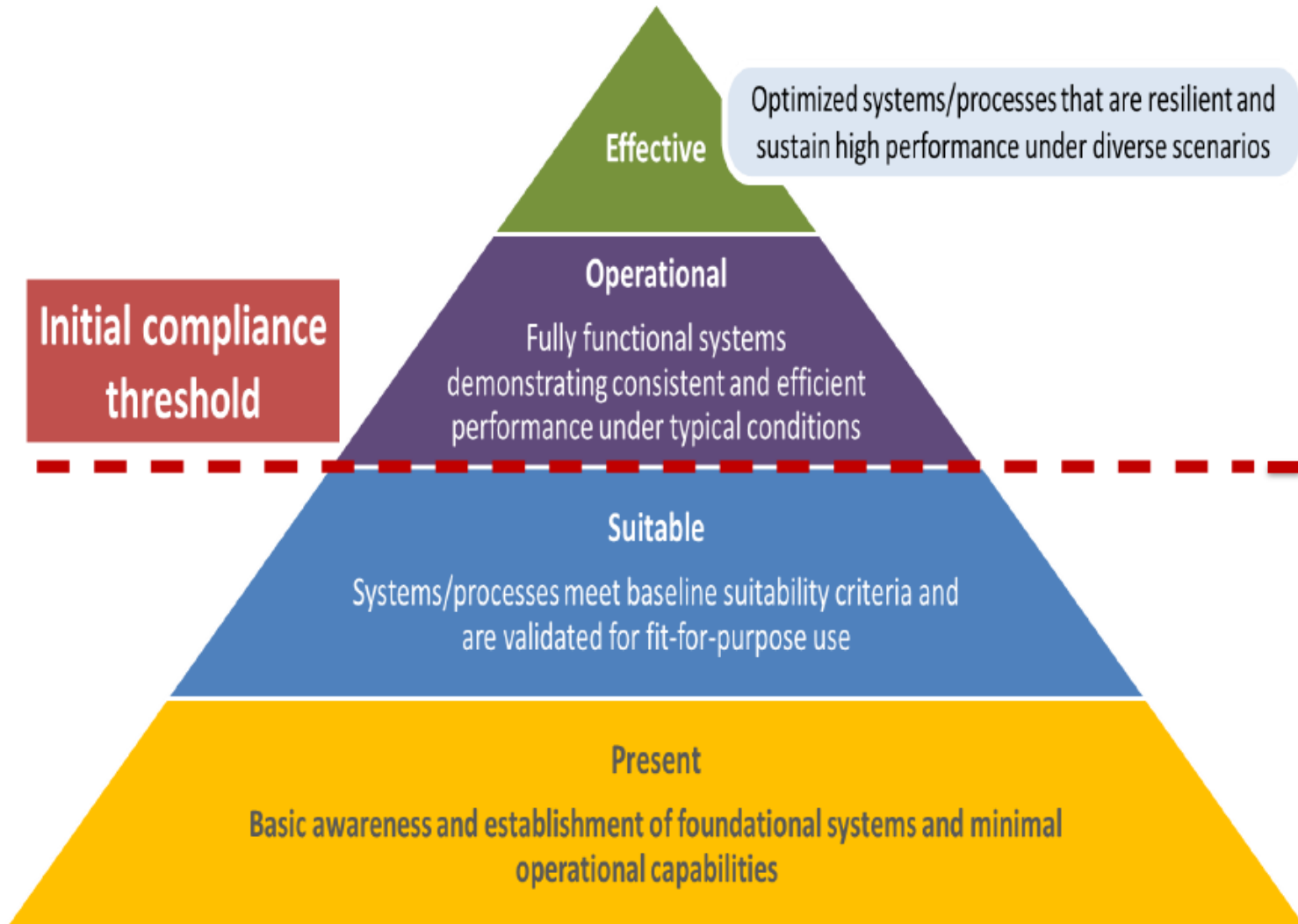
Part-IS Task Force outcomes – Implementation tools and guidance

25.06.2025

Mario Lenitz, Austro Control – Member of Part-IS Task Force



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



How to support?

Bring the rule and the assessment criteria together



Part-IS IS.I.OR.250 (b)

paragraph

The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority.

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.

resulting Part-IS specific requirements

Fully covered by ISO 27001
Continuous ISMM update

requirement	NA	E	O	S	P	NP	AD
ISMM approval	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ISMS initial approved
ISMM retention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	procedure in place
Providing amendments to authorities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	not implemented so far

Assessment Tool
Part-IS on basis of ISO 27001

☐ ☒

Summary

☒ Maturity Assessment

Progress

Part-IS IS.I.OR.200	0 %
Part-IS IS.I.OR.205	0 %
Part-IS IS.I.OR.215	0 %
Part-IS IS.I.OR.250	43 %
Part-IS IS.I.OR.255	0 %

Reset

Topics

#competent authority
#test



Assessment tool

Part-IS IS.I.OR.250 (b)

paragraph

The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority.

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.

resulting Part-IS specific requirements

Fully covered by ISO 27001

Continuous ISMM update

requirement	NA	E	O	S	P	NP	AD
ISMM approval	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ISMS initial approved
Providing amendments to authorities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	procedure in place
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	not implemented so far



Save results (local)



„maturity“ mode

Progress indicator

Assessment Tool

Part-IS on basis of ISO 27001

Summary

☒ Maturity Assessment

Progress

Part-IS IS.I.OR.200	0 %
Part-IS IS.I.OR.205	0 %
Part-IS IS.I.OR.215	0 %
Part-IS IS.I.OR.250	43 %
Part-IS IS.I.OR.255	0 %

Reset

Topics

#competent authority

#test

Assessment tool developed by Alexander Eckert - LBA

Assessment tool detail

Part-IS IS.I.OR.250 (b) req. 2



competent authority requirement

Requirement text

A copy of the initial issue of the ISMM shall be retained by the competent authority.

Save results (local)

What to look for

documentation evidence (e.g.)

„maturity“ mode

Maturity Assessment

Not applicable		
Effective	The retained copy of the initial issue of the ISMM is readily accessible and serves its intended purpose effectively within the competent authority.	<input type="checkbox"/>
Operating	There is confirmation that the competent authority has retained a copy of the initial issue of the ISMM.	<input type="checkbox"/>
Suitable	The retained copy of the initial issue of the ISMM is appropriate for the organization's scale and risk profile.	<input type="checkbox"/>
Present	A copy of the initial issue of the ISMM is documented and recorded as retained by the competent authority.	<input type="checkbox"/>
Not Present	Does not fulfill all requirement for maturity level present	<input type="checkbox"/>

From GM

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

Assessment documentation

Place for evidence

Assessment Tool

Part-IS on basis of ISO 27001

Summary

☒ Maturity Assessment

Progress

Part-IS IS.I.OR.215	0 %
Part-IS IS.I.OR.250	0 %
Part-IS IS.I.OR.255	0 %

Reset

Topics

#competent authority

Recently opened

× Part-IS IS.I.OR.250

× Part-IS IS.I.OR.250 (b)

× Part-IS IS.I.OR.250 (b) req. 2

× Home

close all



Assessment tool

Requirement text

Save results (local)

„compliance“ mode

ISO27001 reference

Progress indicator

Documentation of compliance assessment

Part-IS IS.I.OR.250 (b)

paragraph

The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority.

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.

resulting Part-IS specific requirements

Fully covered by ISO 27001

Continuous ISMM update

requirement	NA	C	RI	U	IC	D/E
ISMM approval	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ISMS initial approved
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	procedure in place
Providing amendments to authorities.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	not implemented so far

Assessment Tool

Part-IS on basis of ISO 27001



Summary

☐ Maturity Assessment

Progress

Part-IS IS.I.OR.200	0 %
Part-IS IS.I.OR.205	0 %
Part-IS IS.I.OR.215	0 %
Part-IS IS.I.OR.250	43 %
Part-IS IS.I.OR.255	0 %

Reset

Topics

#competent authority

#test

Assessment tool developed by Alexander Eckert - LBA

Where to get it?

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

austro
CONTROL

Part-IS-compliance-tool Public


main 1 Branch 0 Tags

Go to file




t

Add file

<> Code

 Mario1645PartIS Add files via upload

c5b4299 · 1 minute ago 4 Commits

 AssessmentTool_Alpha_Test_v4.html	Add files via upload	last week
 AssessmentTool_Alpha_Test_v5.html	Add files via upload	1 minute ago
 README.md	Update README.md	last week

README



Part-IS-compliance-tool

This repository contains the HTML based tool to assess compliance to IS.I/D.ORs stemming from European regulations 2022/1645 and 2023/2023.



Thank You for Your attention!

MARIO LENITZ

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

Official in charge Quality Management

Austro Control GmbH

Tel +43.51703.1906

Schnirchgasse 17

Fax +43(0)2061985024

1030 Wien



Juan Anton Bernalte is a Senior Expert in Continuing Airworthiness Organisations at EASA, with a Master's degree in Aeronautical Engineering. He brings nearly 20 years of experience at EASA, having held key roles such as DOA Section Manager, Cybersecurity Manager—where he led the development of Part-IS and ISMS regulation—and Maintenance Regulations Manager, overseeing Part-CAMO, Part-145, Part-66, and Part-147.

Prior to joining EASA, he spent almost 15 years in the aviation industry, including roles as Engineering and Quality Manager for Spanish airlines, three years managing maintenance of general aviation and fire-fighting aircraft, and four years at Boeing in Seattle working in manufacturing, assembly, and flight testing.

Oversight approach - Overview

25th / 26th June 2025

Part-IS Implementation Workshop

Juan ANTON BERNALTE

Senior Expert – Continuing Airworthiness Organisations

Your safety is our mission.

Guidelines published on 10 March 2025



Part-IS Implementation
Task Force

Guidelines

Part-IS oversight approach

Guidelines for Competent Authorities for the conduct of
oversight activities of organisations implementing Part-IS¹

Part-IS TF G-03

March 2025

Oversight policy main content

Implementation of ISMS in Aviation

Key steps in ISMS implementation and what matters in the foundation stage

Oversight Approach

Proportionality

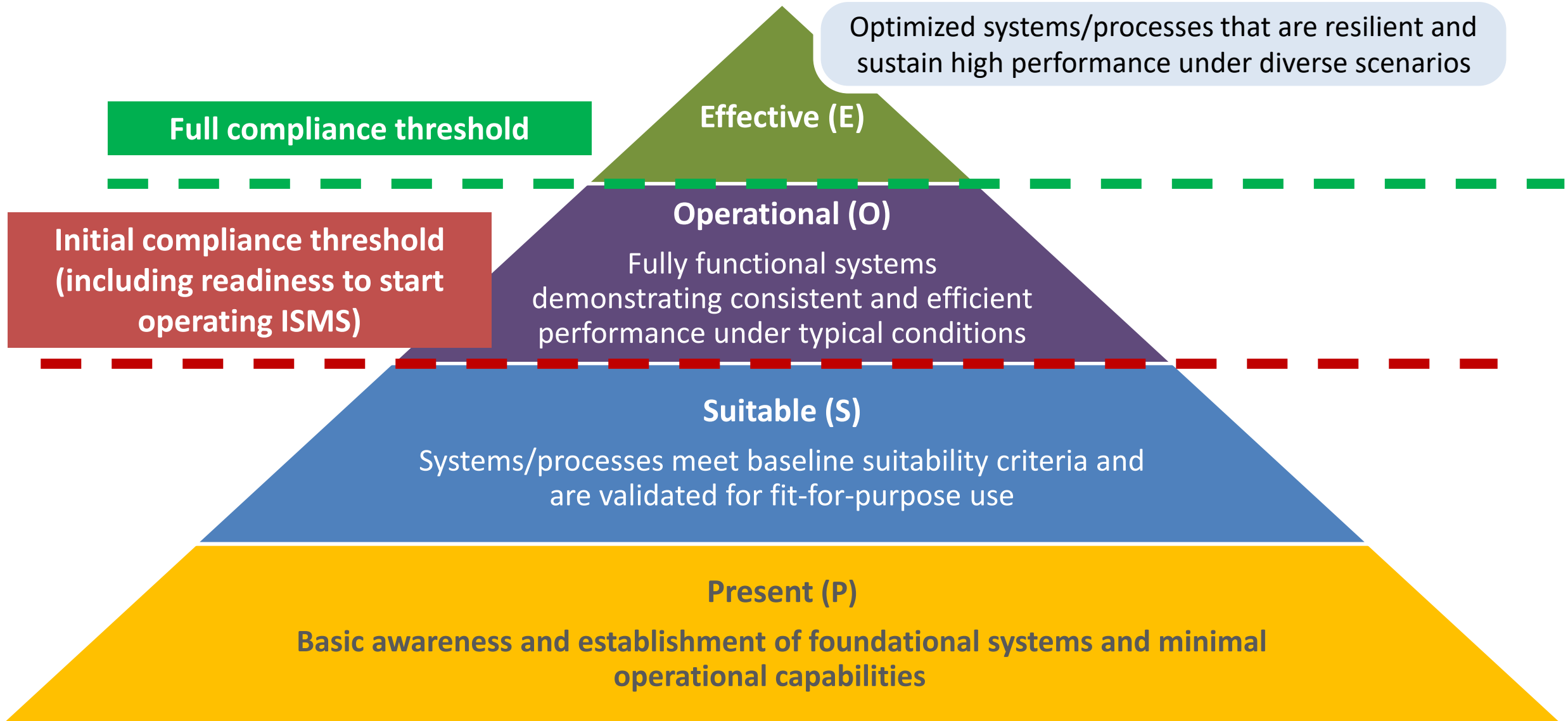
- Indicators of complexity
- Adapting certain aspects of ISMS implementation



A continuous process of growth and maturity

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

PSOE “Implementation Levels”



PSOE “Implementation Levels”

“Present” and “Suitable” levels correspond to the **“ISMS foundation” elements** indicated in the table above.

“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.

The **“Effective” level** corresponds to the subsequent **“continuous improvement” (ref. IS.I/D.OR.260)** that should be pursued by the organisation once compliance with the requirements has been achieved.

In the longer term, achieving higher maturity levels may increase the confidence of oversight authorities, which can have an impact upon the level of oversight activities regarding such organisation.

“PSOE Implementation Levels” vs “Maturity Levels”

To support the implementation of the “Continuous Improvement” requirements contained in points IS.I.OR.260 and IS.D.OR.260 of Part-IS, the concept of “maturity” is introduced.

Once the organisation has met full compliance (P, S and O), and they are in the “effective” phase, in order to continuously improve they need to:

- **Choose a Maturity Model** among those in GM1 IS.I.OR.260(a) and GM1 IS.D.OR.260(a) (or any other existing one).
- **Determine which is the maturity level** (in that Maturity Model) they have reached at the end of the Operational phase.
- **Continuously improve** (i.e. pursue increasing the maturity level).

Continuous Improvement (IS.I/D/OR.260) – Maturity Models (GM1 IS.I/D.OR.260(a))

Mapping to a five-level MM	C2M2	Eurocontrol NM	ISO 21827	NIST CSF 1.1
Initial	MIL 0	Non-Existent	Performed Informally	
Defined	MIL 1 (Initial)	Partial	Planned & Tracked	Partial
Implemented	MIL 2 (Identified)	Defined	Well defined	Risk-Informed
Managed	MIL 3 (Managed)	Assured	Quantitatively Controlled	Repeatable
Improved		Adaptive	Continuously Improving	Adaptive

Table 1: Mapping matrix of an existing MM to a hypothetical five-level MM

Responsibilities of organisations

Organisations should:

- Implement an ISMS at "Present and Suitable" level by the applicability date of Part-IS, and perform, by that date, a Compliance Monitoring activity to ensure that the organisation meets those requirements.
- Start operating such ISMS immediately after the applicability date.

NOTE: Organisations intending to apply for a derogation in accordance with point IS.I.OR.200(e) or IS.D.OR.200(e) and authorities involved in the approval of such derogations may refer to the document ["Implementation guidelines for Part-IS – IS.I/D.OR.200\(e\)"](#) developed by the Part-IS Implementation task Force.

Responsibilities of competent authorities

Competent authorities are responsible for assessing the implementation of ISMS.

A phased approach is proposed:

- The organisation will be deemed to have reached **full Part-IS compliance** once the authority has completed all the phases of investigation for “Present”, “Suitable” and “Operating” implementation levels.
- This process is not expected to be completed until well after the applicability date:
 - Once the organisation’s ISMS has been operating and producing results during a reasonable amount of time, and
 - the authority has performed the appropriate audits, assessments and inspections, and any findings have been addressed.

Initial documents to be submitted by the organisation

Submit the following to the competent authority “sufficiently” in advance of the applicability date:

1. The first version of their “Information Security Management Manual (ISMM)”, which may be integrated with other manuals or expositions already held by the organisation.
2. The procedure described under Part-IS points IS.I/D.OR.255 “Changes to the information security management system”. This procedure may be part of the ISMM or integrated into an existing change procedure.
3. An initial risk assessment identifying:
 - a. the organisation’s activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains
 - b. the equipment, systems, data and information that contribute to the functioning of the elements listed in point (a) above
 - c. the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks
 - d. The major risks and related threat scenarios, both internal and at the interfaces with other organisations
4. Evidence that internal compliance monitoring activities have taken place, describing the organisational level of compliance with all the criteria described in the columns “ISMM” and “Audit” of the checklist in the next slide, identifying any elements where the “Present” and “Suitable” level has not been reached and including a corrective action plan for those elements.

Checklist for “Present/Suitable” + readiness to start operating

Regulatory requirements	Elements to be assessed for “Present” and “Suitable” levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I/D.OR.240 Organisational structure	a) Has the structure been updated to reflect the ISMS (e.g. appointment of an information security manager, reporting structure)?	•	
	○ Is there a link between safety, security and information security functions?	•	•
	b) Where the organisation has decided to appoint a CRP (Common Responsible Person), does the person have sufficient capacity and delegated authority to effectively implement Part IS in the organisation?	•	•
	c) Has the organisation developed a framework/policy to address the different levels of trustworthiness of the workforce? Have the current staff been already assessed for trustworthiness?	•	•
	d) Has the organisation developed a competence framework and evaluation process? Have the current staff been already assessed for competence?	•	•

Checklist for “Present/Suitable” + readiness to start operating

Regulatory requirements	Elements to be assessed for “Present” and “Suitable” levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I/D.OR.200(a)(1) Information security policy	a) Has the organisation developed a clearly defined information security policy?	•	
	○ Is the purpose of the policy clearly stated?	•	
	○ Are the information security objectives defined?	•	
	○ Is the concept of aviation safety an integral part of the policy?	•	
	○ Is the content of the policy appropriate to the complexity of the organisation?	•	•

Checklist for “Present/Suitable” + readiness to start operating

Regulatory requirements	Elements to be assessed for “Present” and “Suitable” levels (including readiness to start operating the ISMS)	ISMM review	Audit
	○ Is there a reference to the organisation's information classification scheme?	•	
	b) Is the policy available to all staff/contracted parties and has been properly communicated?		•
	c) Have criteria been established for the review of the policy?	•	•
IS.I/D.OR.255 Change management	a) Has a procedure for change management been developed by the organisation and has the organisation applied for approval to the appropriate authorit(y/ies)?	•	
IS.I/D.OR.235 Contracted Information Security management activities	a) Has the organisation defined which IS management activities are contracted, if any, to third parties (Ref. IS.D/I.OR.235) and the appropriate contracts have been established?	•	•
	b) Are there procedures defining how the organisation is performing oversight of IS management contracted activities and managing any associated risk?	•	
	c) Has the organisation ensured appropriate access of the Competent Authority to the contracted parties and included this in the corresponding contracts?	•	•

Checklist for “Present/Suitable” + readiness to start operating

Regulatory requirements	Elements to be assessed for “Present” and “Suitable” levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I/D.OR.205(a) and (b) Scope of the ISMS	a) 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?	•	•
IS.I/D.OR.205 and 210 Risk management	a) Has a formal process for information security risk management been established?	•	
	○ Are there the three main processes or procedures (i.e. Risk identification, Risk assessment and Risk treatment) defined within the risk management context?	•	
	○ Are risk acceptability criteria and responsibilities clearly defined?	•	
	b) Has the organisation defined how the risks related to operational contractors/suppliers will be managed (this does not include contracted Information Security management activities covered by points IS.I.OR.235 and IS.D.OR.235, which are addressed further below in this table)?	•	•
	c) Has the organisation performed an initial risk assessment (e.g. major risks and related threat scenarios both internal and at the interfaces)?	•	•
	d) Does the organisation have provisions for an asset inventory (processes, software, hardware) (e.g. template described in the ISMM) ?	•	
	e) Has the organisation already included the applicable assets in the inventory?		•
	f) Has a formal process for information security risk management been established?		•

Checklist for “Present/Suitable” + readiness to start operating

Regulatory requirements	Elements to be assessed for “Present” and “Suitable” levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I/D.OR.220 Incident management (Detect, Respond, Recover)	a) Are there procedures in place to detect information security incidents, including monitoring mechanisms for potential threats?	•	
	b) Are there procedures in place to respond to detected incidents in a timely manner (e.g., initial containment measures)?	•	
	c) Are there procedures in place to recover from incidents and to return to proper safety level after an incident?	•	
	d) Are the implemented measures adequate and suitable to respond to and recover from information security incidents?		•
IS.I/D.OR.215 and 230 Internal and External Reporting	a) Are there procedures for reporting of events within the organisation and from external parties? Are the staff and external parties informed about such procedures?	•	•
	b) Are there procedures and responsibilities defined for evaluation of events and decision of which ones have to be considered incidents or vulnerabilities?	•	
	c) Has the organisation developed a procedure to identify which incidents and vulnerabilities have to be reported through the external reporting system?	•	
	d) Have procedures for external reporting been defined (including all the stages of reporting, root cause analysis, follow up etc.)?	•	
	e) Are the staff involved in the processing of internal and external reports properly identified, trained and authorized?		•

Checklist for “Present/Suitable” + readiness to start operating

Regulatory requirements	Elements to be assessed for “Present” and “Suitable” levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I/D.OR.245 Record keeping	a) Are there procedures defining which records are retained, the retention period and the format of those records?	•	
	b) Has the organisation defined the appropriate records protection (e.g. against damage, alteration, theft, unauthorised access etc.)	•	•
IS.I/D.OR.200(a)(6) and (a)(7) Measures and findings notified by the competent authority	a) Has the organisation defined procedures to implement measures notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety?	•	
	b) Has the organisation defined procedures to address findings notified by the competent authority?	•	
IS.I/D.OR.200(a)(13) Protection of the confidentiality of information received from other org’s	a) Has the organisation defined procedures to protect the confidentiality of information received from other organisations, according to its level of sensitivity?	•	
IS.I/D.OR.200(a)(12) Monitoring of compliance with Part-IS requirements	a) Has the organisation made available an internal compliance monitoring report, describing the organisational level of compliance with all the criteria described in the columns “ISMM” and “Audit” of this table?	•	

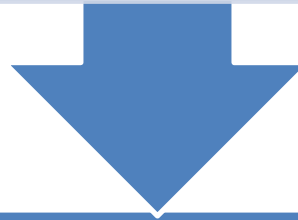
Initial investigation by the Authority

Phase 1 (if possible, before deadline)

Review and comment the Risk assessment

Review and approve the ISMM
(use column ISMM in checklist above)

Review and approve the indirect approval procedure

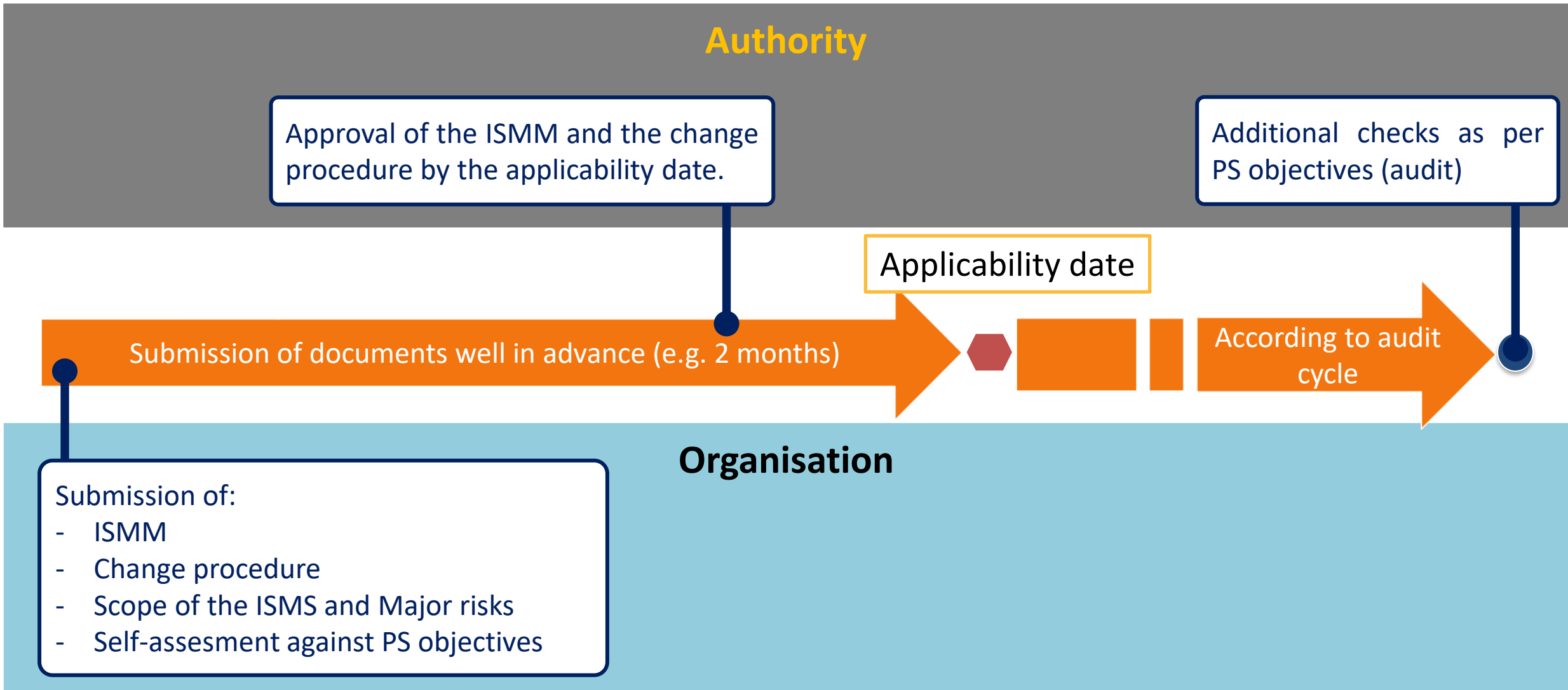


Phase 2 (during oversight cycle)

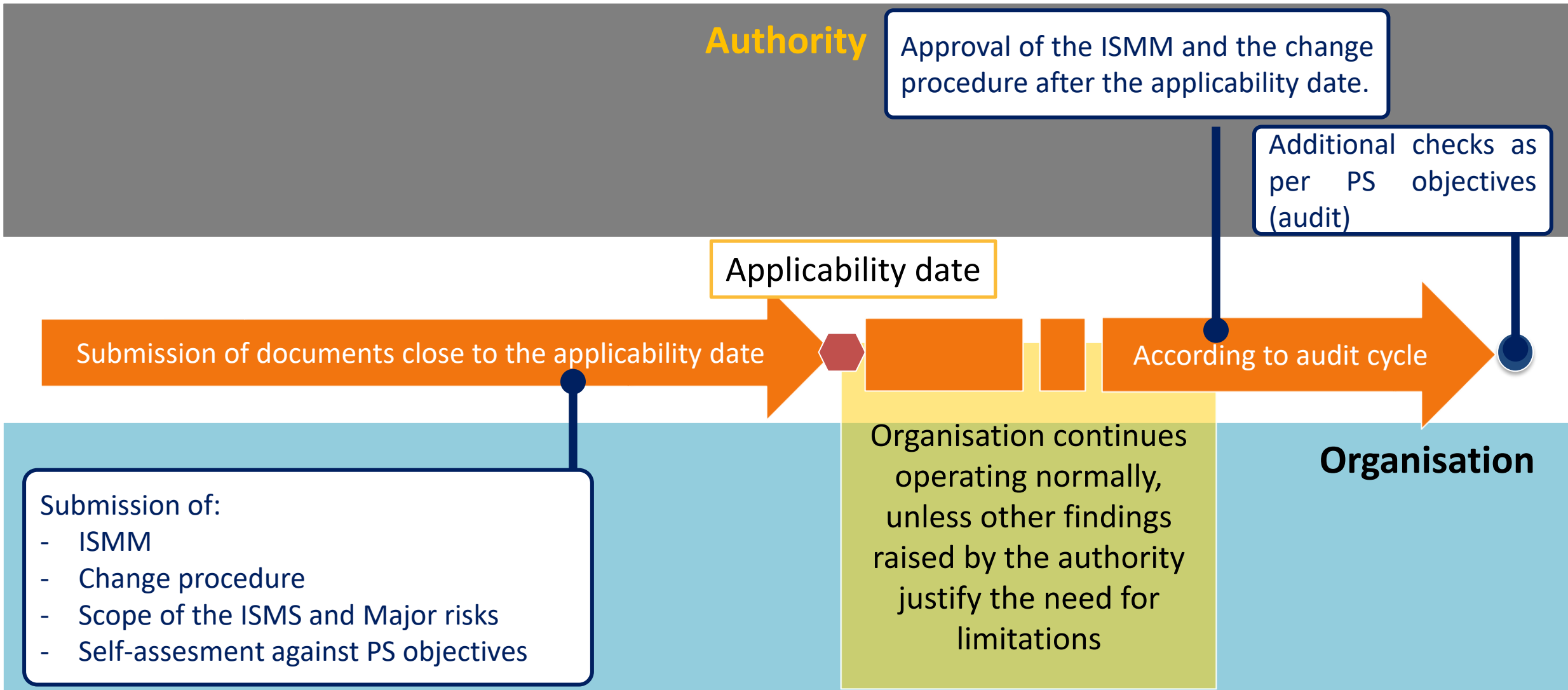
Audit the organisation for P+S level (use column "Audit" in checklist above)

Verify the organisational arrangements

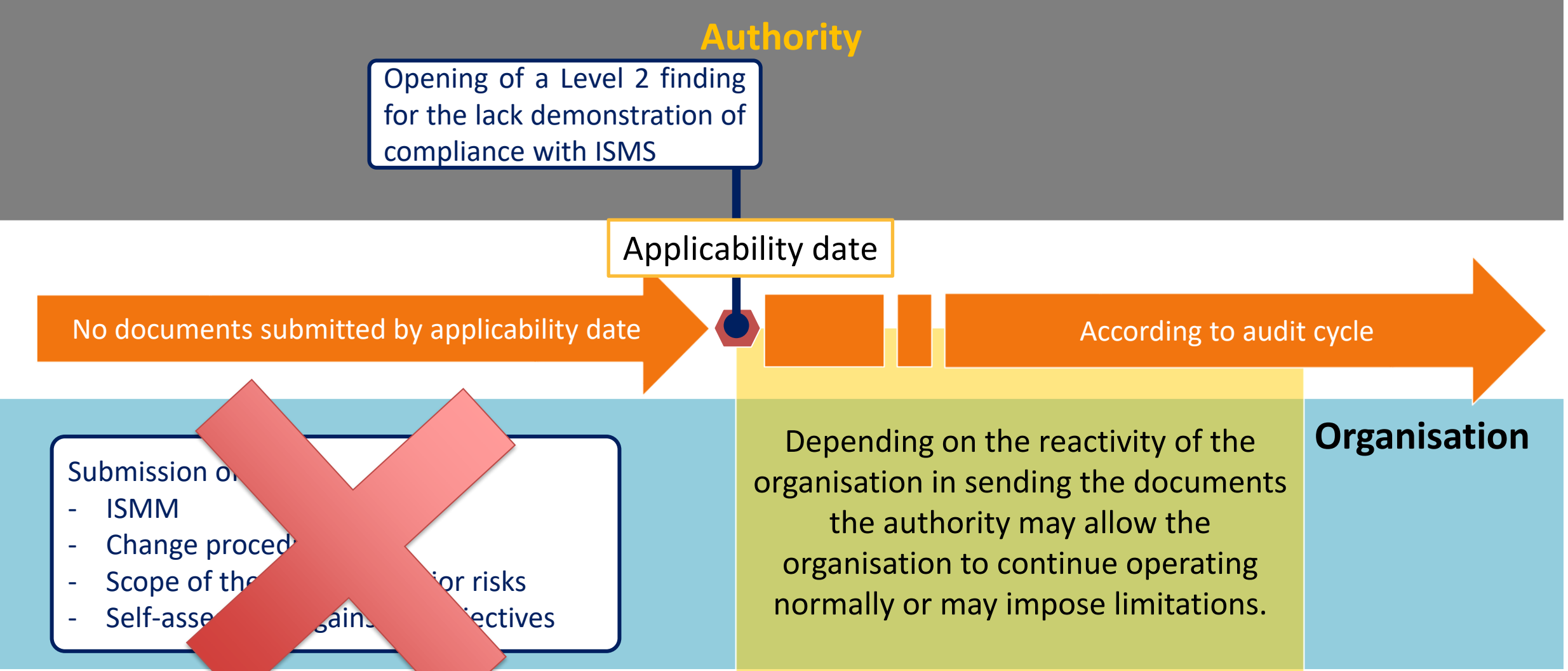
Initial investigation (P+S) – Case 1



Initial investigation (P+S) – Case 2



Initial investigation (P+S) – Case 3



Approval of the ISMM

- As required by Part-IS points IS.I/D.OR.250(b) “*Information security management manual (ISMM)*”, the first issue of the ISMM shall be approved by the competent authority.
- The administrative method used to grant approval of the ISMM (e.g. official letter, etc) will be decided by each competent authority, possibly following similar procedures already used for the approval of the current manuals and/or expositions held by those organisations.
- In those cases where the organisation has integrated the elements of the ISMM in an existing manual/exposition already held by the organisation (e.g. inside the POE for Production Organisations, or inside the MOE for Maintenance Organisations), the approval of the elements related to Part-IS may be granted by approving the revision of the manual/exposition where they have been integrated.
- In the case of organisations holding multiple approvals, the elements of the ISMM may be integrated in a single manual/exposition.

Approval of the indirect approval procedure for changes of the ISMS

As required by Part-IS points IS.I/D.OR.255(a), this procedure shall be approved by the competent authority.

When approving this procedure, the competent authority is expected to pay particular attention to the following:

- The procedure clearly describes the roles and responsibilities of the staff involved in the proposal, analysis, evaluation of impacts, agreement and authorization of the changes.
- The level of understanding of the organisation of the Part-IS requirements by evaluating the completeness and accuracy of the compliance monitoring activities described in point 4 above and by assessing the relevance of the initial risk assessment provided by the organisation in accordance with point 3 above.

The method used to grant approval of this procedure (e.g. official letter, etc) will be decided by each competent authority.

Change Management – Notification examples

Changes with an impact on the ISMS

The organisation integrates another company within its organisational structure

The organisation has identified non-conformities indicating an incorrect scope

The organisation contracts information security management activities as per IS.OR.235

The organisation implements changes to their risk treatment methodology

The organisation changes its incident recovery procedure

Changes with no impact on the ISMS

The organisation replaces the software tool for encrypting sensitive files with another S/W solution

The organisation decides to update an existing preventive control e.g. configuring a new firewall in its internal network

Update in the staff training programme and/or training content as a result of the continuous improvement processes established within the organisation

Future additional guidance

The “Part-IS Implementation Task Force” will develop in the coming months further guidance/checklist for the oversight of the “Operational” Phase.

Proportionality and Complexity Indicators

No clear distinction between complex and non-complex organisations, rather there are elements that, on their own, can influence certain aspects of a proportionate ISMS implementation

Where the organisation is placed in the functional chain and the number and criticality of interfacing organisations/stakeholders

The **complexity of the organisational structure and hierarchies** (e.g. number of staff, departments, hierarchical layers, etc)

The **complexity of the information and communication technology systems and data** used by the organisation and their connection to external parties.

Findings

Inspector raises findings in accordance with the relevant rules for each domain

The organisation addressing the finding shall:

- **Identify the root cause or causes of, and contributing factors to, the non-compliance;**
- **Define a corrective action plan;**
- **Demonstrate the correction of the non-compliance to the satisfaction of the competent authority.**

Those actions shall be carried out within a period agreed with the authority

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



Part-IS Implementation Workshop 2025



Jose DEL CARMEN is a Policy Officer seconded to the European Commission's DG MOVE, working on transport security and cybersecurity strategies.

With over 14 years of experience in public administration, he previously led the AVSEC Technology and Cybersecurity Department at the Spanish Civil Aviation Authority, where he coordinated national cybersecurity efforts and developed threat detection policies.

Jose holds master's degrees in Cybersecurity and Aeronautical Engineering, and a degree in Aerospace Engineering. His background combines technical expertise with strategic policy development, with a strong focus on international cooperation and regulatory innovation in the transport sector.



Juuso Järviniemi is a Policy Officer at the Cybersecurity & Digital Privacy Policy unit of DG CNECT (Communications Networks, Content and Technology). His areas of responsibility include implementation of the NIS2 Directive and other files related to the cybersecurity of critical sectors. Prior to joining the Unit in June 2023, he worked at the Directorates-General for Informatics (DG DIGIT), and for neighbourhood and enlargement (DG NEAR). Juuso Järviniemi holds an MA degree in European Political & Governance Studies, and an MA degree in International Relations.

Mapping of EU Cybersecurity Rules applicable to the aviation sector

AVIATION CYBERSECURITY SUBGROUP

26 June 2025

Juuso JARVINIEMI (CNECT H2)

Jose DEL CARMEN MELERO (MOVE A5)

Interplay between NIS2, AVSEC and SAFETY

NIS2 Recital 29:

*In order to avoid gaps between or duplications of cybersecurity obligations imposed on entities in the aviation sector, national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139 of the European Parliament and of the Council and the **competent authorities under this Directive should cooperate** in relation to the implementation of cybersecurity risk-management measures and the supervision of compliance with those measures at national level.*

The compliance of an entity with the security requirements laid down in Regulations (EC) No 300/2008 and (EU) 2018/1139 and in the relevant delegated and implementing acts adopted pursuant to those Regulations could be considered by the competent authorities under this Directive to constitute compliance with the corresponding requirements laid down in this Directive.

Why an Aviation Cybersecurity Subgroup

- Increasing complexity of the EU regulatory landscape affecting aviation cybersecurity.
- Harmonised and effective application of existing legal frameworks, ensuring coherent implementation of both horizontal and sector-specific rules.
- Clarifying obligations, avoiding duplication, and enhancing coordination across competent authorities.
- Brings together Member States, EASA, ENISA, DG CONNECT, and DG MOVE.
- No new rules, but assists interpretation and implementation of existing frameworks.
- Created by the Aviation Cybersecurity Working Group, anchored in the NIS Cooperation Group (DG CONNECT) and the AVSEC Committee (DG MOVE). Launched in Nov 2023. Operational from Feb 2024.

Scope of the subgroup

- EU-level applicability to aviation organisations
- Key regulatory frameworks.
- Clarify obligations and prevent duplication
- Harmonised application across EU Member States
- Mapping of obligations, oversight, and reporting lines



- Regulation 2019/1583: aviation security requirements



- PART-IS Regulations: aviation safety requirements



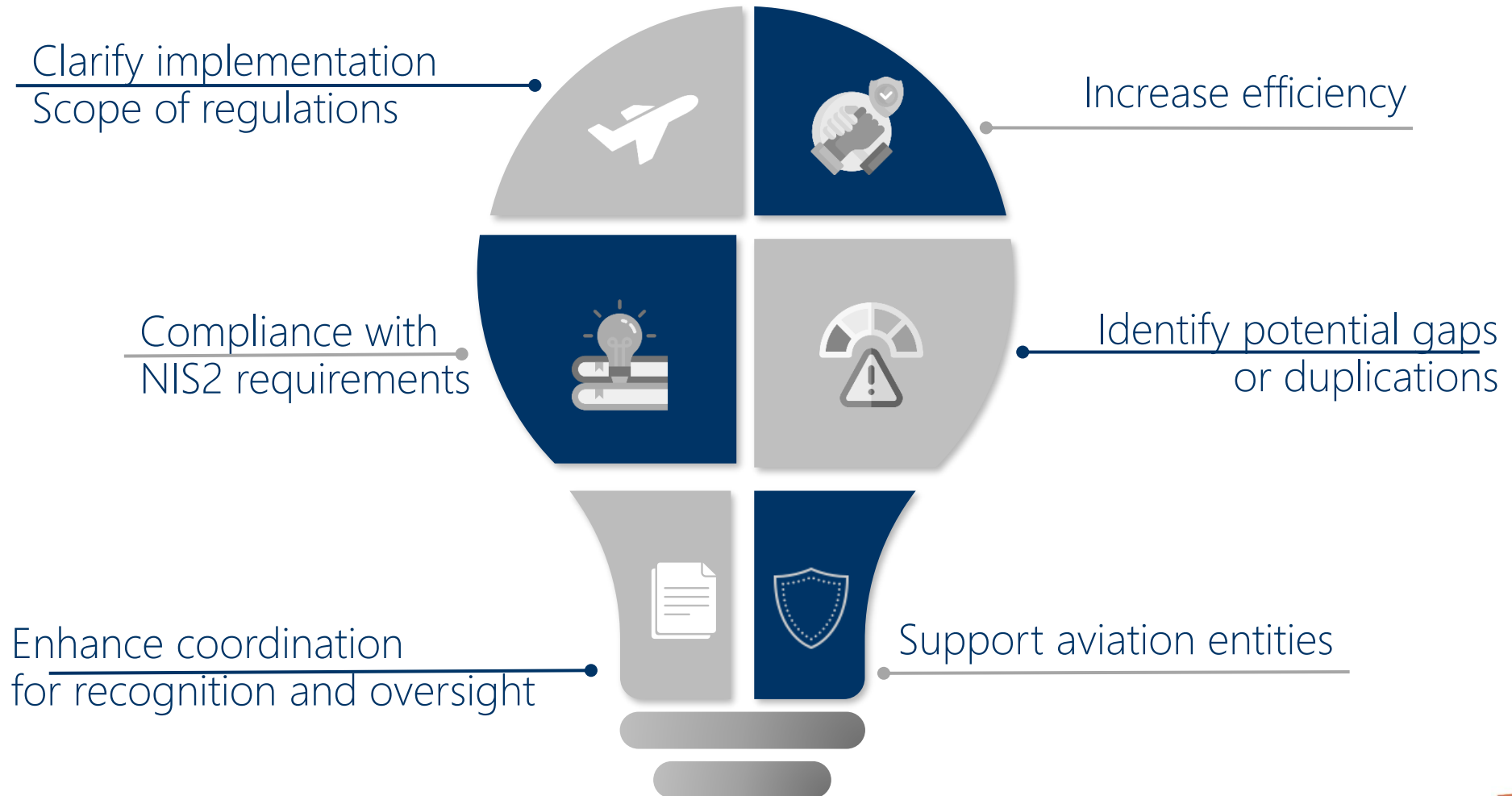
- NIS/NIS2 Directive: cross-sectorial general requirements



Governance & Collaboration

- Co-chaired by DG MOVE and DG CONNECT.
- Strong support from EASA and ENISA.
- Neutral and inclusive forum: for national authorities and EU agencies.
- Cross-disciplinary representation: safety, security, and cybersecurity domains.
- Joint reviews, align regulatory interpretations and shared implementation practices.
- Dedicated Task Forces.
- Collaborative and iterative approach based on consensus.

Key principles



NIS2 – Security measures & Incident reporting requirements

- **Article 20:** Accountability for top management for non-compliance with cybersecurity risk management measures
- **Article 21:** Risk-based approach: appropriate and proportionate cybersecurity measures
- **Article 21:** Defining a minimum set of measures
 - For example risk analysis and information security policy, incident handling, business continuity, supply chain security

(**Article 23:** Reporting of significant incidents)

For further illustration,
see Implementing
Regulation 2024/2690

Subgroup Task Forces

Task Force 1.1 – Scope and Applicability

- Led by Eleanor Travers (Ireland).
- Clarifies which aviation entities are subject to NIS2, Part-IS, and AVSEC.
- Analyses legal definitions and oversight responsibilities.

Task Force 2.1/3.1 – Mapping and Implementation

- Led by Katharina Garbe (Germany).
- Compares regulatory obligations across the three frameworks.
- Identifies overlaps, gaps, and compliance challenges.
- Proposes harmonised implementation approaches.

Meetings & Timelines

- 8 plenary meetings held between February 2024 and April 2025.
- Each meeting built on previous discussions, progressively shaping the guidance material and refining task force outputs.
- Milestones include the launch of task forces and agreement on mapping methodologies



First Draft Version Document

- **Section 1 – Applicability:**
 - Overview of each regulation’s scope.
 - Mapping of obligations to specific types of aviation entities.
 - Explanation of regulatory triggers
- **Section 2 – Requirements Mapping:**
 - Side-by-side comparison of obligations
 - Identification of overlaps and differences across the frameworks.
- **Section 3 – Implementation Guidance:**
 - Practical recommendations and good practices.
 - References to ENISA, EASA, and EU guidance—no duplication of content.
- **Annexes:** Definitions and glossary. Stakeholder mapping table.



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

Next steps

- **Second part on incident reporting obligations**
- **Consolidation** of feedback and final drafting in Q3 2025
- **Final version to be submitted to the NIS CG** (Q4 2025),
- **Non-binding reference document**
- **Aviation Cybersecurity Working group** (2026)


Thank you





Eleanor Travers is the Head of Aviation Security with the Irish Aviation Authority (IAA). Information security regulation for the aviation sector in Ireland for both safety and security is entirely within the remit of the Authority and upon transposition of the NIS 2 Directive, regulatory oversight will transfer to the Authority also.

Eleanor's role in the IAA includes the internal coordination on these matters as well as engaging at European and ICAO level on this topic



Mapping of EU cybersecurity rules applicable to the aviation sector

Part IS Workshop 26/06/2025

Eleanor Travers, Irish Aviation Authority (IAA)

Overview

- Organisation
- Task Force 1.1
- Consultation



Organisation

Aviation Subgroup

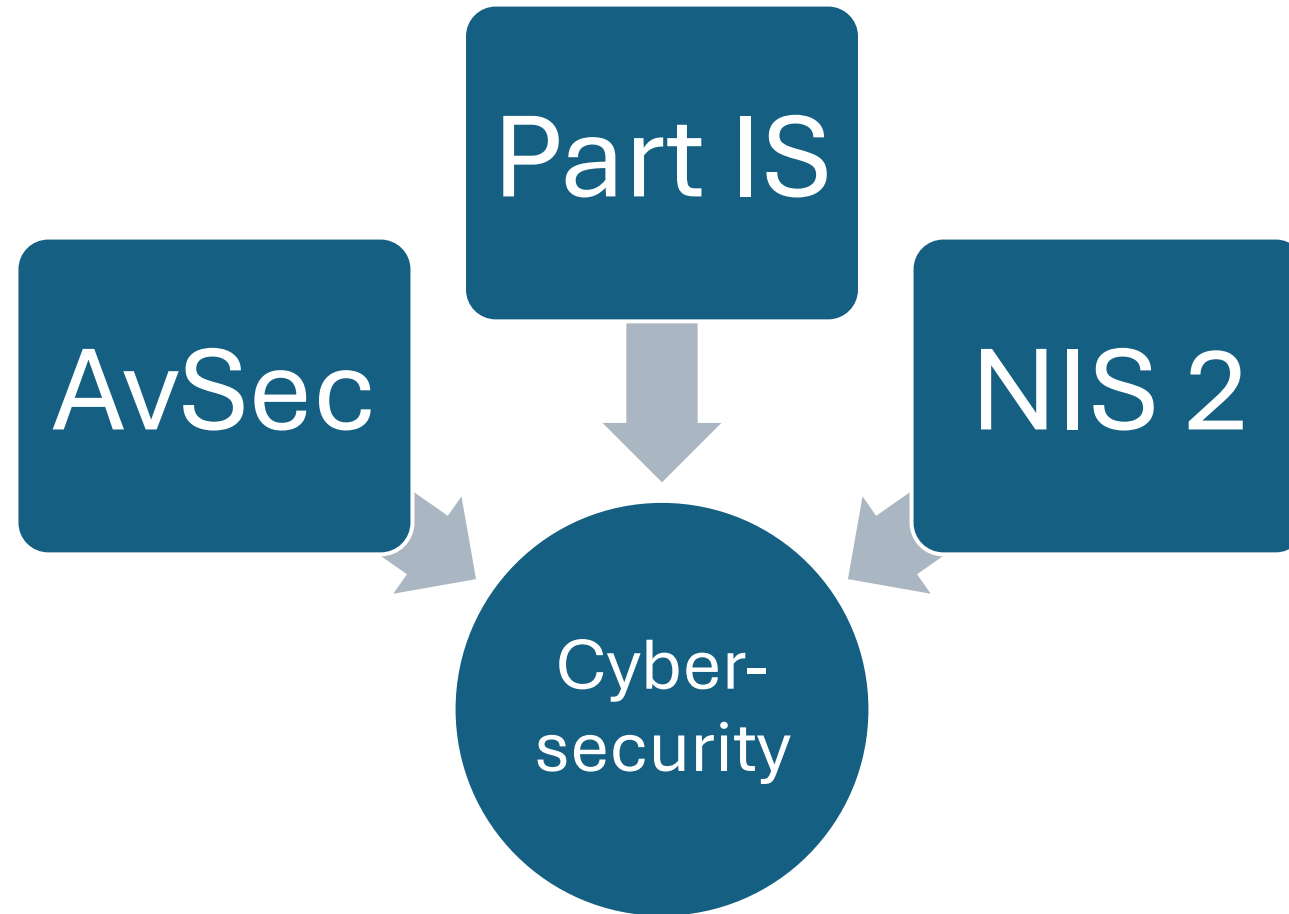


Task Force 1.1: Regulated entities



Task Force 2.1/3.1: Mapping

Regulatory contexts



Process and timeline

Mapping Exercise



```
graph TD; A[Mapping Exercise] --> B[Guidance Material]; B --> C[Merge of Document]; C --> D[Consultation];
```

Guidance Material

Merge of Document

Consultation

Objectives for the Task Force

- Identification and assessment of application of measures to aviation sector entities
- Tool for Member States: to clarify the applicable regulatory requirements including ISMS, risk assessment and incident reporting
- Provide remarks and recommendations for Member States

Example

ENTITY TYPE	AvSec	PART-IS	NIS 2
	CAIS DEFINITION		
AIRPORT OPERATOR – NON- DEROGATED AERODROME	✓	✓ APPLIES TO AERODROME OPERATORS	✓ APPLIES TO AIRPORT MAN- AGING BODIES IF NIS 2 CRITE- RIA* ARE MET <u>ADDITIONAL NA- TIONAL CRITE- RIA MAY APPLY</u>
AIR CARRIER – AOC ISSUED BY EU STATE	✓	✓	✓ IF NIS 2 CRITE- RIA* ARE MET NIS 2 DOES NOT DISTINGUISH ON THE BASIS OF THE STATE




Mapping of EU cybersecurity rules applicable to the aviation sector

Part IS Workshop, 26/06/2025



Katharina GARBE is working at BSI – Federal Office of Information Security near Dresden as a Policy Officer since August 2023. Working in the unit “General Policy” in the Department Cybersecurity in Aviation, she is responsible for EU and International Affairs.

She has been one of the Task Force Leaders of the Aviation Cybersecurity Subgroup under the NIS Cooperation Group leading the activities of Task Force 2.1/3.1 of the group for more than a year.



Mapping of EU cybersecurity rules applicable to the aviation sector

Part IS Workshop 26/06/2025

Katharina Garbe, Federal Office for Information Security (BSI)

Agenda

- Organisation
- Regulation context
- Task Force 2.1/3.1
- Next Steps



Organisation

Aviation Subgroup



Task Force 1.1: Regulated entities



Task Force 2.1/3.1: Mapping

Process and timeline

Mapping Exercise

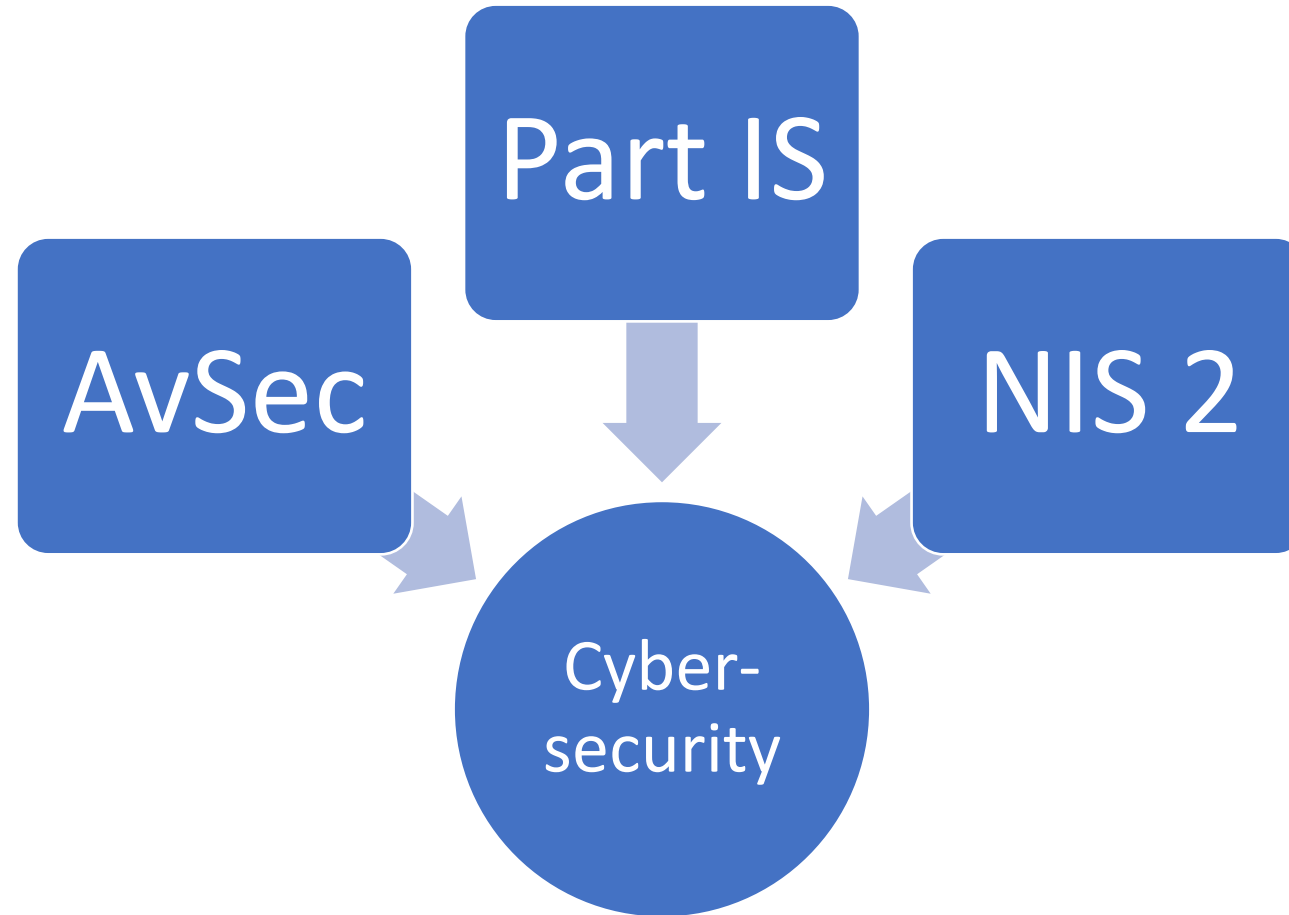
Guidance Material

Merge of Document

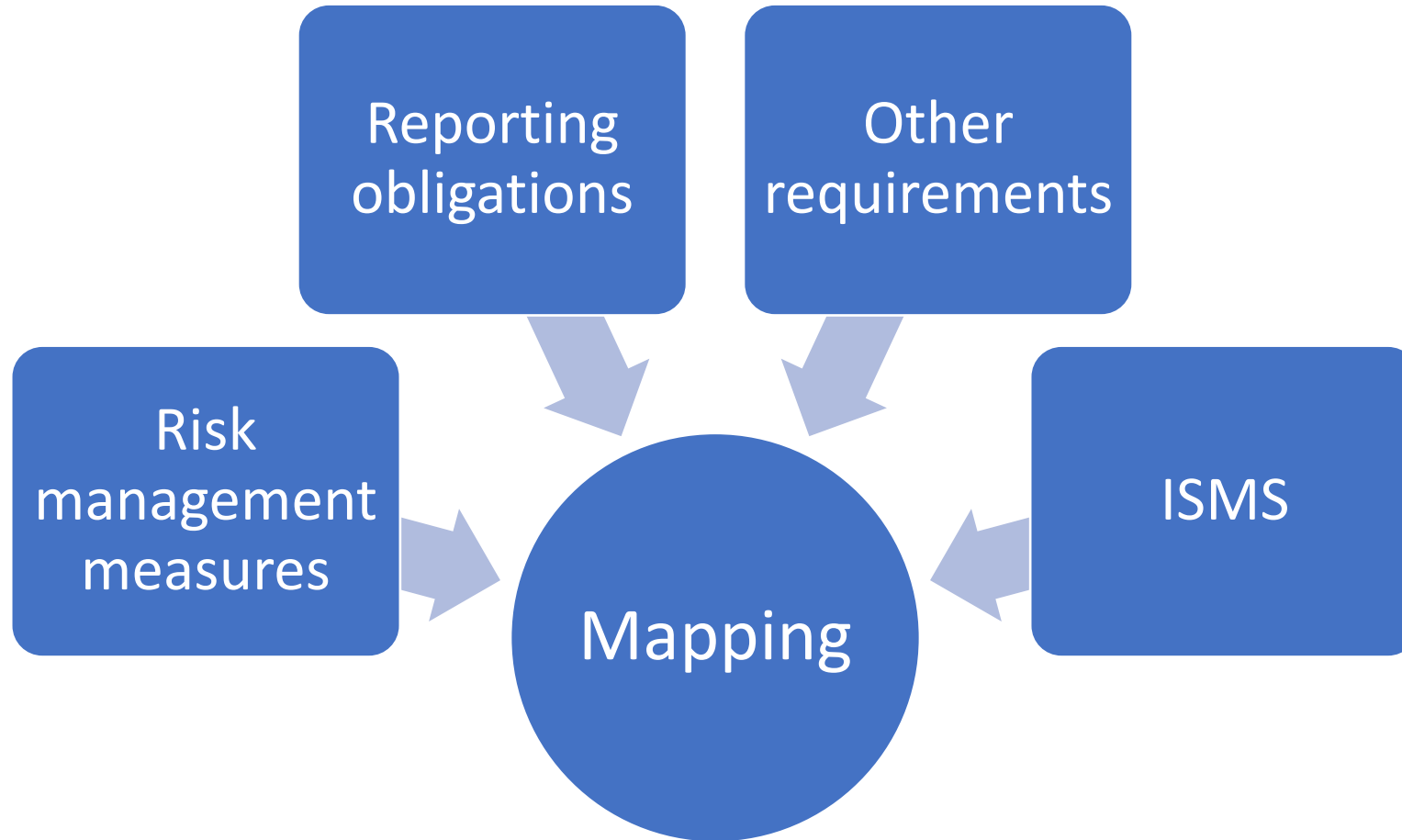
Consultation



Regulatory contexts



Overview




Goal of the mapping

- Identification and assessment of regulatory measures
- Tool for Member States: to clarify the applicable regulatory requirements including ISMS, risk assessment and incident reporting
- Provide remarks and recommendations for Member States

Example: Art 20.2 NIS 2 Directive

Topic	NIS 2	Part IS	Avsec
Basic cyber hygiene practices and cybersecurity training	Art. 20.2	IS.D/I.OR.240(g),	11.2.8.1
		IS.D/I.OR.240(f)	11.2.8.2
		AMC1 IS.D/I.OR.200(a)(1) (h)	



Mapping of EU cybersecurity rules applicable to the aviation sector

Part IS Workshop, 26/06/2025

Part-IS Guidance Material (GM) update

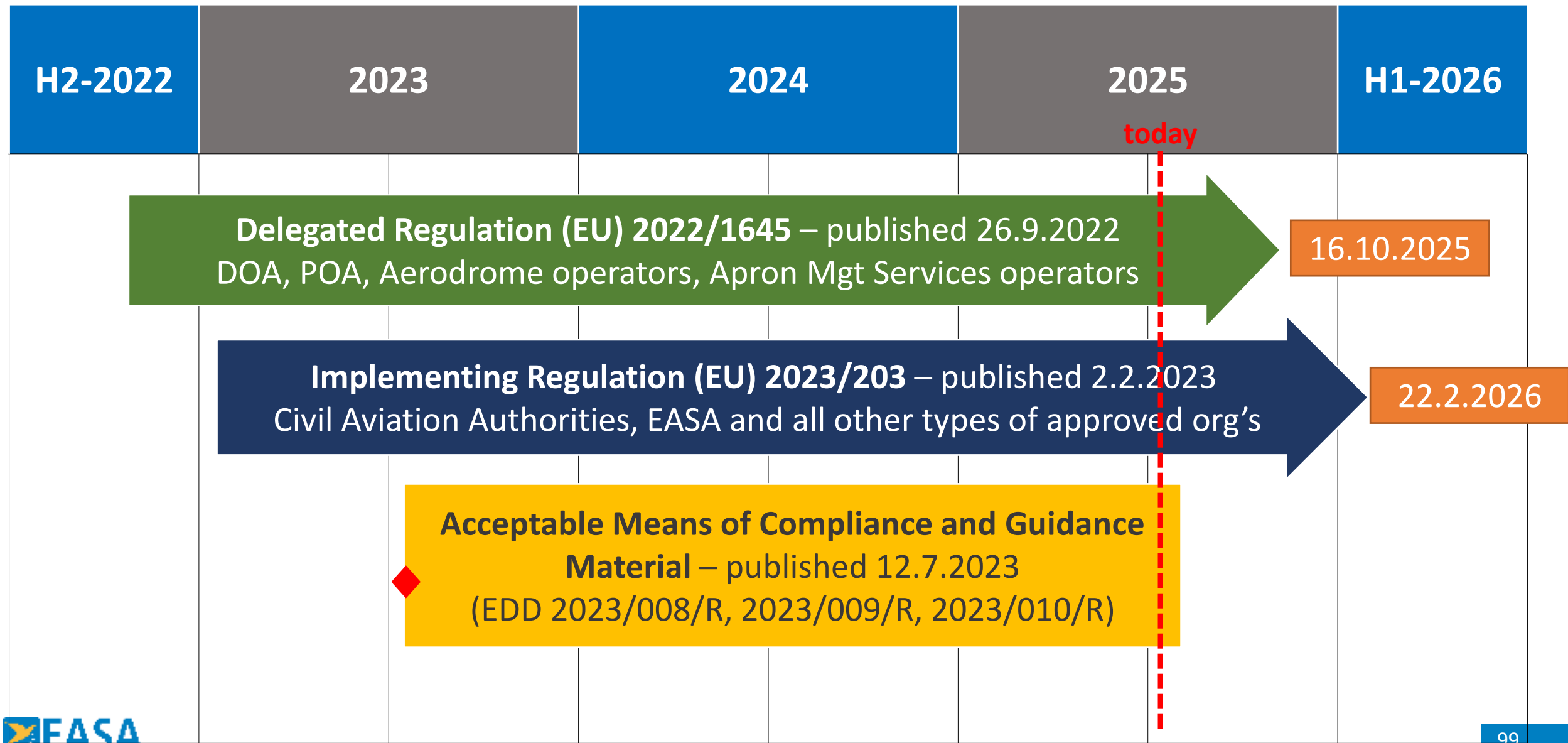


Part-IS Implementation Workshop 2025



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

Part-IS implementation journey



Part-IS Implementation Task Force

EASA has set up a task force (TF) of Member States (MS) Authorities as per MAB decision at its 2022-03 meeting on 25 October 2022.

Objective

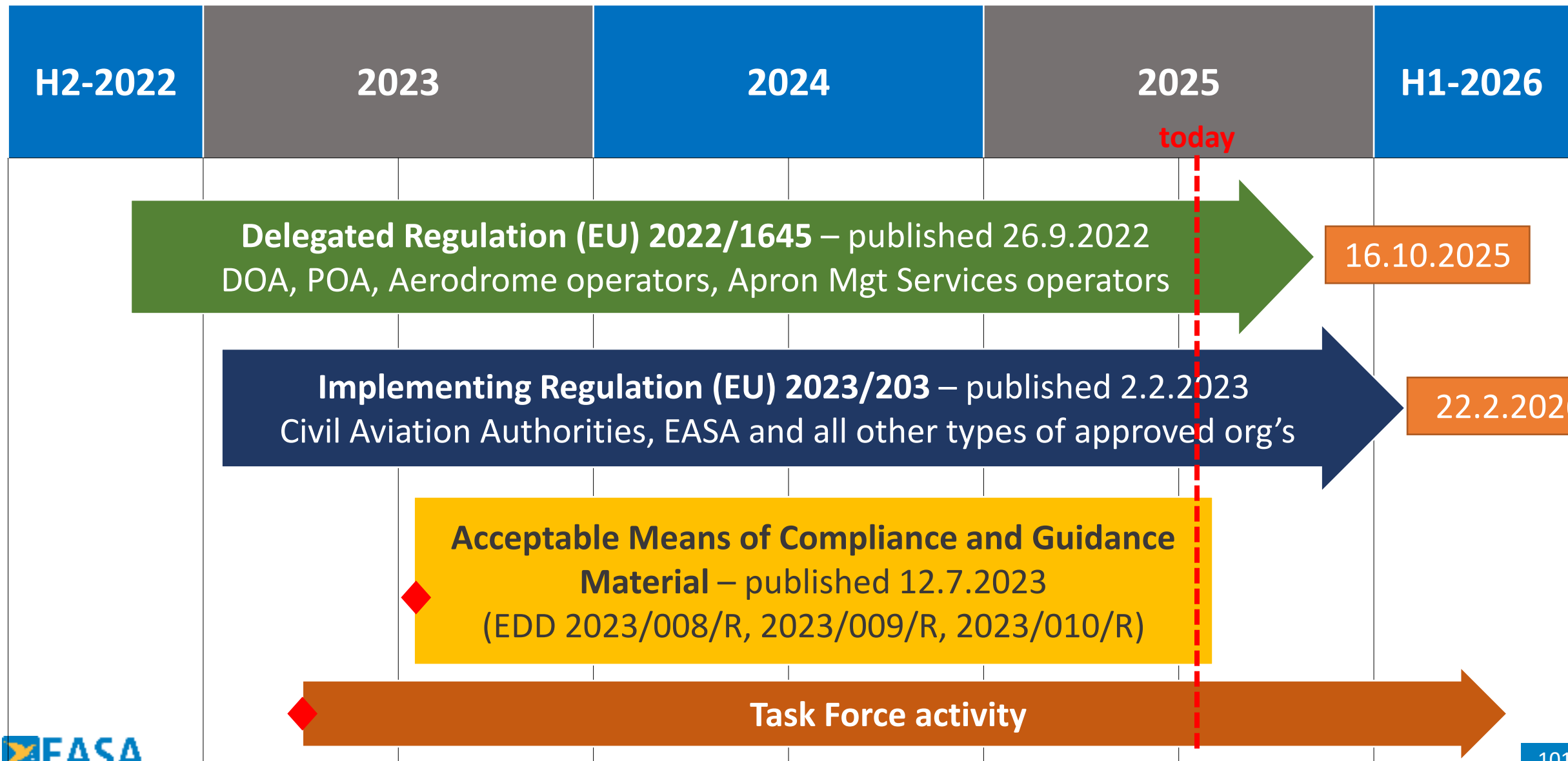
To facilitate a timely and harmonised implementation of Part-IS in all Member States

Deliverables

Further guidance for authorities and organisations

Chaired by Spain - All EU Authorities represented by their experts responsible for Part-IS implementation

Part-IS implementation journey



Outputs of the Task Force

Feedback, experience, exchange

- Inputs for AMC and GM
- Draft user guides and agreed practices
- Overview of pilot projects and ongoing initiatives
- Regular updates

the TF has delivered

Deliverables available in the Cybersecurity Community

Training and competence of inspectors

ISMS Oversight

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

Guidelines oversight policy

Interplay with other
EU Regulations

Comparison tables delivered
to NIS subgroup

Analysis on-going with
NIS and AvSec Authorities

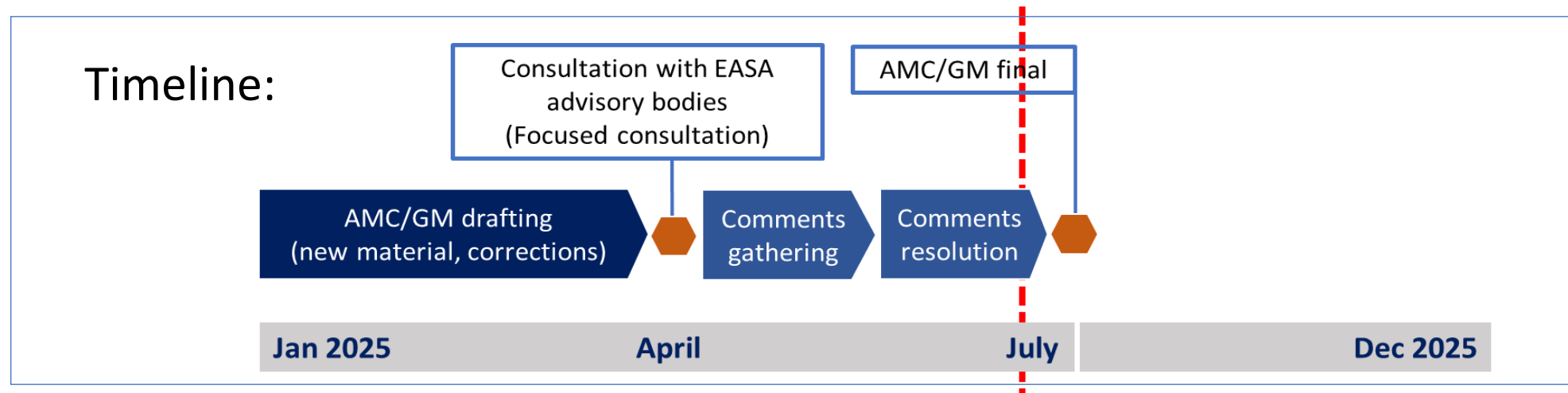
ISO 27001
add-on

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

GM updates and the NPA with Focused Consultation

The Part-IS TF has identified some areas where more guidance would have been useful to support harmonised implementation between Member States (MS).

EASA has therefore proposed updates to the **guidance material** for the application of both the Implementing and Delegated Commission Regulations mostly resulting from the joint activity of MSs.



Summary of GM updates and sources

- Harmonisation activity of EU Commission

- Part-IS compliance guideline for ISO/IEC 27001 certified organisations
- Assessment of requests for derogation
- Oversight Strategy – Proportional implem.

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

- ICAO TFP – Doc 10204 – interaction between safety and infosec

- Additional guidance for Articles regarding interplay with NISD and AVSEC Reg.

- New Appendix IV, references to ISO 27k removed from Appendix II (main tasks)
- GM to IS.I/D.OR.200(e)
- GM to “Indicators of complexity and elements of proportional implementation”

- Included references in GM and new Appendix

- GM to IS.I/D.OR.200

Summary of GM updates and sources

- Harmonisation activity of EU Commission

- Part-IS compliance guideline for ISO/IEC 27001 certified organisations
- Assessment of requests for derogation
- Oversight Strategy – Proportional implem.

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

- ICAO TFP – Doc 10204 – interaction between safety and infosec

- Additional guidance for Articles regarding interplay with NISD and AVSEC Reg.


- New Appendix IV, references to ISO 27k removed from Appendix II (main tasks)
- GM to IS.I/D.OR.200(e)
- GM to “Indicators of complexity and elements of proportional implementation”

- Included references in GM and new Appendix

- GM to IS.I/D.OR.200

Updates on Industry standards development

- Updates of EUROCAE ED-206 (on info. security event management) are ongoing.
- The development of EUROCAE ED-ISMS standard is ongoing. The official publication has been postponed to 2026, however an interim document (EUROCAE Report – ER) is about to be published.



The new material will be assessed for future use in the next update (i.e. revision 3) of AMC or GM.

To ensure alignment with regulators' expectations EASA and the MSs TF participates in the discussion.

Part-IS Regulations

ED Decision 2023/08/R

3 ED Decisions

AMC/GM to Cover
Regulations

ED Decision 2023/09/R

AMC/GM to
Organisation
Requirements

ED Decision 2023/10/R

AMC/GM to
Authority
Requirements

Amdts to existing
AMC/GM for ARs

Delegated
Regulation
No 2022/1645

Cover Regulation

Annex I D.OR

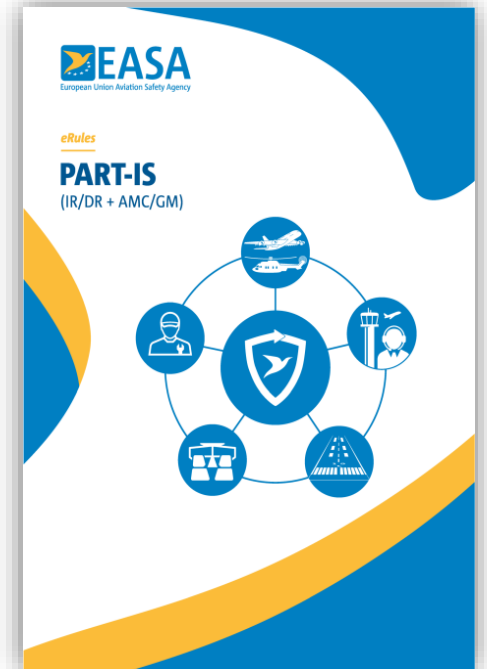
Cover Regulation

Annex II I.OR

Annex I AR

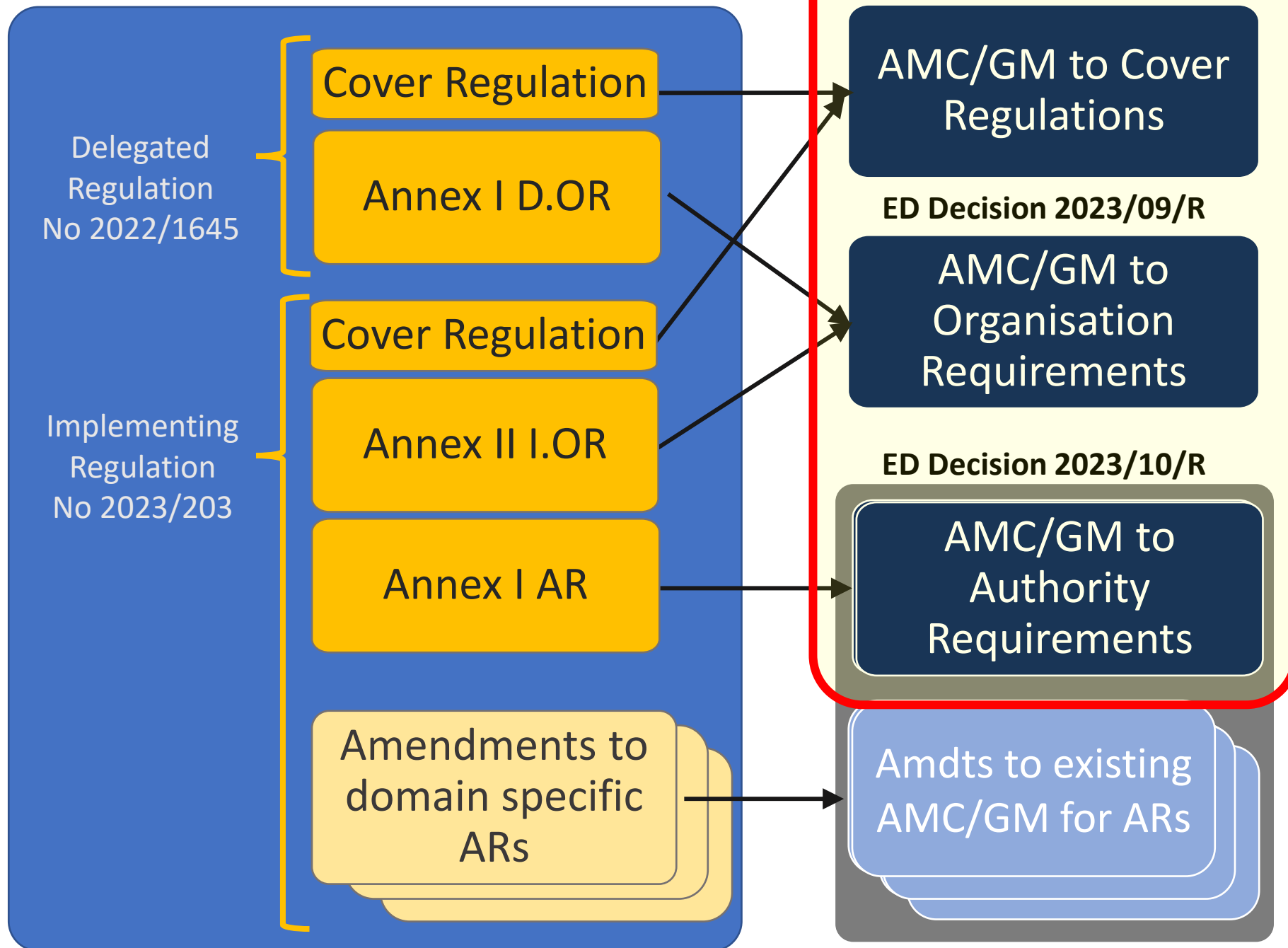
Amendments to
domain specific
ARs

Implementing
Regulation
No 2023/203

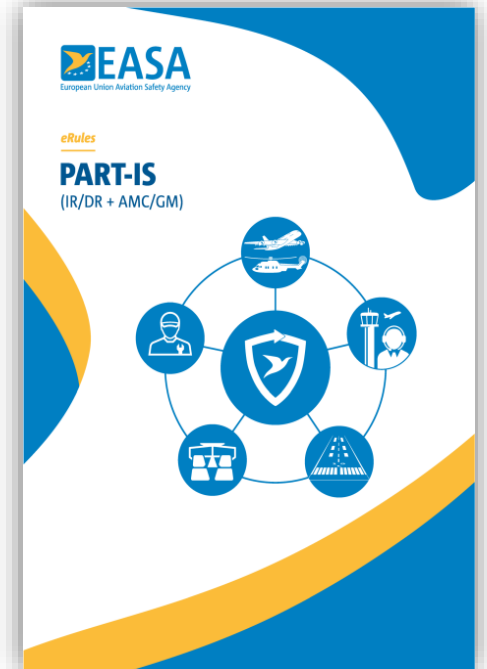


Easy Access Rules

Part-IS Regulations



3 ED Decisions



Easy Access Rules

AMC & GM what's in it

- Non-binding by definition
- To facilitate timely and harmonised application of Part-IS
- No additional requirements. Everything is in the Regulations

Acceptable Means of Compliance

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

Guidance Material

- To address elements in the rule that would require explanation
- To integrate means of compliance by providing guidance on practical or operational aspects
- Background information helping to understand the requirements

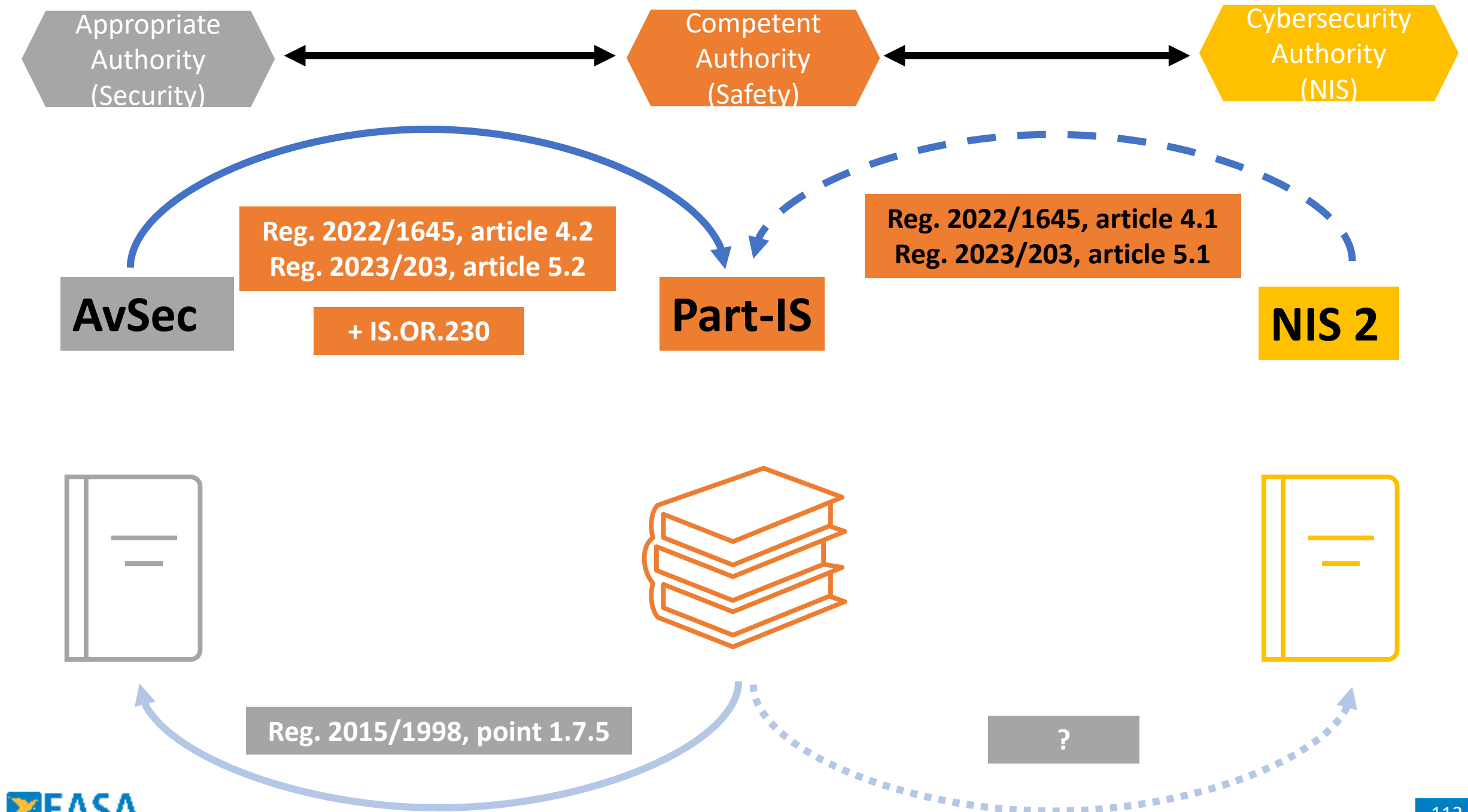
Req.s arising from other Union legislation

IR

- Article 4 (DR) / Article 5 (IR)
- Indicates extent of equivalence between Part-IS and AVSEC Regulation as well as Part-IS and NIS Directive

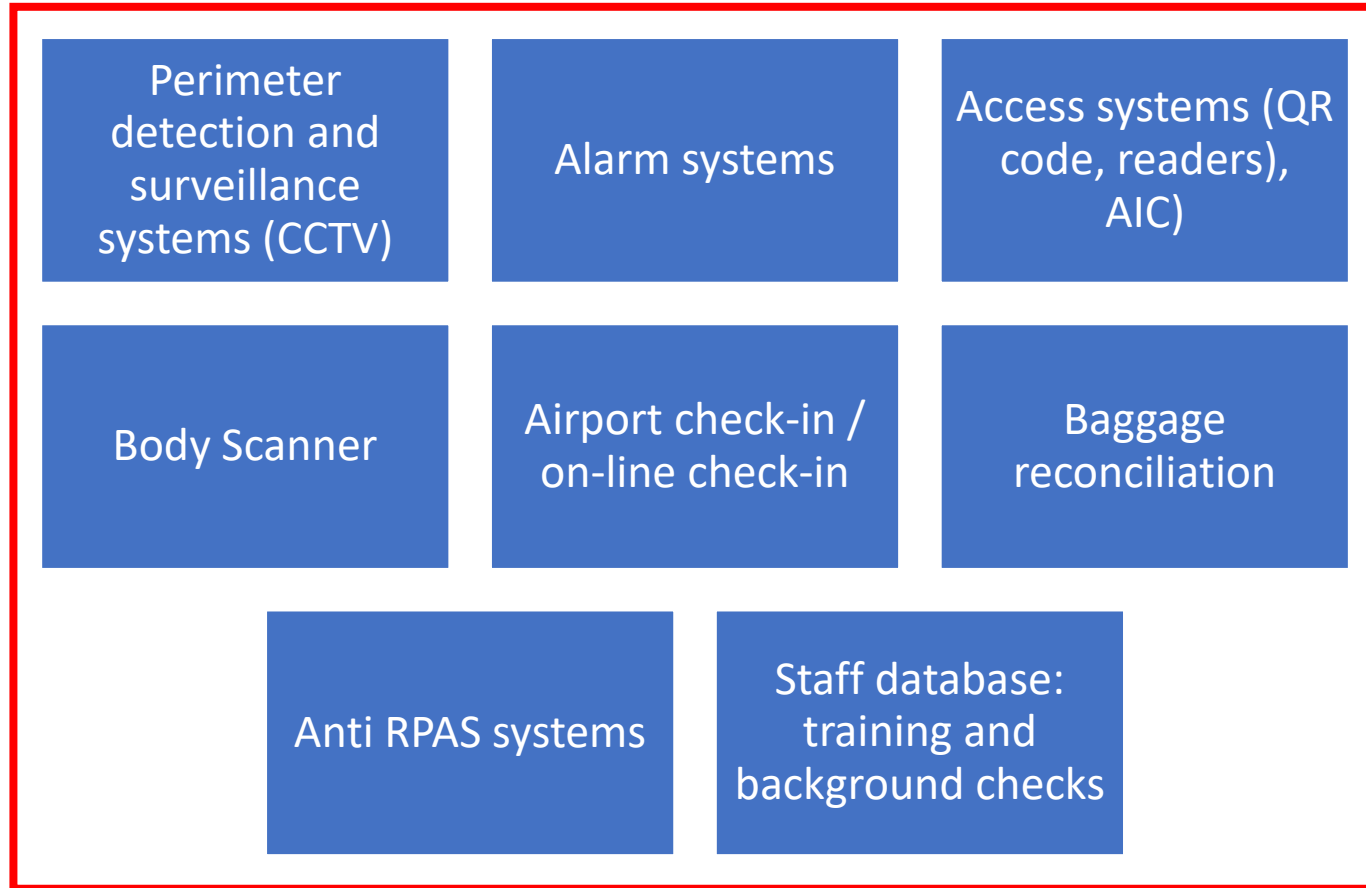
GM

- Clarifies that organisations need to consider the differences in the scope of the rules in terms of which elements are covered under the different regulatory frameworks

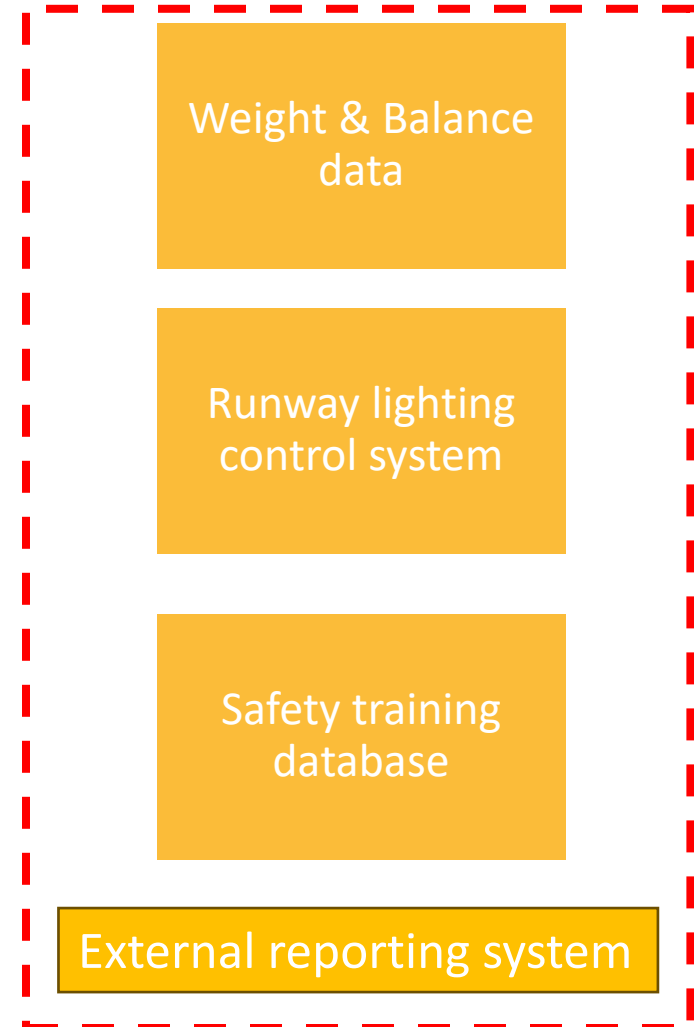


Example: airport operator

AvSec protection measures

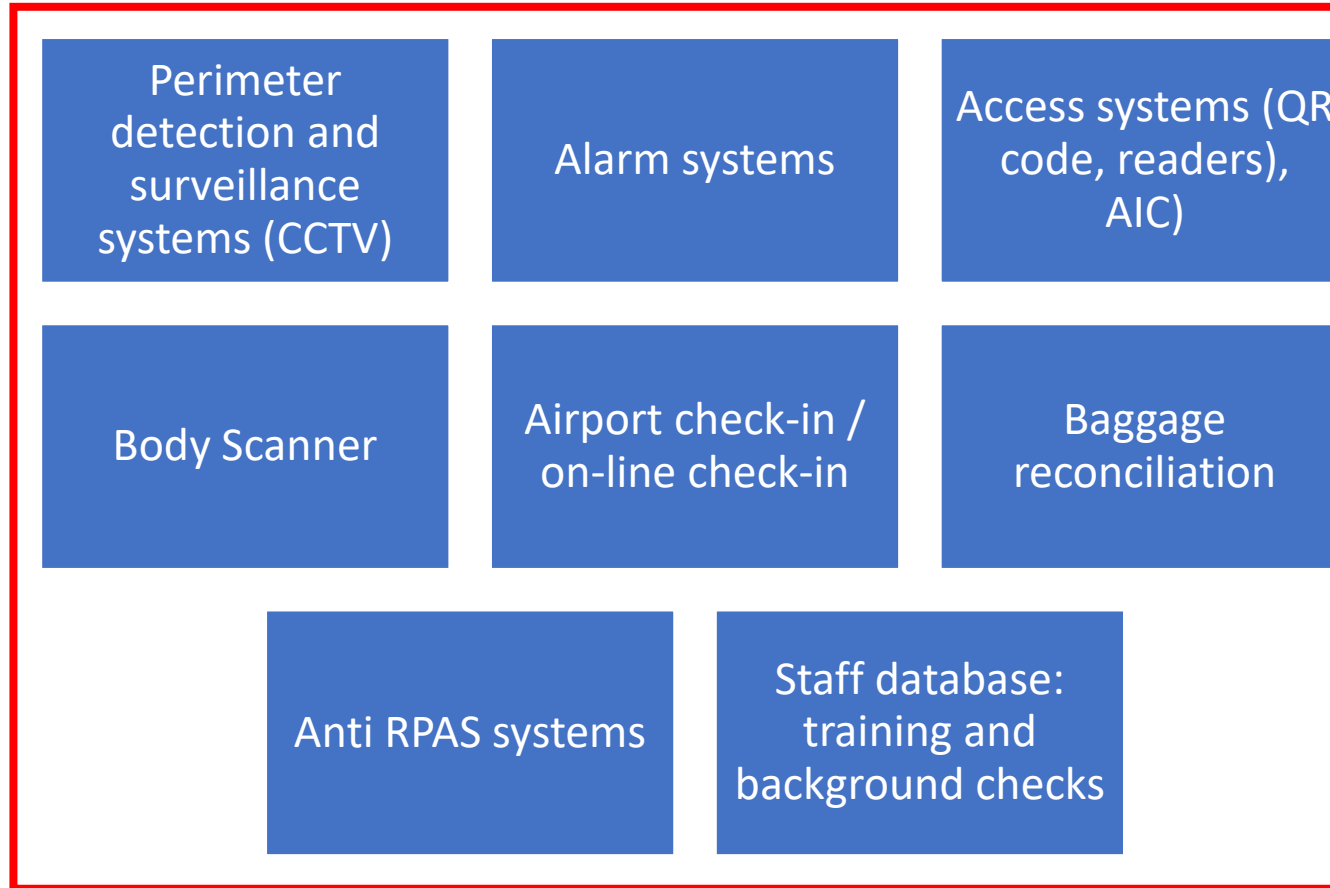


Part-IS protection measures

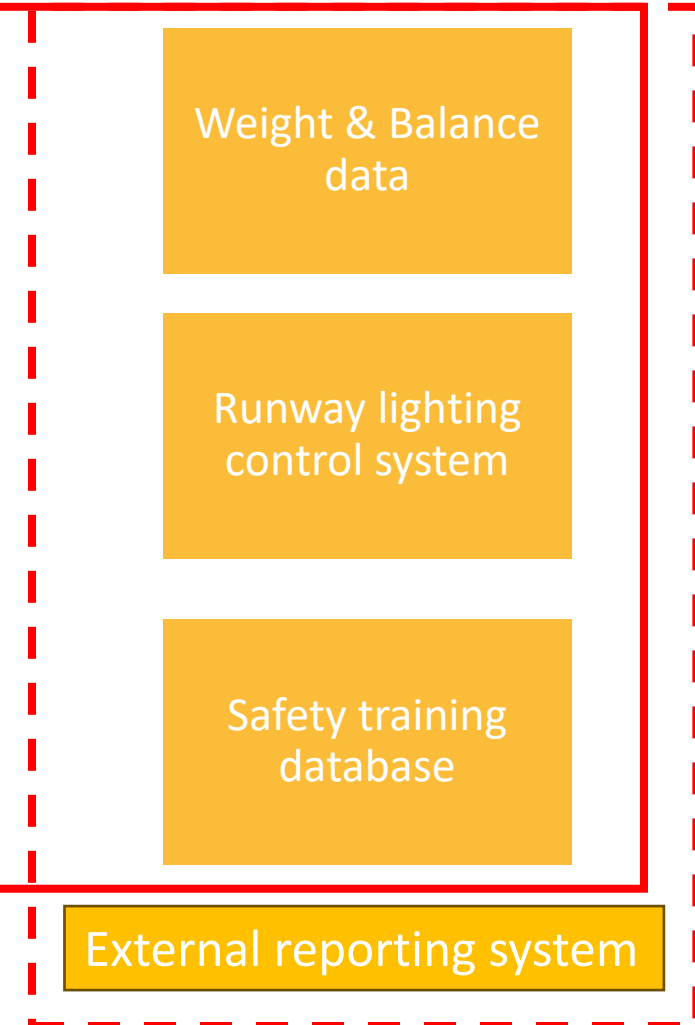


Example: airport – use of equivalence art. 4(2)

AvSec protection measures



Part-IS protection measures



Competent authority for Part-IS

IR

- Article 5 (2) (DR) / Article 6(2) (IR)
- Indicates Competent Authority (CA) for Part-IS oversight and provides MS with the means for alternative assignment to an independent entity

GM

- Clarifies the applicability of Part-IS to competent authority in case of designation of an independent entity as CA

AR/OR.200

IR

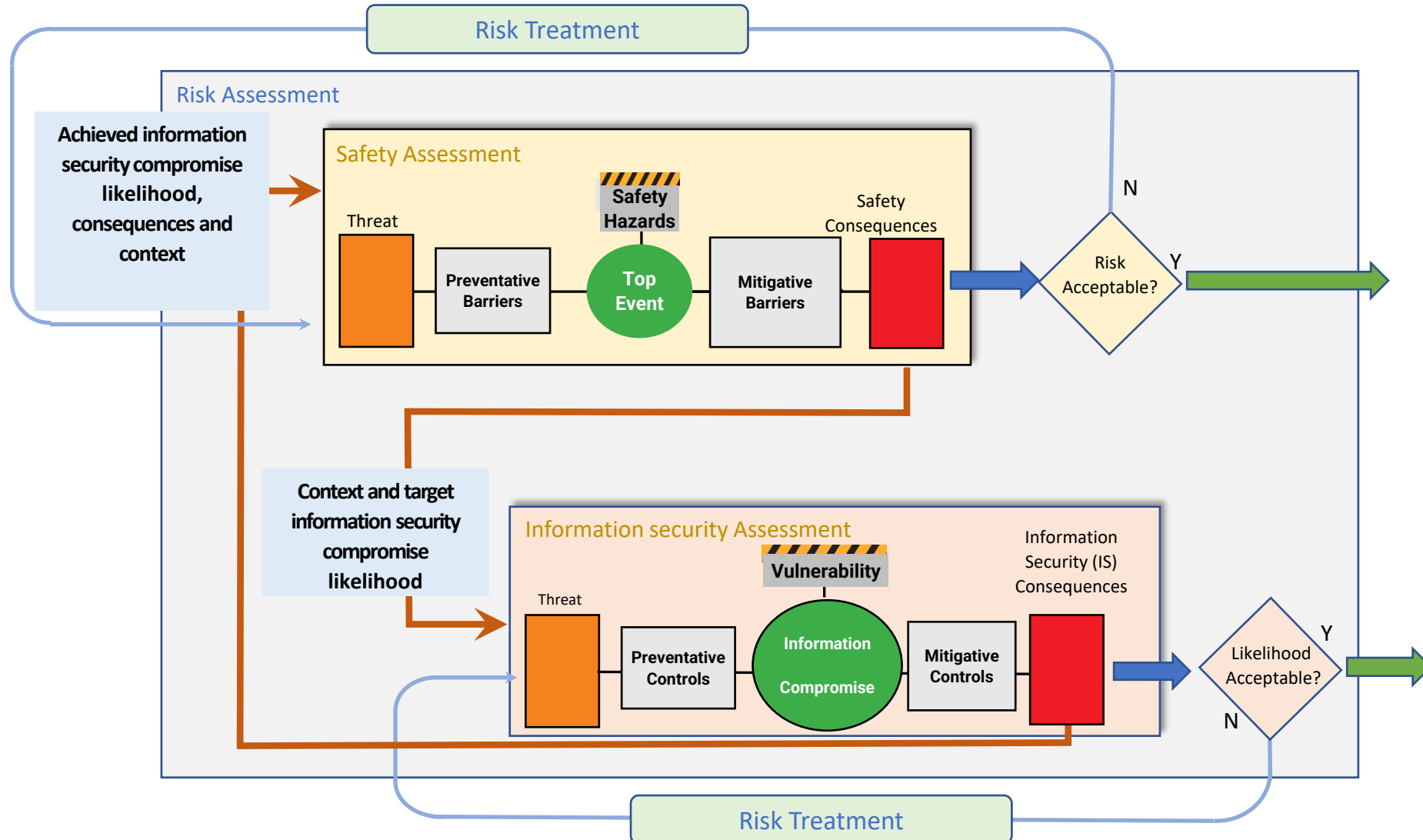
- Main requirement defining the high level provisions for Part-IS Compliance including the need for the implementation of an Information Security Management System

GM

- Alignment to recent ICAO developments
- Reference included to ICAO Doc 10204 “Manual on Aviation Information Security” *

*although not necessary for Part-IS compliance, the document is available on ICAO website (free for ICAO contributors, otherwise subject to fee)

New interacting bow-tie scheme



OR.200 (d)

IR

- **Relates processes, procedures, roles and responsibilities to the nature and complexity of the organisation**

GM

- **Considers the overarching principle of GM1 to Article 1 “While taking measures under this Regulation, affected entities – irrespective of their size – are encouraged to take into account the principle of proportionality of aviation safety risks when ensuring that such measures are appropriate to the nature of their activities”.**
- **Suggests aspects of safety relevance and complexity as drivers for proportionate implementation of the ISMS under Part-IS**
- **Complemented by Appendix V where more details about indicators of safety relevance and complexity as well as examples of activities are provided**

Proportionality vs Safety relevance & Complexity

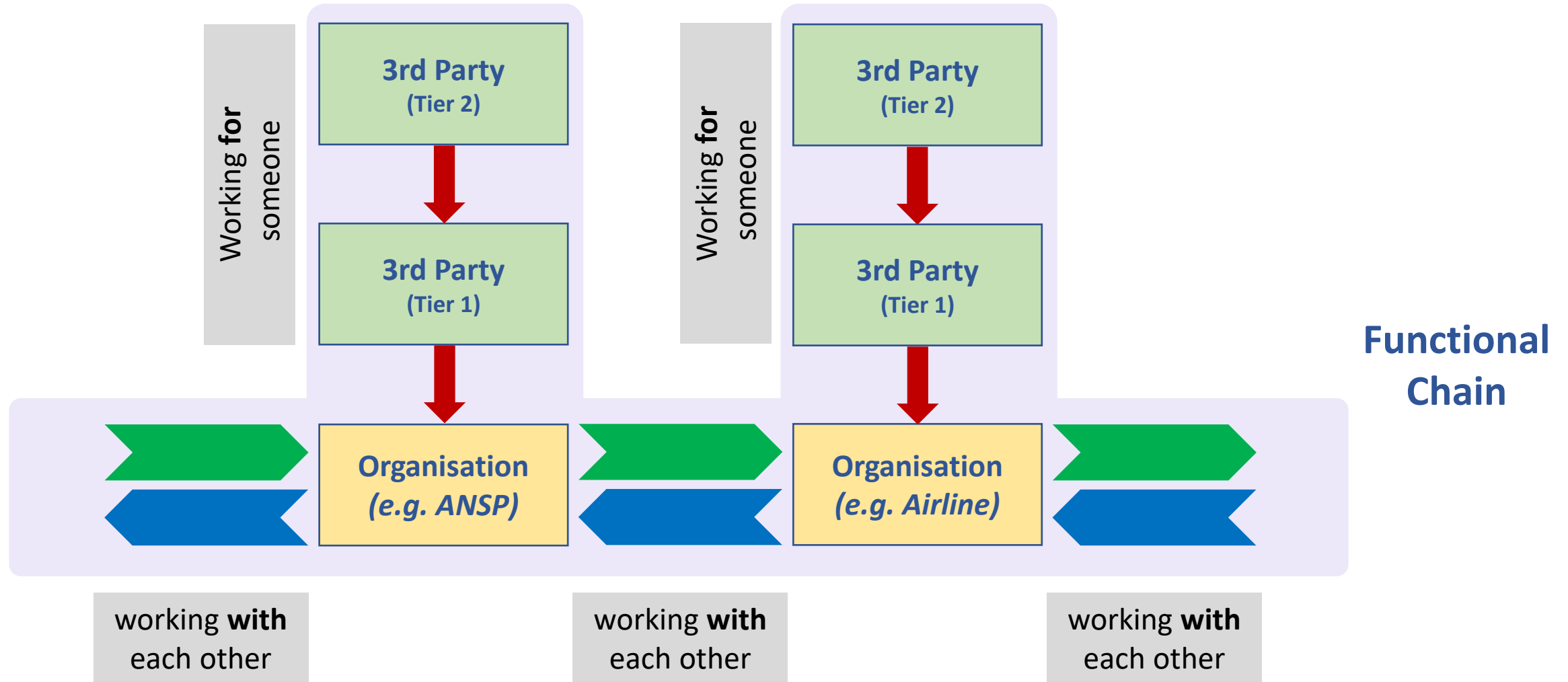
No clear distinction between complex and non-complex organisations, rather there are **elements** that , on its own, **can influence certain aspects of a proportionate ISMS implementation**

The position of the organisation is in the functional chain and the number and criticality of interfacing organisations/stakeholders

The **complexity of the organisational structure and hierarchies** (e.g. number of staff, departments, hierarchical layers, etc)

The **complexity of the information and communication technology systems and data** used by the organisation and their connection to external parties.

Proportionality and Complexity Indicators



OR.200 (e)

IR

- Demonstrate that no potential impact on aviation safety is posed
- Document information security risk assessment results
- Obtain approval by competent authority to not implement requirements

GM

- Further considerations about the preliminary information that should be collected by the competent authority for a pre assessment
- What will be evaluated
- What happens after a derogation has been granted

AR/OR.210

IR

- Address identified unacceptable risks (IS.OR.205)
- Everyone in the organisation informed
- Interfaced organisations informed as well

GM

- Editorial changes

OR.240 (g)

IR

- Sufficient and competent personnel shall be available

GM

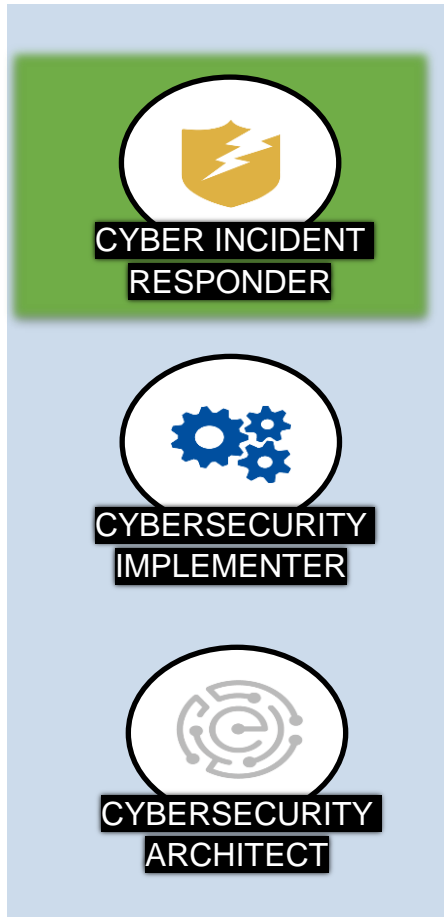
- Revision of Appendix II (Main task stemming from Part-IS) and the link between tasks and competency frameworks (EU eCF and NIST)
- Addition of Role Based competency framework and link to Appendix VI containing an adaptation of the ENISA ECSF to aviation.

Standard roles prosed by ENISA

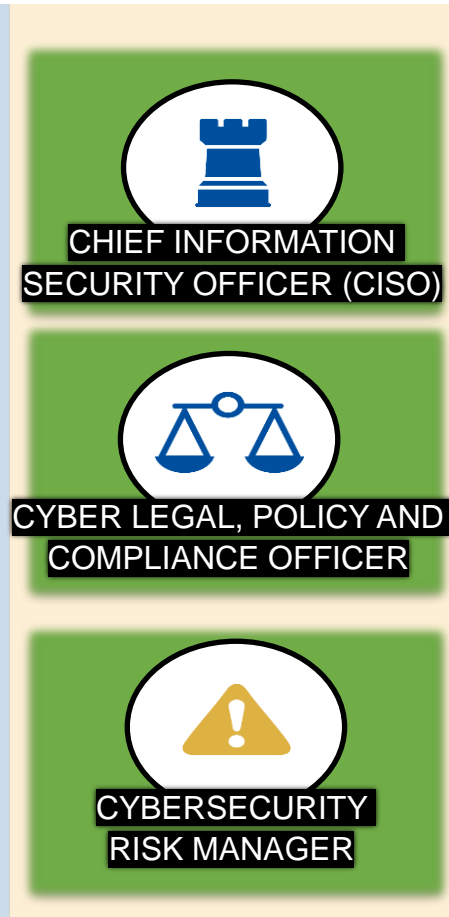


The roles from aviation perspective

1ST LINE OF DEFENCE



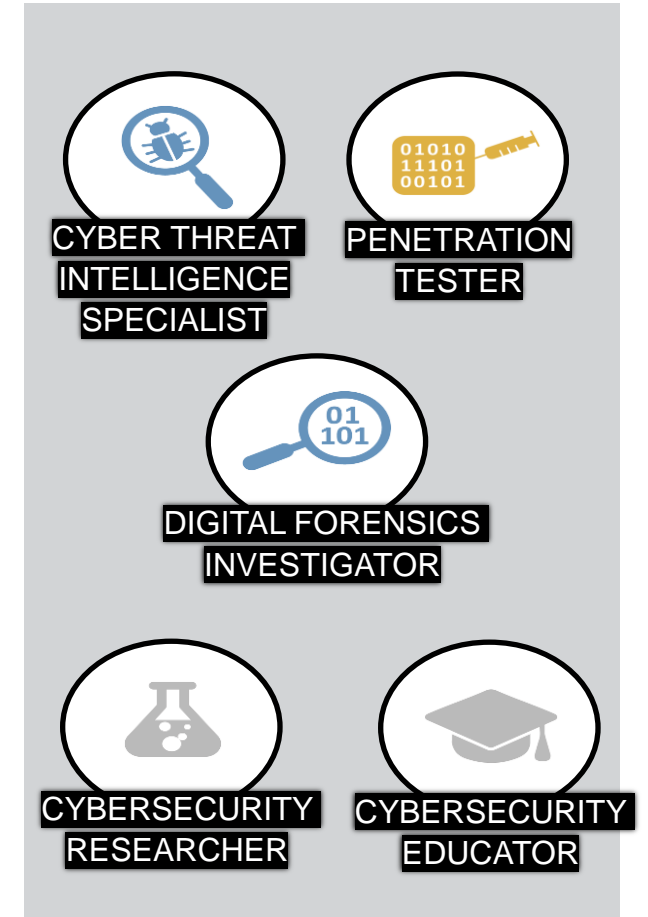
2ND LINE OF DEFENCE



3RD LINE OF DEFENCE



SUPPORTING



OR.245

IR

- Record keeping

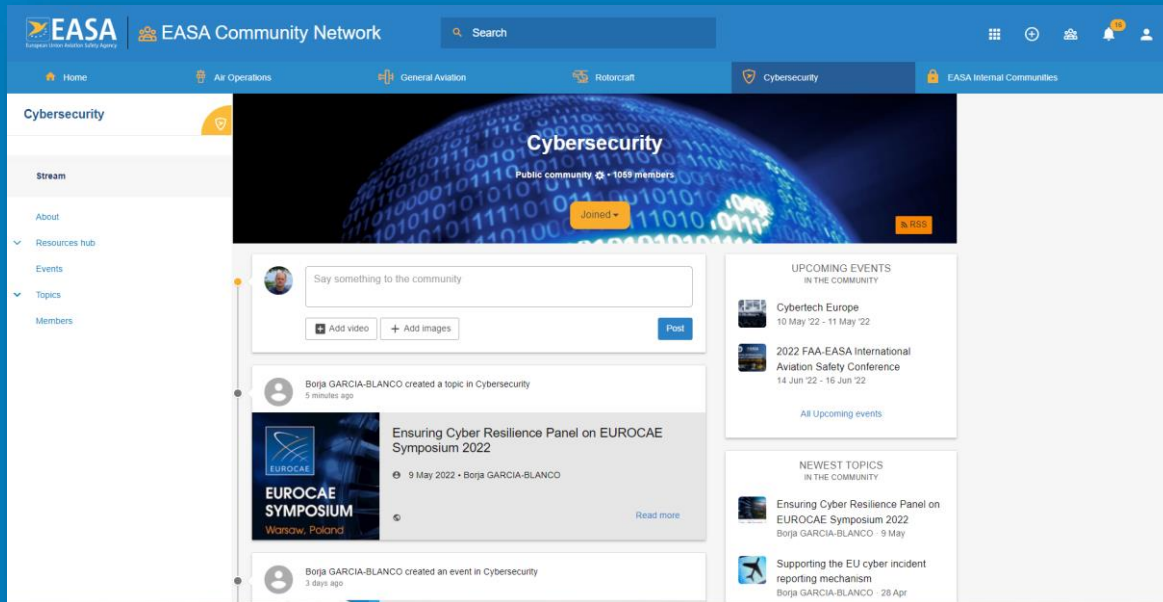
GM

- Provide more precise explanation of “approval received” mentioned in the requirement

Thank you!

Join our Community:

<https://www.easa.europa.eu/community/cybersecurity>



Contact us at:
cybersec@easa.europa.eu

easa.europa.eu/connect



Your safety is our mission.

An Agency of the European Union 

Conclusions – Day 2





Jesper Rasmussen is the Flight Standards Director of EASA. Prior to joining EASA in 2017, Jesper Rasmussen was the deputy director general in the Danish multi-sectoral national authority, where he since 2012 has been responsible for aviation safety as well as railway safety. In this function, he has been a member of the EASA Management Board and represented his country on aviation safety affairs at EU and ICAO level.

Before entering into aviation, Jesper Rasmussen occupied for 20 years other posts in the Danish central government administration, both in the Ministry of Transport and Ministry of Industry, where he was responsible for such domains as road traffic and the construction sector.

FAQs update on Part-IS

A set of (22) answers on common queries and concerns have been published

The FAQs will be expanded within this summer

Your questions will be considered for the next iteration



EASA Cybersecurity Community

Find useful material and guidance for Part-IS Implementation

EASA European Union Aviation Safety Agency

EASA Community Network

Search

Home Air Operations General Aviation Rotorcraft

Cybersecurity Public community • 3633 members

Stream

About Resources hub Events Topics Members

Say something to the community

+ Add video + Add images Post

Vasileios PAPAGEORGIOU created a topic in Cybersecurity 1 hour ago

Cybersecurity in Aviation - Lecture in Hamburg

12 Oct 2023 • Vasileios PAPAGEORGIOU

Read more

Vasileios PAPAGEORGIOU created a topic in Cybersecurity 3 days ago

Cybertech Europe 2023 & EASA participation

UPCOMING EVENTS IN THE COMMUNITY

No upcoming events in this community

All Upcoming events

NEWEST TOPICS IN THE COMMUNITY

Cybersecurity in Aviation - Lecture in Hamburg Vasileios PAPAGEORGIOU • 12 Oct

Cybertech Europe 2023 & EASA participation Vasileios PAPAGEORGIOU • 9 Oct

All topics

NEWEST MEMBERS IN THE COMMUNITY

Join our community



Document Library VERIFIED

Vasileios Papageorgiou • 28 February 2025 in community [Cybersecurity](#)

0 comments 1 likes public Follow content

Part-IS Implementation Task Force

[Part-IS Implementation Task Force - Deliverables](#)

[European Cybersecurity Skills Framework - Application to Aviation](#)

1 like

Thank you
for being with us virtually and in presence



Part-IS Implementation
Workshop 2025

