

Part-IS Implementation

Workshop

Cologne, **November 7 - 8**



Your safety is our mission.

Part-IS Workshop agenda – Day 1

Introduction to Part-IS & organisational impact

Scene setter on Part-IS, links with the other implementing rules for the different domains and the expected impact on the organisational structure.

EASA

Panel 1 - Part-IS early implementers' feedback

Experiences of early implementers of Part-IS, challenges and key aspects.

EASA, Airbus Commercial, Lufthansa Group, Nordic Regional Airlines AB, TRAFICOM

Q&A

Examples of functional chains and shared risks

Examples of risks at the interface between organisations.

EASA, Airbus

External Reporting under Part-IS

External reporting requirements under Part IS and the relationship with Reg. (EU) 376/2014, the reporting tools that will be available.

EASA

ISO/IEC 27000 in relation to Part-IS

Insights on the similarities and differences between ISO/IEC 27000 and Part-IS in order to leverage on existing certification.

EASA

Industry standardisation

European Cyber security for aviation Standards Coordination Group (ECSCG) activities - focus on standards that will support Part-IS implementation.

EASA

Q&A

Part-IS Workshop agenda – Day 2

Part-IS Task Force outcomes & harmonisation activities

Overview of the harmonisation activities carried out by the Task Force, i.e. approval of derogations and the implementation guidance for ISO/IEC 27001 certified organisations.

AESA, AUSTRONCONTROL

Interplay with other EU rules (NIS2 and AVSEC)

Relationship between Part-IS and other EU cybersecurity legislation that may be applicable to aviation entities.

EASA, Polish CAA

Q&A

Panel 2 - Staff competence building

Discussion on cyber security competencies, & possible approaches to recruitment and upskilling the workforce, and the challenges associated with them.

EASA, ENISA, AESA, ILenT-NL, FOCA

ECSF adaptation for Part-IS roles

The tailored version of the ENISA Cybersecurity Skills Framework for use in the aviation context, taking into account in particular the roles introduced by Part-IS.

EASA

Q&A

Welcome to day 2!

Thanks for being with us virtually and in presence



Part-IS Implementation Workshop



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.

Hortensia has over 15 years' experience in the aviation industry, where she managed air traffic controller licences and worked as an aviation security inspector and instructor for SENASA.



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.

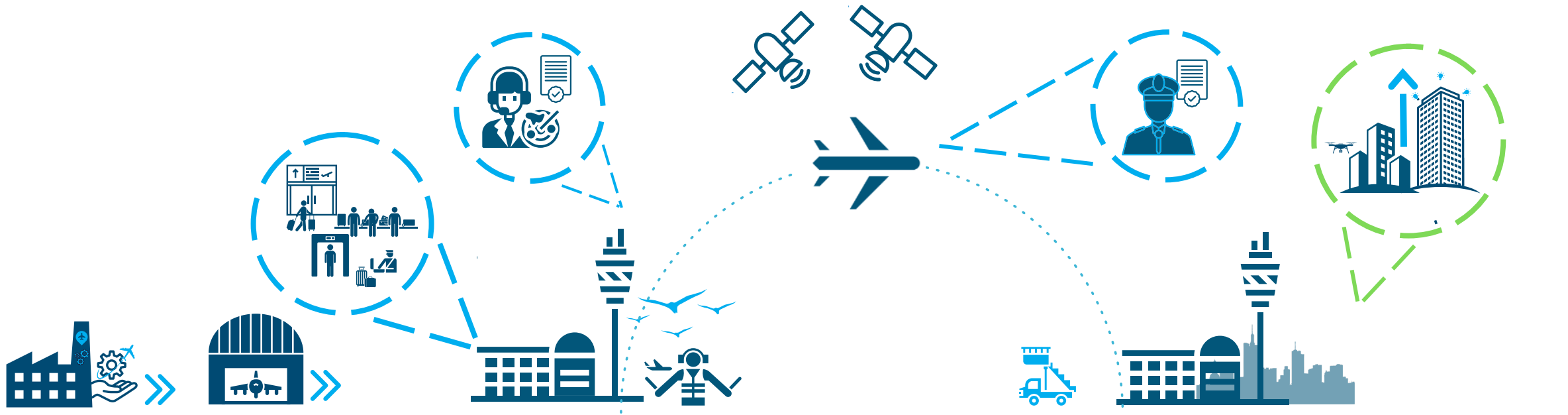
Mario is a communications engineer with nearly 25 years of experience gained also in consulting, IT and banking. He is an accredited ISO/IEC 27001 auditor for information security management systems.

Part-IS Task Force outcomes and harmonisation activities



Part-IS Implementation Workshop

A BIT OF CONTEXT



Airworthiness

Aerodromes

Operations and
Licensing

Drones

ATM/ANS

CAAs CERTIFICATES

EASA CERTIFICATES



WHY A TASK FORCE?

Cyber security
regulation interplay

Responsibilities of
different CAAs

ISMS at the
Authority

Approval and oversight of
ISMS at the Organisation

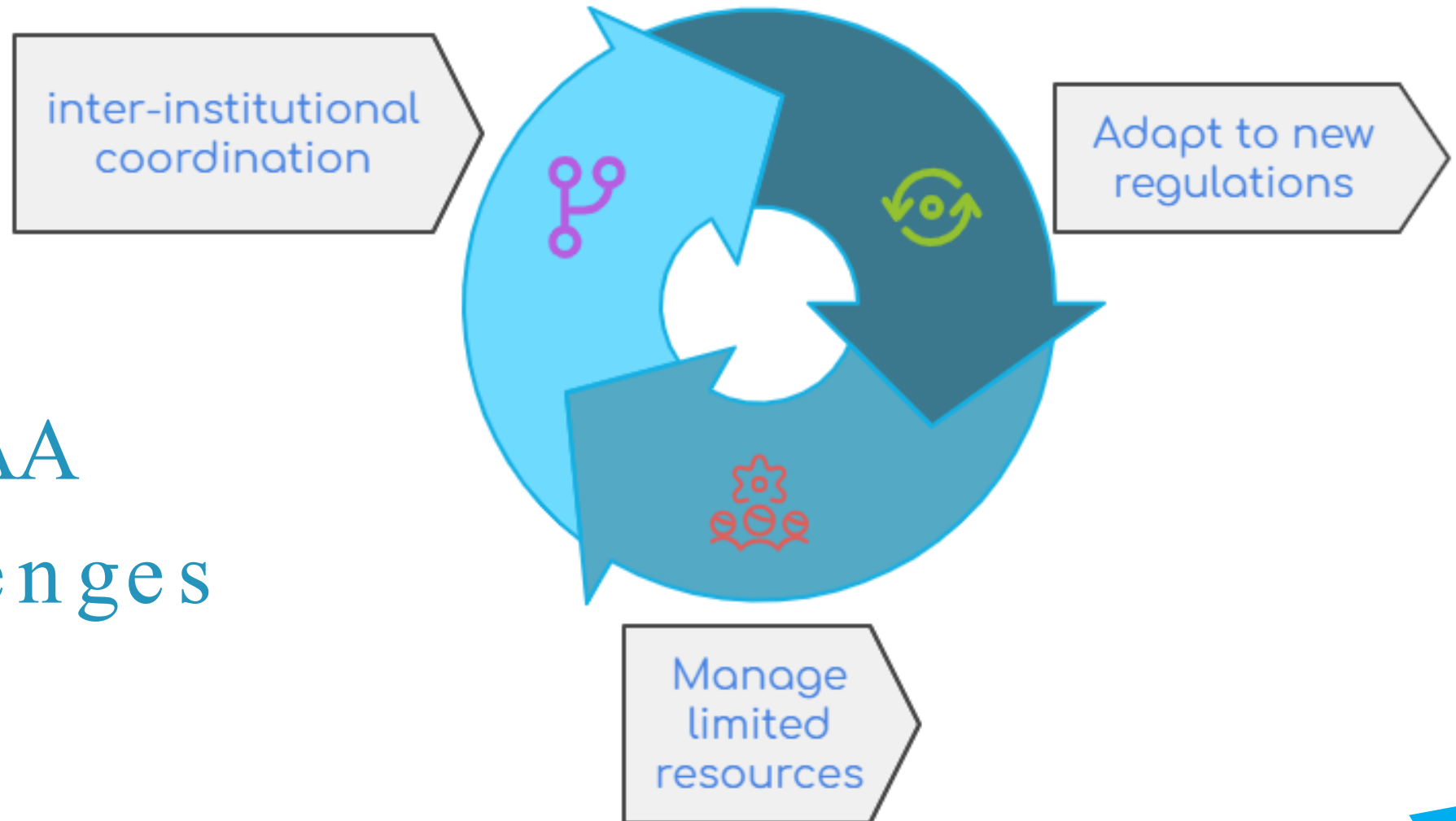
Cyber security
competences

PART-IS Implementation
challenges



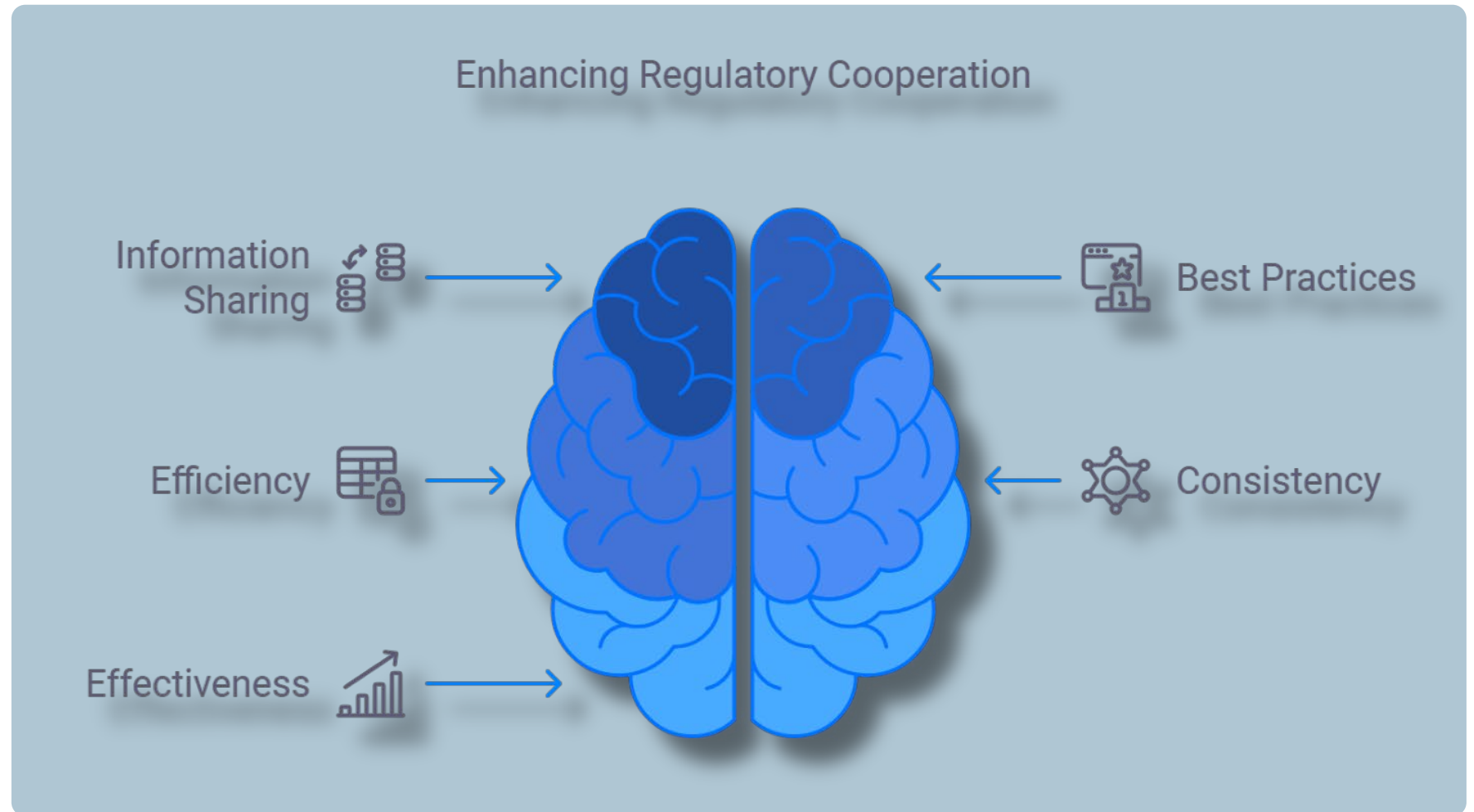
WHY A TASK FORCE?

CAA
challenges



WHY A TASK FORCE?

**Competent
Authorities
collaborative
Platform**
MAB 03/2022



PARTICIPATION



Kick off ---2023

2024

2026



+ 20 Competent Authorities

European Commission, EASA
and ENISA



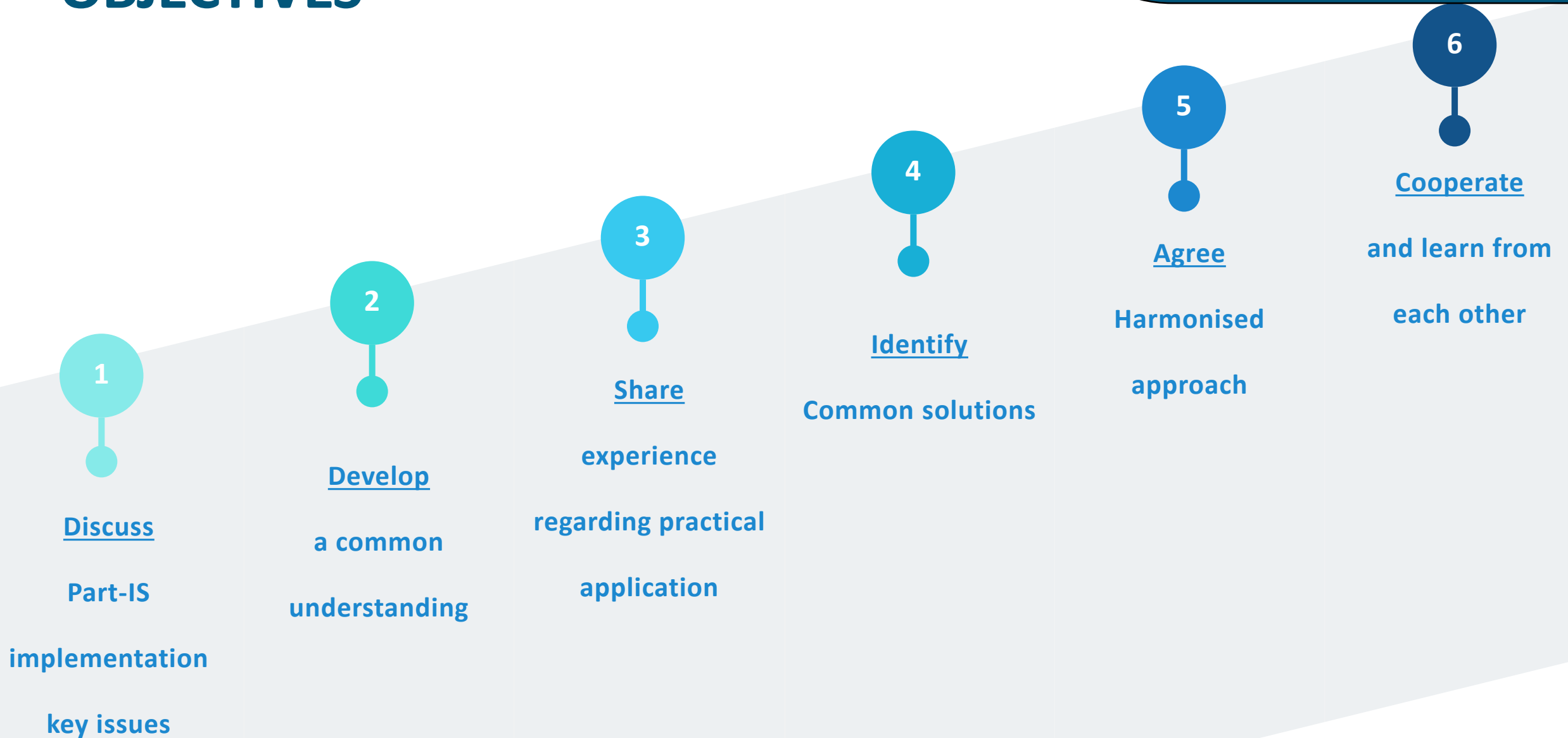
PARTICIPATION



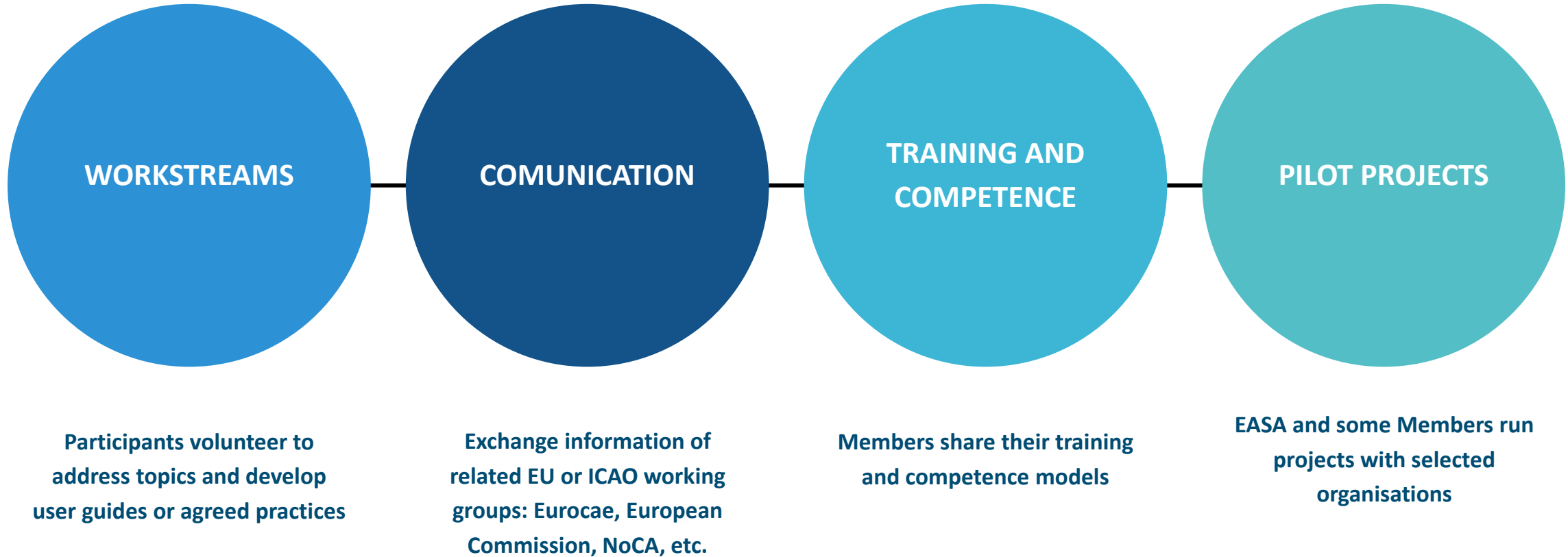
**Diversity of expertise,
knowledge and perspective**



OBJECTIVES



ACTIVITIES DEPLOYED



MAIN OUTCOMES



AMC/GM UPDATE



NIS-AVSEC-PART IS MAPPING



ISO 27001 ADD-ON



OVERSIGHT TOOL



DEROGATION GUIDELINE



COMPLIANCE ASSESSMENT

NON BINDING VALUE



WAY FORWARD

NEW TOPICS TO BE ADDRESSED

- Topics that CAA are more concerned
- Develop guides for implementation

PROGRESS ON INSPECTORS TRAINING

- Prepare inspectors community for implementing new requirements
- Identify additional training needs

COLLABORATION WITH DIFFERENT AUTHORITIES (NCSC, CAA...)

- Entities sitting across the responsibilities of different CAAs
- Discuss an efficient collaboration

DISCUSS INITIAL OVERSIGHT PROCESS

- Agreed practices to perform initial oversight process
- Identify specific needs for less complex organisations
- Discuss to make oversight process more efficient (without duplicating)





TIME FLIES, AND IN A WORLD WHERE INFORMATION SECURITY IS CRITICAL, WE CAN'T AFFORD TO WASTE A SINGLE MINUTE. EVERY SECOND COUNTS IN PROTECTING WHAT MATTERS MOST

Image created with AI



PART-IS TASK FORCE



@AesaSpain



www.seguridadaerea.gob.es



AESA



EASA Part-IS Implementation Task Force – published outcomes

- Implementation guidelines for Part-IS - IS.I/D.OR.200 (e)
- Standard add-on for ISO27001:2022 conform organisations

08.11.2024

Mario Lenitz – group leader WS4



What was the intention?

Scope of work of WS 2

- Oversight and ISMS implementation
- Harmonisation of NAA Oversight: Develop a joint perspective
- Development of Implementation guidelines for Part-IS - IS.I/D.OR.200 (e)

Group Roles

- Davide Martini - EASA
group leader
- Christoph Schnyder - FOCA
pen holder Implementation guidelines
- Various members from NAAs



Deliverable of the Workstream

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

Guidelines

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

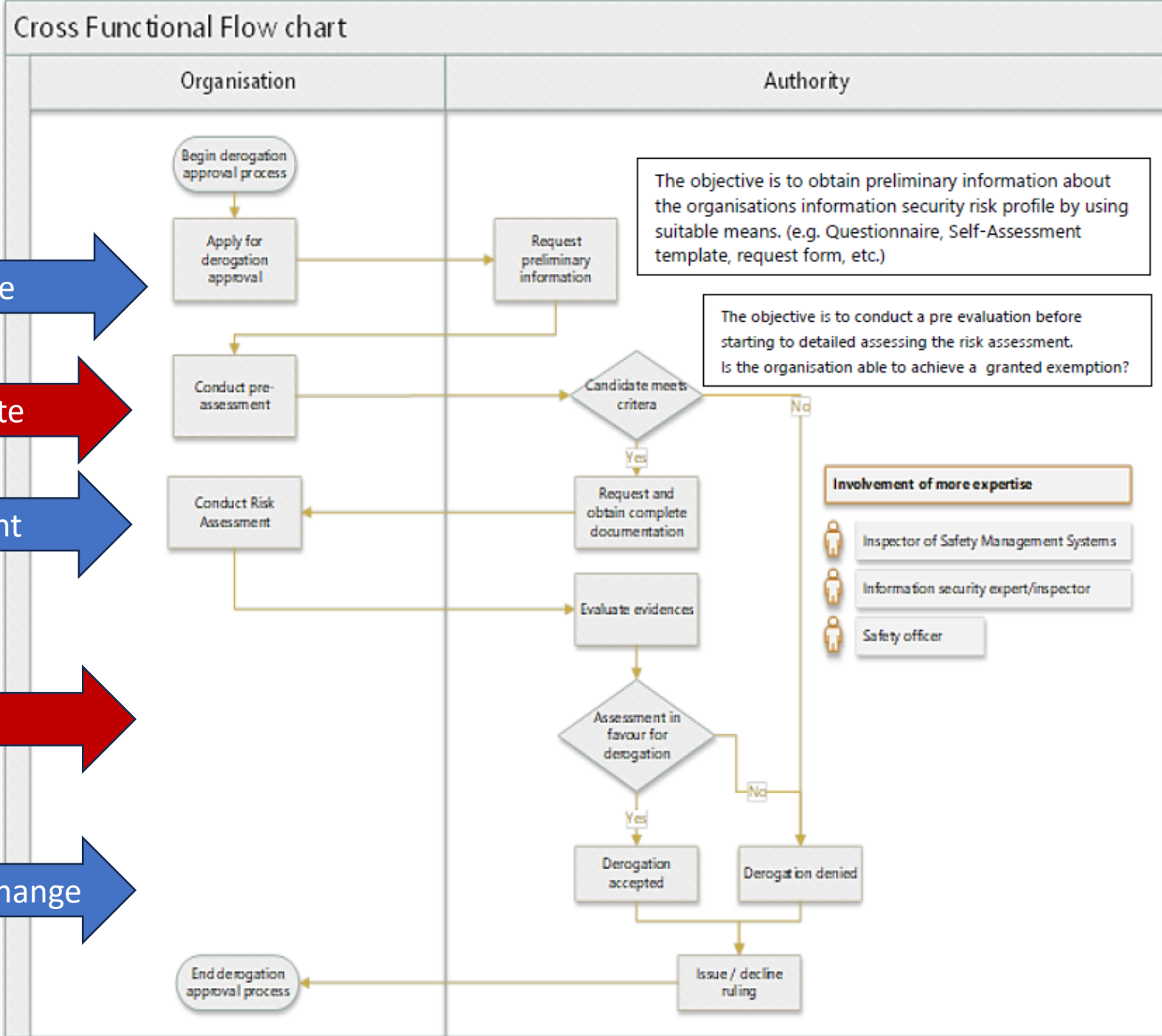
Part-IS TF G-02

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.

How the process works



Deliverable of the Workstream

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).

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

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.

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

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.

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.

The unmodified requirement of Part-IS

The ISO/IEC 27001 counterpart to the requirement

The reason for a specific Part-IS guidance

The add-on guidance

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

Search bar with magnifying glass icon

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

Requirement text

ISO27001 reference

Documentation of maturity assessment

Alpha-test assessment tool developed by Alexander Eckert - LBA

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	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

Save results (local)

„compliance“ 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

Requirement text

ISO27001 reference

Documentation of compliance assessment

Alpha-test assessment tool developed by Alexander Eckert - LBA

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



Marta Jurkiewicz is a senior specialist in civil aviation cybersecurity at the CAA of Poland. She has been dealing with what is broadly understood as information security for over ten years as a digital educator and cybersecurity awareness trainer.

Marta is a specialist in new technology and aviation law, in particular in personal data protection and civil aviation security. She is also a member of international working groups focused on cybersecurity in civil aviation.



Vasileios Papageorgiou is a Junior Expert for Cybersecurity in Aviation and is currently involved in Part-IS implementation support activities and Cyber Threat Intelligence. Prior to joining EASA, Vasileios gained experience in cybersecurity and counter-terrorism research activities, as well as UAS Operations.

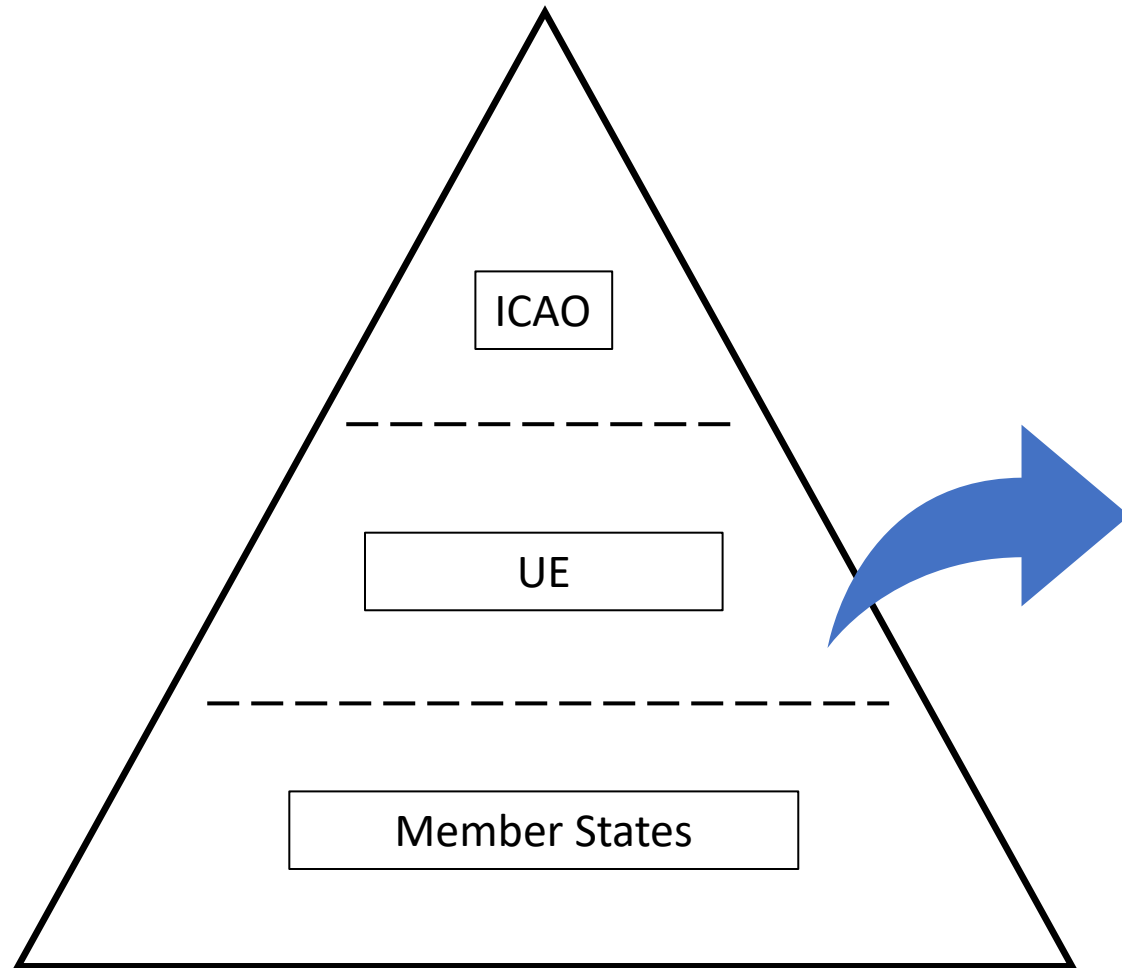
He holds a master's degree in Crisis & Security Management from Leiden University and a Bachelor's degree in International Relations & European Studies from the University of Piraeus.

Interplay with other EU Rules (NIS2 and AVSEC)



Part-IS Implementation Workshop

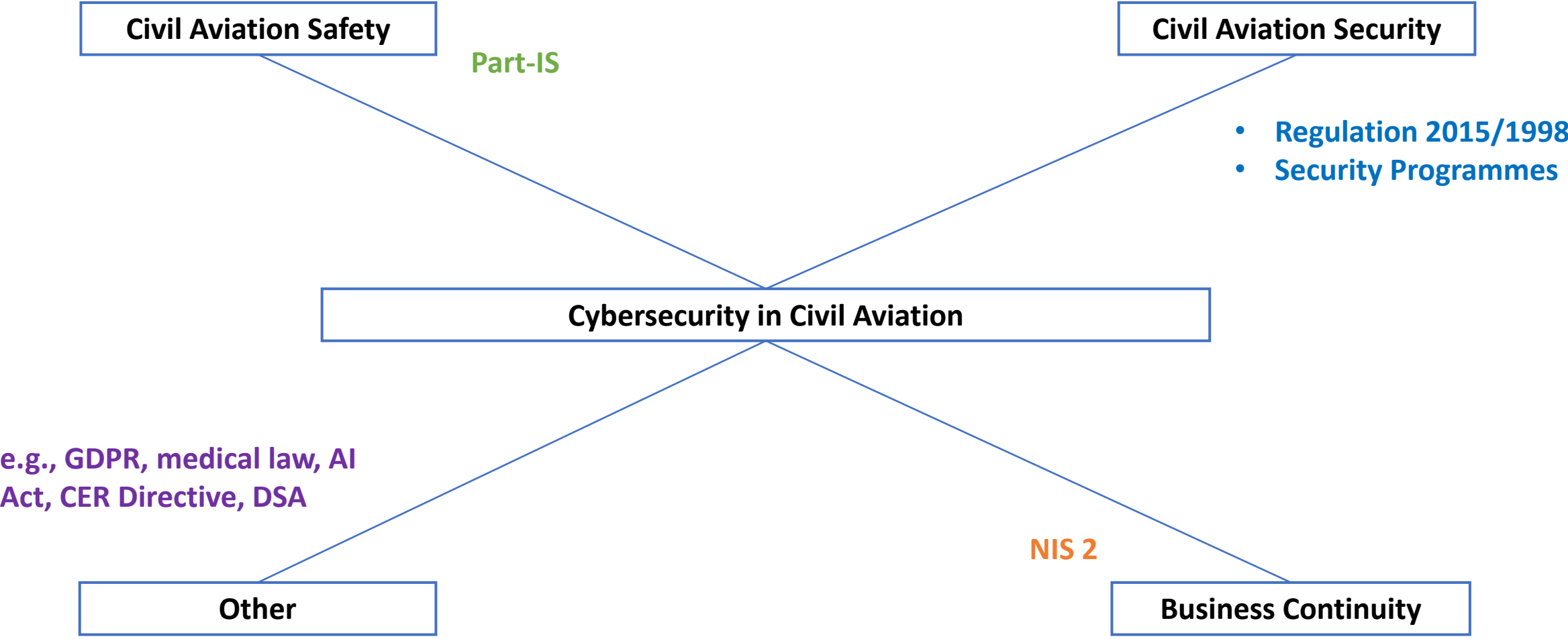
Legal Framework in Civil Aviation



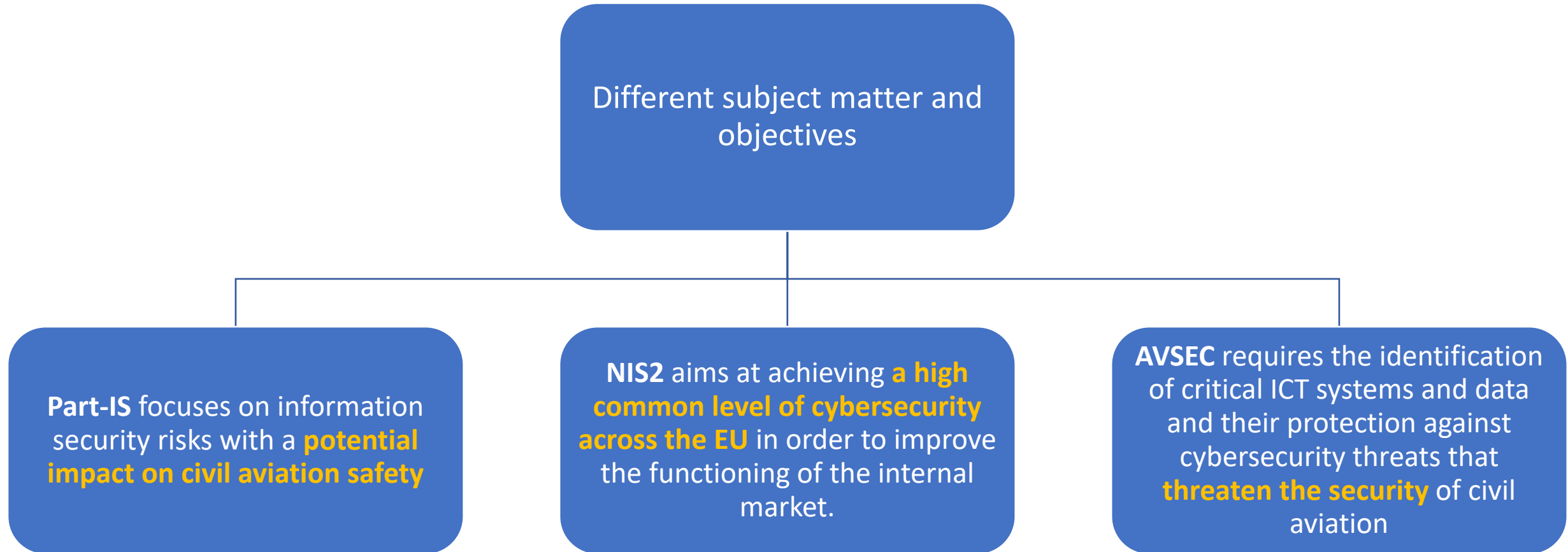
European Economic Area

- Basis for information security including cybersecurity
- Related to human rights

Different types of cybersecurity requirements



Three different set of rules



Legal equivalence established in the Part-IS Regulations

Reg. 2022/1645, article 4.2 & Reg. 2023/203, article 5.2

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

→ **NIS2: Can be credited towards compliance with Part-IS**

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

→ **AVSEC: Automatic credit towards everything in Part-IS except IS.I/D.OR.230 Information security external reporting scheme**

NIS2 – Annex III Correlation Table

Directive (EU) 2016/1148	Directive (EU) 2022/2555 NIS2	Subject
Article 14(1) and (2)	Article 21(1) to (4)	<i>Cybersecurity risk management measures</i>
Article 14(3)	Article 23(1)	<i>Reporting requirements</i>
Article 14(4)	Article 23(3)	<i>Reporting requirements</i>
Article 14(5)	Article 23(5), (6) and (8)	<i>Reporting requirements</i>
Article 14(6)	Article 23(7)	<i>Reporting requirements</i>
Article 14(7)	Article 23(11)	<i>Reporting requirements</i>

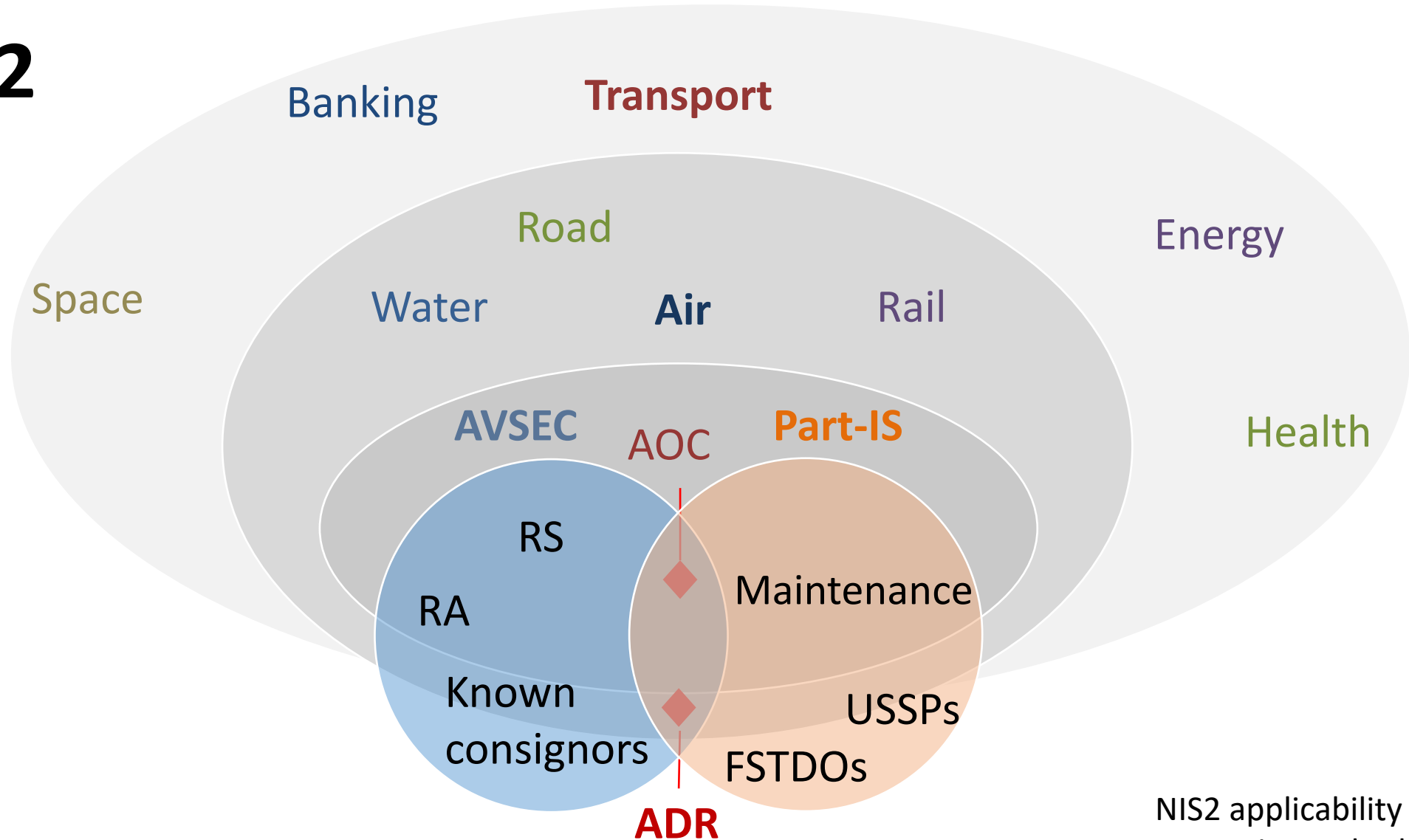
If I prefer to switch from AVSEC regulation to Part-IS?

Point 1.7.5 of the Annex to Reg. 2015/1998, as amended by Reg. 2019/1583

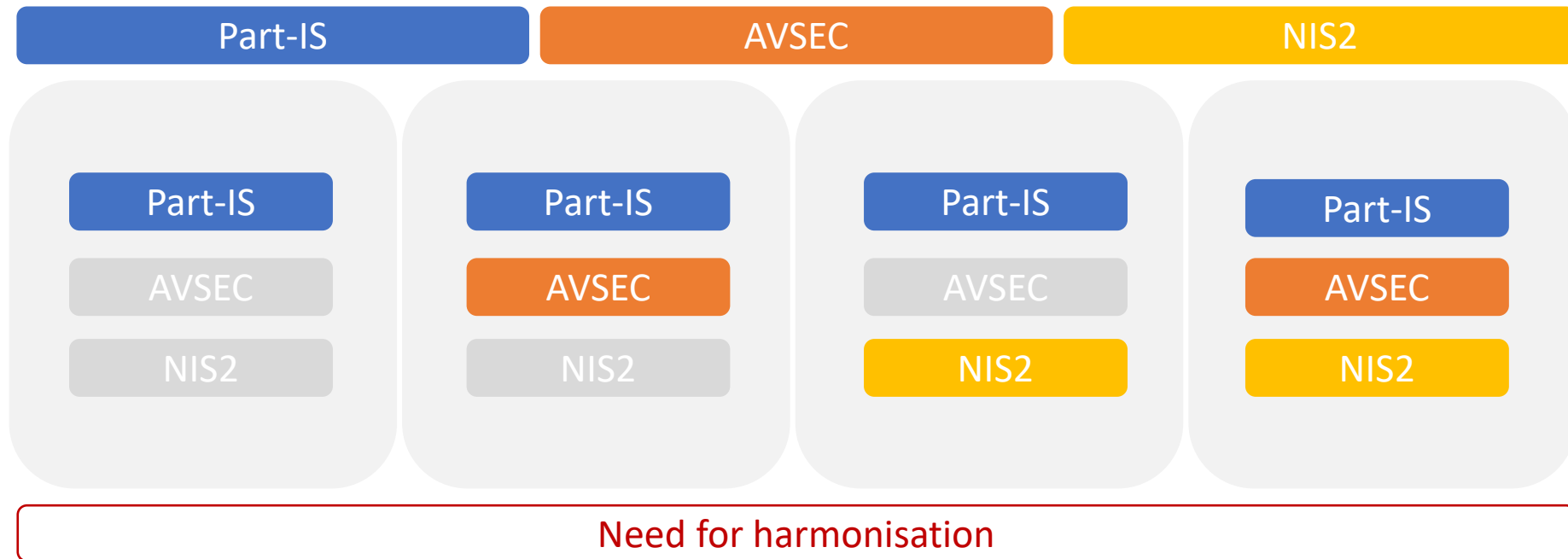
“Where airport operators, air carriers and entities as defined in the national civil aviation security programme are subjected to separate cybersecurity requirements arising from other EU or national legislation, the appropriate authority may replace compliance with the requirements of this regulation by compliance with the elements contained in the other EU or national legislation. The appropriate authority shall coordinate with any other relevant competent authorities to ensure coordinated or compatible oversight regimes.”

Different rules - different scopes

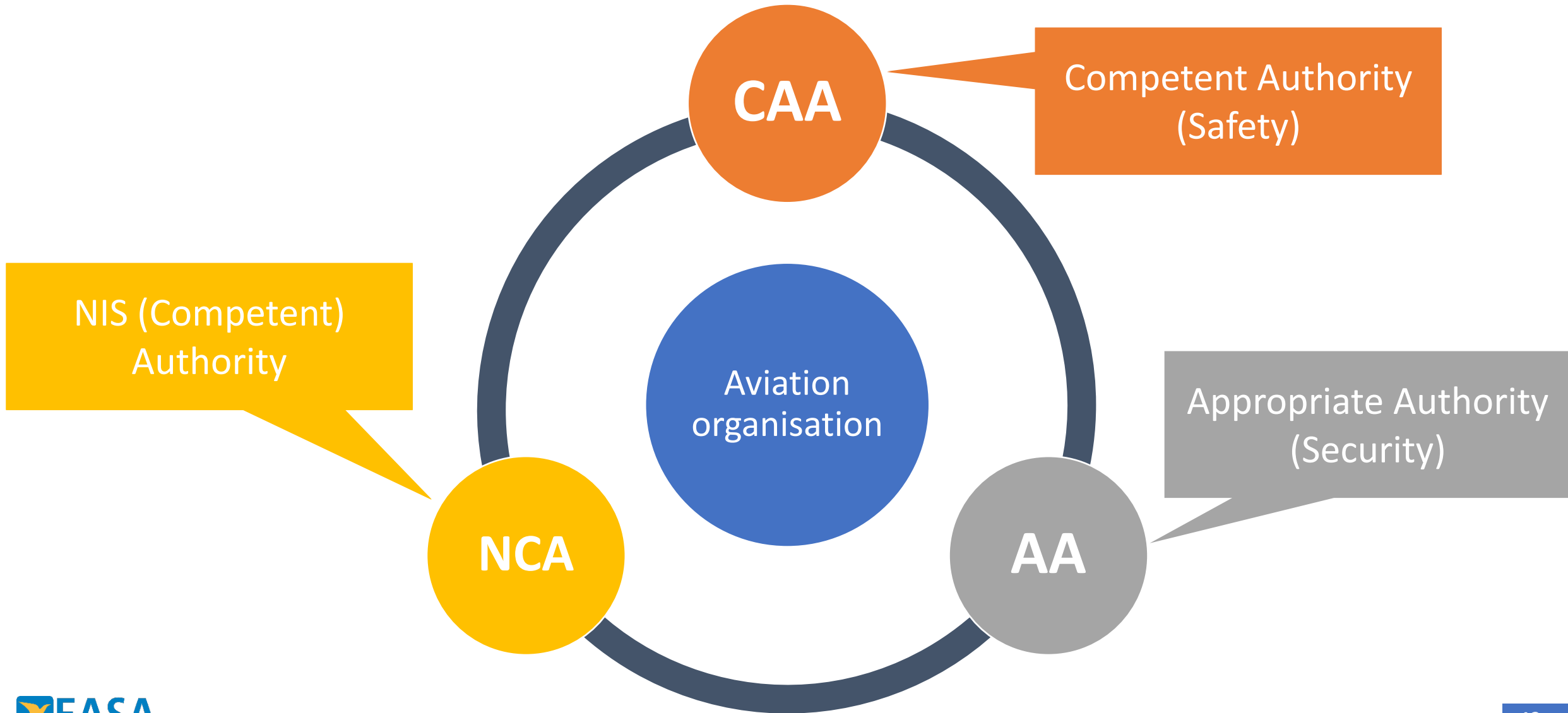
NIS2



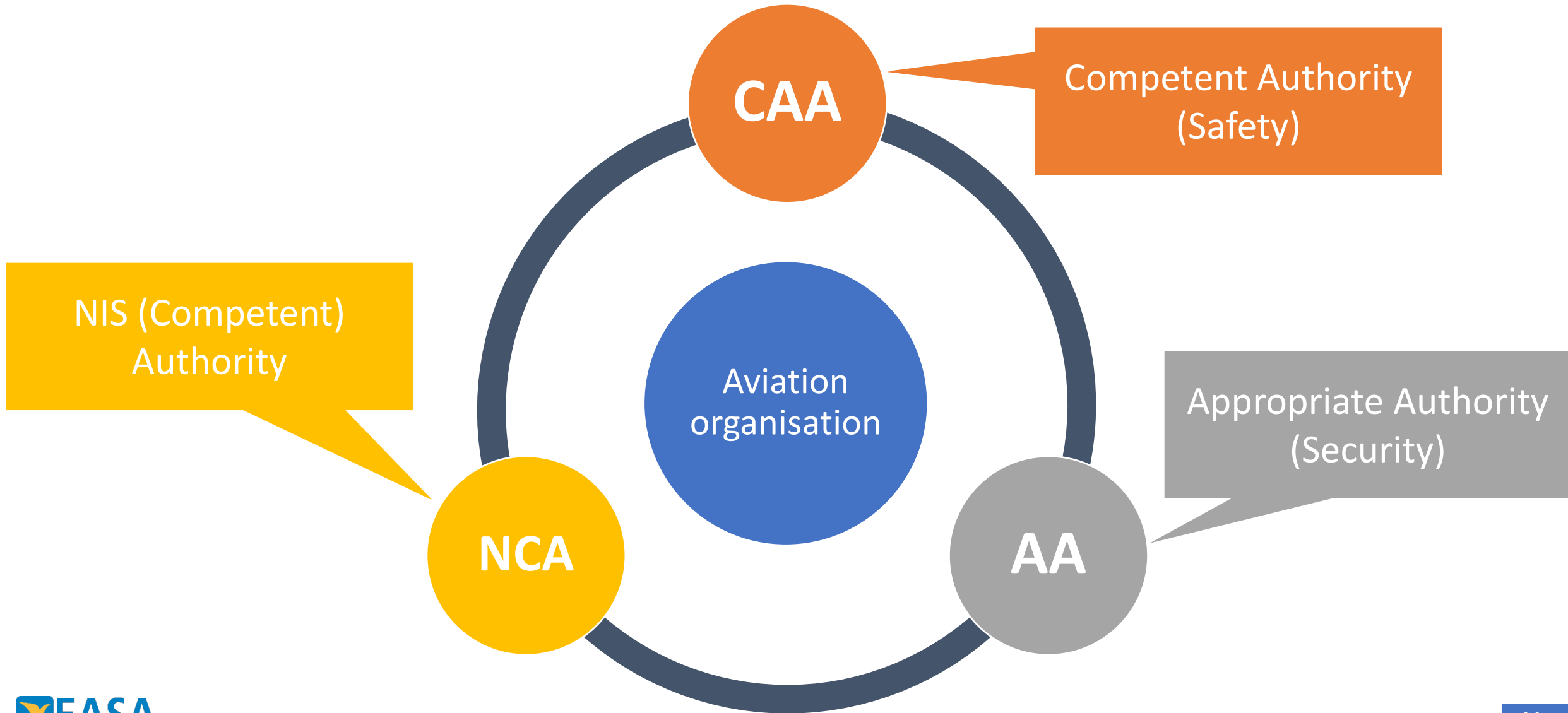
Different Possibilities & Overlaps



Authorities responsible for each regulation



Are the boundaries of an organisation the same?



Applicability of Part-IS vs other requirements - Draft

Organisation	Certificate	Part-IS	NIS 2	AvSec	Remarks
Commercial air carriers	AOC	Y	Y	Y	only Large (> 250 employee) or Medium 50 to 249 employees*
Airports	ADR Management	Y	Y	Y	only Large (> 250 employee) or Medium 50 to 249 employees*
Air traffic control [ATC]	ANSP	Y	Y	(Y)	only Large (> 250 employee) or Medium 50 to 249 employees*
Aircraft Manufacturers	POA, DOA	Y	Y / (Y)		To be determined by the Member State
Equipment Manufacturers	POA, DOA	Y	Y / (Y)		To be determined by the Member State
Maintenance organisations	MOA	Y	(Y)	(Y)	To be determined by the Member State
Maintenance management	CAMO	Y	(Y)	(Y)	To be determined by the Member State
Pilot training organisations	ATO, TRTO	Y			Unlikely – it could be still theoretically possible if the MS decides so
ATCO Training Organisations	ATCO TO	Y			- // -
Simulators' operators	FSTD Ops	Y			- // -
Aeromedical Centres	AeMC	Y			- // -

Key common points and differences

NIS 2	Part-IS	AvSec
Needs to be transposed to the national law of the MS	Directly applicable to concerned organisations & authorities	Same as Part-IS
Size of entity is important for applicability	Size is not important – risk is	Same as Part-IS
Type of entity is important for applicability	Type of entity is how applicability is defined	Type of entity is how applicability is defined
Applicable to smaller entities under conditions*	N/A	N/A
Applicability defined by type of organisation (business units)	Applicability defined by approval (organisations = approval holders)	Applicability defined by type of organisation (business units)
Flexibility on transposition of the rule	Rule has to be applied as such	Rule has to be applied as such
As a Directive, requirements are of a higher level	As a Regulation, there are more granular requirements.	Requirements on cybersecurity are in general of a higher level than in Part-IS
ISMS is not necessary	An ISMS is needed	ISMS is not necessary

Key common points and differences

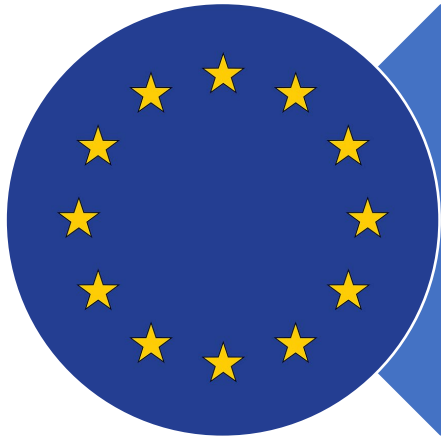
NIS 2	Part-IS	AvSec
Needs to be transposed to the national law of the MS	Directly applicable to concerned organisations & authorities	Same as Part-IS
Size of entity is important for applicability	Size is not important – risk is	Same as Part-IS
Type of entity is important for applicability	Type of entity is how applicability is defined	Type of entity is how applicability is defined
Applicable to smaller entities under conditions	Not applicable	Not applicable
Applicability defined by type of organisation (business units)	Applicability defined by approval (organisations = approval holder)	Applicability defined by type of organisation (business units)
Flexibility on transposition of the rule	Rule has to be applied as such	Rule has to be applied as such
As a Directive, requirements are of a higher level	As a Regulation, there are more granular requirements.	Requirements on cybersecurity are in general of a higher level than in Part-IS
ISMS is not necessary	An ISMS is needed	ISMS is not necessary

What to do?

What are our actions?

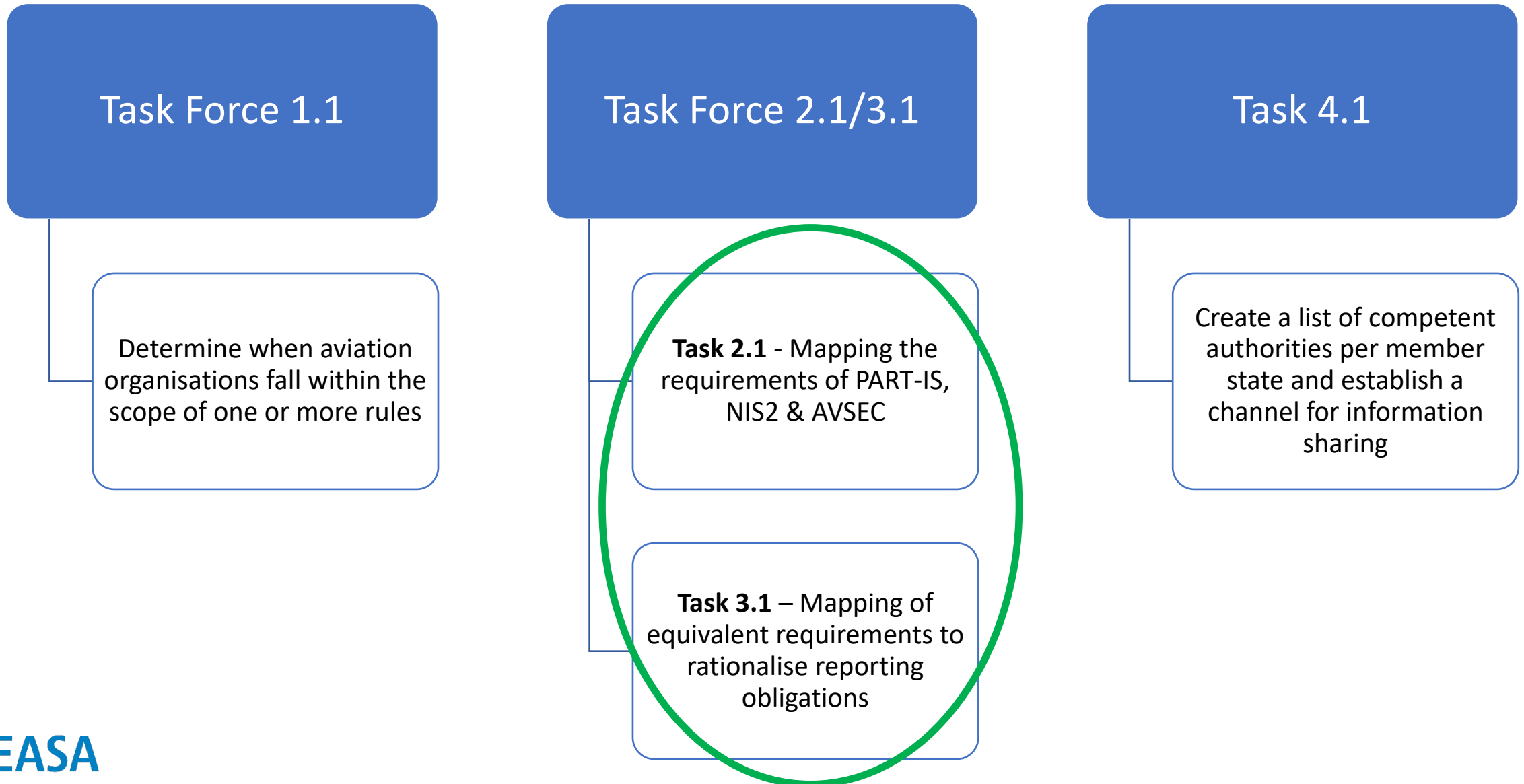


Part-IS Task Force

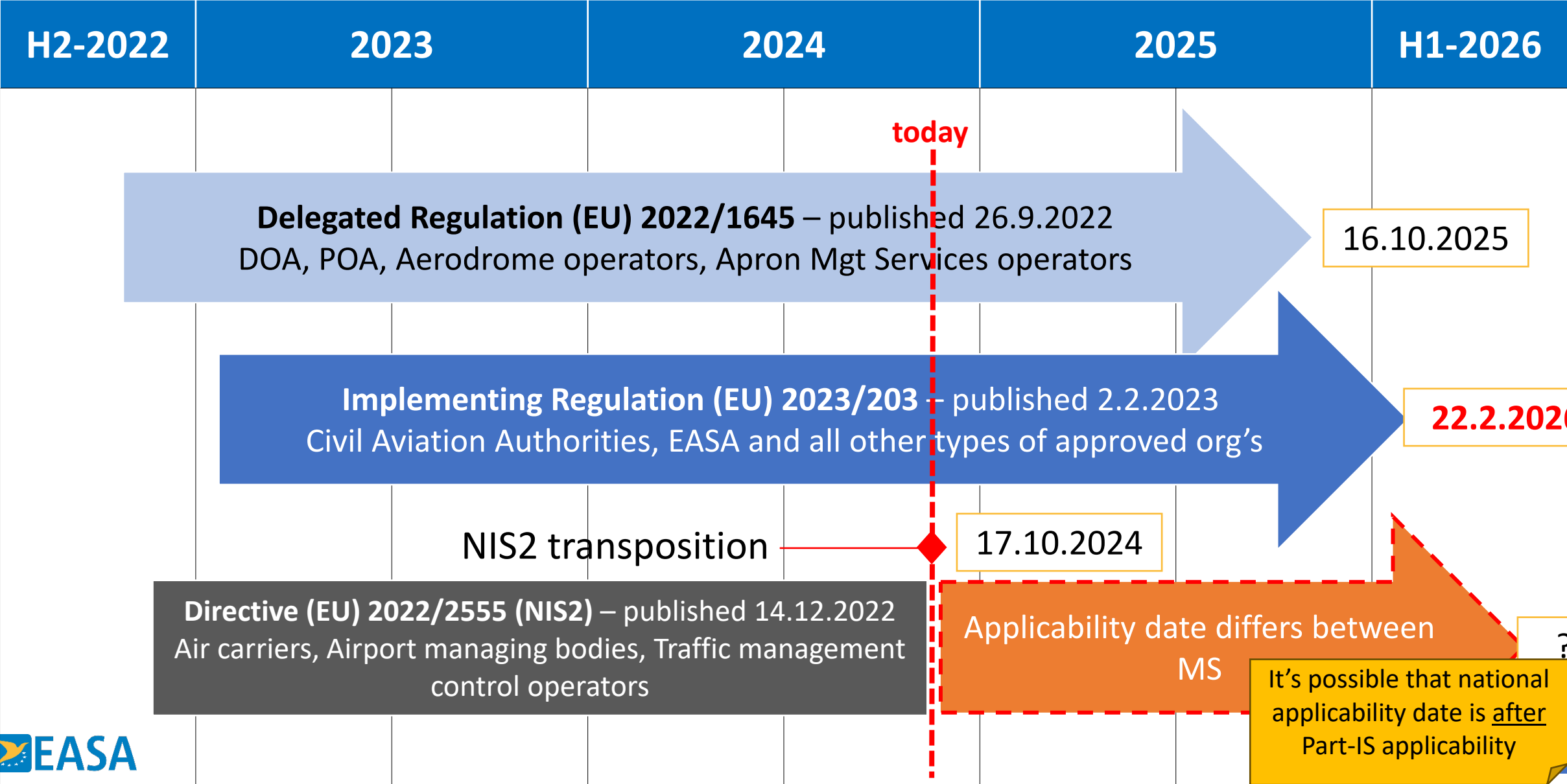


NIS Aviation
Cybersecurity Subgroup

Aviation Cybersecurity Subgroup - Structure



Part-IS implementation journey & NIS2



Q&A – *15 minutes*



Panel 2 - Staff competence building



Part-IS Implementation Workshop



Karl Specht is Principal Coordinator for Organisation Approvals and International Relations at EASA. He joined EASA in 2007 as a DOA Team Leader and later headed the Continuing Airworthiness Organisation section of EASA after holding positions as Engineering Manager and Head of Design Organisation at a German airline.

Karl holds a master's in Aeronautical Engineering.



Fabio Di Franco, at ENISA since 2017, leads the European Cybersecurity Skills Framework (ECSF) initiative, aligning it with regulatory frameworks and EU policies. With over 15 years in public and private sectors, he develops cybersecurity skills across the EU through training and exercises.

Fabio holds a master's and PhD in telecommunication engineering and is a frequent speaker, promoting talent in cybersecurity.



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

Fabio DI FRANCO

Cybersecurity Officer

08 10 2024

THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

*The ECSF provides an open tool to build a **common understanding of the cybersecurity professional roles in the EU** and common mappings with the appropriate skills and competences required.*



the ECSF website:

<https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>

THE 12 CYBERSECURITY PROFILES



**Chief Information
Security Officer
(CISO)**



**Cyber Incident
Responder**



**Cyber Legal,
Policy and
Compliance
Officer**



**Cyber Threat
Intelligence
Specialist**



**Cybersecurity
Architect**



**Cybersecurity
Auditor**



**Cybersecurity
Educator**



**Cybersecurity
Implementer**



**Cybersecurity
Researcher**



**Cybersecurity
Risk Manager**



**Digital Forensics
Investigator**



**Penetration
Tester**



EXAMPLE: CYBERSECURITY RISK MANAGER



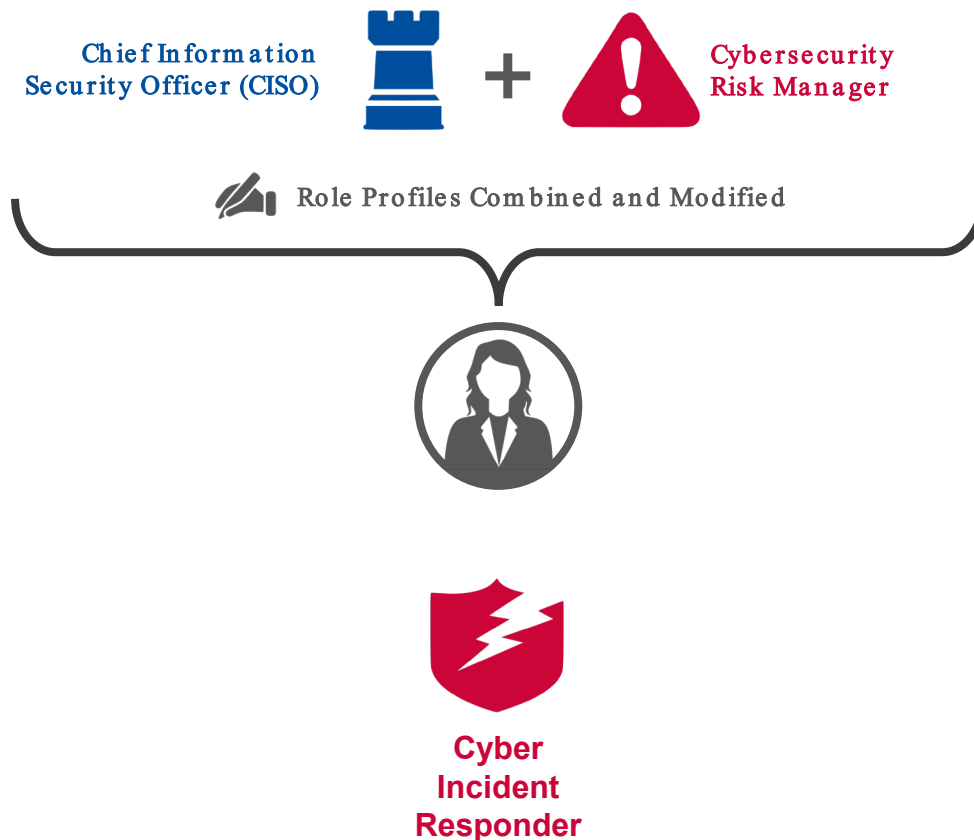
Profile Title	Cybersecurity Risk Manager
Alternative Title(s)	Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor Cybersecurity Impact Analyst Cyber Risk Manager
Summary statement	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.
Mission	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.
Deliverable(s)	<ul style="list-style-type: none"> • Cybersecurity Risk Assessment Report • Cybersecurity Risk Remediation Action Plan
Main task(s)	<ul style="list-style-type: none"> • Develop an organisation's cybersecurity risk management strategy • Manage an inventory of organisation's assets • Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems • Identification of threat landscape including attackers' profiles and estimation of attacks' potential • Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy • Monitor effectiveness of cybersecurity controls and risk levels • Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets • Develop, maintain, report and communicate complete risk management cycle

Key skill(s)	<ul style="list-style-type: none"> • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Analyse and consolidate organisation's quality and risk management practices • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options 	
Key knowledge	<ul style="list-style-type: none"> • Risk management standards, methodologies and frameworks • Risk management tools • Risk management recommendations and best practices • Cyber threats • Computer systems vulnerabilities • Cybersecurity controls and solutions • Cybersecurity risks • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Cybersecurity-related certifications • Cybersecurity-related technologies 	
e-Competences (from e-CF)	E.3. Risk Management E.5. Process Improvement E.7. Business Change Management E.9. IS-Governance	Level 4 Level 3 Level 4 Level 4

What typical outcomes are expected?
(workplace perspective)

What need to know and be able to do?
(learning perspective)

REQUIREMENTS STEMMING FROM PART-IS



- Establish a **policy on information security**
 - Identify and reviews **information security risks**
 - Define and implement **information security risk treatment measures**
-
- **Information security incidents** – detection, response, and recovery

CYBERSECURITY PROFESSIONAL CERTIFICATIONS

Certifications bodies mapped their credentials to the European Cybersecurity Skills Framework (ECSF),

BENEFITS:

- **individuals can identify the relevant certifications to enhance their career prospects and professional development effectively.**
- **organizations can leverage this mapping to create structured upskilling and reskilling pathways for their employees, aligning competencies and skills with specific roles.**



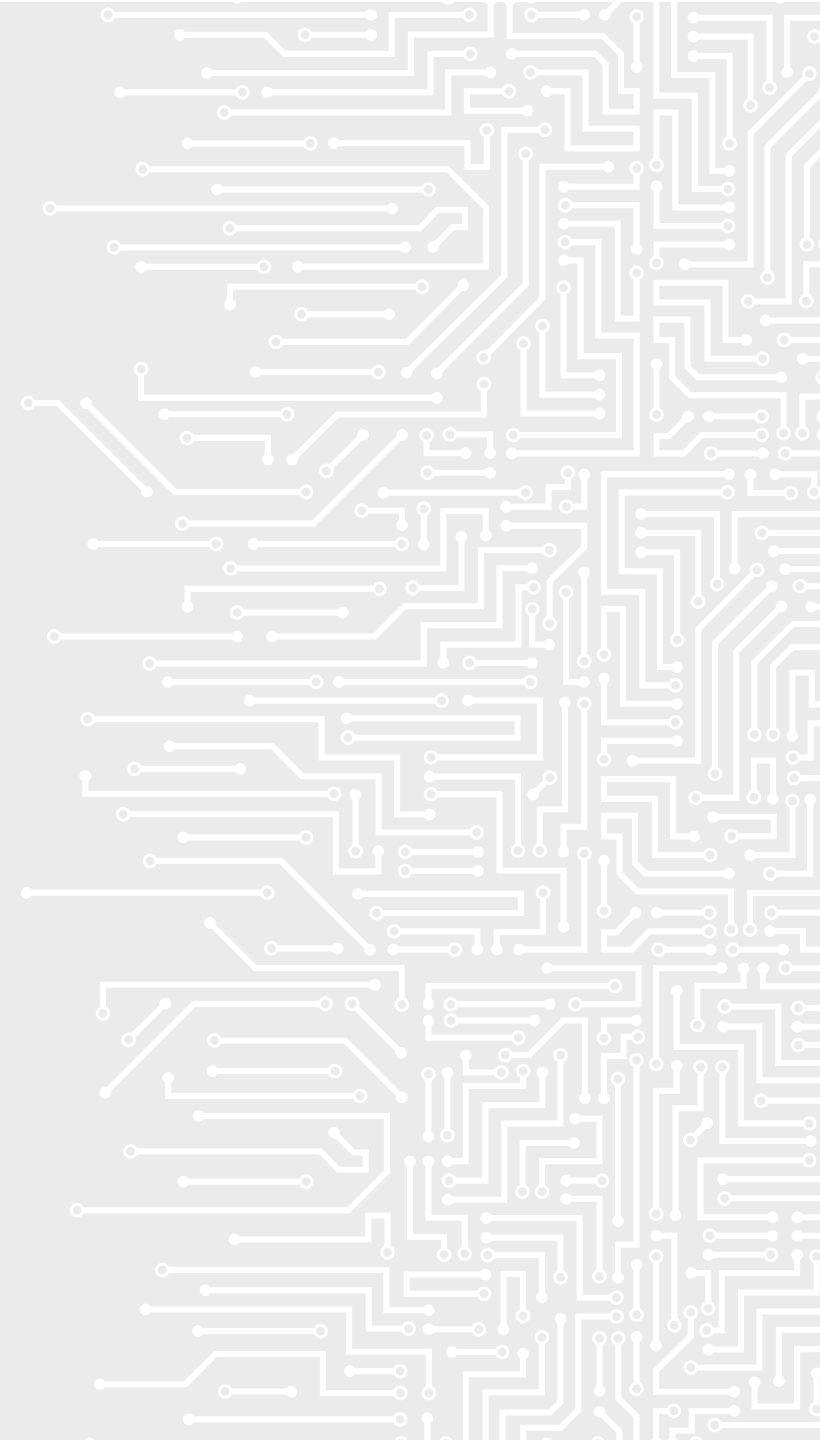
<https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework/certifications>

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

 Fabio.DiFranco@enisa.europa.eu

 www.enisa.europa.eu





David Nieto is Director of Airports and Aviation Security at AESA since 2018. He oversees AVSEC and cybersecurity frameworks in Spanish aviation. With extensive experience in safety, security, and certification, he also moderates the ECAC Cybersecurity Study Group.

David has a background in aeronautical engineering, a master's degree in cybersecurity and a master's degree in leadership and public administration.

STAFF COMPETENCE BUILDING

Cyber security competences



Image created with AI

Training and competence model

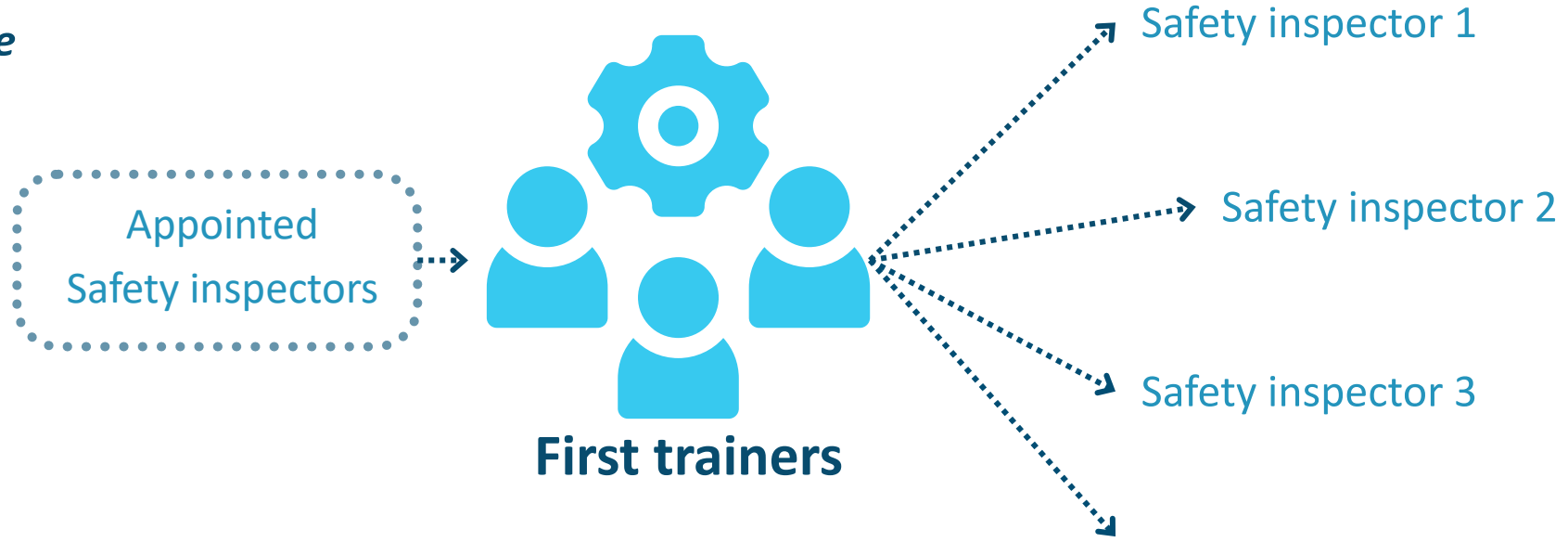
Analysis of PART-IS or ISMS training courses

No PART-IS oversight training course available



TRAINER OF TRAINERS

*Each applicable
PART-IS
Domain*



Staff competence plan and progress

Stage 1

Appointment of First Trainers
Accomplished

Stage 2

Mandatory and recommended
theoretical training
Accomplished

MANDATORY

W/S AESA-EASA (7th May)

COURSES

- Basic Cybersecurity (CCN)
- Introduction to **ISO 27001**

RECOMMENDED

- Social Engineering
- Management of cybercrisis



Stage 3

OJT: Assessments by domain
Desk and/or on-site exercises
In progress

Stage 4

Develop content new training course on
Cyber security and EASA PART-IS
In progress

Stage 5

Planning the appropriate training sessions for
2025
In progress

Stage 6

Improvement Cycle
Not started



Thanks for your attention



@AesaSpain



www.seguridadaerea.gob.es



AESA





Patrick Spelt is Head of Cybersecurity Supervision at the Human Environment and Transport Inspectorate of the Ministry of Infrastructure and Water Management in the Netherlands. He is deeply involved in the cybersecurity oversight for critical infrastructure sectors like Maritime, Rail, and Aviation.

Patrick has previously held key IT and risk management roles in the financial sector.



Part-IS Implementation Workshop

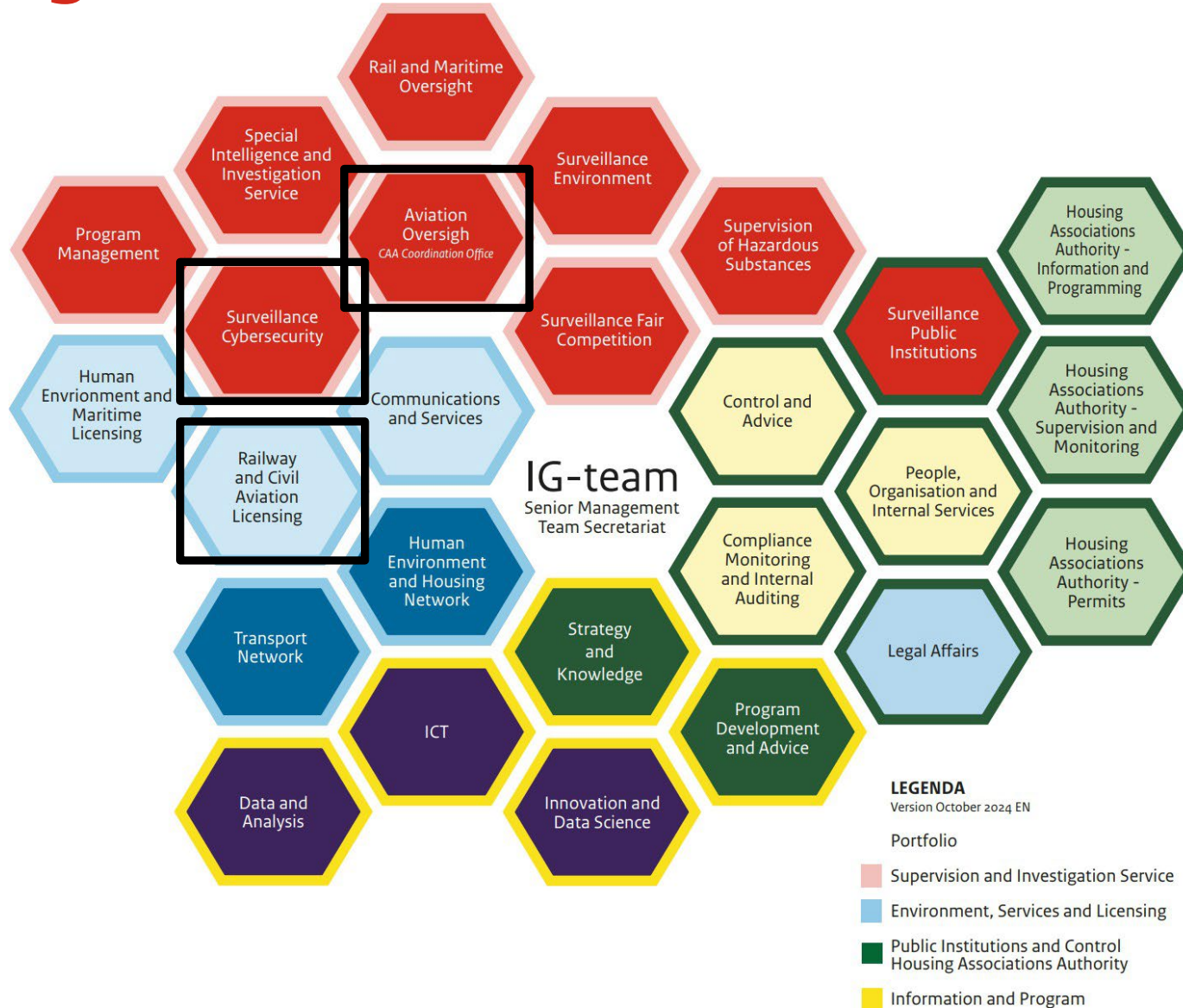
Session: Staff Competence Building

Dutch Civil Aviation Authority (CAA-NL)

7th and 8th of November 2024



Organizational Structure of Competent Staff





Staff Competence building (1)

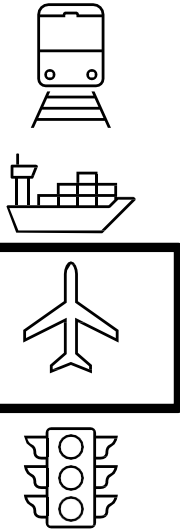
Surveillance
Cybersecurity

17 fte

Transport



Transport

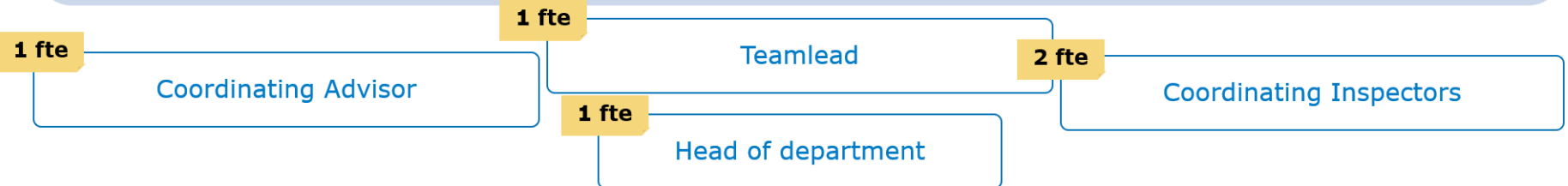


Support (HR, Legal, Data, Control, Communication & Press, Networking etc.)

Cybersecurity Supervision

12 fte

Senior Inspectors





Staff Competence building (2)

Cybersecurity Supervision

12 fte

Senior Inspectors

Curriculum

Generic

- Inspector training (basic and advanced)
- Dutch General Administrative Law
- Advanced Law and Digital Technologies
- Effective Communication (A and B)
- Pyramidal Writing
- IPMA-D Project Management

Cyber IT

- LDR433 Managing Human Risk
- LDR514 Strategic Security Planning, Policy and Leadership
- LDR521 Security Culture for leaders
- SEC504 Hacker Tools, Techniques and Incident Handling
- SEC599 Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses
- EDRP (Disaster Recovery Professional)

Cyber OT

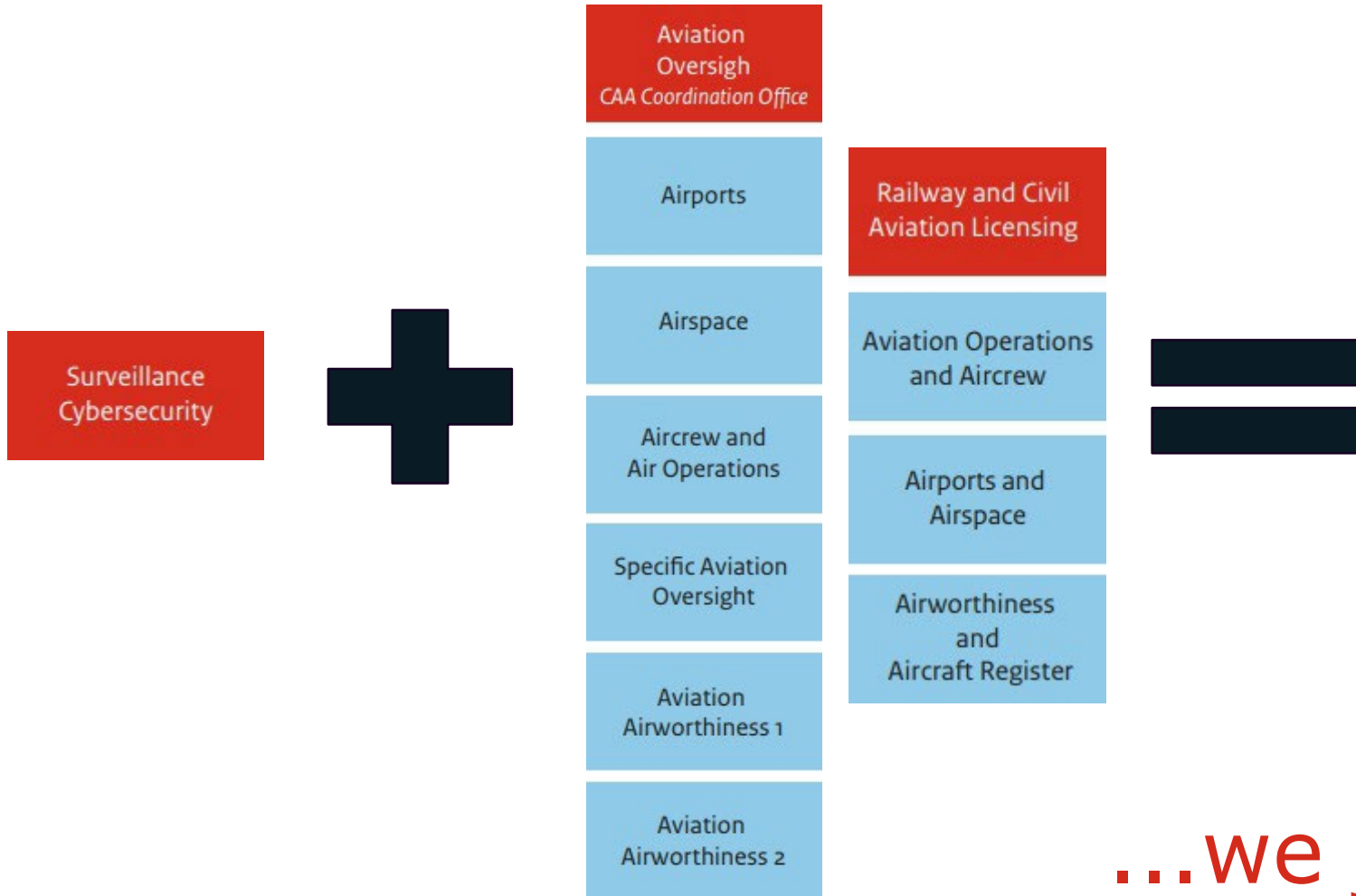
- SCADA security manager
- IEC62443 (cybersecurity for Industrial Automation and Control systems)
- ICS410 (ICS SCADA Security Essentials)
- ICS515 (ICS visibility, detection and response)
- ICS612 (ICS security in-depth)
- SEC566 (Implementing and Auditing CIS Controls)
- CSIR workshop OT security fundamentals

Certification

- CGEIT (Certified in the Governance of IT)
- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Controls)
- CISSP (Certified Information Systems Security Professional)
- ISO/IEC 27001 Lead Auditor
- CEH (Certified Ethical Hacker)



To be really competent...



...we join forces!



Christoph Schnyder is Cyber Security Coordinator at Federal Office of Civil Aviation in Switzerland, responsible for strategy, certification, and EASA Part-IS implementation, with representation in national and international bodies.

He has over 20 years' experience and has held various roles as a software engineer, security engineer and product cyber security expert.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Zivilluftfahrt BAZL
Office fédéral de l'aviation civile OFAC
Ufficio federale dell'aviazione civile UFAC
Federal Office of Civil Aviation FOCA



Information Security Staff competence building

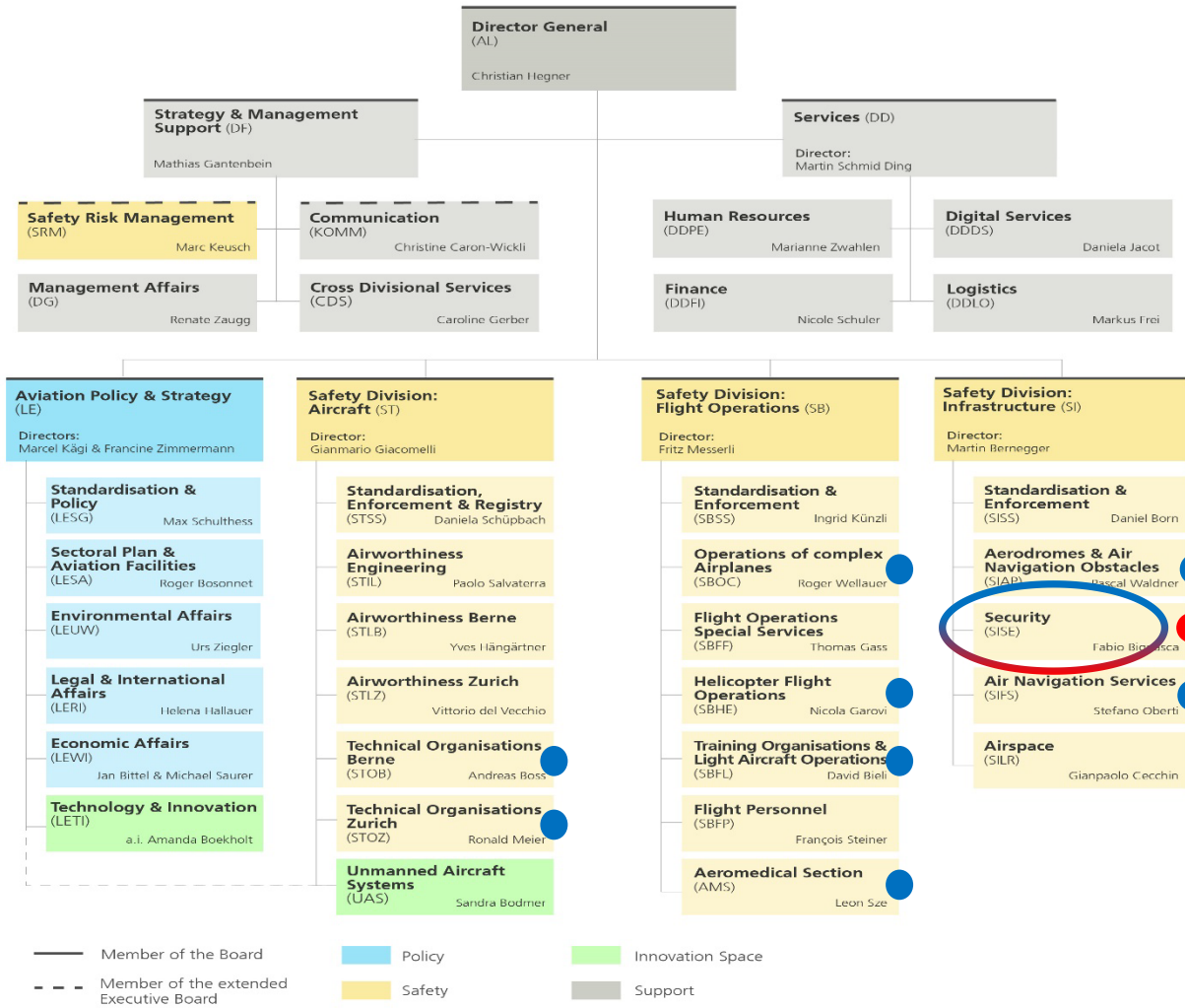
The approach of FOCA

EASA Part-IS Implementation Workshop,
Cologne 07 & 08. November 2024

Christoph Schnyder,
Cyber Security Coordinator / Program Lead



Organisation of Information Security at FOCA



01.10.2024



Dedicated **Information Security SME Group** within AVSEC section.

Gradual step-by step build up to **5 FTE** from 2024 ... 2026



Providing **information security expertise** in certification and oversight activities to safety sections in regard to Part-IS, as members of SMS audit teams.



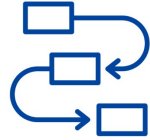
Performing AVSEC audits and inspections in regard to (EU) 2019/1583 and NASP chap. 19

● Aviation Security (EU) 2019/1583

● Aviation Safety (EU) 2022/1645, (EU) 2023/203



Upskilling of people



Processes



People

Tasks

- Certification & oversight regarding information security
- Collection & processing of reported cyber incidents

New tasks & roles

Roles

- ISMS Inspector
- Cyber security expert

Needed competencies

- Auditor
- IT & cyber security
- Safety / security management
- Risk management
- Technical organization knowledge
- Quality assurance

Workload estimation

- First estimation based on experience with audits of NASP chap. 19 and extrapolation

Upskilling strategy

- ISO-27001 Lead Auditor
- ISO-27001 Manager
- CISA (ISACA)
- Basics on cybersecurity

Recruiting needs

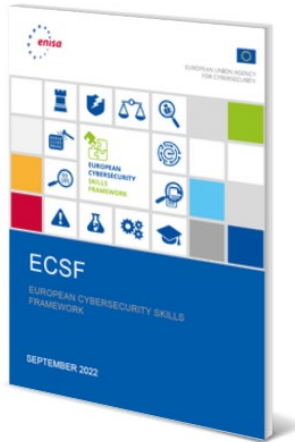
- 5 FTEe approved until 2026
- Multi lingual (GE / F/ I) and E
- Team player
- Communication

Upskilling/training of new and actual employees

start in 2025



Guidance to evaluate staff competencies



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

[European Cybersecurity Skills Framework Role Profiles Manual](#)

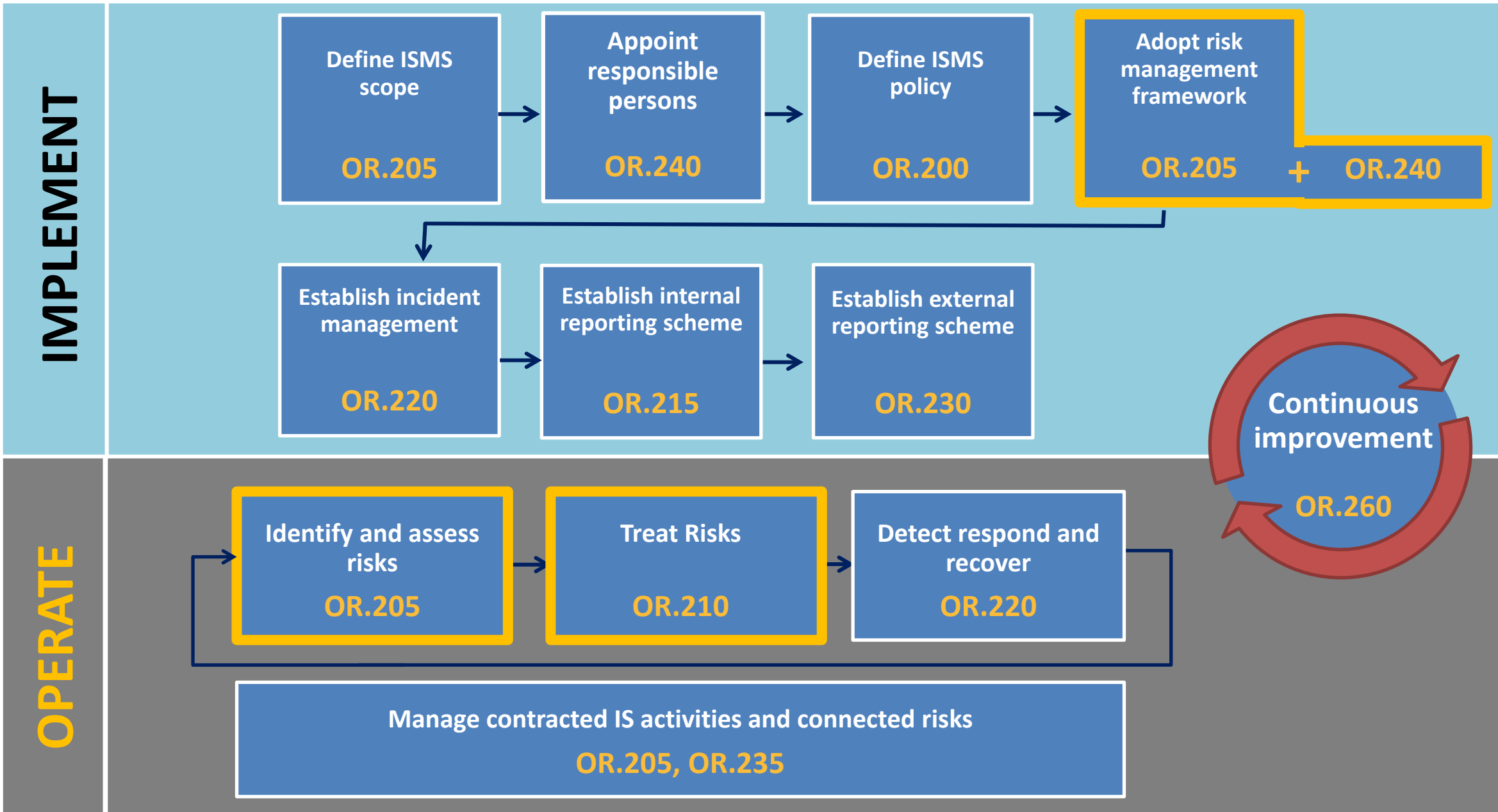
	Oversight and Governance (OG) Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.	Work Roles ▾
	Design and Development (DD) Conducts research, conceptualizes, designs, develops, and tests secure technology systems, including on perimeter and cloud-based networks.	Work Roles ▾
	Implementation and Operation (IO) Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.	Work Roles ▾
	Protection and Defense (PD) Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.	Work Roles ▾
	Investigation (IN) Conducts national cybersecurity and cybercrime investigations, including the collection, management, and analysis of digital evidence.	Work Roles ▾
	Cyberspace Intelligence (CI) Collects, processes, analyzes, and disseminates information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.	Work Roles ▾
	Cyberspace Effects (CE) Plans, supports, and executes cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.	Work Roles ▾

[Workforce Framework for Cybersecurity \(NICE Framework\)](#)

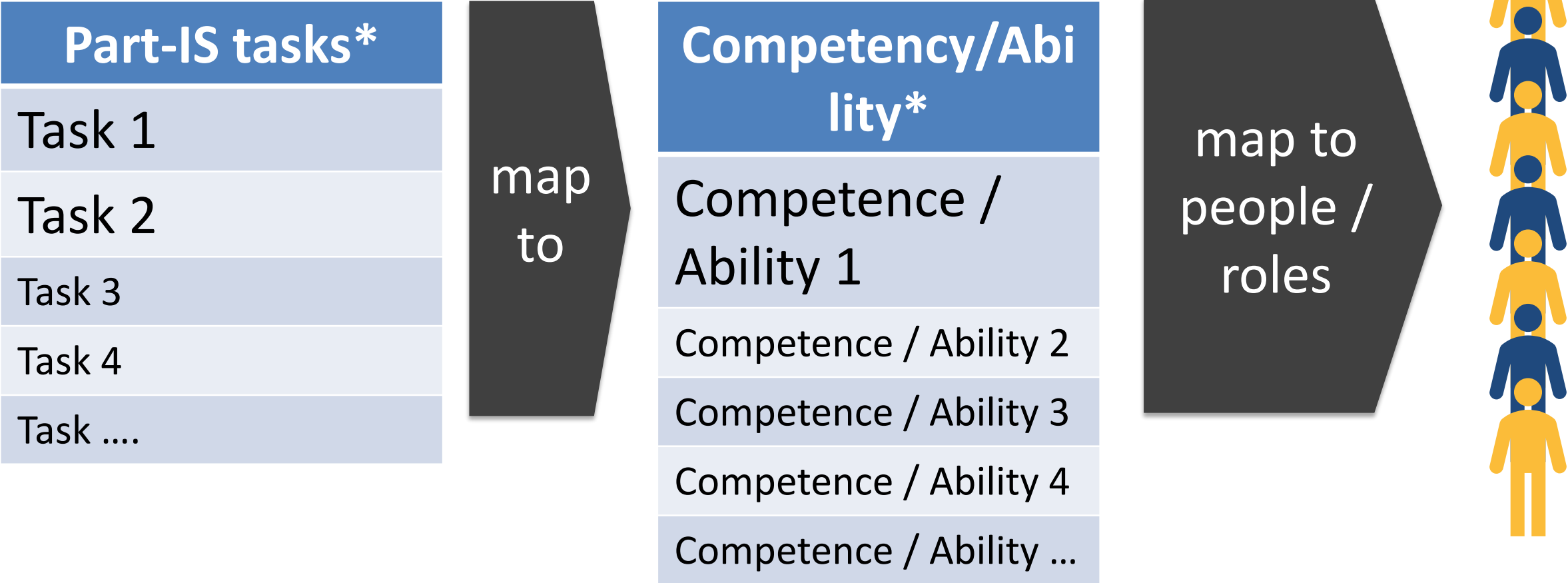


Davide Martini is an Aerospace Engineer and a Senior Cybersecurity Expert at EASA since March 2016. He leads efforts in developing aviation cybersecurity regulations and the implementation of the European cybersecurity strategy for aviation. Previously, he spent over 15 years in the aviation industry.

ECSF adaptation for Part-IS roles



Personnel Competence



In case of lack of competences

→ **Option 1** – upskilling

→ GAP Analysis required

→ **Option 2** – recruitment

→ Job profile needed

Realistic Job Description

Position Summary

- As our **Information Security Maestro**, you'll be the guardian of our digital kingdom, wielding a masterful command of security technologies and a keen eye for emerging threats. You'll be the last line of defense against the hordes of hackers, viruses, and other digital nemeses.

Realistic Job Description

Qualifications

- **Master of the Arcane Arts:** Besides CISM, CISSP, CISA, ITIL, CIPM, CEH qualification, possess a deep understanding of security protocols, encryption algorithms, and network topologies that would make any wizard jealous.
- **Battle-Hardened Warrior:** Have at least 10 years of experience in the field of cybersecurity, facing down the most formidable threats.
- **A Touch of Madness:** Be willing to think outside the box and embrace unconventional strategies to outmaneuver your adversaries.

The effect




How to do it?

Standard roles proposed by ECSF

 Chief Information Security Officer (CISO)	 Cyber Incident Responder	 Cyber Legal, Policy and Compliance Officer
 Cyber Threat Intelligence Specialist	 Cybersecurity Architect	 Cybersecurity Auditor
 Cybersecurity Educator	 Cybersecurity Implementer	 Cybersecurity Researcher
 Cybersecurity Risk Manager	 Digital Forensics Investigator	 Penetration Tester

Source: ENISA



APPLICATION OF THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK TO AVIATION

Contents

- 1. Introduction 2
- 2. Analysis of the situation and the target environment..... 3
- 3. Identification of specific objectives to be achieved..... 4
- 4. Selection of the appropriate ECSF components 4
- 5. Adapting the selected components according to specific needs 7
 - 5.1 Chief Information Security Officer / Responsible Person under Part-IS 8
 - 5.2 Cyber Legal, Policy & Compliance Officer / Compliance monitoring under Part-IS..... 11
 - 5.3 Cybersecurity Auditor / Cybersecurity Auditor within compliance monitoring function..... 12
 - 5.4 Cybersecurity Risk Manager / Appointed person under Part-IS..... 14
 - 5.5 Cybersecurity Incident Responder 16
- 6. Conclusions 17
- 7. Possible developments 18




<https://www.easa.europa.eu/community/topics/application-european-cybersecurity-skills-framework-aviation>

The roles from aviation perspective




Profile Title	Deliverable	Part – IS role considerations
Chief Information Security Officer (CISO)	Cybersecurity Strategy / Policy	Responsible Person
Cyber Legal, Policy & Compliance Officer	Compliance Manual / Compliance Report	Compliance Monitoring
Cybersecurity Auditor	Cybersecurity Audit Plan / Report	Auditor within compliance monitoring function
Cybersecurity Risk Manager	Cybersecurity Risk Assessment Report / Remediation Action Plan	One of the “appointed persons”
Cybersecurity Implementer	Cybersecurity Solutions	Not specified, but expected
Cyber Incident Responder	Incident Response Plan / Incident Report	One of the “appointed persons”

The roles from aviation perspective

1ST LINE OF DEFENCE

- 
CYBER INCIDENT RESPONDER
- 
CYBERSECURITY IMPLEMENTER
- 
CYBERSECURITY ARCHITECT






2ND LINE OF DEFENCE

- 
CHIEF INFORMATION SECURITY OFFICER (CISO)
- 
CYBER LEGAL, POLICY AND COMPLIANCE OFFICER
- 
CYBERSECURITY RISK MANAGER

3RD LINE OF DEFENCE

- 
CYBERSECURITY AUDITOR

SUPPORTING

- 
CYBER THREAT INTELLIGENCE SPECIALIST
- 
PENETRATION TESTER
- 
DIGITAL FORENSICS INVESTIGATOR
- 
CYBERSECURITY RESEARCHER
- 
CYBERSECURITY EDUCATOR


What about competences and skills?

For the time being no adaptations have been proposed

Key skill(s)	<ul style="list-style-type: none"> • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Analyse and consolidate organisation's quality and risk management practices • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options 	
Key knowledge	<ul style="list-style-type: none"> • Risk management standards, methodologies and frameworks • Risk management tools • Risk management recommendations and best practices • Cyber threats • Computer systems vulnerabilities • Cybersecurity controls and solutions • Cybersecurity risks • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Cybersecurity-related certifications • Cybersecurity-related technologies 	
e-Competences (from e-CF)	E.3. Risk Management E.5. Process Improvement E.7. Business Change Management E.9. IS-Governance	Level 4 Level 3 Level 4 Level 4

Although it is suggested that skills, competences, and knowledge should be reviewed to include safety and aviation specificities where appropriate.

Example - CISO

 EASA
European Union Aviation Safety Agency

APPLICATION OF THE EUROPEAN
 CYBERSECURITY SKILLS FRAMEWORK TO
 AVIATION


Contents

- 1. Introduction
- 2. Analysis of the situation and the target envi
- 3. Identification of specific objectives to be ac
- 4. Selection of the appropriate ECSF compone
- 5. Adapting the selected components accordin
 - 5.1 Chief Information Security Officer / Re
 - 5.2 Cyber Legal, Policy & Compliance Offic
 - 5.3 Cybersecurity Auditor / Cybersecurity I
 - 5.4 Cybersecurity Risk Manager / Appointe
 - 5.5 Cybersecurity Incident Responder
- 6. Conclusions
- 7. Possible developments

5.1 Chief Information Security Officer / Responsible Person under Part-IS

<p>Summary statement</p>	<p>Manages an organisation’s cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected, with a strong emphasis on operational safety.</p>
<p>Mission</p>	<p>Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.</p>

Example - CISO



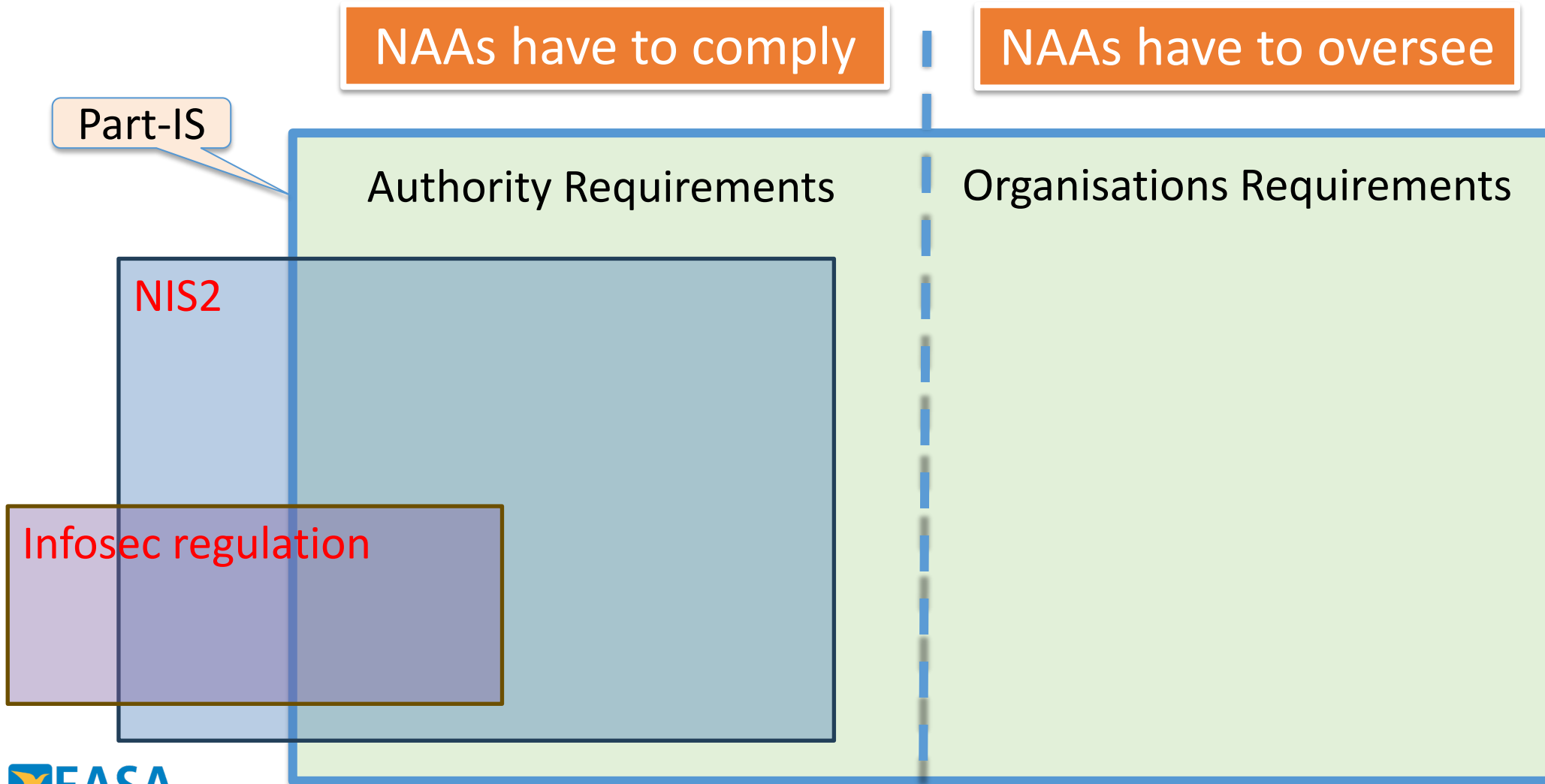
APPLICATION OF THE EUROPEAN
CYBERSECURITY SKILLS FRAMEWORK TO
AVIATION

Contents

- 1. Introduction 2
- 2. Analysis of the situation and the target environment..... 3
- 3. Identification of specific objectives to be achieved..... 4
- 4. Selection of the appropriate ECSF components 4
- 5. Adapting the selected components according to specific needs 7
 - 5.1 Chief Information Security Officer / Responsible Person under Part-IS..... 8
 - 5.2 Cyber Legal, Policy & Compliance Officer / Compliance monitoring under Part-IS..... 11
 - 5.3 Cybersecurity Auditor / Cybersecurity Auditor within compliance monitoring function..... 12
 - 5.4 Cybersecurity Risk Manager / Appointed person under Part-IS..... 14
 - 5.5 Cybersecurity Incident Responder..... 16
- 6. Conclusions 17
- 7. Possible developments 18

Main Tasks	
ECSF original	Adapted
<p>Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives</p>	<p>Define, implement, communicate and maintain cybersecurity goals, requirements, strategies and policies that are aligned with the business strategy to support the organisation's objectives¹ [see note 1], taking into account the safety perspective: In addition to considering cybersecurity objectives, safety perspectives should be integrated into the objectives, requirements, strategies and policies. This will ensure that cybersecurity measures do not compromise the safety of operational systems and processes. Safety considerations should be included in risk assessments, threat modelling and decision-making processes.</p>
<p>Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution</p>	<p>Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution, considering safety implications: When presenting the cybersecurity vision, strategies and policies to senior management, it is crucial to highlight the safety implications and emphasise the importance of aligning cybersecurity measures with operational safety. This will ensure that senior management understands the potential impact of cybersecurity decisions on the overall safety of the organisation.</p>

The future Information Security regulatory landscape applicable to NAAs



How to

NAAAs have to comply

- Requirements are overlapping
- Deadlines are staggered (in some case not known yet)
- A mapping exercise is recommended to define the extent of overlapping and allow prioritisation of tasks
- Compliance can be then streamlined
- An ISMS will offer a structured framework for managing compliance
- Competence building and **training should focus on implementation**

NAAAs have to oversee

- Part-IS to be included in the oversight process for all types of organisations
- Competence building and **training needs to be tailored to oversight activities**

How to

NAAAs have to comply

- Requirements are overlapping
- Deadlines are staggered (in some case not known yet)
- A mapping exercise is recommended to define the extent of overlapping and allow prioritisation of tasks
- Compliance can be then streamlined
- An ISMS will offer a structured framework for managing compliance
- Competence building and **training should focus on implementation**

NAAAs have to oversee

- Part-IS to be included in the oversight process for all types of organisations
- Competence building and **training needs to be tailored to oversight activities**



Included in the OA process

The roles from aviation perspective / NAAs

Profile Title	Deliverable	Part – IS role considerations
Chief Information Security Officer (CISO)	Cybersecurity Strategy / Policy	Person with authority to implement Part-IS
Cyber Legal, Policy & Compliance Officer	Compliance Manual / Compliance Report	Auditing/Compliance
Cybersecurity Auditor	Cybersecurity Audit Plan / Report	Auditing/Compliance
Cybersecurity Risk Manager	Cybersecurity Risk Assessment Report / Remediation Action Plan	Delegated role is expected
Cybersecurity Implementer	Cybersecurity Solutions	Not specified but expected
Cyber Incident Responder	Incident Response Plan / Incident Report	Delegated role is expected

How to

NAAAs have to comply

- Requirements are overlapping
- Deadlines are staggered (in some case not known yet)
- A mapping exercise is recommended to define the extent of overlapping and allow prioritisation of tasks
- Compliance can be then streamlined
- An ISMS will offer a structured framework for managing compliance
- Competence building and **training** should focus on implementation

NAAAs have to oversee

- Part-IS to be included in the oversight process for all types of organisations
- Competence building and **training needs to be tailored to oversight activities**



Included in the OA process

EASA competences objectives for Part-IS

Competence ID	Ref. to EASA Part-IS requirement	
Competence Objective 8	References	
Evaluate how the organisation performs asset management regarding aviation safety	Part-IS	Other guidance
	IS.AR.205 (a)	NIST CF / ISO 27000

Main, overall objective for this competence. Text might be derived directly from the rule

Items to assess
“What do I need to be capable of?”

- Ability to evaluate:**
- If the organisation maintains a list with all activities, facilities and services which could be exposed to information security risks
 - If the competent authority has identified all relevant systems and data which could impact aviation safety
 - If interfaces to other organizations are known and documented
 -

Required competences for the items to assess above, expressed as “Knowledge” and “Ability”

- Required knowledge and abilities:**
- Knowledge of the hardware systems and software systems used in the organization
 - Ability to identify critical systems and services important to the organisation and the civil aviation sector
 -

Competence objectives for NAAs inspectors

Competence Objective 2	Part-IS Ref
Evaluate the suitability of the organisation security governance.	IS.AR.200

2.1 Sub. Objective – management involvement

Interviewing the Management (Accountable Manager, Head of Design Org. or delegated responsible person)

Ability to evaluate if management has been informed and has understood the cybersecurity risk of the organisation.

2.2 Sub. Objective – establishment of cybersecurity governance

Given a description of the organisation's cybersecurity roles, activities and processes and the relevant documents.

Ability to evaluate:

- If cybersecurity roles are defined and assigned to people;
- If policies, procedures, and processes appropriately (in terms of completeness and quality) describe and document how the organisation manages and monitor the cybersecurity risks.

Q&A – *15 minutes*



FAQs on Part-IS

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

A number of topics related to Part-IS and its implementation are covered

Feel free to send additional questions to be considered for the next iteration



EASA Cybersecurity Community

EASA Community Network

Search

Home Air Operations General Aviation Rotorcraft

Cybersecurity

Public community • 3633 members

Say something to the community

UPCOMING EVENTS IN THE COMMUNITY

No upcoming events in this community

NEWEST TOPICS IN THE COMMUNITY

Cybersecurity in Aviation - Lecture in Hamburg

12 Oct 2023 • Vasileios PAPAGEORGIU

Cybertech Europe 2023 & EASA participation

9 Oct

SAFETY WEEK
on [YouTube](#)

Join our community



YouTube

Search

Via webex

FRANKLIN John Nieto Sepúlveda Juan... Tomi Salminenpää Gerardo SARMIENTO Timo Arndal

EASA

EASA Safety Week 2024 – Cybersecurity Session

Gian Andrea Bandieri
Section Manager Cybersecurity in Aviation and Emerging Risks

Vasileios Papageorgiou
Junior Expert – Cybersecurity in Aviation

Your safety is our mission.

25 April 2024

An Agency of the European Union

5:46 / 1:28:55

Announcing
Part-IS Implementation
Workshop 2025



Your safety is our mission.